해운사 보안 요구사항 대응 가이드

Shipping Company Cybersecurity Response Guide

과학기술정보통신부
KISA 한국인터넷진흥원
KR KOREAN REGISTER

CONTENTS

해운사 보안 요구사항 대응 가이드

1. 배경 및 개요 ····· 3

2. 참조 표준 ····· 5

3. 성숙도 및 통제항목 ····· 9

4. 통제항목 상세 ····· 13

5. 결 론 ····· 125

6. 용 어 ····· 129

7. 부 록 ····· 135

1

배경 및 개요

1 배경 및 개요

지난 몇 년간 조선·해양 산업은 각종 장비의 디지털 전환과 선박 스마트화의 가속화로 운영 효율성과 편리성을 높이는 동시에, 각종 사이버보안 위협에 노출되어 왔습니다.

이에 따라 IMO(국제해사기구)의 지침, IACS(국제선급연합)의 사이버 복원력 의무화와 미국·싱가포르 등 주요 20개국 이상에서의 법적 규제 시행은 선박을 운항·관리하는 해운사가 반드시 대응해야 할 국제적 요구사항으로 자리잡고 있습니다.

그러나 국내 해운사는 국가 법령, IMO 지침, IACS UR/UI(선급 규칙), 보험·감사 등의 다양한 기준을 정확히 이해하고 이행하는 데 어려움을 겪고 있습니다.

이는 강제 또는 권고 수준의 제도·규정 측면의 차이와, 선박마다 상이한 IT·OT 네트워크 구조, 인터페이스, 장비 등의 차이를 단일 가이드만으로는 대응하기 어렵기 때문입니다.

이에 본 가이드는 참조 표준 내 6개 가이드를 교차 매핑하여 공통 요건을 도출하고, 해운 특성(운항 시나리오, IT, OT)을 반영해 정책, 조직, 교육, 통제, 리스크, 사고대응 등 전 영역으로 일관된 체계를 통합했습니다.

구체적으로 IMO의 관리체계 원칙을 토대로 BIMCO·DCSA의 실행 지침을 현장 절차로 세분화하고, IACS UR E26의 설계·검증 요건으로 신조/개조 단계의 적합성을 확보했으며, RightShip·OCIMF 심사 항목을 증적·운영 점검 기준으로 연결하여 규정 준수와 감사 대응을 동시에 충족할 수 있도록 구성했습니다.

이를 통해 국내 해운사가 SOP(표준작업절차)와 점검·증적 체계를 확립하고 지속적 고도화를 이어감으로써, 국제 기준을 선제적으로 충족하는 실효적 보안 체계가 공고히 자리잡기를 기대합니다.

2

참조 표준

과학기술정보통신부
KISA 한국인터넷진흥원
KR KOREAN REGISTER

2 참조 표준

2.1 GUIDELINES ON MARITIME CYBER RISK MANAGEMENT Rev.3 (2025, IMO)

- 해사 사이버 리스크 관리를 위한 국제 권고 지침입니다. 원칙·절차 중심의 거버넌스와 지속적 개선 체계를 정립하며, MSC.428(98) 취지에 따라 SMS(안전관리시스템) 내 사이버 리스크 반영을 체계화합니다. 이를 통해 ISM/PSC 감사 및 업계 심사(OCIMF/RightShip 등) 정합성을 확보하고, 사이버 사건의 예방·탐지·대응·복구 역량을 표준화합니다.

2.2 UR E26 Cyber resilience of ships Rev.1(2023, IACS)

- 2024-07-01부터 신조 계약 선박에 통일 적용되는 선급 공통 의무 기준입니다. 설계-시운전-운영 전 생애주기에 걸친 증적 문서 및 시험·검증 요건을 통해 검증 가능한 사이버 복원력을 요구합니다. 운영 단계에서는 변경관리, 패치·원격접속 통제, 이동식 매체, 로그·IR/DR, 백업·복구 시험, 증적 유지 등을 상시 준수·입증 가능한 절차로 내재화합니다.

2.3 THE GUIDELINES ON CYBER SECURITY ONBOARD SHIPS v5 (2024, BIMCO)

- BIMCO를 비롯한 주요 업계 단체가 산업 합의에 기반하여 공동 발행한 운영 단계 권고 가이드입니다. 회사·선박의 SMS(안전관리시스템)에 사이버 리스크 관리 절차를 내재화하도록 설계되었으며, 최신 위협과 상시 재평가 원칙, 현장용 체크리스트·템플릿을 제공하여 구체화된 운영 기준선을 마련합니다.

2.4 DCSA Implementation Guide for Cyber Security on Vessels v1.0 (2020, DCSA)

- 컨테이너 선사의 운영 환경을 대상으로 한 이행 지침으로서, 선박·선대의 사이버보안 통제를 직무별·절차역할·점검항목·증적 양식으로 구체화합니다. IT/OT 세그멘테이션, 원격지원·벤더 접속, 패치·형상 관리 등 핵심 영역을 NIST 기반 리스크 관리·통제 맵핑, 핵심 보안 시스템의 분리 운용 원칙, 복구 시 벤더 지원 연계와 함께 제시하여, 항해·정박·접안 전 과정에서 즉시 적용 가능한 실무 지침을 제공합니다.

2.5 SIRE 2.0 Question Library(2022, OCIMF)

- OCIMF(국제석유회사해사포럼)가 운영하는 선박의 안전·환경·보안·운영 상태를 평가하기 위한 공식 질문집으로, 탱커선의 관리·운항·설비 수준을 객관적으로 검증하는 것을 목표로 합니다. 이에 따라 선사는 SIRE 2.0 요구사항에 부합하는 운영·관리 체계를 체계적으로 수립·이행해야 하며, 각 문항은 SIRE 검사관이 SMS(안전관리시스템) 절차서, 기록, 점검 로그 등 객관적 증적(Evidence)을 근거로 이행 여부를 검증합니다.

2.6 RISQ(RightShip Inspection Ship Questionnaire) v3.1 (2024, RIGHTSHIP)

- 용선 전 리스크 평가에 사용되는 증적 중심의 검사 문항집입니다. 사이버보안 정책·책임, 선원 교육, 계정·접근통제(원격·벤더 포함), 패치·형상관리, 백업·복구, 로그·사고보고 등의 이행 여부를 기록과 자료로 확인하도록 요구합니다. 내부 절차·역할·점검항목·증적과 연결하여 용선 전 자가점검과 현장 점검 대비를 체계화합니다.

2.7 Cyber Security Workbook for On Board Ship Use 6th edition (2025, BIMCO)

- 선내 일상 점검과 사고 대응을 위한 실무형 워크북입니다. 현장 사례와 도식으로 풀이한 구체적인 조치와 선박 일상점검 체크리스트·워크시트를 선별 반영합니다. 이러한 조치들은 점검항목들을 대상으로 무엇을, 어떤 순서로, 어떤 양식에 기록할지까지 예시와 서식으로 제시합니다. 이를 통해 사건 대응·복구 시 단계별 실행력을 높이며, 선박육상 간 협업(연락 체계·역할 분담)도 체계적으로 정돈합니다.

2.8 ENISA Guidelines – Cyber Risk Management for Ports

- 항만·터미널 대상 사이버 리스크 관리 지침으로 성숙도 모델을 참조했습니다. 항만 운영 환경의 보안조치를 정책·조직·기술 영역으로 구분하고, 3단계 성숙도와 수준별 예시/증거를 제시함으로써, 당사가 현재 수준을 객관적으로 진단하고 목표 수준을 단계적으로 설정하며 개선 투자 우선순위를 합리적으로 배분할 수 있도록 합니다.

2.9 정보통신분야_침해사고대응안내서(2025, KISA)

- 국내 법령에 근거한 침해사고 신고 대응 권고 안내서입니다. 대외 신고 기준과 절차를 제시하고,

사고 유형별 점검·조치 항목과 시스템 유형별 대응 지침을 제공합니다. 이에 따라 선박과 본사 간 사고 보고 흐름과 대외 신고(보호나라&KrCERT/CC) 연계를 국내 기준에 맞추어 표준화할 수 있습니다. 이를 통해 선박 운영 단계에서 초기 분류–격리–증적 보존–대외 신고–사후 조치로 이어지는 사고 대응 절차와 점검표를 국가 가이드에 부합하도록 정비합니다.

2.10 해사(海事) 사이버보안의 이해: 개념과 실제, 해광출판사 (2019, 최성민·박재홍)

- 국내 해사 사이버보안의 개념·법제·실무를 체계화한 참고서입니다. 해사 사이버보안의 국제·국내 규제 연혁과 법제(IMO·산업 가이드·국가 법·지침 등)를 선사 실무 관점에서 정리하고, 현장 사례·설명과 함께 연습문제·부록(대조표) 등 교육·자가점검 도구를 제공함으로써, 용어·근거 정합성을 확보하고 국내 현실에 맞춘 교육·점검 체계를 보완합니다.

3

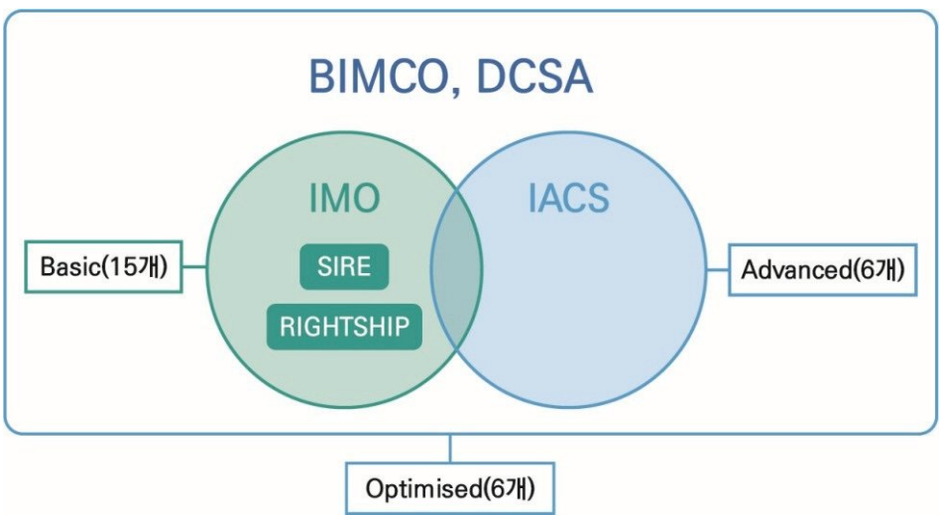
성숙도 및 통제항목

과학기술정보통신부
KISA 한국인터넷진흥원
KR KOREAN REGISTER

3 성숙도 및 통제항목

1. 성숙도

성숙도는 조직의 사이버보안 역량을 세 가지 성숙도 수준에서 평가하고, 역량 발전과 제도화라는 두 가지 진행 방식을 동시에 고려하는 구조로 되어 있습니다. 역량 발전은 조직이 사이버보안 역량(인력, 프로세스, 도구, 자금)을 얼마나 구현했는지를 측정합니다. 제도화는 특정 활동, 통제, 프로세스 및 절차가 조직 내·외부에 얼마나 깊이 자리 잡았는지를 측정합니다. 이러한 요소들이 더 깊이 뿌리내릴수록, 조직은 사건 발생 중이나 이후에도 이를 일관되게 유지할 가능성이 높아집니다.



성숙도	참조문서	설명
Basic	IMO, SIRE 2.0, RIGHTSHIP	보안 목표를 달성하기 위해 구현되는 **최소한**의 보안 조치에 해당한다. 조직은 기본적인 활동 및/또는 역량을 수행하며, 경우에 따라 임시(ad hoc)적으로라도 이를 이행합니다.
Advanced	IACS UR E26	식별된 표준과 모범 사례에 부합하는 보다 **지속적**인 역량에 해당합니다. 조직은 정의된 목표와 운영의 적합성에 따라 역량을 구현, 관리, 모니터링, 측정합니다. 또한 문서(계획·정책)는 특정 활동 또는 조정된 활동에 자원을 적용·활용하는데 지침 역할을 합니다.
Optimized	BIMCO, DCSA	계획, 시험, 정책에 근거하며 반복 가능한 활동 및 역량에 해당합니다. 이러한 활동은 정기적인 감독과 검토를 받아 그 **효과성**을 확인하고, 보안 조치의 구현을 향상시킵니다. 또한 체계적인 변경, 테스트, 훈련을 반영하며, 조직은 정기적으로 역량을 측정해 정의된 성과 목표를 달성·유지하고, 이를 위한 지속적 개선 활동을 지원합니다.

3.2 통제항목

통제영역		통제항목	성숙도		
			Basic	Advanced	Optimized
A. 사이버보안 관리체계	A.1 사이버보안 정책	A.1.1 사이버보안 정책	O	O	O
	A.2 사이버보안 조직 및 외부업체 관리	A.2.1 사이버보안 조직	O	O	O
		A.2.2 사이버보안 외부업체 관리		O	O
	A.3 사이버보안 교육 및 훈련	A.3.1 사이버보안 교육 및 훈련	O	O	O
B. 사이버보안 통제	B.1 사이버 자산 관리	B.1.1 사이버 자산 목록	O	O	O
		B.1.2 네트워크 구성도		O	O
		B.1.3 사이버 자산 변경관리		O	O
	B.2 계정 관리	B.2.1 계정 및 권한 관리	O	O	O
		B.2.2 비밀번호 관리	O	O	O
	B.3 네트워크 접근 통제	B.3.1 네트워크 분리			O
		B.3.2 네트워크 접근 통제		O	O
	B.4 기기 및 출입 통제	B.4.1 기기 반출입 통제	O	O	O
		B.4.2 인원 출입 통제		O	O
C. 사이버 리스크 관리	C.1 사이버 취약점 진단	C.1.1 악성코드 방지	O	O	O
		C.1.2 패치 관리	O	O	O
		C.1.3 보안설정 점검 및 모의해킹		O	O
	C.2 사이버 리스크 평가	C.2.1 사이버 영향도 평가	O	O	O
		C.2.2 사이버 발생빈도 평가	O	O	O
		C.2.3 사이버 리스크 평가	O	O	O
		C.2.4 사이버 리스크 평가 예외			O
	C.3 사이버 리스크 조치 계획	C.3.1 사이버 리스크 조치 계획	O	O	O
	C.4 사이버 복원력 검사	C.4.1 사이버 복원력 검사			O
D. 사이버 사고 대응	D.1 사이버보안 모니터링	D.1.1 사이버 위협 모니터링		O	O
		D.1.2 네트워크 운영 모니터링			O
	D.2 사이버 사고 대응 계획	D.2.1 사이버 사고 대응 절차	O	O	O
	D.3 사이버 복구 계획	D.3.1 사이버 백업 관리			O
		D.3.2 사이버 복구 계획	O	O	O
		D.3.3 사이버 보험			O

해운사 보안 요구사항
대응 가이드

4

통제항목 상세

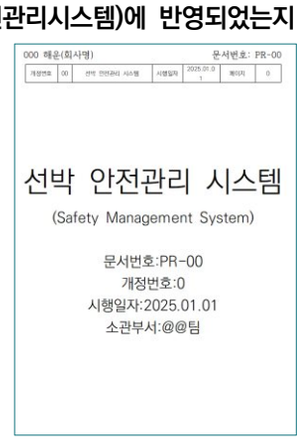
과학기술정보통신부 KISA 한국인터넷진흥원 KR KOREAN REGISTER

4 통제항목 상세

4.1 Basic

A. 사이버보안 관리체계

A.1 사이버보안 정책

통제항목	A.1.1 사이버보안 정책	Basic
점검목적	선박 내 정보 시스템과 자산을 보호하고 관리하기 위해 적합한 보안 정책 및 절차를 마련하여 기밀성, 무결성, 가용성 및 안전성의 요구되는 수준을 보장해야 합니다.	
점검내용	IMO의 요구사항을 반영한 사이버보안 정책 및 절차가 SMS(안전관리시스템)에 기록되어 있는지 확인합니다.	
점검기준	**양호 :** 사이버보안 정책이 SMS(안전관리시스템)에 반영되어 있을 경우 **취약 :** 사이버보안 정책이 SMS(안전관리시스템)에 반영되어 있지 않을 경우	
레퍼런스	[IMO 3.5.1 거버넌스] [IMO 3.5.3.8 보호] [IMO 3.5.3.9 보호] [UR E26 4.2.4.2 타당성] [OCIMF SIRE 2.0 7.5 사이버보안] [RIGHTSHIP 12.7 사이버보안 정책 및 절차가 SMS(안전관리시스템)에 통합되어 있으며, 사이버보안 관리 시스템이 평가 및 인증되었습니까?] [BIMCO 1.5 계획 및 절차] [DCSA 1.2.3 구현] [DCSA 2.4.2 설명] [DCSA 2.4.3 구현]	
증적자료	SMS(Safety Management System), DOC(Document Of Compliance), SMC(Safety Management Certificate)	
조치방법	**1. 사이버보안 정책이 SMS(안전관리시스템)에 반영되었는지 확인합니다.**  000 해운(회사명) 문서번호: PR-00 개정번호 00 선박 안전관리 시스템 시행일자 2025.01.01 페이지 0 선박 안전관리 시스템 (Safety Management System) 문서번호:PR-00 개정번호:0 시행일자:2025.01.01 소관부서:@@팀 [그림 1] SMS 이미지	

통제항목	A.1.1 사이버보안 정책	Basic

000 해운(회사명) 문서번호: PR-00

개정번호	00	선박 안전관리 시스템	시행일자	2025.01.01	페이지	1

- 목차 -

1. 총칙
2. 회사 규정의 운영
3. 보안조직운영
4. 외주관리
5. 정보자산관리
6. 보안교육
7. 인적보안
8. 물리적보안
9. 개발보안
10. 정보시스템보안
11. 접근통제
12. PC보안
13. 침해사고대응

[그림 2] 사이버보안 정책 예시

2. 사이버보안 정책 구성

SMS(안전관리시스템) 내 사이버보안 정책

- 총칙: 목적, 적용범위, 용어정의 방안
- 회사 규정의 운영: 자체규정의 수립, 규정의 승인 및 공표, 규정의 개정, 규정의 준수, 규정의 이행기록, 활동계획수립 및 운영 방안
- 보안조직운영: 목적, 적용범위, 보안조직의 구성 및 운영, 보안조직의 책임과 역할 방안
- 외주관리: 목적, 적용범위, 외부 인력의 계약 시 보안책임 및 서약, 외부 인력의 업무 수행 시 보안대책, 외부 인력의 계약 종료 시 보안대책 방안

통제항목	A.1.1 사이버보안 정책	Basic

- 정보자산관리: 목적, 적용범위, 용어정의, 정보자산의 책임과 권한, 정보자산의 유형, 정보자산의 식별 및 분류, 중요정보의 분류, 정보자산 보안등급 평가, 정보자산 변경, 정보자산 폐기 방안
- 보안교육: 목적, 적용범위, 보안교육 및 홍보계획, 보안교육 수행, 보안교육 프로그램, 보안교육수행방법 및 주기, 보안교육 및 변화관리, 보안홍보 및 인식제고 방안
- 인적보안: 목적, 적용범위, 용어정의, 채용 시 점검사항, 보안교육, 보안 서약, 근무 시 준수사항, 퇴사 및 전출 방안
- 물리적보안: 목적, 적용범위, 용어정의, 보호구역분류기준, 보호구역출입통제, 전산시설보호대책, 사무실보호대책 방안
- 개발보안: 목적, 적용범위, 용어정의, 보안요구사항 정의, 사용자 계정 설계, 비밀번호 설계, 로그인 설계, 입·출력 설계, 안전한 프로그래밍, 소스코드 관리, 악성코드 삽입 금지, 아웃소싱 보안 방안
- 정보시스템보안: 목적, 적용범위, 사용자 계정 관리, 비밀번호 생성 및 관리, 네트워크 보안, 무선통신망 관리, 보안패치 관리, 로그관리, 모니터링, 바이러스 백신 및 설치 운영, 시간의 동기화, 암호화 기술 적용대상, 공개용 서버관리, 백업 방안
- 접근통제: 목적, 적용범위, 용어정의, 접근권한 부여 기준 및 관리, 파일시스템 관리, 접근권한의 할당, 로그온통제, 외부 연결에 대한 인증, 정보 접근 제한, 감사 로그, 모니터링 방안
- PC보안: 목적, 적용범위, PC보안 관리, 웜 및 바이러스예방, 불법 소프트웨어 사용금지, 서비스 팩 및 패치 설치, PC 취약성점검 방안
- 침해사고대응: 목적, 적용범위, 용어정의, 침해사고의정의, 침해사고대응체계구축, 침해사고모니터링 및 대응, 침해사고접수 및 보고, 침해사고분석 및 처리, 사후 대응, 보고서 작성 방안

SSP(선박보안계획서) 내 사이버보안 계획

- 물리적 보안시스템: IT와 OT 시스템에 대한 물리적 접근통제를 위한 적절한 조치 계획

3. 사이버보안 정책 관리

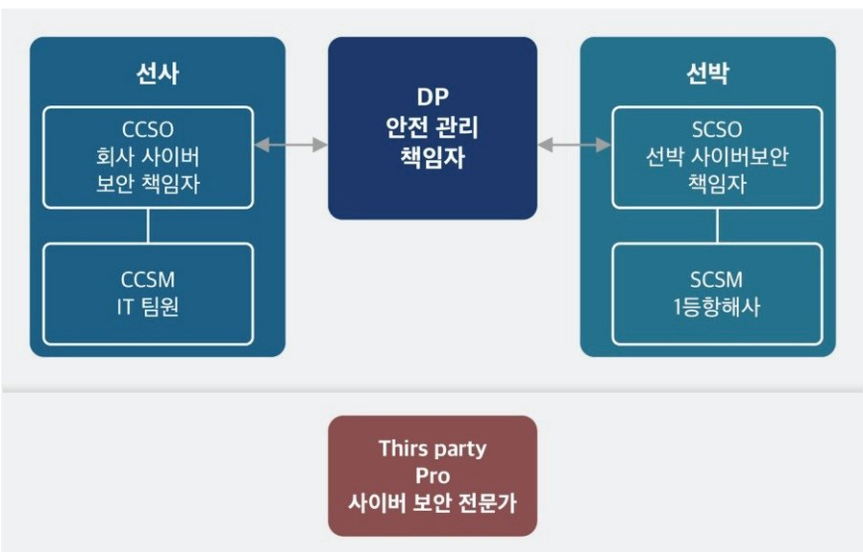
제/개정이력표

개정번호	일자	제/개정내용	비고
1.0	2019.05.27	제정	
1.0	2020.01.02	개정 사항 없음	
1.0	2021.01.05	개정 사항 없음	
2.0	2021.12.16	보안조직의 책임과 역할 수정	
2.0	2022.12.21	개정 사항 없음	
2.0	2023.04.07	개발보안 관련 개정	
2.0	2023.12.06	정보자산의 식별 및 분류 수정	

[그림 3] 사이버보안 정책 제/개정이력표

통제항목	A.1.1 사이버보안 정책	Basic
	■ 사이버보안 정책은 매년 1회 이상 주기적 검토와 함께 업데이트 필요, 정기 심사(Internal Audit, DOC/SMC 갱신 심사) 시점과 연계 • 사이버 사고나 보안 위협 식별 시 즉각적인 정책 업데이트 필요 • CBS(컴퓨터기반시스템) 관련 보안 정책 및 절차는 설계 변경 시 즉시 업데이트 권장 ■ 운영방법, 절차, 책임자들이 명시된 사이버보안 정책서를 하드 카피(Hard Copy) 형식으로 보관 ■ 사이버보안 정책 선내 사무실 벽면에 부착 • 사이버보안 담당자는 선원들의 업무용 PC, 인터넷용 PC가 위치한 곳의 벽면에, 사이버보안 담당자 정보와 컴퓨터·개인용 휴대 저장매체에 대한 사용 정책 부착 ■ 사이버 리스크 관리에 관한 회사 절차서 숙지 **4. 사이버보안 감사** ■ 감사 수행자 • 회사의 CCSO, DP가 내부감사 수행 • 외부 심사원(선급 심사관)이 독립적으로 감사 수행 • 전문 업체를 통한 주기적 외부 검증 진행 ■ 감사 주기 • 내부 감사 - 최소 연 1회 진행 • 외부 감사 - SMC 중간/갱신 심사 시 포함 - DOC 연간 심사 • 추가 감사 - 사이버 사고 발생 후, 주요 시스템 변경 시 즉시 재점검 권고	
비고		

A.2 사이버보안 조직 및 외부업체 관리

통제항목	A.2.1 사이버보안 조직	Basic
점검목적	조직 전반의 사이버 리스크 대응 능력을 강화하고, 책임성과 통제를 확보하여 보안 사고 발생 가능성을 줄이는 것을 목표로 합니다.	
점검내용	선박과 공급망 전반에서 사이버보안 책임과 역할이 명확히 정의·이행되고, 이해관계자의 협력, 유지보수 절차 및 업무 분리 원칙이 효과적으로 적용되고 있는지를 확인합니다.	
점검기준	**양호 :** 사이버보안 조직의 역할과 책임이 정의되어 있을 경우 **취약 :** 사이버보안 조직의 역할과 책임이 정의되어 있지 않을 경우	
레퍼런스	[IMO 3.5.1 거버넌스] [OCIMF SIRE 2.0 7.5 사이버보안] [BIMCO 1.2 고위 경영진의 참여] [BIMCO 1.3 역할, 책임, 그리고 업무] [DCSA 1.3.2 설명] [DCSA 1.3.3 구현] [DCSA 1.3.4 기능적 역할 및 책임] [DCSA 1.3.5 기능적 역할 및 책임] [DCSA 2.3.3 구현] [DCSA 2.5.3 구현]	
증적자료	사이버보안 조직도	
조치방법	**1. 사이버보안 조직 구성**  [그림 4] 사이버보안 조직도 예시	

통제항목	A.2.1 사이버보안 조직	Basic

2. 담당자 역할, 책임, 작업

[표 1] 담당자 역할, 책임, 작업

직책	업무
선박 사이버보안 책임자	**선내 사이버보안 총괄자로서 회사 정책 실행, 교육·훈련, 사고 대응 지휘** ■ 회사 SMS(안전관리시스템) 및 CCSO 지침에 따른 사이버보안 정책 시행 ■ 전 선원 대상 사이버보안 교육 시행, 모의사고 대응 훈련 주관 ■ 네트워크 접근 통제 점검, 백업 및 복원 기능 정기 검증 ■ 사고 발생 시 선내 초기대응 지휘 및 회사에 보고, CCSO/DP와 복구 절차 조율 ■ 제3자의 선내 자산 접근시 절차적·기술적 통제 등
1등항해사 (선박 사이버보안 담당자)	**항해 및 보안 관련 OT자산 책임자로서 장비 보호, 교육 보조, 점검·운영 담당** ■ 항해 장비(ECDIS, AIS, GPS 등) 업데이트 및 데이터 관리 시 보안 절차 준수 ■ 항해 관련 장비 사용자 대상 보안 인식 교육 보조 ■ 항해 데이터 백업 및 복원 점검, 항해 장비 소프트웨어 패치/업데이트 확인 및 기록 ■ 항해 시스템 장애 발생 시 수동 운항 전환, 사고상황 기록 유지 및 SCSO에 보고 ■ 제3자가 항해장비에 접근할 경우 현장 통제자 역할 수행 등
안전관리 책임자	**선박의 안전 운항과 관련된 모든 사항을 최고 경영진에게 보고** • 최고 경영진과 선박 담당자 사이의 원활한 의사소통 책임 • 선박의 안전한 운항을 보장하고 감시 • 선박의 해양 환경 오염 방지를 책임지고 관리 • 선박이 안전하게 운행하는 데 필요한 자원과 육상 지원이 적시에 제공되도록 보장 • 회사의 SMS(안전관리시스템)가 효과적으로 구현되고 유지되도록 보장 등
회사 사이버보안 책임자	**회사 차원의 사이버보안 정책리스크 관리 총괄** • 회사 SMS(안전관리시스템)에 사이버 리스크 관리 포함, 외부업체/공급망 보안 정책 수립 • SCSO 및 선원 대상 교육·훈련 감독, 전문 지원 제공 • 선박별 사이버 리스크 평가 수행, 완화조치 가이드 제공, CBS(컴퓨터기반시스템) 요구사항 감독 • 각 선박의 사이버보안 점검 결과 검토, 감사 대비 증적 관리 • 사이버 사고 보고 접수 및 대응 지휘, 외부 전문업체 협력 및 조사 주관 • 제3자 요구사항 계약 반영, 원격접속 정책 관리 등

통제항목	A.2.1 사이버보안 조직	Basic

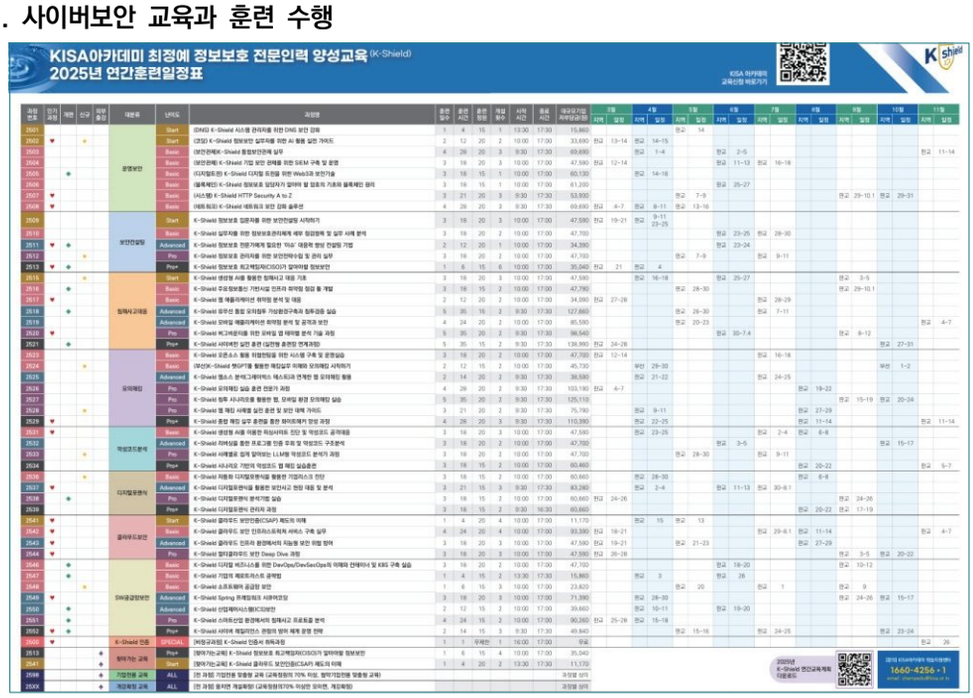
직책	업무
IT팀원 (회사사이버 보안담당자)	**IT/OT 인프라의 기술적 운영·지원 담당** • 네트워크 보안 설정(VPN(가상사설망), 방화벽, VLAN(가상 랜)), 소프트웨어/패치 관리 절차 실행 • 선내 사용자 보안 사용법 교육 지원(USB검사, 이메일 보안), 기술 매뉴얼 제공 • 취약점 분석, 로그 모니터링, 비인가 장치 접속 탐지 및 경보 운영 • 중요데이터 백업 복원 절차 점검 및 운영 • 네트워크 성능 모니터링(NPM) 및 침입탐지 로그 검토 • 사고 로그 수집 및 증적 확보, 원인 분석·복구 작업 지원 • 원격 유지보수 계정 관리, 패치/업데이트 제공업체 검증 등
외부 사이버보안 전문가	**제3자 입장에서 기술적 검증·사고 분석·교육 공급망 검증 지원** • 네트워크 보안 설정(VPN(가상사설망), 방화벽, VLAN(가상 랜)), 소프트웨어/패치 적정성 검증 및 개선 자문 • 선원 대상 맞춤형 교육/훈련 설계 및 실행, 모의 훈련 시나리오 제공 • 취약점 점검, 리스크 평가 및 모의해킹 수행 및 보고. 개선 권고안 제공 • 사고 원인 분석(포렌식), 복구 및 재발방지 대책 제안 • 외부 유지보수 업체의 보안 절차 점검, 원격접속 및 제3자 계정 사용 검증, 계약시 보안 요구사항 자문 등

[표 2] 역할, 책임, 작업을 매트릭스로 매핑한 예시

업무 직책/인사	사이버 안전/보안 정책	선박 OT시스템 사이버 리스크 평가	선박 IT 시스템 사이버 리스크 평가	선박 IT 인프라 관리	승무원 사이버 리스크 관리 교육
임원	책임				
회사 IT 담당자	지원		지원		
선박 IT 담당자	지원	책임	책임	책임	
안전 담당자	지원	지원	지원	지원	지원
구매 담당자	지원			지원	
선대 담당자		지원	지원	지원	지원
훈련 담당자			지원	지원	지원
해상 인사 담당자			지원		책임

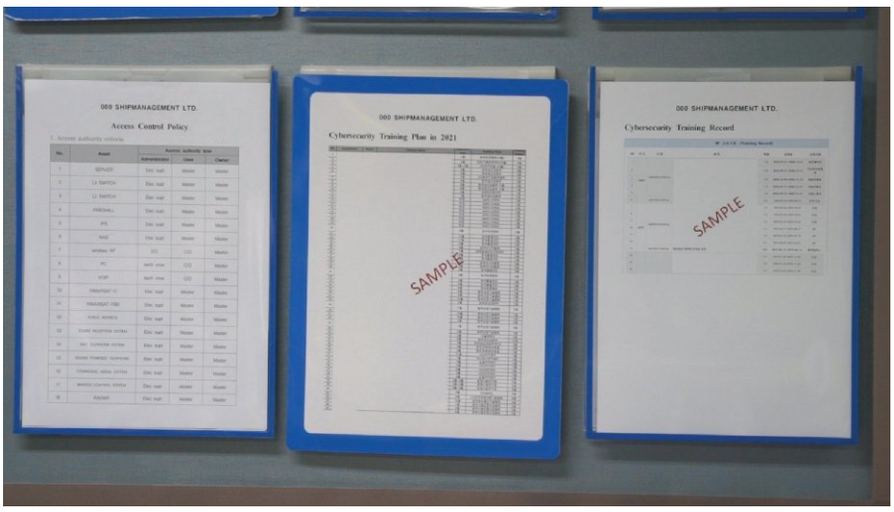
비고	

A.3 사이버보안 교육 및 훈련

통제항목	A.3.1 사이버보안 교육 및 훈련	Basic
점검목적	인적 요소로 발생할 수 있는 사이버 위협을 최소화하기 위해 조직 특성과 직원 권한 수준에 맞는 보안 인식 교육과 훈련이 적절하게 마련·이행되고 있는지를 확인합니다.	
점검내용	선원을 대상으로 한 보안 인식 교육과 훈련, 홍보 활동이 기본 이해, 보안 유지 행동 및 사고 대응 절차를 포함하여 효과적으로 시행되고 있는지 확인합니다.	
점검기준	**양호** : 사이버보안 교육과 훈련을 매년 각 1회 이상 실시하고 있을 경우 **취약** : 사이버보안 교육과 훈련을 매년 각 1회 이상 실시하고 있지 않을 경우	
레퍼런스	[IMO 3.5.3.6 보호] [IMO 3.5.4.2 탐지] [IMO 3.5.5.3 대응] [IMO 3.5.6.2 복구] [UR E26 5.3 선박 운항 기간] [OCIMF SIRE 2.0 7.5 사이버보안] [BIMCO 7.3 절차적 보호 조치] [BIMCO 10.2 사고 대응의 네 가지 단계] [DCSA 2.2.3 구현] [DCSA 4.1.4 선박 내 사고 대응을 위한 주요 권고사항]	
증적자료	연간 교육계획서, 참석자 명단	
조치방법	**1. 사이버보안 교육과 훈련 수행**  [그림 5] 보안교육 연간 계획서 예시(KISA) 출처: KISA 아카데미. '2025 K-shield 교육 연간 일정표' ■ 매년 1회 이상 전 직원 대상 기본 사이버보안 교육 실시 • 직책별 역할에 맞는 교육 실시	

통제항목	A.3.1 사이버보안 교육 및 훈련	Basic

- 선원의 보직 변경 시 교육 실시
- 외부 인력은 자체 교육 프로그램 이수 필요
- 사이버보안 연간 교육 계획을 선내 공지사항 게시판에 부착 여부 확인



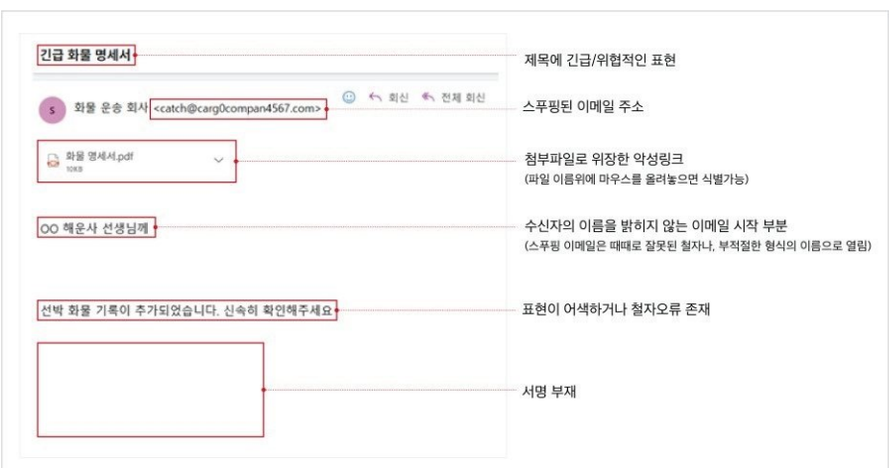
[그림 6] 선내 공지사항 게시판에 부착된 사이버보안 연간 교육 계획 예시
출처: 한국선급, '03. 사이버보안 현존선 인증 요구사항 해설'

■ 사이버보안 훈련 수행
- 선주는 운영 절차를 준비하고 실행하며, 관련 선원 및 육상 관계자를 대상으로 교육· 훈련과 반복 연습(Drill) 진행
- 선박 팀과 육상 팀의 지속적인 교차 훈련 수행
- 사이버 사고 탐지 및 복구 훈련 수행

■ 사이버보안 기본·전문 교육 및 훈련 기록

2. 사이버보안 교육 프로그램

■ 교육 프로그램은 아래의 내용으로 구성



[그림 7] 피싱 이메일 예시

통제항목	A.3.1 사이버보안 교육 및 훈련	Basic

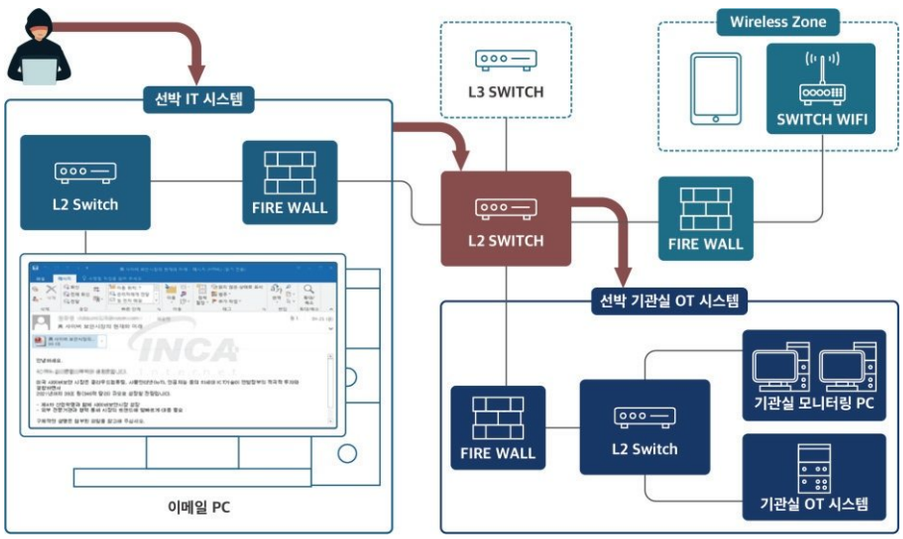
- 이메일 관련 리스크 (예: 피싱 공격으로 악성 사이트 클릭 또는 악성 첨부파일 열기)
- 인터넷 사용 시 유출 방지(예: 소셜미디어, 채팅 포럼, 클라우드 기반 파일 저장소 등에서의 데이터 이동 통제 부족)
- 선박 위치 정보의 외부 노출 시 리스크
- 개인 장비 사용 관련 리스크(보안 패치 누락, 백신 미적용 등으로 리스크 전파 가능)
- 감염된 하드웨어(USB 등)나 소프트웨어를 이용한 설치 및 유지보수로 인한 리스크
- 사용자 정보, 비밀번호, 디지털 인증서 보호 방법
- 외부 인원으로 인한 물리적 리스크(예: 외부 기술자가 감독 없이 장비 작업 시)
- 의심스러운 활동 및 장치의 감지 및 보고 방법
- 사이버 사고가 선박에 미치는 영향 및 대응 방법
- 예방적 유지보수 절차 이해(백신, 백업, 사고 대응 계획 및 테스트 등)
- IT/OT 기기 접근 통제 정책 인지
- 컴퓨터 침해 징후 인지
- 비밀번호 보호 지침 인지

[그림 8] KR 해상 사이버보안 이러닝 교육

통제항목	A.3.1 사이버보안 교육 및 훈련	Basic

3. 사이버보안 훈련 시나리오

#1 피싱 이메일을 통한 선박 OT시스템 사이버 위협 시나리오

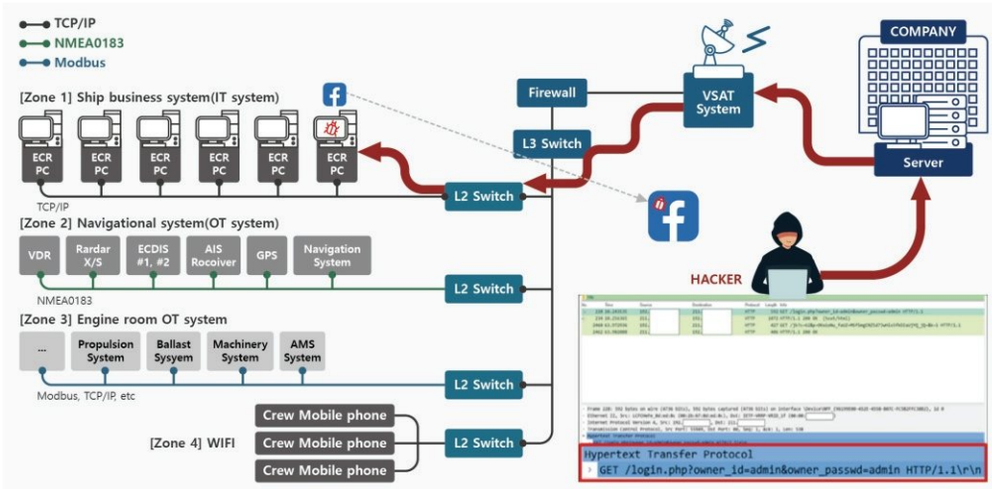


[그림 9] 피싱 이메일을 통한 선박 OT시스템 사이버 위협 시나리오

1. 공격자는 선원 이메일로 “운항 계획 변경” 등으로 위장한 피싱 메일을 발송합니다.
2. 선원이 피싱 메일의 첨부파일을 클릭하면 악성 스크립트가 실행되어 이메일 PC에 악성코드가 설치됩니다. 악성코드는 HTTPS(443)을 통해 공격자의 원격 서버로 접속하여 레지스트리에 암호화되지 않은 상태로 저장된 자동 로그인 계정/비밀번호, 로컬 문서, 네트워크 정보 등을 전송합니다.
3. 악성코드는 같은 L2 Switch 내 다른 PC와 서버를 스캔하여, 공격 대상 PC의 열려 있는 445(SMB)포트의 원격 코드 실행 취약점(EternalBlue, CVE-2017-0144)을 악용하여 악성코드를 주입합니다.
4. 공격자는 SMB 취약점을 이용해 IT망 내 여러 PC로 감염을 확산시킵니다. 이후 허술한 방화벽 정책으로 인해 IT망과 OT망 간 취약한 포트(445/3389)가 열려 있어 직접 선박 기관실의 OT시스템으로 접근합니다.
5. 공격자는 OT 시스템에 진입한 뒤, 변경되지 않은 기본 관리자 계정 또는 암호화되지 않은 백업 파일에서 추출한 계정을 이용해 합법적인 사용자처럼 로그인합니다.
6. 공격자는 기관실 OT망에서 사용하는 Modbus/TCP 프로토콜을 변조하여 Read Holding Registers 명령을 위조시켜, 센서값(압력, 온도)를 정상 값으로 위장하여 선원이 이 상황을 인지하지 못하도록 합니다.
7. 공격자는 IAS(Integrated Automation System)을 통해 제어 시스템 데이터 임의로 조작하여, 연료 공급 밸브를 닫아 선박의 메인 엔진 시동불능 및 급정지 상태를 유발합니다.

통제항목	A.3.1 사이버보안 교육 및 훈련	Basic

#2 워터링홀 공격을 통한 선박 OT 시스템 장악 시나리오

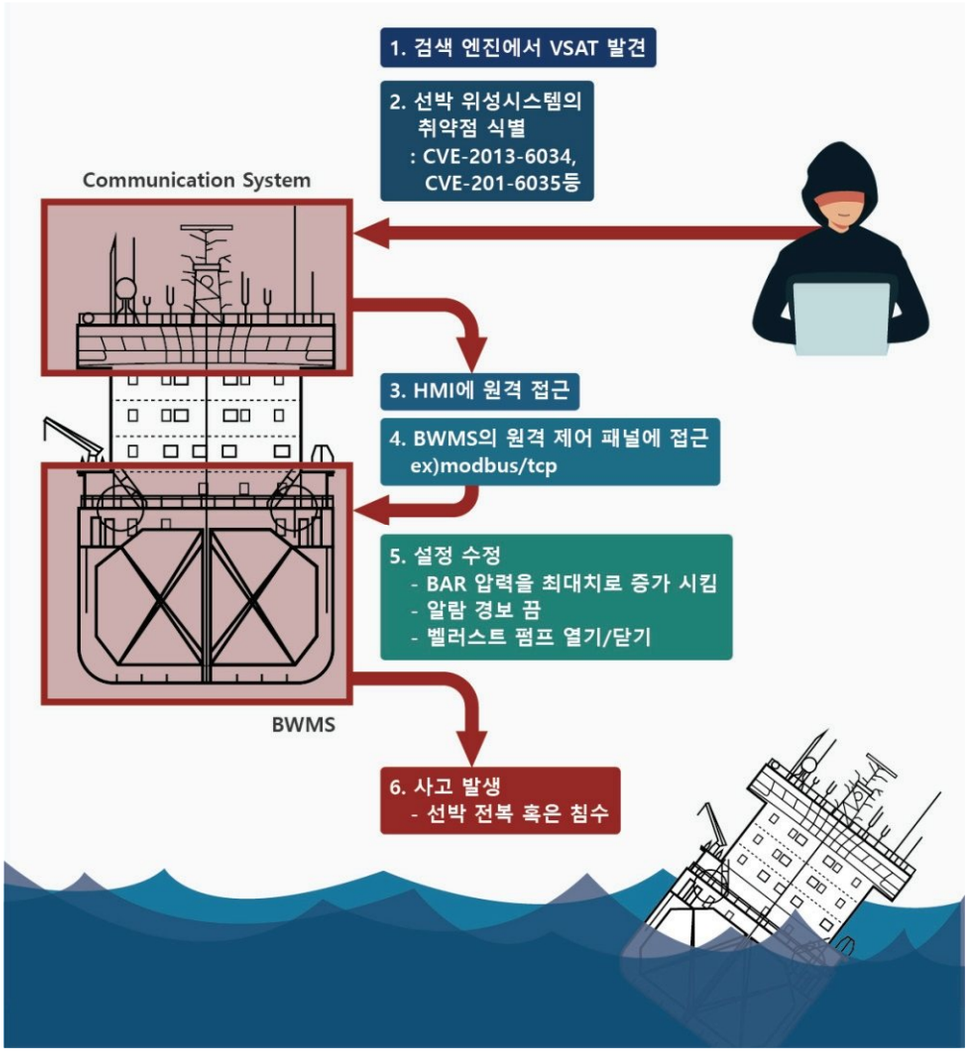


[그림 10] 워터링홀 공격을 통한 선박 OT 시스템 장악 시나리오

1. 공격자는 인터넷에 노출된 선박의 위성통신 장비(VSAT 단말기)를 찾기 위해 Shodan(쇼단)과 같은 하드웨어 검색 엔진을 사용합니다. 찾은 선박의 VSAT 단말기에 열려 있는 포트(HTTPS(443), HTTP(80), Telnet(23), SSH(22))를 이용해 접근합니다.
2. 공격자는 기본 관리자 계정(admin/admin, root/1234)을 사용하고 있는 VSAT 단말기의 관리 인터페이스에 접속하여 라우팅 테이블, DNS Relay 설정을 변조할 권한을 획득하고, 선원들이 자주 접속하는 웹사이트 요청을 공격자가 만든 가짜 피싱 사이트(실제 사이트와 동일한 디자인·UI)로 유도합니다.
3. 가짜 사이트에서 제공한 파일(.exe, 매크로 문서)을 실행하면 악성코드가 ECR PC에 설치되고 Windows UAC(User Access Control) 우회 기법을 이용해 관리자 권한을 획득합니다.
4. 감염된 ECR PC는 연결된 USB에 악성 LNK 바로가기 파일과 숨겨진 실행파일을 심어, 사용자가 로그 파일이나 보고서 파일을 열 때 자동으로 실행되도록 조작합니다.
5. 사용자가 이 USB를 AMS에 연결해 파일을 열면 AMS도 동일한 악성코드에 감염됩니다.
6. 공격자는 AMS에서 기본 관리자 계정이나 암호화되지 않은 비밀번호가 저장된 취약한 OT 소프트웨어 설정 파일을 악용해 제어 권한을 획득합니다.
7. 공격자는 AMS에서 Load sharing을 조작해 특정 발전기를 과부하시켜 직접 차단(Trip) 명령을 내려 모든 발전기의 출력 신호를 끊고, 전력 공급이 중단되면서 선박의 주요 IT/OT 시스템이 동시에 꺼져 조타 불능에 빠지고 본사 혹은 해상 교통관제(VTS)에 구조나 상황보고가 불가능해집니다.

통제항목	A.3.1 사이버보안 교육 및 훈련	Basic

#3 BWMS 사이버 공격을 통한 선박 침몰 시나리오

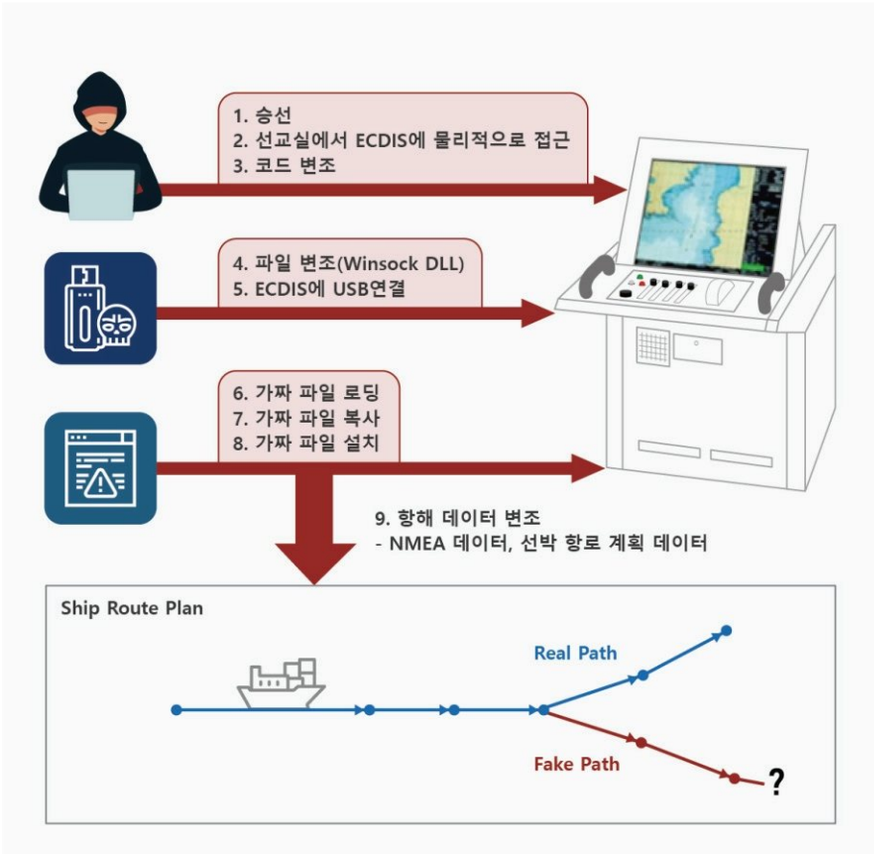


[그림 11] BWMS 사이버 공격을 통한 선박 침몰 시나리오

1. 공격자는 Shodan(쇼단)을 통해 발견된 취약한 VSAT 단말기에 접근하여 CVE-2013-6034(하드코딩된 자격 증명)을 이용해 펌웨어 내부의 고정 저장된 기본 관리자 계정, 비밀번호를 탈취해 관리자 권한을 획득합니다.
2. 공격자는 유효한 계정을 사용하여 선상 네트워크에 액세스합니다.
3. 내부망에 액세스한 후 공격자는 피보팅(Pivoting)을 통해 BWMS에 접근합니다.
4. 공격자는 BWMS에서 사용되는 Modbus/PLC의 명령을 변조해 센서값을 조작하고, 제어 로직을 변경하여 펌프 데이터를 변조하며, 펌프 경보를 끕니다.
5. 그 결과 선박은 전복되거나 침몰합니다.

통제항목	A.3.1 사이버보안 교육 및 훈련	Basic

#4 ECDIS 사이버 공격을 통한 항로 변경 시나리오



[그림 12] ECDIS 사이버 공격을 통한 항로 변경 시나리오

1. 공격자는 외부 협력업체를 위장하여 선박 탑승권을 확보하고, 보안 검증을 거치지 않은 USB 저장장치를 반입합니다.
2. 공격자는 항해 구역에 위치한 ECDIS 장비에 물리적으로 접근합니다.
3. 공격자는 ECDIS 제조사 기본 비밀번호(PW: 0000)를 사용하여 ECDIS 운영체제에 로그인 합니다.
4. 공격자는 USB 삽입을 통해 악성 Winsock DLL(ECDIS 운영체제 내의 네트워크 통신 처리)을 주입하고, 기존 네트워크 통신 DLL을 교체하여 ECDIS가 해당 악성 DLL을 우선적으로 로드하도록 설정합니다.
5. 악성 Winsock DLL 파일은 ECDIS와 GPS/AIS 센서 간의 NMEA데이터를 Hooking(후킹)하여 좌표·속도 정보를 변조하거나 송신되는 항로 데이터를 위조하고, ECDIS 화면에는 잘못된 항로가 표시되도록 만듭니다.
6. 항해사는 레이더·AIS와의 불일치 경보가 무력화되어 이상을 인지하지 못하고, 잘못된 항로를 따라 운항하다가 실제 항로를 이탈해 좌초됩니다.

비고	

B. 사이버보안 통제

B.1 사이버 자산 관리

통제항목	B.1.1 사이버 자산 목록	Basic
점검목적	통신 장치, 네트워크 장비, 소프트웨어 및 서비스 등 사이버 자산 목록을 체계적으로 점검하고 문서화하여, 선박의 안전한 운항과 사이버 복원력을 강화합니다.	
점검내용	선박 내 모든 IT/OT 자산이 문서를 통해 관리되고, 최신화되었는지 확인합니다.	
점검기준	**양호 :** 선박 내 모든 사이버 자산 목록을 최신 버전으로 문서화하여 관리하는 경우 **취약 :** 선박 내 모든 사이버 자산 목록을 최신 버전으로 문서화하여 관리하지 않는 경우	
레퍼런스	[IMO 3.5.2.1 식별] [UR E26 4.1.1.1 요구사항] [UR E26 4.1.1.3 세부 요구사항] [UR E26 4.1.1.3.1 하드웨어] [UR E26 4.1.1.3.2 소프트웨어] [OCIMF SIRE 2.0 7.5 사이버보안] [BIMCO 3.2 IT와 OT 시스템 문서화] [BIMCO 3.7 시스템 및 소프트웨어 유지관리] [BIMCO 3.4 선박-육상 간 인터페이스] [DCSA 1.1.3 구현] [DCSA 1.1.4 자산 목록] [DCSA 2.3.2 설명] [DCSA 2.3.3 구현] [DCSA 2.4.3 구현]	
증적자료	자산목록 관리대장	
조치방법	**1. 자산목록 관리대장 작성** ■ 선박에 존재하는 CBS(컴퓨터기반시스템)와 이들과 연결된 네트워크의 하드웨어·소프트웨어(응용 프로그램, 운영 체제, 펌웨어 및 기타 소프트웨어 구성요소) 자산목록 문서화	

자산목록관리대장

□ 기관명
□ 담당자

자산명	자산 유형	제조사	모델명	일련번호	버전	위치	관리 부서	중요도	변경이력

[그림 13] 자산목록 관리대장 예시

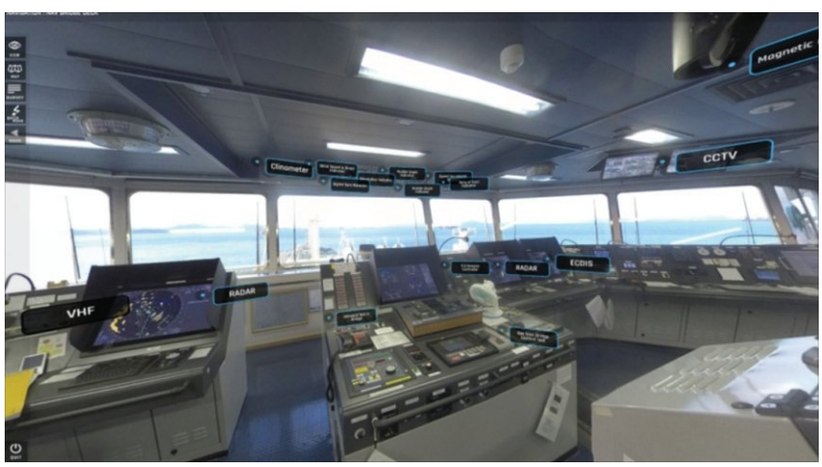
통제항목	B.1.1 사이버 자산 목록	Basic

■ 사이버 자산 분류 기준에 따라 자산 그룹화 및 그룹코드 부여(예: INF-ROT-001)

대분류		중분류	
Infrastrucure System	INF	서버(Server)	SVR
		라우터(Router)	ROT
		스위치(Switch)	SWT
		방화벽(FireWall)	FWL
		보안 게이트웨이(Unified Threat Management)	UTM
		침입방지시스템(Instrusion Precention System)	IPS
		네트워크 결합 스토리지(Network Attached Storage)	NAS
		가상 로컬네트워크(Virtual LAN)	VLN
		가상 사설 네트워크(Virtual Private Network	VPN
Bridge System	BRS	위성항법시스템(Global Positioning System)	GPS
		조난 및 안전시스템(Golbal Maritime Distress and Safety System)	GMD
		전자해도표시장치(ECDIS)	ECD
		자동식별장치(Automatic Identification System)	AIS
		레이더(RADAR Equipment)	RAD
		항해기록장치(Voyage Data Recorder)	VDR
		Bridge Navigational Watch Alarm System	BNW
		기타 항해통신 시스템(Other Bridge System)	OBS
		추진제어시스템(Propulsion Control System)	PRO
		타계제어시스템(Steering Control System)	STE
Comunication System	COM	통합통신시스템(Integrated Communication system)	ICO
		위성통신시스템(Satellite communication system)	SAT
		기타 통신 시스템(Other Communication System)	OCS

[그림 14] 자산 그룹화 예시

■ 아래의 CBS(컴퓨터기반시스템)는 자산목록 내 반드시 포함되어야 합니다.

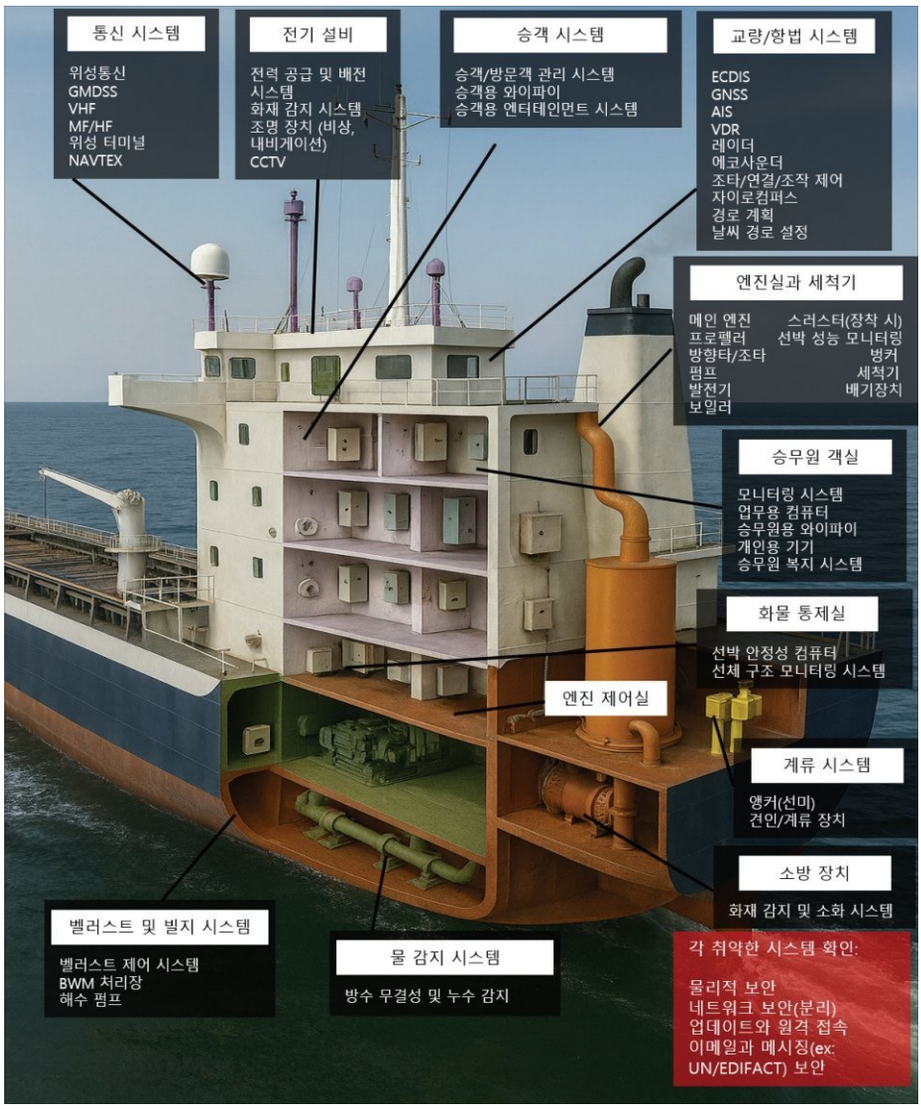


[그림 15] 선박 내 주요 사이버 자산 예시

출처: 한국선급. '확장현실기반의 선박 친숙화 솔루션 KR-Real360 소개'

- 조타(Steering)
- 추진(Propulsion)
- 항해(Navigation)
- 통신(Communication)
- 화재 안전(Fire Safety)
- 전력 관리(Power Management)
- 화물 취급(Cargo Handling)
- 환경 제어(Environmental Control)
- 인명 안전 시스템(Life Safety Systems)

통제항목	B.1.1 사이버 자산 목록	Basic



[그림 16] 잠재적으로 취약한 선박 시스템 예시

■ 자산목록 내 작성 항목 예시

- 자산명
- 자산 유형
- 제조사 및 모델명
- 일련번호
- OS/펌웨어/소프트웨어 버전
- 인터페이스/포트
- 물리적 위치
- 관리 부서
- 담당자
- 중요도
- 네트워크 정보
- 변경이력

통제항목	B.1.1 사이버 자산 목록	Basic

1. Bridge System

NO	ZONE	CATEGORY	Code	Service	Asset	IP	OS/Ver	Vendor	MODEL	Anti-Virus	Location	담당자	관리자	책임자	C	I	A	자산가치등급	취약점진단	비고
1	OT	선교시스템-레이더	BRS-RAD-001	BAND-RADAR	BAND-RADAR			ORANGE	OR-100			SCSM	SCSM	MASTER	3	5	4	4		
2	OT	선교시스템-ECDIS	BRS-ECD-001	ECDIS	ECDIS			ORANGE	OR-200			SCSM	SCSM	MASTER	3	5	5	4		

[그림 17] 자산 목록 관리 대장 작성 항목 예시

- 자산 목록에 IP, 프로토콜, 포트 번호 등 기밀 정보가 포함되는 경우 권한이 있는 인원에게만 접근을 제한

비고	

B.2 계정 관리

통제항목	B.1.1 사이버 자산 목록	Basic
점검목적	최소 권한 원칙을 준수하여 불필요한 접근을 사전에 차단하고, 내부자 위협 및 계정 탈취와 같은 보안 사고를 예방하며, 사고 발생 시 행위 추적성을 확보하여 보안 체계를 강화합니다.	
점검내용	사용자 계정의 생성·삭제 절차와 불필요한 계정 여부를 점검하고, 직무별 최소 권한 원칙과 관리자 권한 통제 현황을 확인합니다.	
점검기준	**양호 :** 사용자 계정이 최소 권한 원칙과 절차에 따라 생성·삭제되고 있을 경우 **취약 :** 사용자 계정이 최소 권한 원칙과 절차에 따라 생성·삭제되고 있지 않을 경우	
레퍼런스	[IMO 3.5.3.1 보호] [UR E26 4.2.4.3.5 사용자 인증정보 관리] [UR E26 4.2.4.3.6 최소 권한 원칙] [OCIMF SIRE 2.0 7.5 사이버보안] [BIMCO 7.3 절차적 보호 조치] [DCSA 2.1.2 설명] [DCSA 2.1.3 구현]	
증적자료	계정 및 권한 리스트, 계정 생성·변경·삭제 절차서	
조치방법	**계정 관리** ■ 계정 관리 적용 시스템의 예시 • 최종 사용자 장치 (예: 회사 노트북, PC) • 네트워크 인프라 (예: 무선 공유기) • OT 시스템 ■ 계정 승인 • 선박 담당자가 신규 계정 필요 사유, 역할, 접근 범위를 명시해 요청서 제출	

사용자계정 신청서

시스템 명칭			
소 속			
신 청 목 적			
이 름		직 급	
주 민 번 호		E-Mail	
전 화 번 호		FAX번호	
신 청 구 분	□ 등 록 □ 변 경 □ 폐 기		
	재발급, 폐지 사유	□ 소속 및 개인정보 변경 □ 비밀번호 분실 □ 기타 ( )	

상기와 같이 정보시스템 사용자계정을 신청합니다. 「정보통신보안업무세부지침」 사용자계정관리 지침을 준수하며, 본 신청서 관련 정보를 해당 분야의 정보시스템관리자가 관리하는 것에 동의합니다.

신청인 : 서명 또는 (인)

위와 같이 정보시스템 사용자계정 신청을 확인합니다.

년 월 일

보안 담당자 : 서명 또는 (인)

OO 해운사 귀하

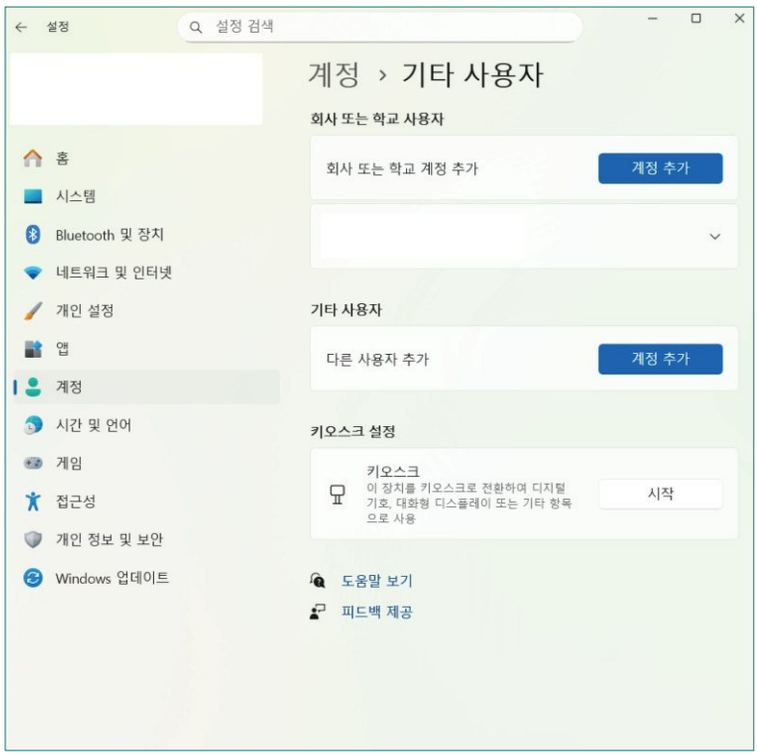
[그림 18] 사용자계정 신청서 예시

통제항목	B.1.1 사이버 자산 목록	Basic

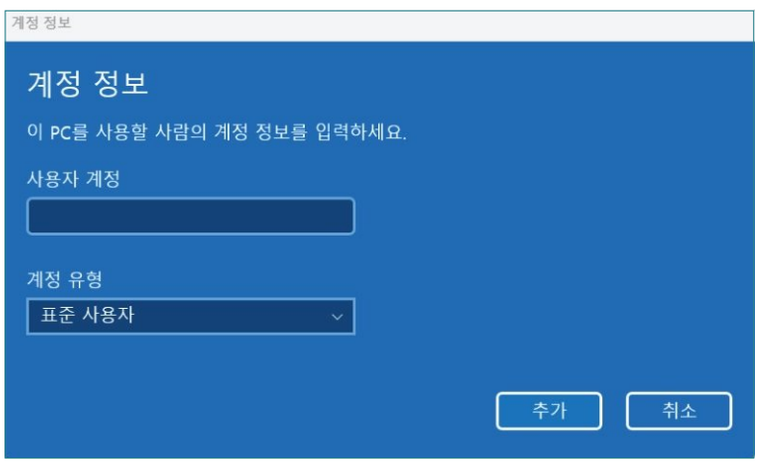
- 자산 관리 목록에 명시된 담당자가 검토 후 승인
- 최소 권한·업무분리 원칙 준수
- 승인 로그·문서를 SMS(안전관리시스템) 내 보관

■ 계정 생성

- IT/CCSM 팀이 승인서에 따라 최소 권한 원칙을 준수하여 사용자 계정 생성
- 사용자 관리가 용이한 환경 (예: 윈도우 컴퓨터)에서는 각 개인 사용자를 위한 계정 생성 권장
- 계정 생성 방법(Windows 11): 시작 〉 설정 〉 계정 〉 기타사용자 〉 회사 또는 학교 사용자/다른 사용자 추가 〉 계정 추가 〉 계정 유형 선택하여 사용자 및 관리자 계정 추가



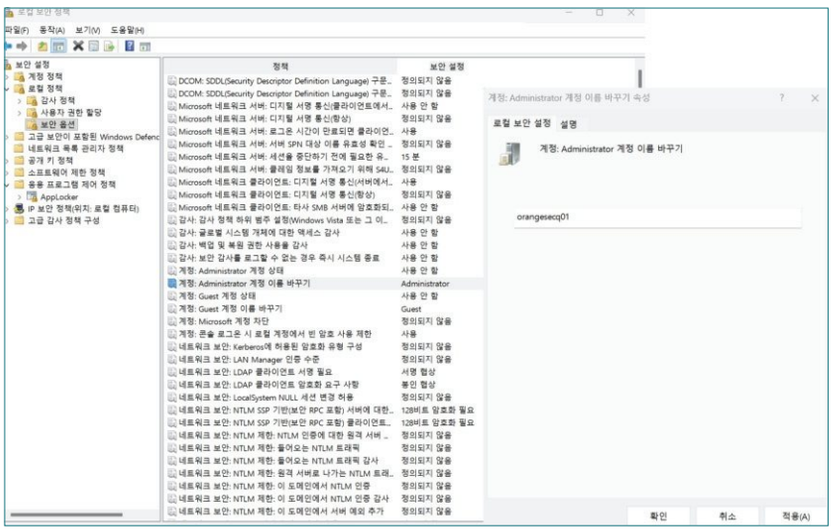
[그림 19] 계정 추가



[그림 20] 사용자/관리자 계정 추가

통제항목	B.1.1 사이버 자산 목록	Basic

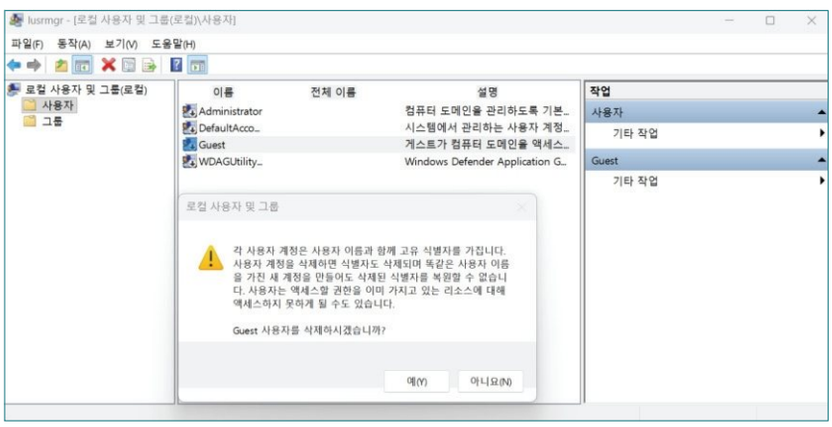
- 기본 사용자 이름 변경 권장(admin, Administrator(관리자), sa(시스템 관리자), root, user, operator, test 등)
- Administrator(관리자) 계정명 변경 방법(Windows 11)
  - Windows + R 〉 로컬 보안 정책 〉 로컬 정책 〉 보안옵션 〉 계정: Administrator(관리자) 계정 이름 바꾸기 〉



[그림 21] Administrator(관리자) 계정명 변경

■ 계정 삭제

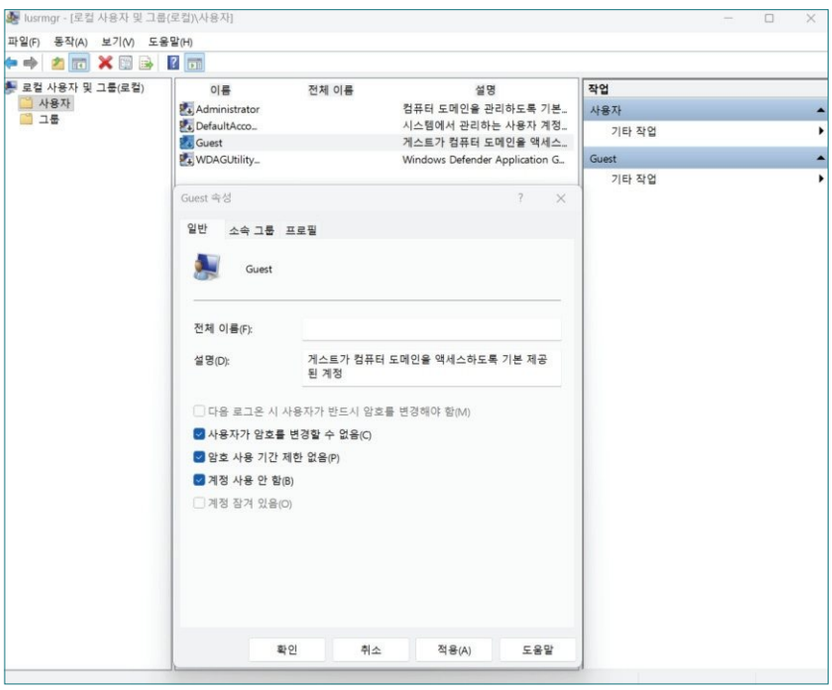
- 퇴사자 또는 불필요한 계정은 비활성화 및 삭제
- 계정 삭제 방법(Windows 11): Windows + R 〉 LUSRMGR.MSC 〉 사용자 〉 삭제할 계정 선택 〉 우클릭 후 삭제 〉 "예" 클릭



[그림 22] 계정 삭제

통제항목	B.1.1 사이버 자산 목록	Basic

• 계정 비활성화 방법(Windows 11): Windows + R 〉 LUSRMGR.MSC 〉 사용자 〉 비활성화할 계정 선택 〉 우클릭 후 속성 〉 "계정 사용 안 함"에 체크



[그림 23] 계정 비활성화

■ 공용 계정 관리

• 공용 계정 이용시 시스템, 직책, 성명, 선원번호, 이용기간 등을 포함한 기록을 문서화하여 관리

공용계정관리대장

시스템	직책	성명	선원번호	ID	P/W	이용기간
ECDIS	1등항해사	홍길동	ab2021312345	asdf4724	qwe123	241201~250213
ECDIS	2등항해사	성춘향	cd2023041223	asdf4724	qwe123	250214~250313

[그림 24] 공용계정관리대장 예시

2. 권한 관리

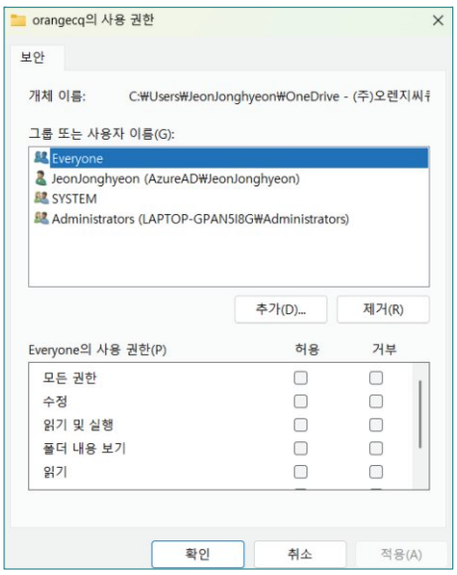
■ CBS(컴퓨터기반시스템)에 대한 전체 접근 권한은 회사 또는 선박 내에서 공식적으로 승인되고, 적절한 교육을 이수한 인력에게만 부여

■ 관리자 권한은 선사의 IT 부서에 유보하거나, 승선 중인 지정된 직원이 사용하는 단일 전용 계정으로 제한

■ 관리자 권한의 영구적 부여는 피해야 하며, 시간 제한 사용자 계정 사용

■ 직원의 역할 변경 시 해당 권한 즉시 삭제

■ 선박 환경에서는 공급자·계약자 등 외부 이해관계자도 시스템 접근 권한을 가질 수 있으므로, 권한의 범위와 기간을 명확히 정의하고 관리

통제항목	B.1.1 사이버 자산 목록	Basic
	■ 계정 권한 설정 방법(Windows 11) ■ 시작 〉 제어판 〉 사용자 계정 〉 계정 유형 변경 〉 변경하려는 계정 선택 〉 계정 유형 변경 〉 표준 or 관리자 유형 선택 [그림 25] 계정 유형 변경 ■ 폴더 권한 설정 방법(Windows 11) • 접근 권한 제한이 필요한 폴더의 권한 변경 • 폴더 우클릭 〉 속성 〉 보안 〉 편집 〉 추가 및 제거  [그림 26] 폴더 권한 추가 및 제거
비고	

통제항목	B.2.2 비밀번호 관리	Basic
점검목적	비밀번호 복잡성 관련 정책 설정과 다중 인증 설정으로 비인가자의 공격에 대비합니다.	
점검내용	비밀번호 작성 규칙 설정 여부와, 높은 수준의 접근 보안이 요구되는 경우 다중 인증 또는 암호화 키의 사용 여부를 확인하여, 접근 가능성을 최소화합니다.	
점검기준	**양호 :** 복잡한 비밀번호 규칙을 사용하는 경우 **취약 :** 복잡한 비밀번호 규칙을 사용하지 않는 경우	
레퍼런스	[IMO 3.5.3.2 보호] [UR E26 4.2.4.3.5 사용자 인증정보 관리] [OCIMF SIRE 2.0 7.5 사이버보안] [BIMCO 7.3 절차적 보호 조치] [DCSA 2.1.3 구현]	
증적자료	비밀번호 관리 정책서	

조치방법

1. 복잡한 비밀번호 정책 적용

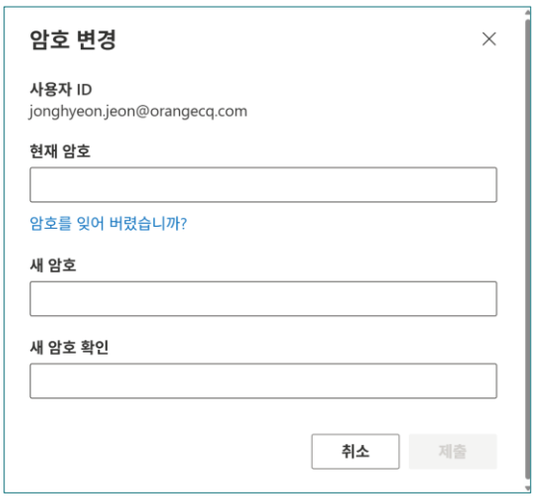
2024년 최악의 비밀번호 순위

순위	비밀번호	특징/설명
1	123456	가장 많이 사용되는 단순 숫자 조합
2	password	사전 단어, 너무 흔함
3	123456789	긴 숫자지만 여전히 단순
4	12345	짧은 숫자 조합
5	qwerty	키보드 상단 열 패턴
6	12345678	단순 연속 숫자
7	111111	반복 숫자
8	123123	반복되는 숫자 패턴
9	abc123	알파벳+숫자 단순 조합
10	password1	흔한 단어에 숫자만 덧붙임

[그림 27] 취약한 비밀번호 예시

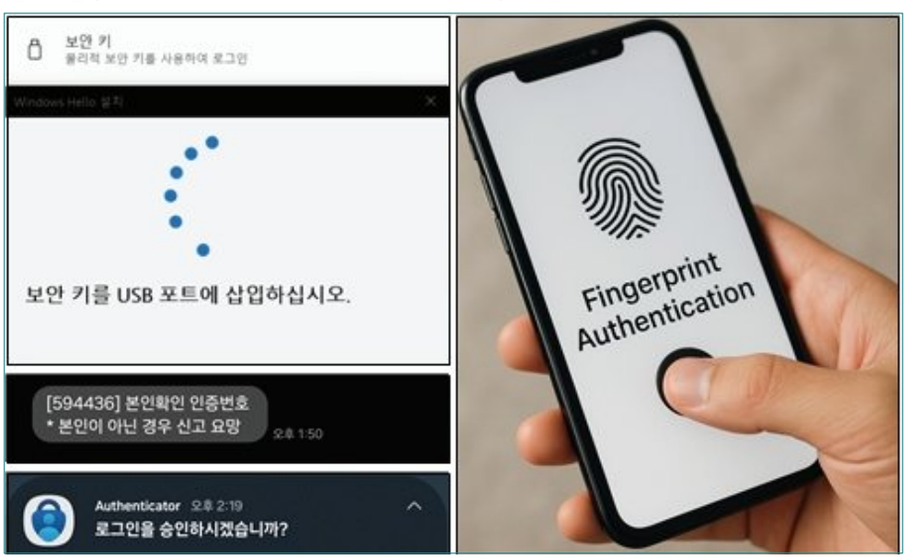
- 모든 장치의 기본 아이디, 비밀번호 반드시 변경 필요
- 복잡한 비밀번호 사용, 단순한 비밀번호 사용 금지
- 비밀번호 작성규칙 예시:
  - 영어 대, 소문자, 숫자, 특수문자 2종류 조합 시 10자리 이상
  - 영어 대, 소문자, 숫자, 특수문자 3종류 조합 시 8자리 이상
- 비밀번호 변경 방법(Windows 11):
  - 시작 〉 설정 〉 계정 〉 로그인 옵션 〉 암호 〉 변경 〉 이전암호 입력 후 로그인 〉 새 암호 입력 후 제출

통제항목	B.2.2 비밀번호 관리	Basic



[그림 28] 비밀번호 변경

2. 다중 인증(MFA: Multi-Factor Authentication) 적용



[그림 29] MFA(다중인증) 인증 방식

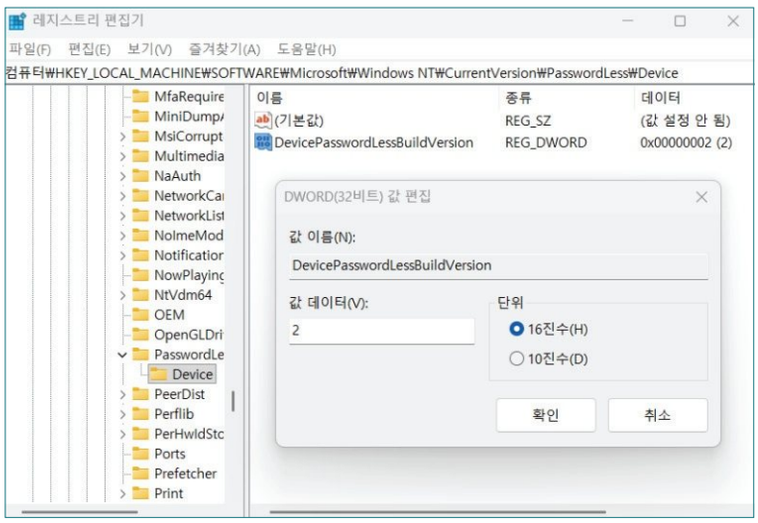
- 보안 수준을 높이기 위해 비밀번호 정책에 추가적으로 다중 인증 적용
- MFA(다중인증) 예시:
  - 모바일 앱 푸시 알림
  - SMS(안전관리시스템)/전화 코드
  - OTP(모바일 앱 확인 코드)
  - 생체 인식(지문, 얼굴, 홍체 인식)
- 높은 수준의 접근 보안이 요구되는 경우, 사용자의 소유 요소(토큰·장치) 추가 활용

통제항목	B.2.2 비밀번호 관리	Basic

3. 안전한 비밀번호 관리

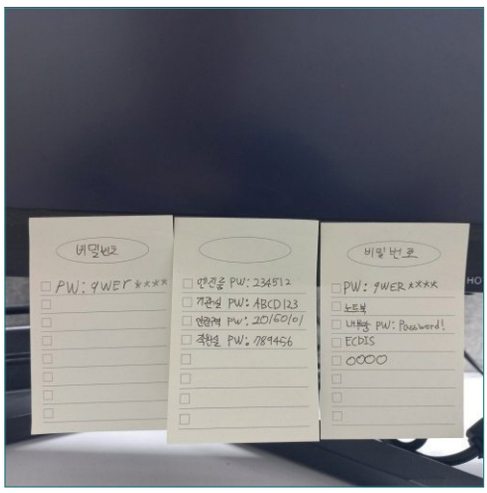
■ 자동로그인 방지 방법(Windows 11)

• Windows + R 〉 regedit 〉 레지스트리 편집기의 아래의 경로로 접근 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\PasswordLess\Device 〉 DevicePasswordLessBuildVersion의 값을 2로 설정



[그림 30] 레지스트리를 이용한 자동로그인 방지

■ 비밀번호가 기록된 포스트잇 부착 금지

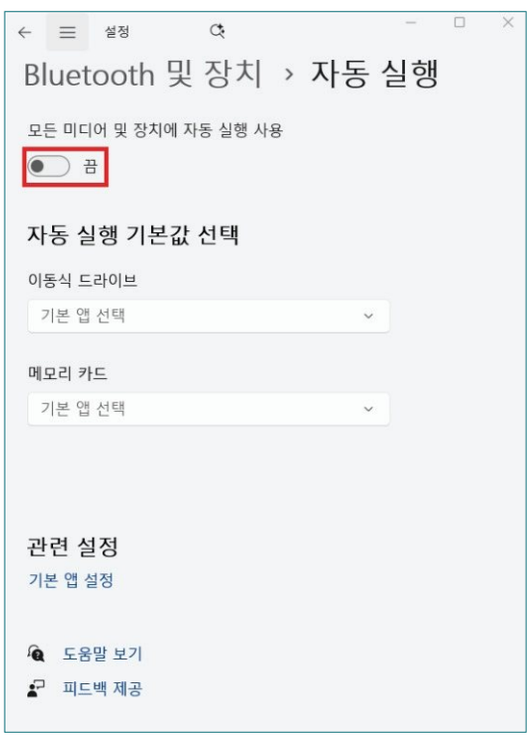


[그림 31] 포스트잇 부착된 PC 예시

■ 비밀번호 공유 금지

비고	

B.4 기기 및 출입 통제

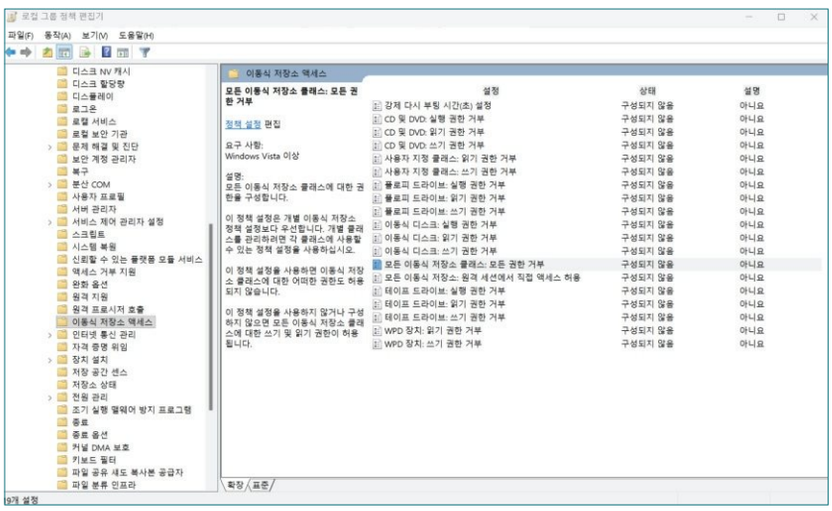
통제항목	B.4.1 기기 반출입 통제	Basic
점검목적	이동식 매체 및 외부 장치로 인한 악성코드 유입과 민감 정보 유출 리스크를 최소화하고, 물리적·논리적 접근 통제와 엄격한 사용 정책을 통해 안전한 환경을 유지합니다.	
점검내용	USB 포트를 비활성화하고 잠금하며 자동 실행을 차단합니다. 또한 사용 기록을 남기고, 이동식 매체 사용 전에는 악성코드 검사 절차를 운영합니다. 아울러 중요 장비의 포트 접근 통제 상태를 점검하고, 방문자의 이동식 장치 사용을 제한하여 안전을 강화합니다.	
점검기준	**양호 :** 이동식 매체 사용의 통제가 이루어지는 경우 **취약 :** 이동식 매체 사용의 통제가 이루어지지 않는 경우	
레퍼런스	[IMO 3.5.3.5 보호] [UR E26 4.2.4.3.4 이동식 미디어 통제] [OCIMF SIRE 2.0 7.5 사이버보안] [RIGHTSHIP 12.8 선박 내 컴퓨터에서 USB 메모리 스틱, CD, DVD, 디스켓 등의 이동식 미디어 사용을 통제하기 위한 조치가 마련되어 있습니까?] [DCSA 2.6.2 설명]	
증적자료	기기 반·출입대장	
조치방법	**1. 이동식 매체 및 외부 장치 연결 제한** ■ 이동식 매체 자동 실행 기능 비활성화(Windows 11) • 시작 〉 설정 〉 장치 〉 Bluetooth 및 장치 〉 자동 실행 〉 모든 미디어 및 장치에 자동 실행 사용 〉 끔  [그림 32] USB 포트 자동 실행 기능 비활성화	

통제항목	B.4.1 기기 반출입 통제	Basic

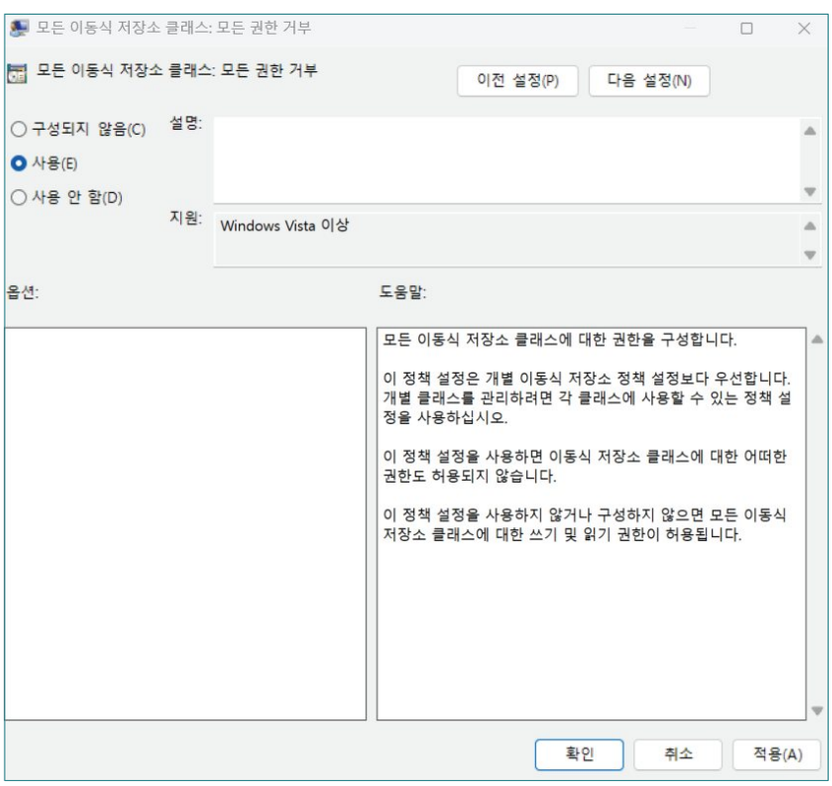
■ 이동식 매체 차단 정책 설정

• 이동식 매체 차단 정책 설정(Windows 11)

– Windows + R 〉 gpedit.msc 〉 로컬 그룹 정책 편집기 〉 로컬 컴퓨터 정책 〉 컴퓨터 구성 〉 관리 템플릿 〉 시스템 〉 이동식 저장소 액세스 〉 모든 이동식 디스크 액세스 클래스: 모든 권한 거부 〉 사용 〉 확인 후 재부팅



[그림 33] 로컬 그룹 정책 편집기: 이동식 저장소 액세스



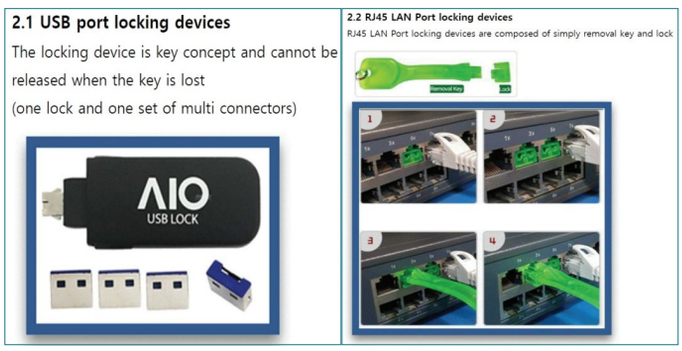
[그림 34] 모든 이동식 저장소: 모든 권한 거부 사용

통제항목	B.4.1 기기 반출입 통제	Basic

- 이동식 저장소 액세스에서 정책 설정을 통해 CD/DVD, 플로피 드라이브, 이동식 디스크 등의 매체 실행·읽기·쓰기 권한 세분화 가능(Windows 11)

■ 이동식 매체 물리적 차단

- 물리적으로 접근 가능한 모든 컴퓨터 및 네트워크 포트에 이동식 미디어 차단 장치(USB 포트 블로커 등) 설치 권고



[그림 35] USB 포트 블로커 설치 이미지

출처: 한국선급, '03. 사이버보안 현존선 인증 요구사항 해설'

- 차단 장치 훼손 여부 주간 점검 진행

■ 이동식 매체의 악성코드·바이러스 검사 및 제거를 위한 전용 PC 설치

[그림 36] 바이러스 검사 PC

[그림 37] 이동식 매체 바이러스 검사

통제항목	B.4.1 기기 반출입 통제	Basic

- 악성코드·바이러스 검사 전용 PC는 선박 내 네트워크와 완전 분리
- 이동식 매체 검사를 위한 백신 프로그램 설치
- 백신 프로그램 주기적 보안 패치 진행 및 최신화
- 이동식 매체에서 악성코드·바이러스 발견 시 감염 원인을 조사하고 폐기 처리

2. 장비 반출입 관리대장 작성

■ 이동식 매체·장비 반출입 관리대장

- 대장 항목: 장비명, 일련번호, 관리번호, 사용자, 반출입 목적 일시 등
- 전자·종이 대장의 이중 서명 보관 및 정기 검토를 통한 관리 정확성·신뢰성 유지

휴대용 저장매체 반출입 관리대장

□ 기관명 :

□ 관리책임자 :

장비명	관리번호	취급자 (사용자)	반출(입)목적	반출(입)일시	확인

[그림 38] 휴대용 저장 매체 반출입 관리대장 예시

장비 반출입 관리대장

□ 기관명 :

□ 관리책임자 :

장비명	일련번호	관리번호	반출내역			반입내역		비고
			반출 일자	반출 사유	인수자	반납 일자	반입자	

[그림 39] 장비 반출입 관리대장 예시

통제항목	B.4.1 기기 반출입 통제	Basic

3. 승무원 개인기기 관리

■ 사전 승인 등록
- 개인 기기(노트북, 스마트폰, USB 등)는 업무 목적·승인 없는 사용 금지
- 승선 시 기기 등록서 제출, 승무원 개인기기 목록 유지

■ 개인기기 정기 점검
- 개인 USB·외장디스크는 승선 시 및 매월 1회 이상 전용 PC로 악성코드 스캔
- 점검 결과 '승무원 기기 점검 기록부' 기재 및 보관

■ 보관
- 근무 중 사용하지 않는 개인기기는 잠금식 개인 라커 또는 격리함 보관

4. 방문자 기기 사용 제한·금지

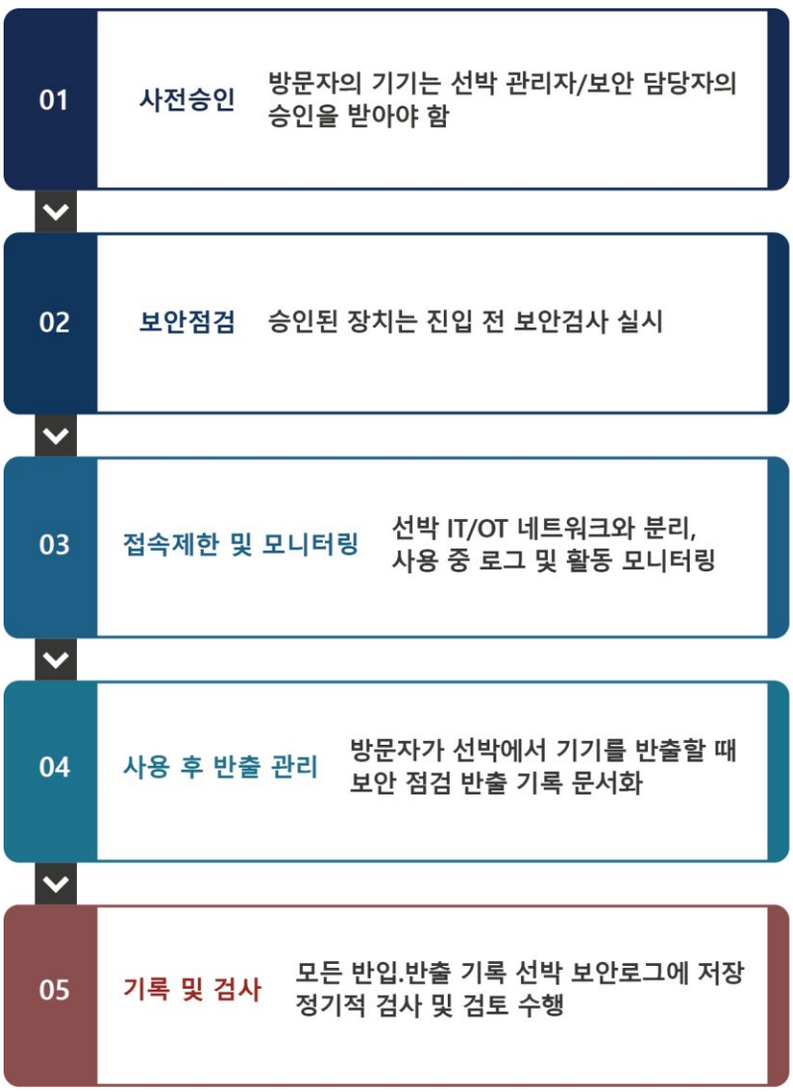
■ 방문자 사용 제한·금지 기기

[표 3] 방문자 사용 제한·금지 기기 예시

구분	예시 장비
이동식 저장매체	USB, SD 카드, 외장 HDD/SSD
휴대형 스마트기기	노트북, 태블릿, 스마트폰, 스마트워치
네트워크 장비	개인 공유기, 무선 AP, 휴대용 라우터
광/자기 매체	CD, DVD, 블루레이 등
기타	개인 방화벽 보안장비 등 무선/유선 통신 가능 장비 전부

통제항목	B.4.1 기기 반출입 통제	Basic

■ 방문자 기기 통제 절차



[그림 40] 방문자 기기 통제 절차 예시

- 보안 담당자는 방문자의 승선 전 반입 예정 기기 목록을 접수해 사전 승인 진행
- 승선 허가서에 기재된 최종 승인 기기를 확인하고, 승인 목록 외 기기의 반입 금지
- 방문자 대상 보안 서약서 징구
- 승선 시 X-ray 또는 휴대형 매체 스캐너로 휴대기기·매체 실물 검사 진행

5. 악성 매체 격리·폐기 절차

■ 악성 매체 발견 시 이중 잠금 보관함에 임시 격리

■ 폐기 시 2인 입회·서명으로 확인 후 파기

비고	

C. 사이버 리스크 관리

C.1 사이버 취약점 진단

통제항목	C.1.1 악성코드 방지	Basic
점검목적	CBS(컴퓨터기반시스템)는 바이러스, 웜, 트로이 목마 등 악성코드로부터 보호되어야 하며, 이는 금전적 손실, 시스템 성능 저하 및 데이터 손상을 유발할 수 있습니다. 악성코드는 전자메일, 첨부파일, 웹사이트, 이동식 미디어, 감염된 노트북 등 주요 경로를 통해 접근하므로 백신 프로그램이 악성코드 침입을 차단하고 사전 탐지·제거하여 예방적 보호 기능을 수행 해야합니다.	
점검내용	백신 설치 대상 기기에 백신 업데이트가 정기적으로 진행되는지 확인하고 백신 프로그램이 최신상태로 관리되어져 있으며 악성코드를 탐지하고 처리하기 위한 스캐닝 기능이 지속적으로 유지되어져 있는지 확인합니다.	
점검기준	**양호 :** 최신 악성코드 방지 소프트웨어가 설치되어 있는 경우 **취약 :** 최신 악성코드 방지 소프트웨어가 설치되어 있지 않는 경우	
레퍼런스	[IMO 3.5.3.4 보호] [UR E26 4.2.3.2 타당성] [UR E26 4.2.3.3 세부 요구사항] [OCIMF SIRE 2.0 7.5 사이버보안] [BIMCO 7.2 기술적 보호 조치] [BIMCO 8.2 악성코드 탐지]	
증적자료	백신 솔루션 설치 화면	
조치방법	**1. 백신프로그램 설치** ■ 백신 설치 대상 PC, OT시스템 목록 • PC(Windows, Linux, MAC, UNIX, SOLARIS 등) • Device(스마트폰, 테블릿, 노트북) • OT(백신 설치가 가능할 경우: 항해장비, 조타 시스템, 화물 시스템 등) ■ 백신 프로그램 설치 • 안랩(V3), 이스트시큐리티(알약), 오피스키퍼, McAfee, Microsoft Defender, Kaspersky 등 - 안랩: https://www.ahnlab.com - 알약: https://www.estsecurity.com - 오피스키퍼: https://www.officekeeper.co.kr - McAfee: https://www.mcafee.com/ko-kr - Kaspersky: https://www.kaspersky.co.kr	

통제항목	C.1.1 악성코드 방지	Basic

■ 실시간 스캔 기능 활성화로 지속적인 악성코드·바이러스 탐지 및 대응 기능 유지

[그림 41] 스캐닝 기능 활성화

■ 주기적인 PC 악성코드 검사 수행, 신뢰할 수 없는 파일 검사 수행

■ 악성코드·바이러스 탐지 기록 보관

2. 백신 프로그램 최신화를 위한 업데이트 절차

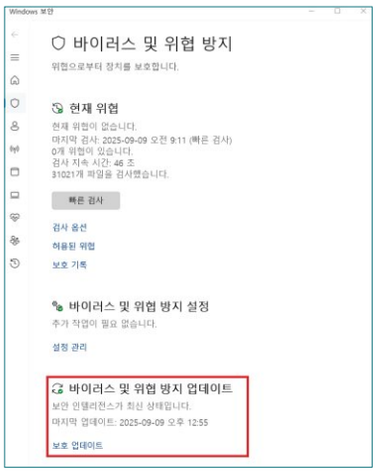
■ 자동업데이트(권장 방식)

- 백신 정책에서 최신 백신 업데이트마다 자동으로 업데이트 설정(인터넷 연결되는 환경)
- 주 1회 이상 업데이트 로그, 최신화 여부 확인 및 기록

■ 수동업데이트(네트워크 제한 환경 시)

- 선사 보안 담당자가 검증된 매체(USB·DVD 등)를 활용하여 최신 백신 패치 다운로드
- 업데이트 파일의 공급사 서명 확인 후 진행
- 패치 담당자가 최소 월 1회 이상 관리자 권한으로 수동 패치 적용 후 재부팅
- 적용 일시·버전·담당자를 업데이트 로그에 기록 후 본사에 보고
- Windows Defender 수동업데이트 방법(Windows 11 기준)
  - 시작 〉 설정 〉 개인 정보 및 보안 〉 Windows 보안 〉 바이러스 및 위협 방지 〉 바이러스 및 위협 방지 업데이트에서 보호 업데이트 클릭

통제항목	C.1.1 악성코드 방지	Basic

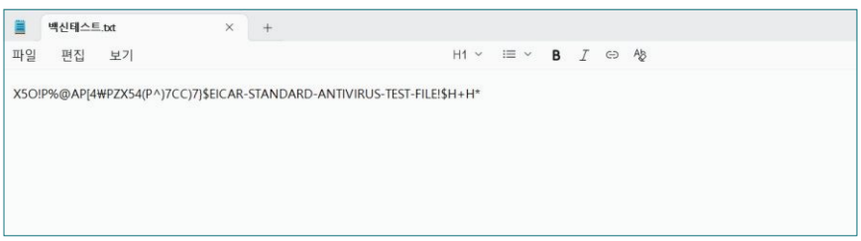


[그림 42] 백신 업데이트

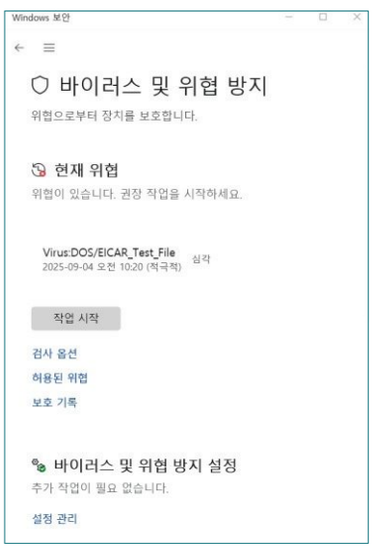
■ 백신 소프트웨어 검증

• text파일에 아래의 텍스트를 입력 후 저장 시 바이러스로 인식하여 백신 프로그램의 테스트 진행 가능

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H



[그림 43] 백신 테스트용 텍스트



[그림 44] Windows Defender 위협 탐지

통제항목	C.1.1 악성코드 방지	Basic

3. 대체 보안 조치 수행

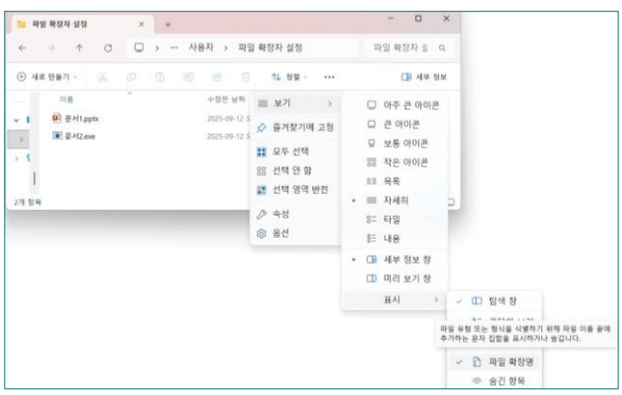
■ 백신프로그램이 장비 성능·서비스 저해 시 대체 보안 조치 적용

- 디지털 서명 확인: 외부에서 배포되는 소프트웨어·파일이 공인된 디지털 서명(Certificate)으로 증명되어 출처가 보장되는지 확인
- 승인된 미디어 사용: 이동식 매체(USB, DVD 등)는 사전 승인된 것만 사용
- 사전 승인 절차: 외부 소프트웨어, 드라이버, 데이터 설치 시 보안 담당자 사전 승인 후 진행

4. 악성코드 예방 PC 설정 방법

■ 파일 탐색기 파일 확장자 설정

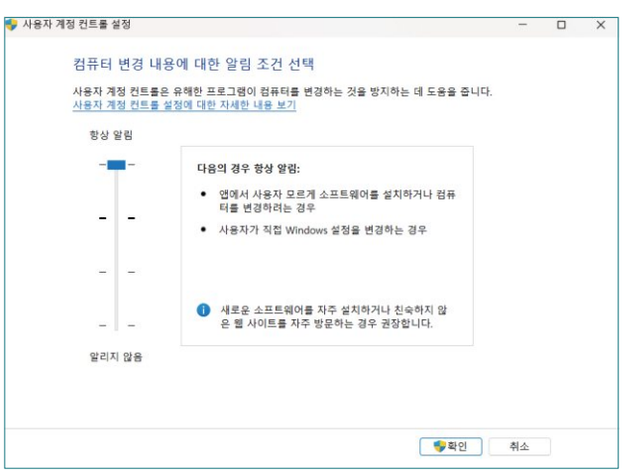
- 파일의 확장자를 확인하여 위장한 악성코드(.exe 등) 실행 회피
- 파일 확장자 표시 방법(Windows 11): 파일 탐색기 〉 보기 〉 파일 확장명 선택



[그림 45] 파일 확장자 식별 설정

■ 사용자 계정 컨트롤 설정(User Account Control Settings)

- 권한 없는 애플리케이션의 자동 설치 차단, 시스템 설정 변경 방지
- 사용자 계정 컨트롤 설정 방법(Windows 11): 시작 > UAC 검색 > 사용자 계정 컨트롤 설정 항상 알림 선택



[그림 46] 사용자 계정 컨트롤 설정

비고	

통제항목	C.1.2 패치 관리	Basic
점검목적	패치 절차를 통해 선박의 보안 취약점을 선제적으로 차단하여 운항 중단 리스크를 줄이고, 국제 규제와 선급 요구를 충족시켜 지속 가능한 유지보수 체계를 확보합니다.	
점검내용	선박 시스템 관련 소프트웨어, 하드웨어에 보안 업데이트가 권고 주기에 맞춰 적용되는지 확인합니다. 특히 OT 시스템의 호환성과 운영 영향에 대한 사전 테스트 및 무결성 검증이 이루어져야 하며, 적용이 불가능할 경우 보완조치가 이행되야합니다. 모든 유지보수 활동은 사이버보안 책임자의 검증과 승인, 정기적인 재검토를 통해 체계적으로 관리되어야 합니다.	
점검기준	**양호 :** 적절한 승인 절차에 따라 최신 패치가 적용 되어있는 경우 **취약 :** 적절한 승인 절차에 따라 최신 패치가 적용 되어있지 않은 경우	
레퍼런스	[OCIMF SIRE 2.0 7.5 사이버보안] [BIMCO 7.2 기술적 보호 조치] [BIMCO 7.3 절차적 보호 조치] [DCSA 2.5.2 설명] [DCSA 2.5.3 구현]	
증적자료	패치 이력 관리 보고서	
조치방법	**1. 보안 업데이트 및 패치 로드맵 수립**	

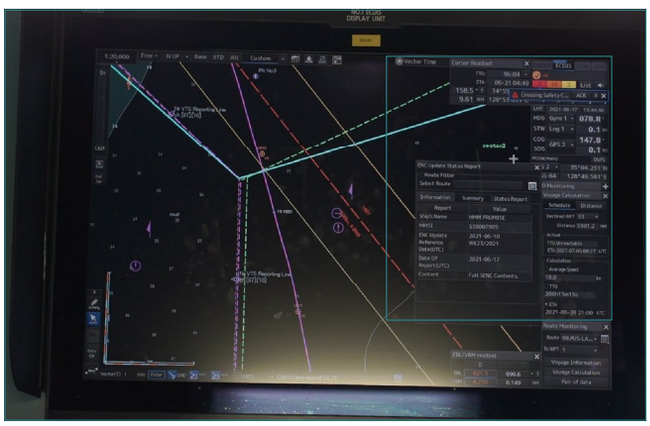
소프트웨어 패치 이력서

선박명	장비명	소프트웨어명	패치명/ID	패치 유형	이전 버전	적용 후 버전	취약점 정보	적용 일시	적용자/책임자	검증 및 테스트 결과	관련 문서	비고
ORANGE	ECDIS	ECDIS Core SW	2025-09 Security Patch	Security	v3.2.1	v3.2.2	CVE-2025-12345	2025-01-01 14:30	김선장 / 벤더 기술자	정상 동작 확인	벤더 릴리스 노트	

[그림 47] 패치 로드맵 예시

■ 중요 선박 시스템 보안 패치 진행

- 위성통신 장비(VSAT), 항해 장비(ECDIS), 엔진 제어 시스템 등 제조사 제공 패치 적용



[그림 48] ECDIS 패치 버전 예시

출처: 한국선급, '03. 사이버보안 현존선 인증 요구사항 해설'

- OT 시스템의 경우 벤더를 통해 업데이트 진행
- 패치 주기는 한 달 이내에 수행 권장
- 선박 운영에 지장이 없는 범위 내에서 업데이트 진행

통제항목	C.1.2 패치 관리	Basic

■ 소프트웨어 및 하드웨어용 패치 로드맵 마련 권장
- 소프트웨어: 선박 관리 시스템의 분기별 보안 업데이트
- 하드웨어: 방화벽, 라우터, 위성통신 모뎀의 펌웨어 업데이트 일정을 제조사 권고 주기에 맞춰 반영

■ 중요 장비 사전 검증
- 중요한 OT 시스템은 패치 테스트 및 호환성 평가 진행
- 방화벽과 같은 중요 장비는 패치 적용 전 점검, 특히 방화벽 룰셋이 업데이트되면서 항해 장비 통신 차단 여부 사전 검증 진행

2. OT 시스템의 운영 영향 고려

■ OT 시스템은 업데이트 주기가 길거나 일부 패치가 불가능할 수 있음:
- 주요 패치를 적용할 수 없을 경우 망분리 필요 등 네트워크 격리 조치 적용

3. 소프트웨어 유지보수와 지원 종료 대응

■ 제조사의 보안 패치 지원이 종료된 경우 자산 교체 필요:
- Windows 7, Windows Server 2008 등 지원 종료 된 시스템 → Windows 10/11, 최신 Server 버전으로 업그레이드

[그림 49] Windows 11 이미지

- 기존 장비와 호환 불가 시, 가상화 환경으로 이전하여 점진적으로 교체

■ 라우터, 스위치, 방화벽, OT 장비 펌웨어도 정기적 패치 필요
- 선박 엔진 제어 장비, 발전기 모듈, ECDIS 등 → 제조사 제공 펌웨어 업데이트 확인
- 호환성 문제 방지를 위해 육상에서 테스트 후 선박 반영
- 제조사를 통해 업데이트·유지보수 진행

통제항목	C.1.2 패치 관리	Basic

서비스 보고서

SUPPORT TIME	Date:	
	Start Time:	End Time:
CUSTOMER INFORMATION	Vessel:	Last Inspection Time:
	Name:	Tel:

ACCESS METHOD	VENDER	PRODUCT	IP Add	OS Ver.	SERIAL.NO.
WORK CHECK					
☐ Regular check	☐ Troubleshooting		☐ Others ( )		

WORK SUMMARY
TITLE : [정기점검] 방화벽

1. 점검 요약					
점검 결과					
H/W	☐ 정상	☐ 비정상	S/W	☐ 정상	☐ 비정상
비고					

2. 점검 정보					
Check Items	Verify		Remark		
	Y	N			
1. IPS 전원 인가 여부 및 LED 점등 상태 점검					
2. 평소와 다른 소음/진동 발생 여부 확인					
3. 주위 온도 확인(0 ~40 도씨 내 정상)					
4. 장비 시리얼번호 /호스트네임 / 구동시간					
5. 펌웨어 버전 확인 및 업그레이드					
6. IPS 현재 시간 확인 및 수동 동기화 조치					
7. CPU 사용률 확인(모델별 상이하나, 0~15 % 내 정상)					
8. MEMORY 사용률 확인(모델별 상이하나, 10% ~50% 내 정상)					
9. SESSION 사용률 확인(모델별 상이하나, 0~1000개 내 정상)					
10. 인터페이스 연결 상태 확인 (DUPLEX FULL, CRC 에러값 없어야 정상)					
11. 방화벽 시스템 에러 및 이상로그 발생여부 확인					
12. 관리자 계정(admin) 생성 및디폴트 계정 삭제 조치					
13. 방화벽 트래픽 로그 NAS SYSLOG 연동 조치 및 정상 연동 확인					
14. 방화벽 표준화 정책 설정 및 정책 변경여부 비교 점검					
15. 방화벽 정책 설정 확인					

[그림 50] 방화벽 유지보수 보고서 예시

4. 패치 절차 및 방법

- 패치와 업데이트는 적절히 훈련된 인력이 수행
- 유지보수 및 패치 주기는 한 달 이내에 수행 권장
- 사이버보안 책임자(CySO)가 패치 활동 검증 및 승인
- 패치대상:
  - IT시스템(서버, 데스크탑/노트북, 네트워크 장비(라우터 스위치 방화벽))
  - OT시스템(선박 제어 시스템, 통합 모니터링 장치)

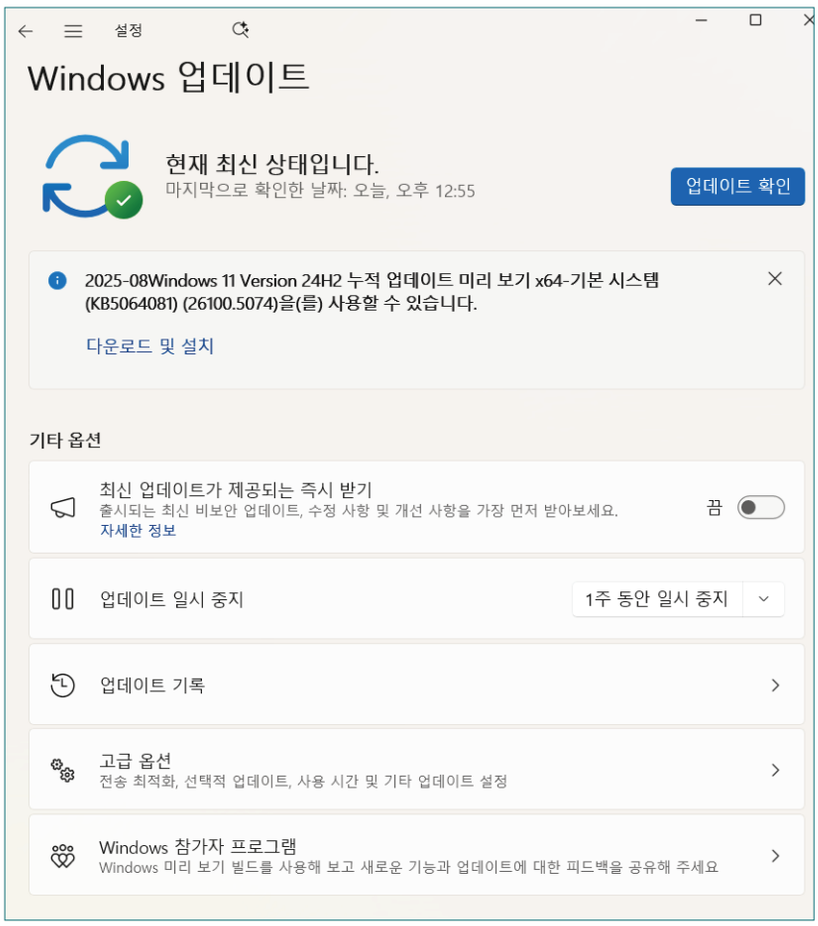
통제항목	C.1.2 패치 관리	Basic

■ 패치방법:

- 사전 준비(패치 적용 전 백업, 패치 적용 대상 목록 확인, 적용 일정 수립(운항 스케줄과 충돌 최소화))
- 적용 방식(자동 업데이트: OS, 일부 서버, 수동 업데이트 OT시스템, 특수 장비, 테스트 환경에서 적용 후 실제 시스템 적용)
- 검증(패치 적용 후 정상 동작 확인)

■ 사용자 컴퓨터 보안 패치 진행:

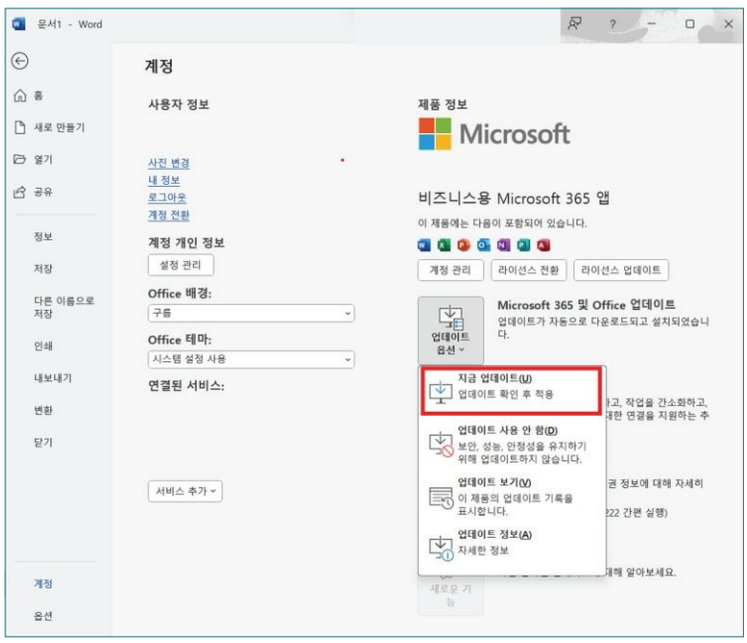
- 윈도우 업데이트는 자동 실행 혹은 알람을 보는 즉시 설치
- Windows 업데이트 방법(Windows: 시작 〉 설정 〉 Windows 업데이트 〉 업데이트 확인하기



[그림 51] Windows 패치 이미지

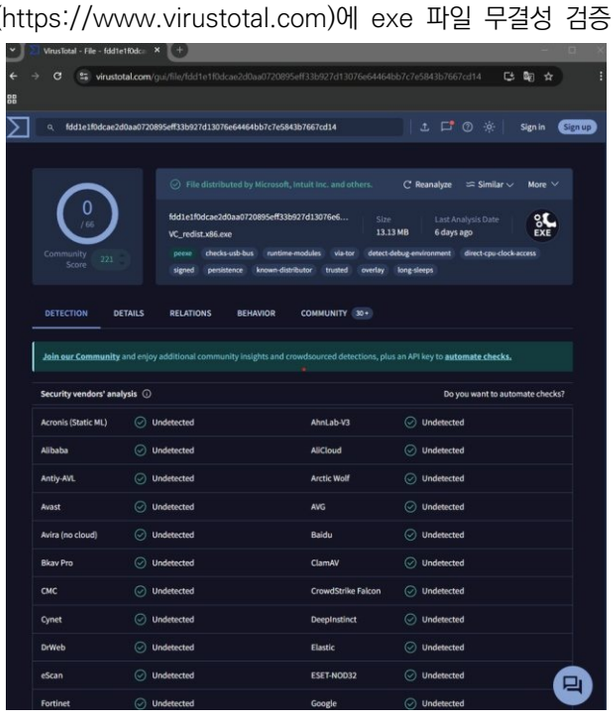
통제항목	C.1.2 패치 관리	Basic

• 오피스 업데이트 방법: 오피스 프로그램 열기 〉 계정 〉 Office 업데이트 〉 지금 업데이트



[그림 52] 오피스 업데이트 이미지

• 사용하지 않는 불필요한 소프트웨어 삭제 및 소트프웨어에서 제공하는 업데이트 즉시 적용
• 소프트웨어 공급업체가 제공한 exe 파일 이용한 수동 패치
 - 바이러스토탈(https://www.virustotal.com)에 exe 파일 무결성 검증 후 사용

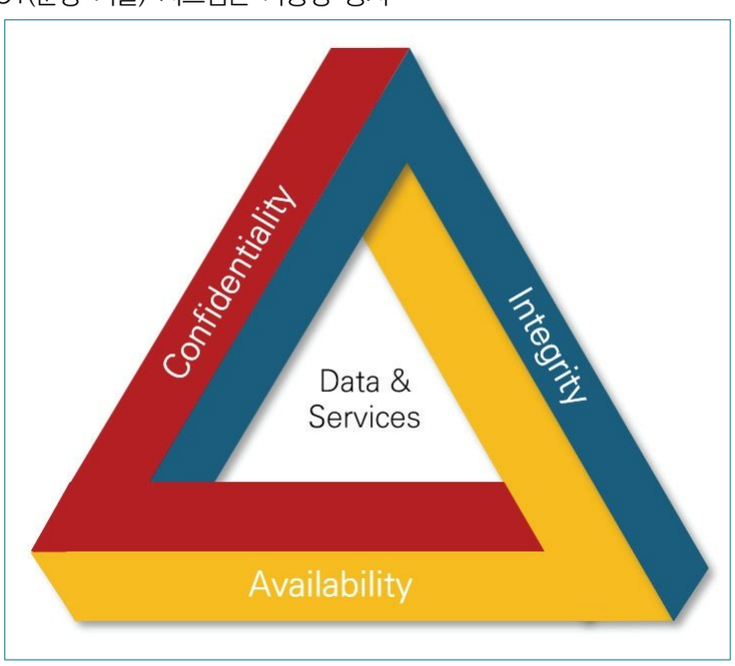


[그림 53] 바이러스토탈 이미지

• 오프라인 이동식매체 사용 시 악성코드 사전 스캔 필수

통제항목	C.1.2 패치 관리	Basic
	■ 패치 예외 처리: • 특정 패치가 시스템 기능이나 안전 장치와 호환되지 않을 경우 - 예외 사유 및 영향 문서화: 해당 시스템, 패치 미적용 사유, 운항에 미칠 영향 - 리스크 평가 수행: 보안 리스크와 운항 영향에 대해 정량 평가 - 승인 절차: 선장·안전책임자·회사사이버 담당자에게 리스크 평가서 전달, 검토 후 승인 - 대체 안전조치 적용: 방화벽 설정 강화, 중요 장비 분리, 관리자 비밀번호 변경 등 - 예외 패치 주기 재검토: 분기별 1회 또는 새 패치가 나올때마다 검증	
비고		

C.2 사이버 리스크 평가

통제항목	C.2.1 사이버 영향도 평가	Basic
점검목적	사이버 사고의 자산별 영향도를 평가하여 선박 운영과 안전에 미치는 결과를 객관적으로 파악하고, 그 중요도에 따라 적절한 보호 조치와 복구 자원을 배분하도록 합니다.	
점검내용	영향도 평가 대상과 필요성을 파악하고 있으며, 적절한 평가 모델을 기반으로 영향도 평가를 진행하고 있는지 확인합니다.	
점검기준	**양호 :** 정기적인 영향도 평가를 진행하고 있을 경우 **취약 :** 정기적인 영향도 평가를 진행하고 있지 않을 경우	
레퍼런스	[BIMCO 3.4 선박-육상 간 인터페이스] [BIMCO 5.1 CIA 모델] [BIMCO 5.2 영향 정량화] [BIMCO 5.3 "중요" 장비 및 기술 시스템]	
증적자료	IT·OT 통합 현황 보고서, 자산별 영향 평가 결과서	
조치방법	**1. 영향도 평가 방법** ■ CIA 모델 기반 영향도 평가 • CIA 모델: 기밀성(Confidentiality), 무결성(Integrity), 가용성(Availability) 관점의 사이버 사고 영향도 평가 프레임워크 • 정보/데이터의 사용 목적에 따라 C.I.A 중요성 변경됨 • 데이터 기밀성은 일부 낮게 평가될 수 있으나 무결성·가용성 손실 영향은 높음 • 선박 내 OT(운영 기술) 시스템은 가용성 중시  [그림 54] C.I.A 모델 이미지 ■ 자산 영향도 산정(C.I.A 모델, 5단계) • 자산을 5단계 척도(점점 심각해지는 수준)로 구분된 영향도 산정 기준 예시	

통제항목	C.2.1 사이버 영향도 평가	Basic

• 자산 C.I.A 평가값 산정 기준 예시

[표 4] 자산 C.I.A 평가값 산정표 예시

구분	LEVEL	설명	종류
기밀성 (C)	5	치명적	정보가 유출될 경우 인명, 자산, 환경에 치명적인 리스크를 초래할 수 있음, 조직에 심각한 재정적 손실, 매우 장기적인 사업 중단/비용, 사망 가능성 야기함
	4	중요한	정보가 유출될 경우 조직에 중대한 재정적 손실, 장기간의 사업 중단/비용, 영구적인 신체적 상해 야기함
	3	보통	정보가 유출될 경우 인명, 자산, 환경에 중간 정도의 리스크를 초래할 수 있음, 중간 정도의 재정적 손실, 중기적인 사업 중단/비용, 단기적인 부상 야기함
	2	사소한	정보가 유출될 경우 경미한 금전적 손실, 단기 사업 중단/비용, 응급 처치 부상 야기함
	1	무시할 만한	정보가 유출되더라도 인명, 자산, 환경에 리스크를 초래할 수 없음, 경미한 재정적 손실, 매우 단기적인 사업 중단/비용 야기함
무결성 (I)	5	치명적	정보가 변조될 경우 인명, 자산, 환경에 치명적인 리스크를 초래할 수 있음, 조직에 심각한 재정적 손실, 매우 장기적인 사업 중단/비용, 사망 가능성 야기함
	4	중요한	정보가 변조될 경우 조직에 중대한 재정적 손실, 장기간의 사업 중단/비용, 영구적인 신체적 상해 야기함
	3	보통	정보가 변조될 경우 인명, 자산, 환경에 중간 정도의 리스크를 초래할 수 있음, 중간 정도의 재정적 손실, 중기적인 사업 중단/비용, 단기적인 부상 야기함
	2	사소한	정보가 변조될 경우 경미한 금전적 손실, 단기 사업 중단/비용, 응급 처치 부상 야기함
	1	무시할 만한	정보가 변조되더라도 인명, 자산, 환경에 리스크를 초래할 수 없음, 경미한 재정적 손실, 매우 단기적인 사업 중단/비용 야기함
가용성 (A)	5	치명적	시스템이 중단될 경우 인명, 자산, 환경에 치명적인 리스크를 초래할 수 있어 15분 이내에 복구(장애 조치)가 완료되어야 하는 경우, 심각한 재정적 손실, 매우 장기적인 사업 중단/비용, 사망 가능성 야기함
	4	중요한	시스템이 중단될 경우 인명, 자산, 환경에 심각한 리스크를 초래할 수 있어 15분~1시간 이내 복구가 필요한 경우, 중대한 재정적 손실, 장기간의 사업 중단/비용, 영구적인 신체적 상해 야기함
	3	보통	시스템이 중단될 경우 인명, 자산, 환경에 중간 정도의 리스크를 초래할 수 있음, 1~6시간 이내 복구가 필요한 경우, 중간 정도의 재정적 손실, 중기적인 사업 중단/비용, 단기적인 부상 야기함
	2	사소한	시스템이 중단될 경우 인명, 자산, 환경에 경미한 리스크를 초래할 수 있어 1일 이내 복구가 필요한 경우, 조직에 경미한 금전적 손실, 단기 사업 중단/비용, 응급 처치 부상 야기함
	1	무시할 만한	시스템이 중단되더라도 인명, 자산, 환경에 리스크를 초래할 수 없음, 1주일 이상 장애 발생 시에도 감내가 가능한 경우, 경미한 재정적 손실, 매우 단기적인 사업 중단/비용 야기함

통제항목	C.2.1 사이버 영향도 평가	Basic

• 영향도 기준 예시

[표 5] 영향도 예시

Level	영향도
5	사망 또는 영구적인 장애. 운영, 환경, 자산, 재정, 회사 평판에 대한 광범위하고 심각한 피해
4	중대한 인체 피해 또는 심각한 부상. 지역적이지만 운영, 환경, 자산, 재정, 회사 평판에 대한 중대한 피해
3	일시적 인체 피해 또는 경미한 부상. 운영, 환경, 자산, 재정, 회사 평판에 대한 경미한 피해
2	경미한 인체 피해 또는 부상, 운영, 환경, 자산, 재정, 회사 평판에 대한 매우 경미한 피해
1	인체 피해·부상 없음. 운영, 환경, 자산, 재정, 회사 평판에 대한 피해 없음

• 영향도 산정 기준 예시

[표 6] 자산 영향도 산정표 예시

영향도	평가기준
5	기밀성 평가값 + 무결성 평가값 + 가용성 평가값이 13 ≤ X ≤ 15 인 경우
4	기밀성 평가값 + 무결성 평가값 + 가용성 평가값이 10 ≤ X ≤ 12 인 경우
3	기밀성 평가값 + 무결성 평가값 + 가용성 평가값이 7 ≤ X ≤ 9 인 경우
2	기밀성 평가값 + 무결성 평가값 + 가용성 평가값이 5 ≤ X ≤ 6 인 경우
1	기밀성 평가값 + 무결성 평가값 + 가용성 평가값이 3 ≤ X ≤ 4 인 경우

• 영향도 평가 예시(화물 관리 시스템)
- 기밀성: 보통 3점 (화물 데이터 유출 시 금전 손실)
- 무결성: 치명적 5점 (벨브 펌프 제어 변조 시 사고 리스크)
- 가용성: 치명적 5점 (시스템 중단 시 운항 중지)
- 화물 관리 시스템: 3(기밀성)+5(무결성)+5(가용성) = 13 => 영향도 5

• 영향도 점수 고려사항 예시
- 영향도 5: 조타·기관 제어 시스템 침해
- 영향도 4: 항해 시스템(ECDIS, GPS 등) 랜섬웨어 감염
- 영향도 3: 선박 내 일부 OT 장비(예: 엔진 모니터링 시스템) 오작동
- 영향도 2: IT 네트워크 감염, 업무 지연
- 영향도 1: 개별 PC 감염

통제항목	C.2.1 사이버 영향도 평가	Basic
	2. 주요 시스템 영향도 ■ 화물 관리 시스템 장애 시 운송·안전·재정적 영향 ■ 브리지 시스템(항해, 전자해도) 장애 시 운항 안전 영향 ■ 기관 및 전원 제어 시스템 무력화 시 추진·운항 안전 영향 ■ 출입 통제 및 감시 시스템 장애 시 물리적 보안 영향 ■ 여객 서비스·공용 네트워크를 통한 안전 및 보안 위협 가능성	
비고		

통제항목	C.2.2 사이버 발생빈도 평가	Basic
점검목적	선박 IT/OT 시스템 내 사이버 위협과 취약성 요소를 체계적으로 식별하고, 사이버 공격의 실제 발생 빈도를 파악하여 자산에 대한 공격 대응 우선순위를 설정하는 것을 목적으로 합니다.	
점검내용	선사의 점수 산정 기준에 따라 공격 가능성(위협 요인)과 취약성으로 발생빈도를 종합해 정량화하고 있는지 확인합니다.	
점검기준	**양호 :** 발생빈도를 평가하는 경우 **취약 :** 발생빈도를 평가하지 않는 경우	
레퍼런스	[BIMCO 1.4 IT와 OT 시스템의 차이점] [BIMCO 2.1 위협 행위자] [BIMCO 2.2 사이버 위협의 유형] [BIMCO 2.4 위협의 정량화] [BIMCO 3.1 공개적인 취약점] [BIMCO 3.3 일반적인 취약 시스템] [BIMCO 4.1 위협과 취약성의 곱으로서의 발생빈도] [BIMCO 4.2 발생빈도의 정량화]	
증적자료	발생빈도 평가 결과표	
조치방법	**1. 발생빈도 정량화** ■ 사이버 공격 종류	

[표 7] 사이버 공격 종류

공격 유형	공격 종류	설명
비표적 공격	악성코드 (Malware)	소유자의 인지 없이 컴퓨터에 접근하거나 손상을 입히도록 설계된 악성 소프트웨어. 트로이목마, 랜섬웨어, 스파이웨어, 바이러스, 웜 등이 있으며, 시스템에 침투해 데이터를 암호화하고 몸값을 요구하기도 함. 보안 업데이트가 되지 않은 비즈니스 소프트웨어의 취약점을 악용하는 경우가 많음. "Exploit"은 일반적으로 취약한 소프트웨어나 코드, 또는 하드웨어 문제를 조작하기 위한 소프트웨어 또는 코드의 사용을 의미하며, 예: 코드 버그, 시스템 취약점, 설계 결함 등. 이러한 취약점은 원격 또는 로컬에서 실행될 수 있고, 악성 링크나 이메일 첨부파일을 통해 실행되기도 함
	워터홀링 (Waterholing)	가짜 웹사이트를 만들거나 진짜 웹사이트를 손상시켜, 방문자를 악용하는 방법
	스캐닝 (Scanning)	인터넷의 광범위한 영역을 무작위로 검색해 악용 가능한 취약점을 탐지하는 기법
	타이포스쿼팅 (Typosquatting)	URL 탈취나 유사 도메인을 활용하여 사용자가 웹 주소를 오타로 입력했을 때 악성 웹사이트로 유도하는 수법

통제항목	C.2.2 사이버 발생빈도 평가	Basic

공격 유형	공격 종류	설명
표적 공격	사회공학(Social engineering)	사이버 공격자가 내부 관계자를 조작해 보안 절차를 우회하도록 유도하는 비기술적 기법, 보통 소셜미디어를 통해 접근
	무차별 대입 (Brute force)	가능한 모든 암호 조합을 시도하여 시스템에 침투하는 방식
	자격 증명 (Credential stuffing)	이미 유출된 사용자 ID/비밀번호 또는 흔히 사용되는 조합을 활용해 시스템 접근을 시도
	서비스 거부 공격 (DoS)	대량의 데이터를 네트워크에 전송해 정상적인 접근을 방해함. DDoS는 여러 시스템을 동시에 동원함
	피싱 (Phishing)	많은 사용자에게 이메일을 보내 민감한 정보(예: 암호, 계좌 정보)를 탈취하거나 악성 첨부파일 또는 링크를 클릭하도록 유도
	스피어 피싱 (Spear-phishing)	특정 대상에 대해 맞춤형으로 설계된 피싱 공격. 보통 기존의 이메일 양식을 위조하여 친숙한 사람으로 위장함
	공급망 침해 (Subverting the supply chain)	선박이나 회사에 납품되는 장비, 소프트웨어, 지원 서비스 등을 손상시켜 침투하는 방식

- 관련 위협 사건의 업계 발생 사례 및 전례 분석
  - 최근 해운·위성통신 대상 악성코드, 랜섬웨어, APT(지능형 지속 위협) 동향 등
- 회사 SMS(안전관리시스템)와 연계된 리스크 매트릭스를 통한 발생빈도 단계 산정
- 위협과 취약성의 점수 산정 기준을 설정하고 두 점수의 곱으로 발생빈도 정량화 진행

통제항목	C.2.2 사이버 발생빈도 평가	Basic

2. 위협 산정 예시

■ 위협을 식별할 때, 기업은 잠재적 위협 행위자의 능력(Capability), 기회(Opportunity), 공격 의도(Intent)와 같은 구체적인 측면 고려

- 위협(Threat) = 능력 × 기회 × 의도 공식을 통한 위협 정량화
- 합산 평균 곱셈 이나, 의도의 비중을 낮추는 등 조직이 정한 모델로도 정량화 가능
- 능력, 기회, 의도 점수 기준 예시

[표 8] 능력, 기회, 의도 점수 산정 예시 표

점수	능력	기회	의도
5	국가급 APT·지속적 공격 가능	광범위한 노출, 다단계 침투 용이	군사 정치적 전략 목적
4	고급 제로데이·OT 공격 능력	공급망/위성 선박 네트워크 다수 노출	산업·정치 목적의 표적
3	상용 취약점 툴·중간 수준 APT	위성통신/원격지원 계정 일부 노출	금전·산업 스파이 목적
2	스크립트 자동화 툴 수준	제한적 원격접속, 주기적 패치 양호	금전 동기 낮음
1	해킹 기술 도구 거의 없음	네트워크 완전 분리, 외부 접근 거의 불가	단순 호기심·우발

- 위협 점수 기준 예시 (능력·기회·의도를 곱한 점수 이용)

[표 9] 위협 산정 예시 표

위협	구분	위협 설명	점수 기준 (X = 능력x기회x의도)
5	확실한	대상 자산 또는 유사한 자산이 자주 반복적으로 표적 또는 공격 받음	101 ≤ X ≤ 125
4	가능성 있는	몇 가지 보안 조치가 있지만 완전하고 효과적인 응용 프로그램이 없으므로 공격이 비교적 쉽게 성공 가능	65 ≤ X ≤ 100
3	가끔	일부 효과적인 보안 조치가 마련되어 있지만 기존 대응 조치는 여전히 손상 가능성 존재	28 ≤ X ≤ 64
2	희미한	효과적인 보안 조치가 마련되어 있지만 적어도 하나의 취약점 존재	9 ≤ X ≤ 27
1	불가능	실제 또는 계획된 위협의 이력 없음	0 ≤ X ≤ 8

통제항목	C.2.2 사이버 발생빈도 평가	Basic

3. 취약성 산정 예시

■ 사이버 공격이 발생했을 때 자산에 대한 공격의 성공 확률을 고려하여 점수 산정

• 취약성 산정 예시

[표 10] 취약성 산정 예시 표

취약성	구분	설명
5	매우 높음	현재 매우 비효율적인 보안 조치가 시행되고 있으므로 적이 쉽게 성공 가능
4	높음	몇 가지 보안 조치가 있지만 완전하고 효과적인 응용 프로그램이 없으므로 공격이 비교적 쉽게 성공 가능
3	중간	일부 효과적인 보안 조치가 마련되어 있지만 기존 대응 조치는 여전히 손상 가능성 존재
2	낮음	효과적인 보안 조치가 마련되어 있지만 적어도 하나의 취약점 존재
1	매우 낮음	효과적인 보안 조치의 여러 계층이 존재

4. 발생빈도 산정 예시

■ 발생빈도는 위협과 취약성의 곱으로 산정

[표 11] 발생빈도 산정 예시 표

발생 빈도	사이버 공격 시나리오	점수 기준 (X = 위협x취약성)
5	해당 작업을 수행할 때 자주 발생	21 ≤ X ≤ 25
4	자사 내에서 가끔 발생, 보통 장비 문제 또는 승선 중 종종 일어나는 인적 실수로 인한 경우	16 ≤ X ≤ 20
3	자사 내에서 발생한 적 있는 사건, 보통 장비 결함이나 인적 실수로 인한 경우	11 ≤ X ≤ 15
2	업계에서는 들어본 적 있지만, 극히 드물고 불운한 사건들이 연쇄적으로 일어났을 때 발생	6 ≤ X ≤ 10
1	업계에서 들어본 적도 없는 사건, 상상할 수 없을 정도로 드문 수준	1 ≤ X ≤ 5

■ 회사의 SMS(안전관리시스템)에는 일반적으로 리스크 평가 매트릭스가 포함되어 있으며, 특정 사건이 발생할 발생빈도는 5단계 척도로 측정

■ SMS(안전관리시스템)에서 이미 사용 중인 발생빈도 척도를 사용하는 것은 사이버 관련 리스크를 설명하는 데 친숙한 언어와 개념을 사용할 수 있다는 점에서 강점

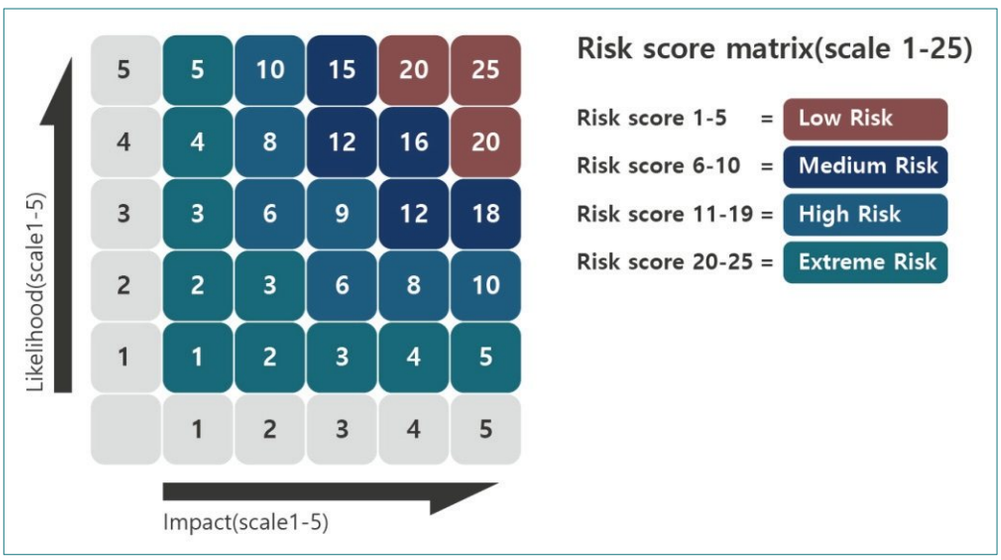
비고	

통제항목	C.2.3 사이버 리스크 평가	Basic
점검목적	선박 IT·OT 자산에 대한 사이버 리스크를 체계적으로 식별·평가하여, 조직적 관리와 보호 조치를 확보합니다.	
점검내용	자산 식별 및 문서화, 위협·취약점 파악, 리스크 평가·처리, 제3자 검토, 문서화 및 지속적 개선 여부를 확인 합니다. 리스크 평가는 일회성이 아닌 1년주기로 갱신해야 합니다.	
점검기준	**양호 :** 연 1회 이상 리스크 평가를 수행하는 경우 **취약 :** 연 1회 이상 리스크 평가를 수행하지 않는 경우	
레퍼런스	[IMO 3.5.2 식별] [IMO 3.5.2.3 식별] [BIMCO 1.1 해운 산업의 사이버보안 특성] [BIMCO 1.4 IT와 OT 시스템의 차이점] [BIMCO 6.1 리스크에 영향을 미치는 요소 간의 관계] [BIMCO 6.2 리스크 평가의 네 가지 단계] [BIMCO 6.3 제3자 리스크 평가] [DCSA 1.4.2 설명] [DCSA 1.4.3 구현] [DCSA 1.4.4 문서화] [DCSA 1.4.5 정보 보안 리스크 평가 예시] [DCSA 1.4.6 처리 과정] [DCSA 1.4.7 리스크 조치 방법]	
증적자료	리스크 평가 보고서	
조치방법	**1. 리스크 평가** ■ 리스크 평가 주기 • 정기 평가: 연 1회 • 수시 재평가: - 주요 시스템·네트워크의 주요 변경이 있을 때 수행 - 사이버보안 사고 발생 후 즉시 수행 ■ 리스크 평가 순서: 1. 사전 평가 활동 2. 선박 평가 3. 보고 및 브리핑 4. 제조사 브리핑 ■ 리스크 평가를 수행하기 위한 프로세스, 인력, 도구, 시간 확인 ■ 내부·외부 위협 목록, 공급업체 보안보고, 과거 사고 기록 수집 ■ 리스크 평가를 위한 문서: • 회사 보안 정책 • 자산 목록 - 영향도, 취약성 포함 없을 시 산정 필요 • 위협 식별 목록 • 발생 빈도 산정 목록	

통제항목	C.2.3 사이버 리스크 평가	Basic

■ 리스크 = 영향도 × 발생빈도(위협 x 취약성)로 리스크 평가
(C.2.1사이버 영향도 평가, C.2.2사이버 발생빈도 평가 참조)

• 리스크 점수 측정 예시



[그림 55] 리스크 점수 측정 예시

■ 리스크 산정 예시:

• 발생빈도: 선원이 외부에서 가져온 USB를 자주 사용함(발생빈도 5)
영향도: 항해 시스템이 감염되면 운항에 큰 차질 발생(영향도 5)
리스크: 5(발생빈도) x 5(영향도) = 25 =〉 매우 높은 리스크(Extreme Risk)

■ 리스크 조치 기간:

• Extreme Risk: 즉시 조치 필요
• High Risk: 한 달 이내 조치 필요
• Medium Risk: 세 달 이내 조치 필요
• Low Risk: 1년 이내 조치 필요

2. 보고 및 문서화

■ 자산 목록, 위협/취약점, 영향 평가를 포함하여 리스크 평가를 문서화 및 보고 필요

통제항목	C.2.3 사이버 리스크 평가	Basic

3. 리스크 완화 및 보호 조치

- 리스크 처리 전략(수용, 회피, 완화, 이전)을 상황에 맞게 선택

[표 12] 리스크 평가 및 완화 조치 식별 예시

시스템	영향	발생 빈도	초기 리스크	완화 조치	잔존 리스크
ECDIS	점수 5, 좌초 및 충돌과 같은 치명적인 사고의 리스크	점수 4	리스크 = 5X4=20	비밀번호 보호 및 ECDIS 전용으로만 PC 사용 제한	리스크=5X3=15
				관리 네트워크 연결 차단	리스크=5X2=10
				USB 포트 물리적 차단	리스크=5X1=5

4. 리스크 평가시 고려사항

- 내부 역량 보완을 위한 외부 전문가/제3자 참여 권장
- 리스크 관리 프로그램은 단순하지 않아 고위 경영진의 지속적인 참여 필요
- 리스크 관리의 범위·메트릭·거버넌스를 먼저 정의하고, 책임자 및 역할 지정
- 비용, 효율성, 현실성을 고려하여 절차적·기술적 통제 적용

비고	

C.3 사이버 리스크 조치 계획

통제항목	C.3.1 사이버 리스크 조치계획	Basic
점검목적	조직 내 사이버 리스크 관리 체계가 이해관계자 중심으로 사이버 리스크를 적절히 식별, 분석, 평가 및 통제하며, 선박 운영의 사이버 회복력을 확보하도록 지원하는지 확인합니다.	
점검내용	고위 경영진이 사이버 리스크에 대한 인식과 교육을 꾸준히 수행하며, 조직 전체에 효과적인 리스크 관리 체계가 잘 운영되고 있는지 점검합니다. 선박 시스템에는 사이버 회복력을 갖춘 보안 기능이 적용되고, 문서 보호와 사고 대응 절차가 체계적으로 이행되는지 확인합니다. 아울러 다중 보호 계층과 통합된 보안 조치가 적절히 시행되어 전반적인 리스크가 최소화되고 있는지도 평가합니다.	
점검기준	**양호 :** 리스크 관리 체계가 이행되어 리스크 감소가 이루어질 경우 **취약 :** 리스크 관리 체계가 미흡하여 리스크 감소가 이루어지지 않을 경우	
레퍼런스	[IMO 3 사이버 리스크 관리 요소] [OCIMF SIRE 2.0 7.5 사이버보안] [BIMCO 7.1 심층 방어와 광역 방어] [BIMCO 7.2 기술적 보호 조치] [BIMCO 7.3 절차적 보호 조치] [DCSA 1.4.3 구현] [DCSA 4.4.2 설명] [DCSA 4.4.3 구현-인적요소] [DCSA 4.4.3 구현-물리적] [DCSA 4.4.3 구현-절차] [DCSA 4.4.3 구현-기술 I] [DCSA 4.4.3 구현-기술 II]	
증적자료	사이버 리스크 처리 계획서	
조치방법	**1. 리스크 조치 계획 및 일정 수립** ■ 리스크 식별 후 완화 조치 후보 검토 및 문서화 ■ 조치 계획에 실행 방식, 소요 비용, 필요한 자원 상세 포함 ■ 리스크 소유자의 승인과 효과성 모니터링, 절차 개선 지속 수행 ■ 조치 일정 수립: • 조치 완료 목표일 및 단계별 일정 설정 • 긴급 조치(즉각 대응)와 장기 개선 조치(중장기 계획)로 구분	

통제항목	C.3.1 사이버 리스크 조치계획	Basic

부서명		리스크 조치 계획서	실행부서 (작성부서)	작성	검토	승인
작성일시			확인부서 (주관부서)	작성	검토	승인
작성자						

리스크 내용	코드 번호	개선대책	개선대책의 실시			확인일자	비고
			조치결과	일정	담당자		

[그림 56] 리스크 조치 계획서 예시

2. 주요 사이버보안 통제

- 사람(교육), 절차(정책), 기술(방화벽·백신)을 함께 적용해 사고를 신속하게 발견하여, 기밀성, 무결성, 가용성 보호
- SSP(선박보안계획서)에 포함할 요소:
  - 물리적 보안, 네트워크 분리, 침입 탐지, 방화벽, 정기 취약점 점검, 허용된 소프트웨어만 실행, 사용자 권한·비밀번호·USB 관리
- 내부 위협 대비:
  - 내부자의 실수나 악의적 행위까지 고려

3. 인적 요소 관리

- 책임자(선박 사이버보안 책임자, IT 운영 관리자)지정
- 선박 데이터 및 시스템 접근 대상, 범위, 방법 명시
- 원격 접근 필요 여부 및 통제 권한 설계
- 선장과 선원들이 사이버보안 리스크 관리 절차에 친숙한지 확인
- 계약직, 임시직, 파견직 포함 모든 직원 대상 입사 시 사이버보안 교육 시행
- 보안 위협 및 변화에 대한 정기 브리핑 실시
- 중요 직무자의 보안 검증 및 지속적 모니터링 수행
- 주요 직무자(IT 운영 관리자, 보안 담당, 정보관리, 구매, 인사 등) 예시 제공

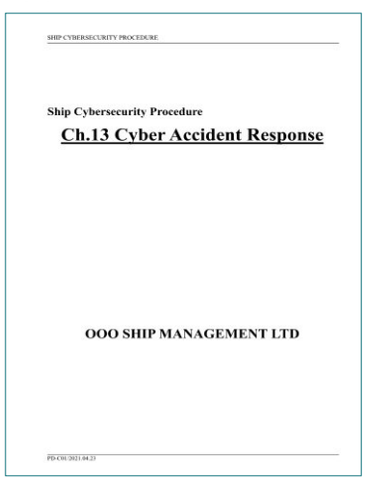
통제항목	C.3.1 사이버 리스크 조치계획	Basic
	4. 물리적 보안 조치 ■ 무단 접근 방지: IT 장비, 제어 및 보안 시스템, 안전 필수 기능 시스템 포함 ■ 장비 도난·손상 방지: 저장매체, 케이블, 데이터 포함 ■ 네트워크 및 통신 인프라 보호: 고의적·우발적 손상, 변조, 서비스 거부 방지 ■ 보안 경계 설정, 경보 시스템과 CCTV 설치, 심층 방어 적용 **5. 기술적 완화 조치** ■ 시스템 보안 및 성능 유지 위한 엔지니어링 및 공급업체 협력: • 공급업체와 정기 보안 패치 일정 협의 • 장비 교체/펌웨어 업그레이드 시 제조사 가이드 준수 ■ IT 제어 및 보안 시스템 손상 방지를 위한 보호 조치: • 핵심 CBS(컴퓨터기반시스템)에 접근제어(계정 최소 권한) 적용 • 관리자 로그 실시간 모니터링 ■ 보안 시스템 분리 인프라 운영 권고: • OT시스템과 IT시스템 간 트래픽 최소화 • 선원 WiFi와 운항 장비 네트워크 완전 분리 ■ 데이터 저장·사용·전송 시 암호화 적용: • 데이터 저장: 장비 로그 및 기밀 파일을 암호화 저장 • 데이터 사용: 선박 관리 시스템 로그인 시 MFA(다중인증) 적용 • 데이터 전송: 선박-육상 간 통신 시 VPN(가상사설망), TLS(전송 계층 보안)적용 ■ GNSS 장애/사이버 사고 대응 조치(GNSS 신호가 위·변조(Jamming, Spoofing)되거나 상실될 경우): • 대체 항법 수단 사용: - 레이더/ARPA로 인접 지형, 선박과의 상대 위치 확인 - 자이로·마그네틱 나침반 활용 - Dead Reckoning(추측항법): 속력계, 침로 기록으로 추적 • 중복 장비 확인: - GPS 외 GLONASS, Galileo, BeiDou 등 다중 GNSS 수신 장치 활용 - 신호 무결성 점검 (RAIM, SBAS 등) • 사이버보안 점검 - 항해장비 콘솔 및 네트워크 포트 점검 - 불필요한 연결 차단, 의심 파일/USB 사용 금지 ■ GMDSS 장애/사이버 사고 대응 조치(GMDSS 통신 장비가 마비되거나 해킹된 경우): • 대체 통신 수단 확보: - MF/HF 무선, 위성통신(Inmarsat-C, Iridium) 등 다른 GMDSS 서브시스템 활용 - VHF 채널 16(긴급 호출 채널)로 비상통신 시도 • 육상 연계 - 인근 선박 또는 RCC(Rescue Coordination Center)에 도움 요청 • 사이버보안 점검 - GMDSS 장비는 보통 전용망이지만, IT 네트워크 연결 여부 확인	

통제항목	C.3.1 사이버 리스크 조치계획	Basic
	- 장비 리부팅/분리 후 정상 작동 여부 점검 [그림 57] VHF 채널 16 이미지 **6. 데이터 삭제 및 장비 폐기** ■ 폐기 장비 내 상업적·기밀 데이터 완전 삭제 절차 마련: • 폐기 전 하드디스크, SSD 등 저장매체를 전문 소프트웨어(예: Blancco 등)로 완전 삭제 ■ 탈자 장비 등 제조사 지침에 따른 데이터 복구 불가능한 삭제 시행 **7. 운영 관리 및 절차** ■ 조직별 특성 반영한 정책 수립 유지: • 각 부서 특성에 맞는 데이터 관리, 장비 폐기 정책 작성 ■ 정책 무시·비공식 관행 방지 위한 교육 및 지속적 관리: • 정책 준수 강조를 위한 정기 교육, 점검 시행	
비고		

D. 사이버 사고 대응

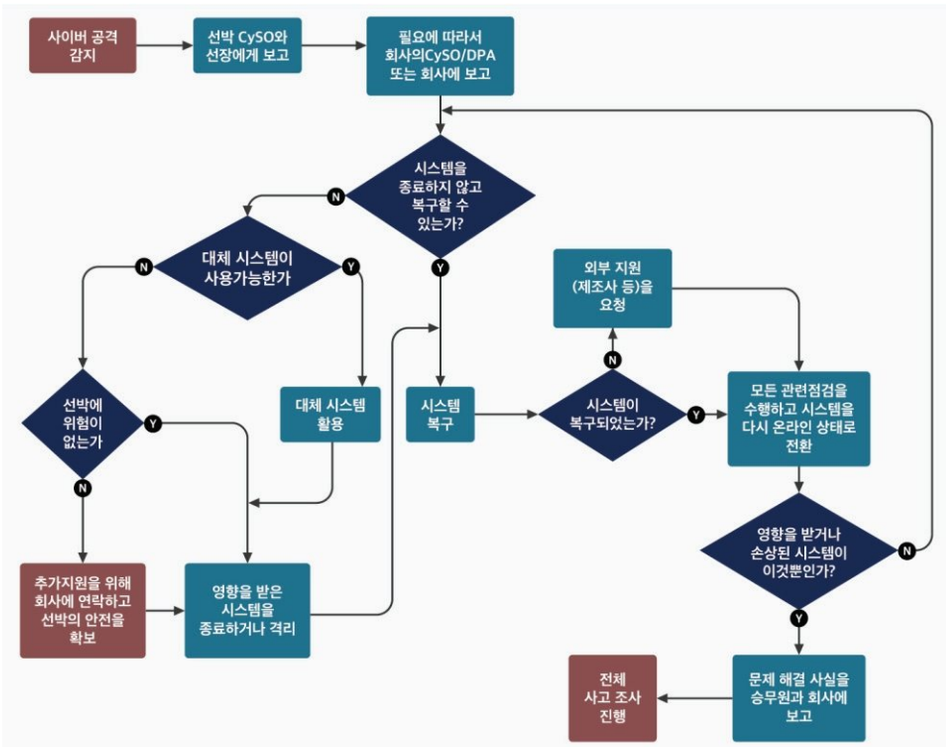
D.2 사이버 사고 대응 계획

통제항목	D.2.1 사이버 사고 대응 절차	Basic
점검목적	사이버 사고 발생 시 선박의 핵심 시스템과 승무원, 자산을 보호하고, 사고를 신속히 탐지·보고하며, 효과적인 대응 절차를 통해 선박 안전과 운영 연속성을 보장합니다.	
점검내용	사이버 사고 대응 조직과 계획, 감지·통지·격리·복구 절차, 커뮤니케이션 및 협력 체계, 네트워크 격리와 최소 리스크 상태 전환 능력 등을 종합적으로 확인합니다.	
점검기준	**양호 :** 사고 대응 절차가 수립되어 있는 경우 **취약 :** 사고 대응 절차가 수립되어 있지 않은 경우	
레퍼런스	[IMO 3.5.3 보호] [IMO 3.5.5 대응] [IMO 3.5.5.1 대응] [IMO 3.5.5.2 대응] [UR E26 4.4 대응] [UR E26 4.4.1.1 요구사항] [UR E26 4.4.1.2 근거] [UR E26 4.4.1.3 세부 요구사항] [UR E26 4.4.3.1 요구사항] [UR E26 4.4.3.2 근거] [UR E26 4.4.3.3 세부 요구사항] [UR E26 4.4.4.1 요구사항] [UR E26 4.4.4.2 근거] [UR E26 4.4.4.3 세부 요구사항] [OCIMF SIRE 2.0 7.5 사이버보안] [BIMCO 9 비상 계획 수립] [BIMCO 10.1 효과적인 대응] [BIMCO 10.2 사고 대응의 네 가지 단계] [BIMCO 10.5 사이버 사고 조사] [BIMCO 10.7 사이버 사고 보고] [DCSA 2.4.3 구현] [DCSA 3.3.3 구현] [DCSA 4.1.2 설명] [DCSA 4.1.3 구현] [DCSA 4.1.4 선박 내 사고 대응을 위한 주요 권고사항] [DCSA 4.1.5 사고 대응 프로세스의 예시와 해당 단계들] [DCSA 4.1.6 사고 확대를 영향 수준 표 예시에 연결하는 사고] [DCSA 4.2.3 구현] [DCSA 4.3.2 설명] [DCSA 5.1.3 구현]	
증적자료	사이버 사고 대응 계획서	

통제항목	D.2.1 사이버 사고 대응 절차	Basic
조치방법	**1. 사고 대응 조직 및 책임 체계** ■ 사이버보안 책임자 지정 및 전담 사고 대응팀 구성: • 선박별 CySO(Cyber Security Officer) 지정 (A.2.1 사이버보안 조직) • 사고 전담 대응팀: IT/OT 담당자 + 선장 + 외부 기술 지원 포함 ■ 선박 내외부 이해관계자 및 서비스 제공자와의 긴밀한 협조 체계 마련 **2. 사고 대응 역할** ■ 선내 CySO/선장: 최초 인지·선내 지휘, 즉시 격리 조치 승인/지시, SBAR로 본사 보고 필요 ■ CCSO(본사): 사건 등급 결정, 대응전략 수립·승인, 외부 통지 판단, 복구·재가동 승인, 사후 개선 총괄 ■ DPA(육상 지정 담당자): ISM/SMS(안전관리시스템) 준수 관점의 조정·기록·대외 커뮤니케이션 지원(규정·안전 연계) ■ IT/OT 기술팀(내·외부): 포렌식/격리/패치/복구 실행, OT 영향평가 **3. 사고 대응 계획 수립 및 문서화**  SHIP CYBERSECURITY PROCEDURE Ship Cybersecurity Procedure Ch.13 Cyber Accident Response OOO SHIP MANAGEMENT LTD PD-C01(2021.04.23) [그림 58] 사고 대응 계획서 ■ 사고 대응 절차 하드카피 형태로 문서화 필요 • 사이버 비상 대응 계획서 (ECDIS, GNSS, GMDSS, 추진, 조타 장비 등)의 하드카피 ■ 사고 대응 절차: • 감지, 대응, 확산 제한, 복구 ■ 선박 내 IT·OT 시스템에 영향을 미친 사이버 사고의 원인과 취약점 악용 방식 파악 ■ 사고 시 디지털 증거 수집, 디스크 이미지 확보: • 조사팀 공유 ■ 사고 발생 시 관계당국에 신속히 통지하고, 사고 증거를 체계적으로 수집·보고 ■ 증거 보존 체계(Chain of Custody)를 준수하여, 디지털 증거의 변조 여부를 입증하고 법적 효력 확보 필요 ■ 격리 지점 설정, 시스템 최소 리스크 상태 전환 계획 포함	

통제항목	D.2.1 사이버 사고 대응 절차	Basic

■ 사고 대응 계획은 인쇄본으로도 보관하여 전자 접근이 불가한 상황 대비



[그림 59] 사이버 공격 대응 흐름도

4. 커뮤니케이션 전달

■ 내부: 보안 책임자, 기술 담당자, 전체 보안팀 간 정보 공유·연락망 유지

■ 외부: 선급, 공급망 관계자, 관련 기관과 연락망 유지

■ 긴급 상황 시 명확하고 일관된 정보 전달을 위한 SBAR 프로토콜 채택

■ SBAR 프로토콜:

- S – Situation(상황): 지금 발생한 문제를 간단·명확하게 설명
- B – Background(배경): 관련된 배경 정보, 시스템 상태, 최근 작업 내역 등
- A – Assessment(평가): 현재 상황에 대한 본인의 판단·분석
- R – Recommendation(권고/요청): 앞으로 취해야 할 조치나 필요한 지원 요청

■ 사고 관련 커뮤니케이션 계획서에 시점, 일정, 대체 수단 명시

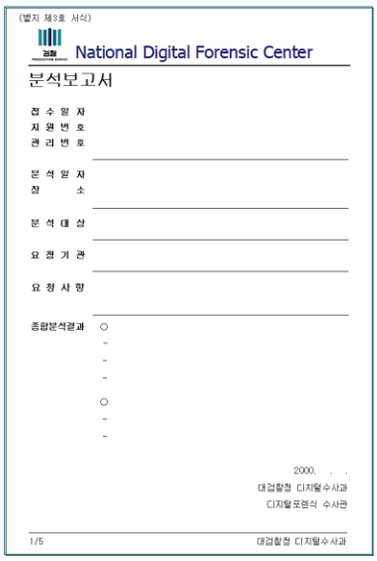
5. 사고 대응 및 복구 절차

■ 사고 원인 분석 → 포렌식 자료 확보 → 법집행기관 협력

■ 사고 확산 방지 위한 물리적·논리적 격리 및 네트워크 분리

■ 최소 리스크 상태 전환 → 비즈니스 연속성 보장

■ 사고 기록 유지 → 후속 대응 모니터링

통제항목	D.2.1 사이버 사고 대응 절차	Basic
	 (별지 제8호 서식) National Digital Forensic Center 분석보고서 접수일자 지원번호 관리번호 분석일자 장소 분석대상 요청기관 요청사항 종합분석결과 ○ - - - ○ - - 2000. . . 대검찰청 디지털수사과 디지털포렌식 수사관 1/5 대검찰청 디지털수사과 [그림 60] 포렌식 분석보고서 **6. 사이버보안사고 연락망** ■ 해양경찰청(https://www.kcg.go.kr/) 신고번호: 122 ■ 해양수산부(https://www.mof.go.kr/) 신고번호: 119 ■ 경찰청(https://www.police.go.kr/) 신고번호: 112 ■ 한국인터넷진흥원(https://www.kisa.or.kr/) 신고번호: 118	
비고		

D.3 사이버 복구 계획

통제항목	D.3.2 사이버 복구 계획	Basic
점검목적	사이버 복구 계획을 구축합니다. 복구테스트를 실행하여 실제 사고 발생 시 핵심 시스템과 데이터를 신속하고 안전하게 복원하여 선박의 항해·운항 연속성을 확보하고, 업무 중단과 피해를 최소화하는 효과를 기대합니다.	
점검내용	사이버 복구 계획이 수립·관리 되어 있으며, 복구 목표에 시간과 시점을 명시하였는지 백업 매체를 통해 복구테스트를 수행한 내용이 있는지 확인합니다.	
점검기준	**양호 :** 필수 시스템에 대한 사이버 복구 계획이 관리되고 있는 경우 **취약 :** 필수 시스템에 대한 사이버 복구 계획이 관리되고 있지 않는 경우	
레퍼런스	[IMO 3.5.6 복구] [IMO 3.5.6.1 복구] [IMO 3.5.6.3 복구] [UR E26 4.5 복구] [UR E26 4.5.1.1 요구사항] [UR E26 4.5.1.2 근거] [UR E26 4.5.1.3 세부 요구사항] [UR E26 4.5.2.3.1 복원 기능] [UR E26 4.5.3.1 요구사항] [UR E26 4.5.3.2 근거] [UR E26 4.5.3.3 세부 요구사항] [OCIMF SIRE 2.0 7.5 사이버보안] [BIMCO 10.2 사고 대응의 네 가지 단계] [DCSA 5.1.2 설명]	
증적자료	사이버 복구 계획서 (Cyber Recovery Plan Document)	
조치방법	**※ 기존 복구 계획에 사이버 사고 복구 계획이 포함되어야 합니다.** **1. 사이버 복구 계획 수립 및 관리** ■ 선주의 책임 • 복구 계획 수립, 복구 수단 및 담당자 지정 - 선박 내 IT/OT 관리자: 1차 현장 복구 조치, 로그 확보 - 선장: 최종 승인 및 복구 지시, 안전성 판단 - 사이버 대응팀(CSOC/IT팀): 원격 지원, 백업 복구 실행, 공급망 협력 - 외부 전문업체/제조사: 특수 시스템(항해 장치, 기관 제어 등) 복구 지원 ■ 복구 계획 문서화 • 선박 내외부에서 하드카피(종이 문서처럼 물리적이고 영구적으로 보존될 수 있는 형태의 정보) 형태로 보관 • 선내·육상 양측에 인쇄본 및 전자본 보관하여 접근성 확보 • 관련 인원(승무원·외부 지원팀)이 쉽게 이해할 수 있도록 작성	

통제항목	D.3.2 사이버 복구 계획	Basic

■ 복구 목표 정의

- 각 시스템 및 하위 시스템별 목표 복구 시간(RTO: Recovery Time Objective)와 목표 복구 시점(RPO: Recovery Point Objective) 명시
- OT 시스템의 안전 운항 데이터에 짧은 RPO 설정 (예: 실시간/1시간 이내)
- 우선순위에 따른 통신/업무 시스템의 RTO 차등 설정

[표 13] 시스템 복구 목표 설정 예시

구분	영향도	긴급도	RTO*
복구 1순위	■ 전체 조직과 관련된 중요한 업무 프로세스에 심각한 영향 ■ 선박 운항 및 화물 운송에 중요한 업무 프로세스에 심각한 영향	즉각적 해결	최대 12시간 이내
복구 2순위	■ 중요한 업무 프로세스의 부분적으로 심각한 영향 ■ 선박 운항 및 화물 운송 업무의 부분적으로 심각한 영향	가능한 신속한 해결	최대 3일 이내
복구 3순위	■ 전체 조직 운영에 미미한 영향 ■ 선박 운항과 무관한 영향	어느 정도 대응시간을 가지고 해결	최대 30일 이내

※ RTO(Recovery Time Objective)에 필요한 시간은 회사가 결정
출처: 한국선급. 'KR Maritime Cyber Safety News from KOREAN REGISTER Feb 2022'

■ 복구 계획에 포함되야 되는 정보

- 고장난 시스템 복구 지침 및 절차
- 백업 및 안전 저장 절차
- 최신 상태의 논리적 네트워크 다이어그램
- 시스템 복구 담당 인원 및 외부 지원 연락망(벤더, 네트워크 관리자 등)
- 모든 구성요소의 현재 설정 정보
- 복구 대상:
  - 핵심 OT 시스템: 항해 장치, 기관 제어 시스템, 통신 장비
  - IT 시스템: 이메일, ERP, 선박 관리 시스템, 파일 서버
  - 지원 시스템: CCTV, 보조 모니터링 장비
  - 데이터: 운항 데이터, 화물 데이터, 승무원 기록
- 복구 예외:
  - 포렌식 자료: 증거 보존 목적으로 바로 복구/삭제하지 않고 보관
  - 의심 장비/파일: 악성코드 감염 흔적이 있는 경우 복구 제외 후 분석

통제항목	D.3.2 사이버 복구 계획	Basic

사이버보안 복구 계획서

1. 목적 및 범위

당사의 핵심 정보시스템과 선박 운영 네트워크에서 발생 가능한 랜섬웨어, 데이터 유출, 서비스 거부 공격 등 사이버사고에 대응하여 중요 업무를 신속히 복구하고 피해를 최소화하기 위한 계획이다.

적용 대상: 선박 운영 네트워크, 선박-육상 통신 시스템, 중요 데이터 저장소 및 백업 시스템.

2. 조직 및 책임

복구 총괄 책임자: 복구 계획 발동 승인·지휘

기술 담당: 사고 격리·복원·증거 보전

커뮤니케이션 담당: 내부·외부 보고 및 대외 공지

외부 지원: 포렌식·법률·규제 대응

3. 중요 자산 및 복구 목표

중요 자산: 선박 운항 제어시스템, 중앙 데이터베이스, 원격 접속 서버

RTO: 8시간 이내 복구

RPO: 1시간 이내 데이터 손실 허용

4. 복구 절차

사고 확인 → 2) 격리·제어 → 3) 시스템·데이터 복원 → 4) 서비스 정상화

5. 백업 및 데이터 복원

백업 주기: 매일 증분, 주 1회 전체

보관 위치: 오프사이트 및 오프라인 저장 이중화

복원 방법: 마지막 정상 상태 백업 사용, 해시값으로 무결성 검증

6. 커뮤니케이션

내부 보고: 사고 인지 즉시 총괄 및 경영진 보고

외부 통보: 규제기관·고객·협력사 24시간 이내 통지

대언론 발표: 필요 시 공식 대변인 발표

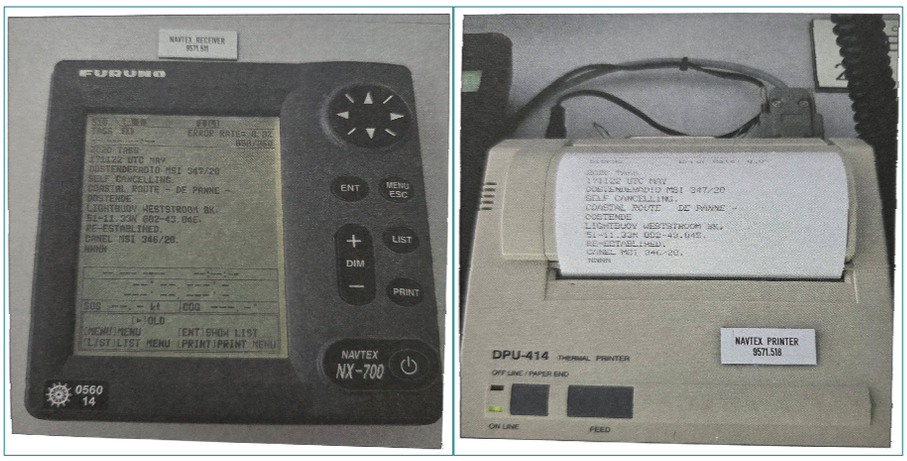
7. 사후 점검 및 개선

계획은 연 1회 이상 또는 주요 사고 후 즉시 갱신

[그림 61] 사이버 복구 계획서 예시

통제항목	D.3.2 사이버 복구 계획	Basic
	2. 데이터 백업 체계 및 복구 테스트 진행 ■ CBS(컴퓨터기반시스템)의 백업 및 복원 기능 확보 • 복사본 또는 이미지 파일로부터 데이터 복원 • 백업 자료는 안전한 저장소(선상, 육상)에서 관리 ■ 주요 IT/OT 시스템의 정기적 백업 스캐줄 수립 ■ 백업 매체의 암호화, 물리적 보관 및 무결성 검증 수행 ■ 백업 실효성 확인을 위한 복구 테스트 진행 • 연 1회 이상 복구 훈련을 통해 복구 가능성 검증 • 실제 백업으로부터 복구 테스트 진행 • 테스트 진행 시 실제 운항에 영향을 주지 않도록 주의 필요 • 복구 완료 후 시스템 정상 동작하는지, 데이터의 유실은 없는지 확인 • 복구 계획상 부족한 부분은 복구 계획서에 반영 **3. 복구 절차 및 실행 지침** ■ CBS(컴퓨터기반시스템) 및 네트워크 복구 기능 확보 • 정상종료 (Controlled Shutdown) - 연결된 시스템들이 보유중인 트렌잭션 완료 및 롤백 - 프로세스 및 연결 종료 • 초기 상태로의 재설정 (Reset to an Initial State) - 공장 초기화 (Factory Reset) - OS 재설치 - 제조사 제공 리커버리 이미지 적용 - 장치 초기화 • 안전한 상태로의 롤백 (Roll-back to a Safe State) • 전원 차단 후 재시작 (Restart from a Power-off Condition) **4. ECDIS 복구 절차 및 실행 지침** ■ 최우선적으로 ECDIS 백업 이용한 복구 수행 ■ 대부분의 경우, 소프트웨어는 다음을 포함하여 완전히 재설치 필요: • 운영체제(OS) • ECDIS 소프트웨어, 설정(일관된 공통 기준점(CCRP)) 및 사용 가능한 모든 소프트웨어 업데이트 • ENC(전자해도)와 관련 업데이트 • 항해 계획 ■ 그 후, ECDIS가 정상적으로 작동하는지 정보 확인: • 만약 승무원이 선내에서 ECDIS를 복구할 수 없는 경우, 서비스 엔지니어가 수행 ■ ECDIS장비는 수신된 NAVTEX 메시지를 표시할 수 있으나, 해당 메시지가 실제이며 변조되지 않았음을 확인: • NAVTEX 장비 화면을 직접 확인하거나, NAVTEX 장비에서 출력된 메시지(NMEA 프로토콜을 통해 전송된것)를 확인	

통제항목	D.3.2 사이버 복구 계획	Basic



[그림 62] NAVTEX 장비 메시지 출력

■ 복구 절차의 운영 원칙
- 복구 전 사고 증거(로그, 덤프, 네트워크 트래픽 등) 보존
- 데이터·네트워크 무결성 확보
- 필요 시 외부 대응팀 지원 확보

■ 절차서 기반의 실행 지침 제공

5. 지원체계 및 지속 개선

■ 지원체계
- 외부 벤더 및 네트워크 관리자 연락처 확보
- 최신 네트워크 다이어그램과 설정 정보 정기 업데이트

■ 보고체계
- 선내 보고: 선원 → IT/OT 관리자 → 선장
- 육상 보고: 선장 → 회사 DPA(육상 지정 담당자)
- 외부 보고: 필요 시 선급, 법집행기관, 보험사 통보

■ 지속 개선
- 정기 훈련을 통해 계획 검증 및 업데이트
- 사고 발생 시 RCA(근본 원인 분석) 수행 후 교훈 반영

비고	

4.2 Advanced

A. 사이버보안 관리체계

A.2 사이버보안 조직 및 외부업체 관리

통제항목	A.2.2 사이버보안 외부업체 관리	Advanced
점검목적	외부 서비스 제공업체, 공급업체, 대리점 등과의 계약 및 협력 과정에서 사이버보안 요건이 반영되고 있는지를 확인하여, 외부업체의 보안 취약점이 선사의 IT·OT 시스템으로 전이되는 것을 예방하고, 공급망 전반의 보안 수준을 확보하는 것을 목적으로 합니다. 사고 사례 사고: 선박 대리점과 선주 간 랜섬웨어 사고 한 선박 대리점은 회사의 비즈니스 네트워크가 랜섬웨어에 감염되었으며, 이는 피싱 이메일 첨부파일을 통해 전파된 것으로 보인다고 보고하였습니다. 해당 랜섬웨어는 서로 다른 시점에, 의도치 않게 두 명의 선박 대리점을 통해 유입된 것으로 밝혀졌습니다. 일부 선박도 영향을 받았지만, 피해는 비즈니스 네트워크에 국한되었고 항법 시스템이나 선박 운항은 영향을 받지 않았습니다. 한 건의 사례에서는 선주가 랜섬머니를 지불하기도 했습니다. 이 사건이 주는 중요한 시사점은, 공급망 전체에 걸쳐 신뢰할 수 있는 비즈니스 파트너 및 제조사들과의 관계에서 사이버보안을 조화롭게 구축하는 것이 필수적이라는 점입니다. 개별 조직이 자사를 보호하기 위한 노력을 하는 것은 용기 있고 의도는 좋을 수 있지만, 그것만으로는 부족할 수 있습니다. 공급망 내 모든 당사자가 협력하고 정보를 적절히 공유해야 사이버 리스크를 효과적으로 완화할 수 있습니다.	
점검내용	외부 이해관계자(선주, 선박 관리자, 대리점, 공급업체 등)와의 계약 요건에 사이버 리스크 관련 요구사항이 반영되어 있는지 확인하고, 외부업체의 IT·OT 장비 유지보수 활동이 승인 절차, 데이터 보호, 보안 통제 점검, 기록 관리 절차에 따라 수행되는지 확인합니다.	
점검기준	**양호 :** 작성된 외부 업체 보안 서약서가 있는 경우 **취약 :** 작성된 외부 업체 보안 서약서가 없는 경우	
레퍼런스	[UR E26 4. 요구사항] [BIMCO 1.6 선주와 선박 관리자 간의 관계] [BIMCO 1.7 선주와 선박 대리점 간의 관계] [BIMCO 1.8 공급업체 및 기타 외부 당사자와의 관계]	
증적자료	외부업체/공급망 보안 관리 정책서, 공급업체 및 외부업체 보안 평가 보고서, 외부업체 보안 서약서	
조치방법	**1. 외부업체 계약서 작성 시 포함해야 할 요구사항** ■ 사이버보안 조항 명시 • 공급망 보안 책임 및 역할 분담 명시(데이터 보호, 시스템 무결성 보장) • CBS(컴퓨터기반시스템) 접근 시 보안 요구사항 (MFA(다중인증), VPN(가상사설망), 로깅) • 원격접속 및 유지보수 시 네트워크 분리 원칙 준수 ■ 취약점 관리와 패치 의무 • 주기적인 보안 패치 제공과 취약점 보고 절차 문서화	

통제항목	A.2.2 사이버보안 외부업체 관리	Advanced

■ 교육 및 역량 요구
- 외부업체 인력의 선박 사이버보안 교육 이수

■ 사고 대응 책임
- 사이버 사고 발생 시 즉각 보고 및 공동 대응 의무

■ 데이터 보호 조항
- 계약 종료 후 데이터 폐기/반환 절차 및 기밀 유지 조항 포함

2. 외부업체 및 본사 수행 사항

외부업체 보안 서약서

소 속(업체명)		성 명	
주민등록번호 (앞 7자리)	-	직 위	
연 락 처		출입기간	

상기 본인은 ㅇㅇ사 협력업체 근무자로서 정보 및 지적재산권 보호에 관한 제반 규정(이하 정보보안업무규정)을 충분히 숙지하고 이해하였으며 ㅇㅇ사 정보보안업무규정을 준수할 것을 다음과 같이 서약합니다.

◆ ㅇㅇ사의 정보보안규정과 정책을 반드시 준수하겠습니다.	확인
1. ㅇㅇ사의 업무 수행 중 습득한 업무내용에 대하여는 업무범위 외 사용하거나, ㅇㅇ사의 사전승인 없이는 어떠한 경우에도 외부기관 및 제3자에게 무단공개, 유출하거나 제공하지 않겠습니다.	□
2. ㅇㅇ사의 업무를 위해 사용하는 전사/통신장비 등 모든 설비를 개인 목적으로 사용하지 않을 것이며, 본인이 전산/통신장비(e-mail, 무선 LAN, 위성 통신장비 등)를 통해 발송하는 통신내용을 정보보안 주관부서가 사전, 사후에 검색할 수 있음에 동의합니다.	□
3. 물품, 서류, 카메라, PC 및 주변기기와 저장매체 등의 반/출입과 관련하여 ㅇㅇ사 정보보안규정 및 기타 지침을 준수할 것이며, PC수록자료 확인 등 정보보안 주관부서에서 실시하는 검색에 동의합니다.	□
4. ㅇㅇ사 출입카드 등의 출입증을 본인 외에 제3자에게 빌려주거나 본래의 용도 외 목적으로 사용하지 않겠으며, 업무수행 시 항상 패용하겠습니다. 또한 업무 종료시에는 반드시 ㅇㅇ사에 출입증을 반납하겠습니다.	□
5. 출입제한구역에 관련부서의 승인 없이는 일제 출입을 하지 않겠습니다.	□
6. ㅇㅇ사의 PC 등 정보시스템, 정보통신망, 전사시설 등에 무단 접근하여 시스템을 변경하거나 파괴 또는 정보를 획득하거나, 사외로 유출하는 등의 행위를 하지 않겠습니다.	□

상기 사항을 준수하지 않음으로 인한 ㅇㅇ사에 유형, 무형의 손해를 끼친 경우에는 관련 법 등에 의거 손해배상 등 민사, 형사상의 어떠한 책임도 감수하고 이의를 제기하지

따라서, 본 서약서 내용을 모두 확인하였고 성실히 준수할 것을 동의함 ( )

20 년 월 일

서약인 : (인)

[그림 63] 외부업체 보안 서약서

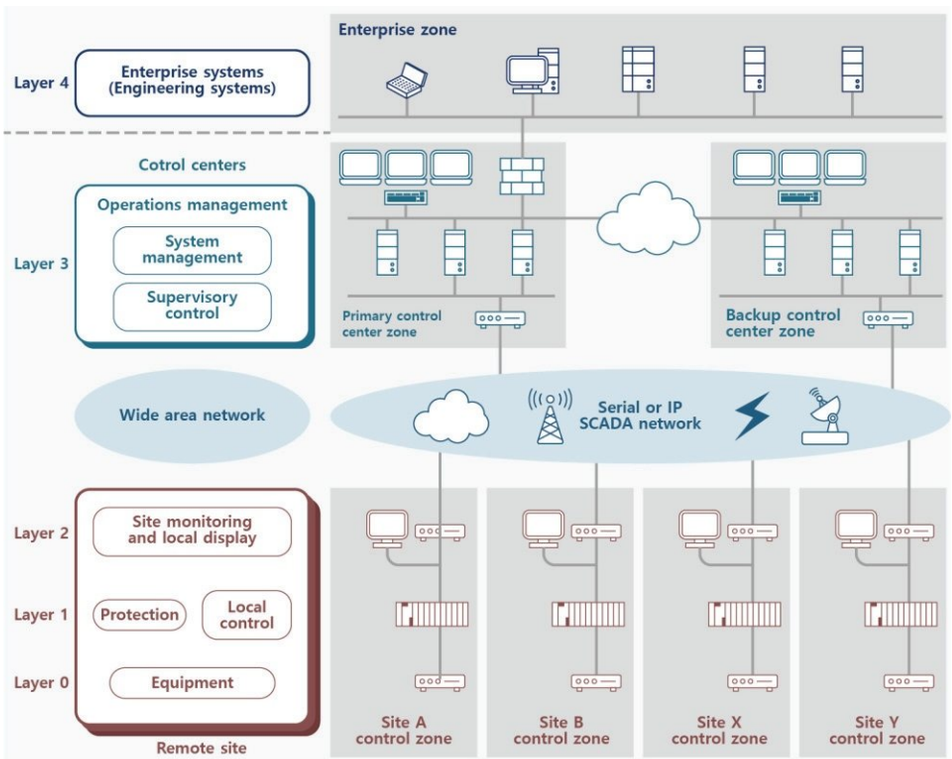
■ 외부업체 수행
- 승선 전 보안 서약서 및 교육 이수 증빙 제출
- 작업 시 사용 장비(노트북, USB 등) 보안 검사 결과(악성코드 스캔 로그) 제출
- CBS(컴퓨터기반시스템)/네트워크 접근 로그 기록(접속 계정, 시간, 목적) 제출
- 원격 유지보수 시 VPN(가상사설망) 접속 기록, MFA(다중인증) 인증 내역 증적 제출
- 취약점 보고서 및 패치 적용 증빙 문서 제출

■ 본사 수행
- 계약서 내 보안 요구사항 이행 여부를 정기 점검
- 외부업체의 접근 승인 절차 기록
- 외부업체 작업 전·후 변경 관리 기록

통제항목	A.2.2 사이버보안 외부업체 관리	Advanced
	• 외부업체 사이버보안 감사 기록 • 외부업체의 사고 대응 훈련 참여 여부 기록 **3. 계약 후 필요사항** ■ 데이터 관리 • 계약 종료 시 외부업체가 보유한 선박 관련 데이터 폐기/반환 증빙(폐기 확인서, 반환 영수증) ■ 정기 감사 및 재평가 • 외부업체 보안 준수 여부를 연간 혹은 주기적 감사 ■ 교육 및 역량 강화 • 외부업체 갱신 계약 시 최신 사이버보안 교육 이수 확인(교육 수료증) ■ 지속적 개선 • 보안 통제 결함 발견 시, 차기 계약에 개선 조항 반영	
비고		

B. 사이버보안 통제

B.1 사이버 자산 관리

통제항목	B.1.2 네트워크 구성도	Advanced
점검목적	선박 내 디지털 자산과 시스템 간 연계성을 명확히 파악하여, 중요 자산 및 서비스가 중단될 경우 미치는 리스크를 최소화 합니다.	
점검내용	네트워크 구성도에 보안 구역별 자산(CBS(컴퓨터기반시스템), 서버, 라우터 등)과 이들의 물리적 위치, 보안 구역 배정, 네트워크 통신 흐름이 도식화되어 있으며, 구성도가 최신 상태로 유지되고 있는지 확인합니다.	
점검기준	**양호** : 네트워크 연결 구성도를 최신 버전으로 관리하고 있을 경우 **취약** : 네트워크 연결 구성도를 최신 버전으로 관리하고 있지 않을 경우	
레퍼런스	[IMO 3.5.2.2 식별] [UR E26 4.1 식별] [UR E26 4.2.1.4.1 보안구역 네트워크 분리/설계] [UR E26 4.4.2.1 요구사항] [UR E26 4.4.2.3 세부 요구사항]	
증적자료	선사/선박별 네트워크 구성도	
조치방법	**1. 네트워크 구성도**  [그림 64] 자산, 서버, PC, 라우터가 포함된 네트워크 구성도	

통제항목	B.1.2 네트워크 구성도	Advanced
	■ 자산 목록을 기반으로 각 보안 구역 내 시스템 명시 • IT, OT 자산 • 서버 • PC • 라우터 • 방화벽 • IDS(침입 탐지 시스템) ■ 각 CBS(컴퓨터기반시스템)를 간략하게 도식화하고, 해당 CBS(컴퓨터기반시스템)가 배정된 보안 구역 명시 ■ CBS(컴퓨터기반시스템)장비의 물리적 위치 기록 ■ 보안 구역 내/외 에서 시스템 간의 네트워크 통신 흐름 도식화	
비고		

통제항목	B.1.3 사이버 자산 변경관리	Advanced
점검목적	선박 및 관련 시스템에서 발생하는 모든 변경 사항에 대해 일관된 방식으로 평가하고 승인·기록함으로써, 변경으로 인한 사이버 보안 위협을 사전에 식별하고, 시스템의 안정성, 보안성 및 운영 연속성을 유지합니다.	
점검내용	자산 목록 변경 시 변경 이력을 기록하고 장비 설치 시 작업내역서를 작성 하고있는지 확인합니다.	
점검기준	**양호 :** 사이버 자산 목록 변경 이력을 기록하는 경우 **취약 :** 사이버 자산 목록 변경 이력을 기록하지 않는 경우	
레퍼런스	[UR E26 4.1.1.3 세부 요구사항] [UR E26 4.1.1.3.1 하드웨어] [UR E26 4.1.1.3.2 소프트웨어] [UR E26 4.1.1.4.4 운영 단계]	
증적자료	자산 목록 변경 이력, 작업내역서	

조치방법

1. 자산 목록 변경관리

■ 자산의 변경·업데이트 사항은 자산 목록에 반영하여 최신화

• 자산 목록에 없는 항목은 기재하지 않거나 비고로 작성

개정 이력

버전	날짜	개정 내용	담당자
0.1	2023-01-01	초기버전 작성	홍길동
1.0	2023-02-01	업데이트 작성	홍길동
2.0	2024-12-01	자산 업데이트	성춘향
2.1	2025-01-01	Zone 업데이트	성춘향

[그림 65] 자산 목록 관리 대장 개정 이력 예시

1. Bridge System

NO	ZONE	CATEGORY	Code	Service	Asset	IP	OS/Ver	Vendor	MODEL	Anti-Virus	Location	담당자	관리자	책임자	C	I	A	자산가치등급	취약점진단	비고
1	OT	선교시스템-레이더	BRS-RAD-001	BAND-RADAR	BAND-RADAR			ORANGE	OR-100			SCSM	SCSM	MASTER	3	5	4	4		
2	OT	선교시스템-ECDIS	BRS-ECD-001	ECDIS	ECDIS			ORANGE	OR-200			SCSM	SCSM	MASTER	3	5	5	4		

[그림 66] 자산 목록 관리 대장 작성 항목 예시

■ 자산 목록의 변경·업데이트 유형 예시

• 자산 코드 변경

• 자산 변경·업데이트

- 자산 추가 설치
- 자산 교체
- 자산 제거·삭제

통제항목	B.1.3 사이버 자산 변경관리	Advanced

- OS·펌웨어·버전 업그레이드
- IP 변경
- 공급업체
  - 공급업체 변경
  - 공급업체명 변경
  - 업체 담당자 변경
- 백신 프로그램 설치·교체·제거
- 물리적 위치 변경
- 담당자, 관리자, 책임자 교체
- 중요도 변경
- 보안등급 변경
- 네트워크 구성도 변경

2. 작업내역서 작성

작업내역서

지원 내역	날짜:	작업자:	전화번호:
	시작 시간:	완료 시간:	
선박 정보	선박:	담당자:	전화번호:

공급업체	제품명	IP 주소	OS버전	일련번호
작업 구분	☑ 장비 설치	☑ 장비 제거	☑ 장비 점검	
작업 내용				
비고				

상기와 같이 작업되었음을 확인합니다.
2025년 1월 1일
결재인 성명 :
처리자 성명 :

[그림 67] 작업내역서 예시

■ 설치 작업 확인
- 제품 설치 위치·일정 확인
- 공급업체명, 작업자, 작업자 연락처 확인
- 제품 설치 진행 확인

통제항목	B.1.3 사이버 자산 변경관리	Advanced
	■ 작업내역서 작성 세부내용 • 작업 날짜, 시작 시간, 완료 시간 • 선박명, 담당자, 담당자 전화번호 • 제품명, IP 주소, OS버전, 일련번호 • 공급업체명, 작업자, 작업자 전화번호 • 작업 구분, 작업 내용 • 책임자, 담당자 서명 ■ 작업 완료 보고 • 작업완료 시 작업내역서 담당자에게 전달 및 완료 보고	
비고		

B.3 네트워크 접근 통제

통제항목	B.3.2 네트워크 접근 통제	Advanced
점검목적	CBS(컴퓨터기반시스템) 및 네트워크 전반에 대해 명확한 접근 통제와 보호 원칙을 적용하여 사이버 사고 리스크를 최소화하고, 무선 및 원격 접속의 보안성을 확보하며, 방문자 및 제3자 접근을 엄격히 통제하여 네트워크의 기밀성, 무결성, 가용성 보호를 강화하는 데 있습니다.	
점검내용	네트워크 접근 권한 정책 수립 및 준수 여부, 최소 기능 원칙 적용과 계층별 네트워크 보호체계, 무선 통신의 암호화 및 인증 현황, 원격접속 통제 정책과 기능(승인, 세션 관리 등) 적용 여부, 네트워크 장비 포트 및 서비스 통제 상태, 방문자와 제3자 네트워크 접근 통제 조치, 위성 통신 보안 대책, 그리고 종합적 접근 통제 정책 및 다층 보호 기능 운용 현황을 확인합니다.	
점검기준	**양호** : 주요 시스템에 대한 네트워크 접근 통제가 이루어지는 경우 **취약** : 주요 시스템에 대한 네트워크 접근 통제가 이루어지지 않는 경우	
레퍼런스	[UR E26 4.2.2.1 요구사항] [UR E26 4.2.2.2 타당성] [UR E26 4.2.2.3 세부 요구사항] [UR E26 4.2.4.1 요구사항] [UR E26 4.2.4.3 세부 요구사항] [UR E26 4.2.5.1 요구사항] [UR E26 4.2.5.3 세부 요구사항] [UR E26 4.2.6.1 요구사항] [UR E26 4.2.6.2 근거] [UR E26 4.2.6.3 세부 요구사항] [UR E26 4.2.6.3.1 설계] [UR E26 4.2.6.3.2 원격 유지보수를 위한 추가 요구사항] [BIMCO 7.2 기술적 보호 조치] [BIMCO 7.3 절차적 보호 조치] [DCSA 2.3.2 설명] [DCSA 2.3.3 구현] [DCSA 2.6.2 설명]	
증적자료	네트워크 접근 통제 정책 문서	
조치방법	**1. 네트워크 접근 통제 대상** ■ CBS(컴퓨터기반시스템) • 항해 시스템 (Navigation CBS, ECDIS, GPS, AIS 등) • 통신 시스템 (GMDSS, 위성통신 장비 등) • 기계/엔진 제어 시스템 (Engine Control, PMS, Propulsion CBS 등) • 화물 관리 시스템 (Cargo Monitoring/Control, Ballast CBS 등) • 보안/안전 관련 CBS (Fire Detection, CCTV, Access Control CBS 등) ■ 네트워크 인프라 • 라우터, 스위치, 방화벽, 보안 게이트웨이 • 무선 AP (WiFi, LTE/5G 장비) • 원격 접속 게이트웨이 (VPN(가상사설망) 장치 등)	

통제항목	B.3.2 네트워크 접근 통제	Advanced

■ 사용자 단말 및 주변기기

- 선박 내 컴퓨터(워크스테이션, 서버 포함)
- 관리자 노트북, 유지보수 장비, USB 등 이동식 매체
- 무선 통신 단말기(스마트폰, 태블릿, 무전기 IP단말 등)

2. 네트워크 접근통제 방안

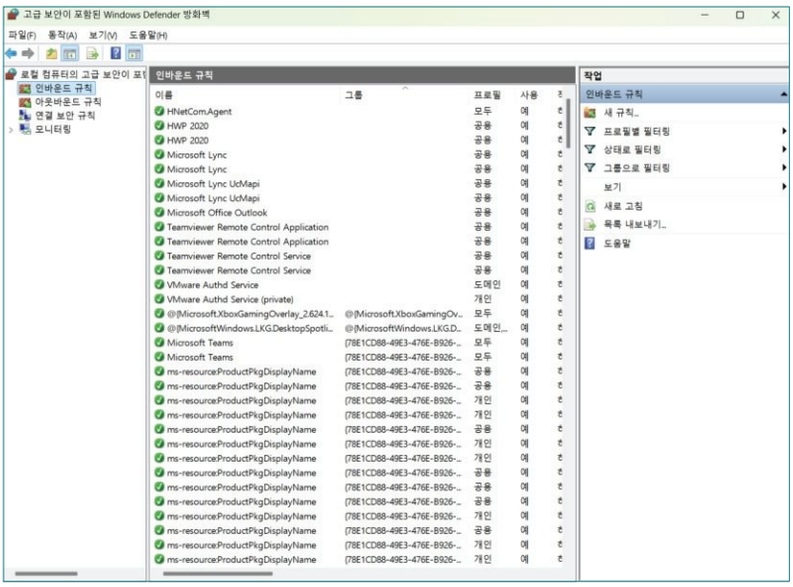
■ 통신 제어

- 방화벽 설정을 통해 네트워크 보호
  - Windows 방화벽 설정(Windows 11): 시작 〉 제어판 〉 시스템 및 보안 〉 Windows Defender 방화벽 〉 설정 사용자 지정 〉 Windows Defender 방화벽 사용

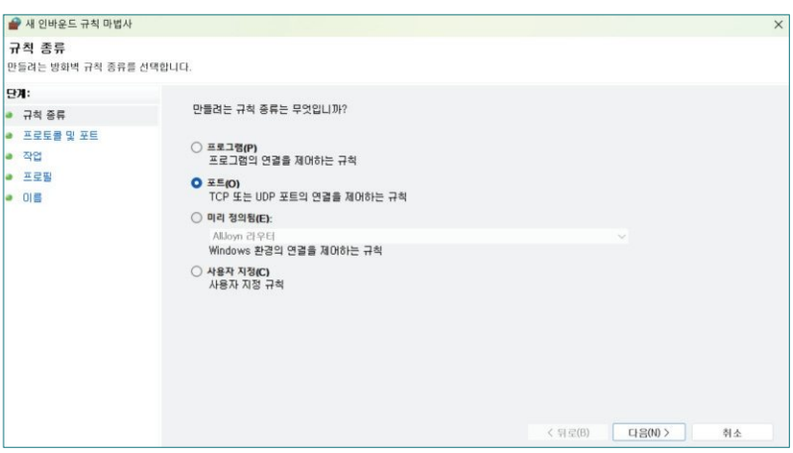
[그림 68] Windows 방화벽 설정

- 방화벽을 통한 화이트리스트 기반 포트/프로토콜 허용(Windows 11)
  - Windows키 + R 〉 wf.msc 입력 〉 왼쪽 메뉴에서 인바운드 규칙 〉 새 규칙 선택〉 포트 선택 〉 TCP/UDP 설정, 특정 로컬 포트 선택 〉 연결허용 선택 〉 규칙 적용 시기 선택 〉 규칙 이름 지정 후 완료

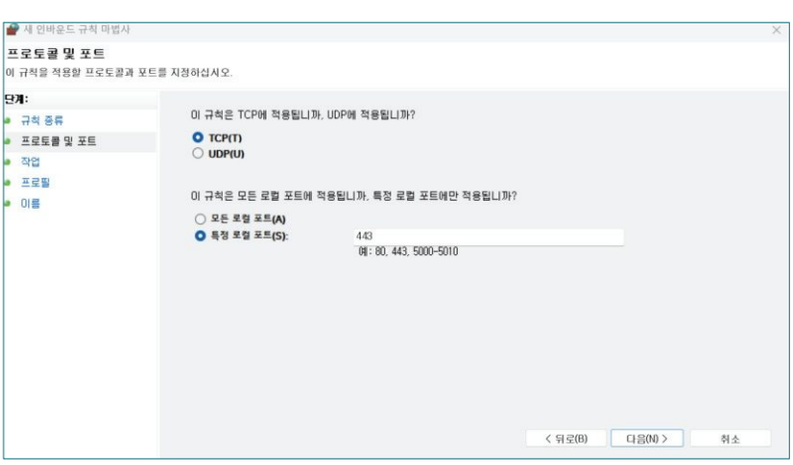
통제항목	B.3.2 네트워크 접근 통제	Advanced



[그림 69] Windows 방화벽 인바운드 규칙



[그림 70] 새 인바운드 규칙 마법사



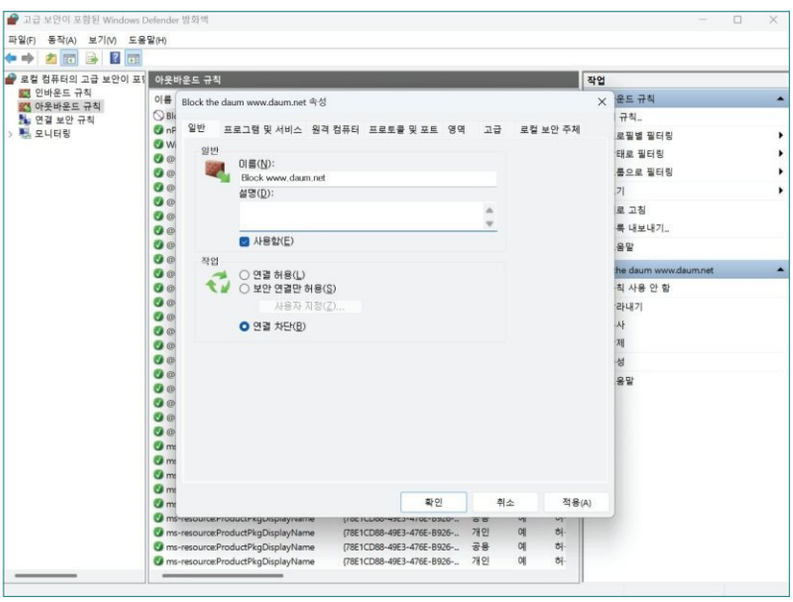
[그림 71] 새 인바운드 규칙 마법사 프로토콜 및 포트 설정

통제항목	B.3.2 네트워크 접근 통제	Advanced

[그림 72] 새 인바운드 규칙 마법사 프로토콜 및 포트 정책 설정

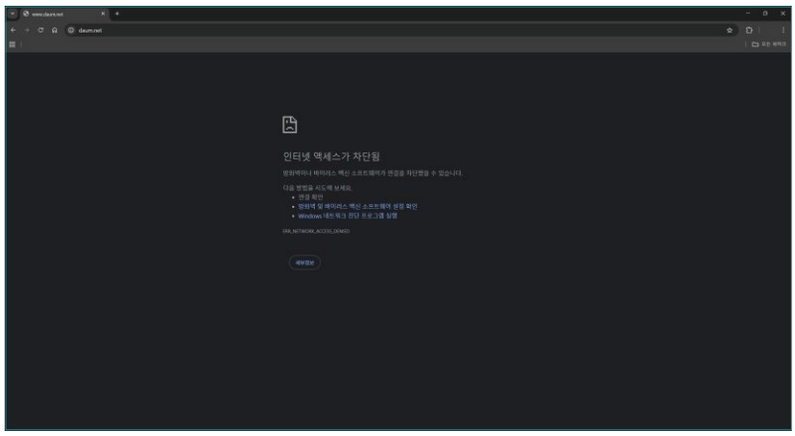
• 방화벽을 통한 사이트 접속 차단(Windows 11)

- Windows키 + R 〉 wf.msc 입력 〉 왼쪽 메뉴에서 아웃바운드 규칙 〉 새 규칙 선택 〉 사용자 지정 선택 〉 모든 프로그램 선택 〉 기본값 그대로 선택 〉 범위: 원격 IP 주소에 nslookup으로 확인한 IP주소 입력 〉 연결 차단 〉 도메인, 개인, 공용 모두 선택 〉 규칙 이름 지정(예: Block 사이트명) 후 완료



[그림 73] 방화벽 아웃바운드 규칙 설정

통제항목	B.3.2 네트워크 접근 통제	Advanced



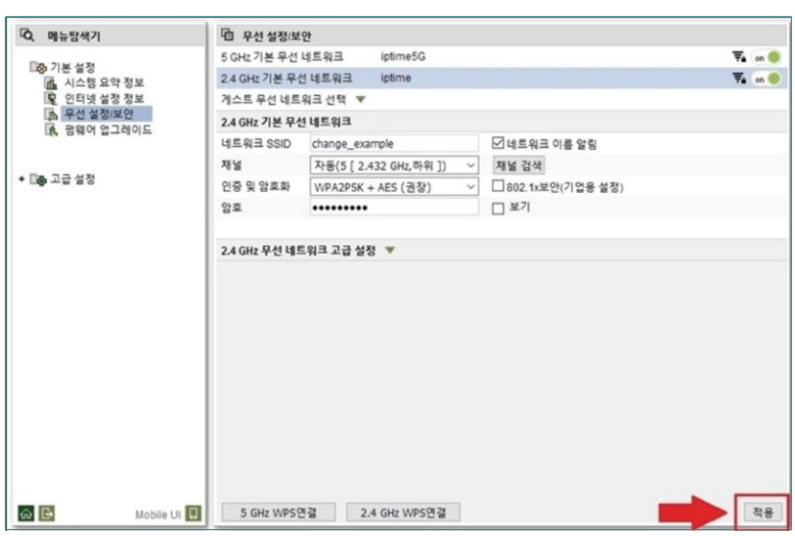
[그림 74] 사이트 접근 차단

- IDS/IPS(침입 탐지 시스템/침입 방지 시스템)를 통해 공격 시도 및 비인가 접근 차단
- NAC 장치를 통해 비인가 기기의 네트워크 연결 차단

■ 인증 및 권한 관리

- 사용자/장치 인증 (계정, MFA(다중 인증), 디지털 인증서 등)
- 최소 권한 원칙(Least Privilege) 적용
  - CBS(컴퓨터기반시스템)는 업무상 필요한 경우에만 접근 허용
  - 사용자, 프로세스, 장치 모두 최소 권한만 부여
  - 네트워크 장비 및 CBS(컴퓨터기반시스템)의 불필요한 포트, 서비스, 프로토콜 비활성화
- 관리자 권한은 별도 관리

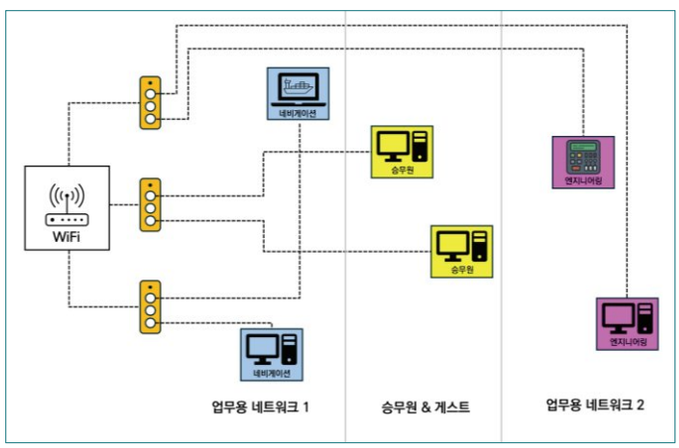
■ WiFi 접근 통제



[그림 75] WiFi 네트워크 보안 설정 예시

통제항목	B.3.2 네트워크 접근 통제	Advanced

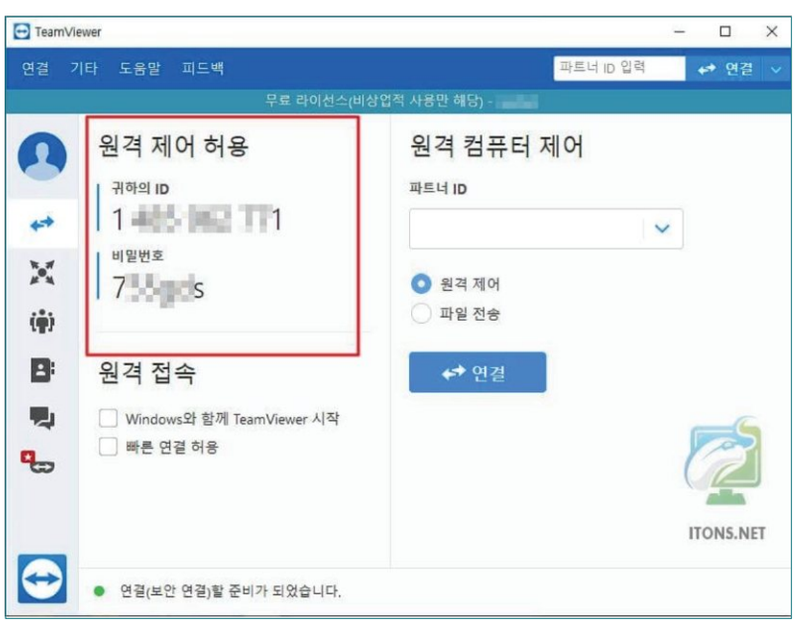
• WiFi 네트워크 보안 설정
- 무선 공유기의 기본 아이디, 비밀번호 변경
- 네트워크에 인증 및 암호화 적용
  (WPA2 + AES, 가능하면 WPA3-Enterprise + 802.1X(EAP-TLS) 로 적용)
- 단말사용자 인증서 유효기간을 1년 이내로 설정하고 자동 갱신



[그림 76] WiFi 네트워크 물리적 분리 예시

• WiFi 네트워크 분리 및 관리
- 게스트용 네트워크를 설정하여 업무용과 개인용 분리
- 업무용 네트워크의 경우 추가적인 보안(RADIUS, WIPS 등) 적용
- 무선 공유기와 랜선을 보이지 않게 설치

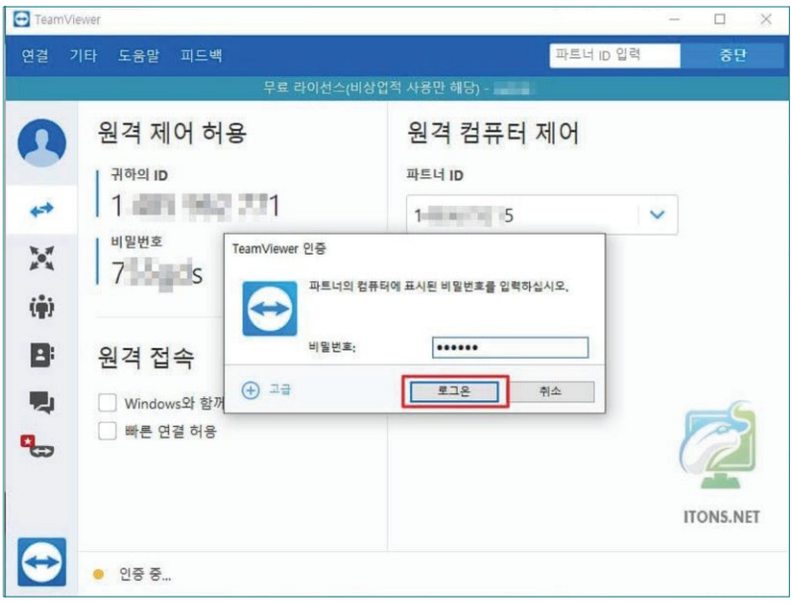
■ 원격접속 접근 통제



[그림 77] 원격 접속 제어 페이지

출처: 한국선급, '03. 사이버보안 현존선 인증 요구사항 해설'

통제항목	B.3.2 네트워크 접근 통제	Advanced



[그림 78] 원격 접속 제어 비밀번호 입력

출처: 한국선급, '03. 사이버보안 현존선 인증 요구사항 해설'

- 원격접속 시 통제 절차
  - 원격접속 전 사전 승인절차 적용, 책임자의 승인 전까지 불가
  - 자동 원격접속 되지 않도록 주의
  - 원격접속 시 VPN(가상사설망)을 통해서만 접근 허용
  - 다중 인증과 같은 강화된 인증 절차 사용
- 원격접속 연결 관리
  - 원격 세션 중 중단 관리, 접속 시도 실패 제한, 강제·자동 연결 종료 기능 제공
  - 원격 유지보수 접속은 일회성/시간 제한 권한 부여
  - 원격 명령 실행, 무선 접속 등 불필요한 기능은 비활성화
  - 원격접속 전용PC, 원격접속 작업기록 녹화 등 추가 보호 수단 고려

■ 제3자의 네트워크 접근은 승인 및 절차에 따라 조정

■ 중요 IT/OT 시스템에 대한 외부로컬·원격접속 승인 기록

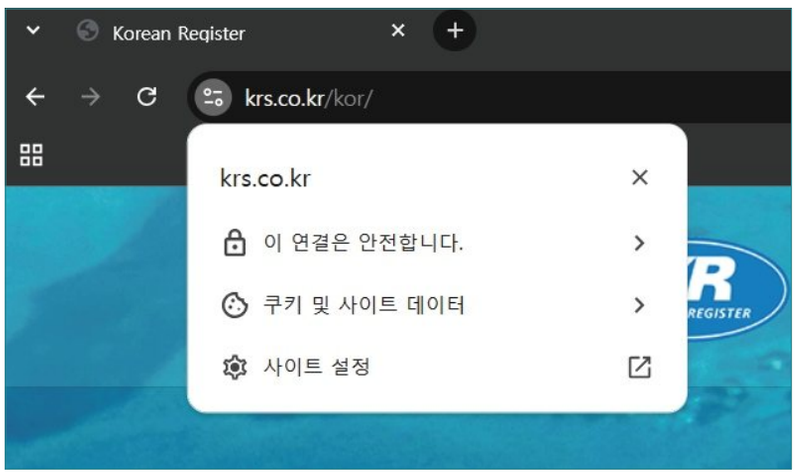
3. 항만에서의 네트워크 접근통제 방안

■ 모바일 데이터 연결

- 상용 VPN(ExpressVPN, NordVPN, Surfshark 등)을 사용하여 악의적인 감청으로부터 기기 보호

■ 항만에서 육상 와이파이 연결

- 육상 와이파이 접속 시 안전하고 신뢰할 수 있는 공유기 사용
- 신뢰할 수 있는 상용 VPN(ExpressVPN, NordVPN, Surfshark 등)을 사용하여 안전하지 않은 공공 무선 공유기(공항, 호텔, 상점, 바 등에서 발견되는 공유기) 연결
- SSL 인증서가 있는 웹사이트에만 접속하도록 주의, 특히 민감한 정보가 있는 웹사이트(예: 온라인 뱅킹) 에 접속할 때는 더욱 주의 필요

통제항목	B.3.2 네트워크 접근 통제	Advanced
	 [그림 79] SSL 인증 예시	
비고		

B.4 기기 및 출입 통제

통제항목	B.4.2 인원 출입 통제	Advanced
점검목적	제한구역 및 CBS(컴퓨터기반시스템)에 대한 물리적 접근을 엄격히 통제하고, 방문자의 출입 관리와 사용자 행동 통제를 통해 무단 접근과 보안 사고를 방지하는 데 있습니다.	
점검내용	제한구역 설정 및 관리, CBS(컴퓨터기반시스템)의 위치와 물리적 통제, 방문자 출입 기록 및 감독 절차 이행, 출입 권한 관리, 그리고 장비 보호·정기 점검 수행 여부를 점검합니다.	
점검기준	**양호 :** 제한구역에 대한 물리적 접근이 승인된 절차에 따라 관리되는 경우 **취약 :** 제한구역에 대한 물리적 접근이 승인된 절차에 따라 관리되지 않는 경우	
레퍼런스	[UR E26 4.2.4.3.2 방문자에 대한 물리적 접근 통제] [UR E26 4.2.7.3 세부 요구사항] [BIMCO 3.5 선박 방문] [BIMCO 7.2 기술적 보호 조치]	
증적자료	선내 제한구역 배치도, 물리적 보안 정책서	
조치방법	**1. 물리적 출입 통제 및 구역 관리** ■ ISPS 코드에 따른 제한구역 설정 및 관리 • 네트워크 장비가 포함된 서버실, VSAT 랙이 설치된 곳을 추가적인 제한구역으로 지정 필요 • 서버 랙에 잠금장치 설치 ■ CBS(컴퓨터기반시스템) 장비는 제한구역에 설치하여 무단 접근 방지 • 제한구역은 잠금 장치 설치를 통해 비인가 접근 차단, 이중 잠금(전자식 도어락 + 키, 도어락 + 생체) 권고 • CCTV를 설치하여 보안 수준 강화(갱웨이, 주변 사각지대 최소화), 영상 최소 90일 보관 권장 • 제한구역은 출입자 명부 작성을 통해 관리 • 출입시 담당자(선박 보안 책임자, IT 담당자)의 승인 필요	

통제구역 출입자 명부

일자	소 속	직급/성명	연락처	출입목적	결재 책임자
			□ 개인정보 제공 동의		
			□ 개인정보 제공 동의		
			□ 개인정보 제공 동의		
			□ 개인정보 제공 동의		
			□ 개인정보 제공 동의		
			□ 개인정보 제공 동의		
			□ 개인정보 제공 동의		
			□ 개인정보 제공 동의		
			□ 개인정보 제공 동의		

[그림 80] 제한구역 출입자 명부 예시

통제항목	B.4.2 인원 출입 통제	Advanced

2. 방문자 출입 통제

■ 사전 승인 절차

- 외부업체, 항만 관계자 등 선박 방문자는 목적, 작업범위, 접근구역, 반입장비를 명시한 사전신청서로 CSO/SSO의 사전 승인 진행, 승인서에는 허용 구역, 시간, 동행 책임자 지정

■ 갱웨이(탑승구) 출입 통제

- 출입 기록(방문객 출입관리대장) 작성

방문객 출입관리 대장

기 간 : 2025 년 01 월 01 일	결재	기안	실의	결정
		/	/	/

No.	출입시간			출입자					출입증		피방문자			비고
	일자	입	출	국적	주소(소속)	생년월일	성명	방문목적	번호	반납	부서	성명	장소	

[그림 81] 방문객 출입관리대장 예시

- 임시출입증 발급(색상/구역별), 방문 중 상시 출입증 착용 의무 부여
- 개인 노트북·USB·휴대폰 등은 격리함 보관 또는 승인된 작업용(하드닝·백신 등) 장비만 반입. 무승인 매체는 선내 반입 금지

■ 체류 중 운영 통제

- 모든 선박 방문자는 지정 담당자의 동행 하에 허용 구역만 이동
- OT/IT 변경·점검은 작업허가서로 관리, 완료 후 구성변경 기록과 출입 로그 대조

■ 퇴선·사후 조치

- 출입명부와 대조하여 인원 전원 퇴선 확인, 임시출입증과 대여 매체 회수

통제항목	B.4.2 인원 출입 통제	Advanced
	3. 장비 보호 ■ PC에 화면보호기 설정 적용 [그림 82] 화면보호기 설정 ■ 네트워크 장비·콘솔·HMI는 랙 잠금과 봉인 씰 적용, 훼손 시 알림·조사 **4. 정기 점검** ■ 도어락, 리더기, 경보, CCTV 월 1회 점검·기록 ■ 포트 봉인 미사용 포트 상태 분기 1회 점검·기록	
비고		

C. 사이버 리스크 관리

C.1 사이버 취약점 진단

통제항목	C.1.3 보안설정 점검 및 모의해킹	Advanced
점검목적	선사, 선박 내 정보시스템과 운항 안전에 영향을 줄 수 있는 사이버 취약점을 사전에 발견하고 개선하여 보안을 강화합니다. 또한, 실제 공격 상황을 모의해킹으로 재현하여 대응 역량을 점검하고 사고 발생 시 신속한 대응과 복구가 가능하도록 준비하는 데 있습니다.	
점검내용	선박 내 IT 및 OT 자산, 네트워크 장비, 서버, 애플리케이션 등 모든 자산에 대하여 보안 정책 및 국제 표준에 부합하는지 체계적으로 점검합니다. 점검 시 기본 설정값 변경 여부, 접근 권한 관리, 암호화 적용 상태, 백신 및 패치 관리, 로그 수집과 네트워크 접근 제어 등 다양한 항목을 점검하며, 모의해킹을 병행하여 전체적인 보안 상태를 평가합니다.	
점검기준	**양호 :** 주요 자산에 대한 취약점 점검이 정기적으로 이루어지는 경우 **취약 :** 주요 자산에 대한 취약점 점검이 정기적으로 이루어지지 않는 경우	
레퍼런스	[BIMCO 2.2 사이버 위협의 유형] [BIMCO 3.1 공개적인 취약점]	
증적자료	인프라 진단 결과 보고서, 모의해킹 결과 보고서	
조치방법	**※ 전문가를 통해 취약점 점검과 모의해킹을 수행하여, 사이버 취약점을 미리 발견하고 개선합니다.** **1. 보안설정 점검 프로세스** ■ 범위 및 대상 선정 • 식별된 자산을 대외/대내 서비스로 분류 • 내 외부 요구사항 검토 및 담당자 인터뷰를 통한 대상 확정 • 점검 범위 및 대상 협의 ■ 보안설정 점검 수행 • 점검 대상별 점검 방법 검토 • 컨설턴트의 수동점검 • 자동 점검 스크립트 • 기타 자동 점검 툴 ■ 이행 점검 • 점검 결과보고서의 취약점별 개선 계획, 책임자, 목표 일정, 변경 관리 승인 내역을 검토 • 보안 패치, 설정 변경, 접근통제 개선 등 실제 시스템 설정을 재점검(수동/자동) • 최종 결과를 보고서로 작성하여 경영진·선사 SMS(안전관리시스템) 기록에 반영 **2. 보안설정 점검 항목** ■ 보안 설정 점검 대상: • 서버(Linux, Unix, Windows 등) • 네트워크장비(계정 관리, 접근 관리, 패치 관리 등) • DBMS(DataBase Management System, 데이터베이스 관리 시스템) • PC(계정 관리, 서비스 관리, 패치 관리, 보안 관리)	

통제항목	C.1.3 보안설정 점검 및 모의해킹	Advanced

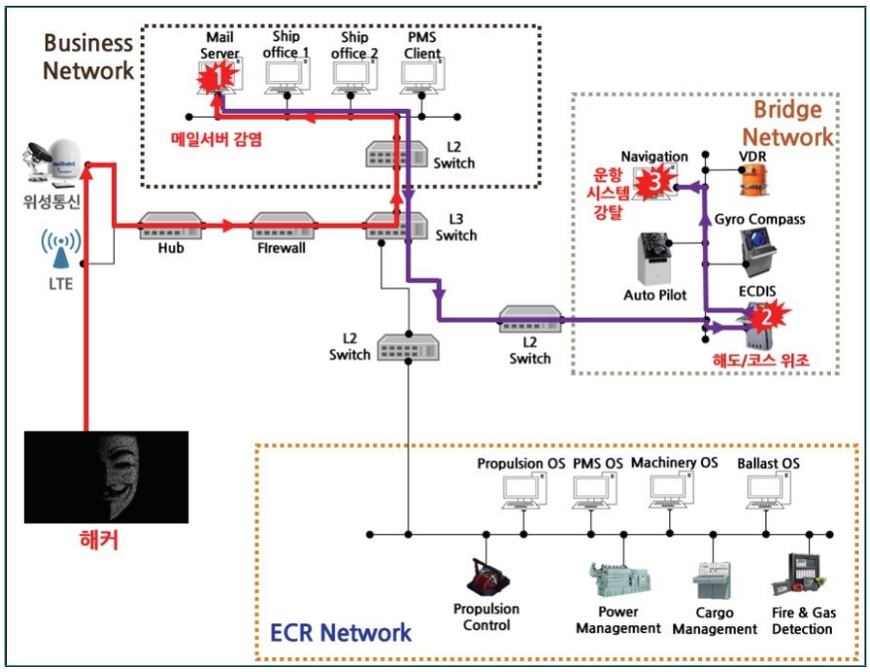
[그림 83] 보안설정 점검 예시

3. 모의해킹 프로세스

[표 14] 모의해킹 프로세스

단계	내용
사전 협의 단계	모의해킹 수행 이전 담당자와 진단 대상에 대해서 협의하는 과정
정보 수집 단계	진단자는 공개출처정보(OSINT)를 활용해 외부로 노출된 대상의 정보를 수집하여 Nmap, Burp Suite 등의 진단 도구를 활용해 사전에 수집할 수 있는 최대한의 정보를 확보
위협 모델링 단계	수집한 정보를 토대로 진단 대상이 가지고 있는 잠재적인 보안 위협을 식별
취약점 분석 단계	위협모델링단계에서 모델링한 위협을 대상으로 실제 해당 보안 위협을 활용한 공격이 가능한지 분석하는 단계
내부 침투 단계	외부 서비스의 취약점을 기반으로 1차 침투에 성공했을 경우, 2,3차 침투를 시도하는 단계 ex) 만약 1차적으로 쉘을 획득하여 내부침투에 성공했을 경우 성공한 대상에서 ARP 스캔, Netstat 정보 등을 수집하여 추가적인 침투 대상을 탐색하고 대상을 발견했을 경우 해당 대상의 취약점을 활용해 2차 침투 시도
보고서 작성	내부 모의해킹까지 모두 수행하고 난 이후 도출된 취약점을 기반으로 시나리오가 포함된 보고서 작성 보고서 포함 내용: - 식별된 취약점 및 리스크 - 취약점 식별 방법 - 취약점 대응 방안

통제항목	C.1.3 보안설정 점검 및 모의해킹	Advanced



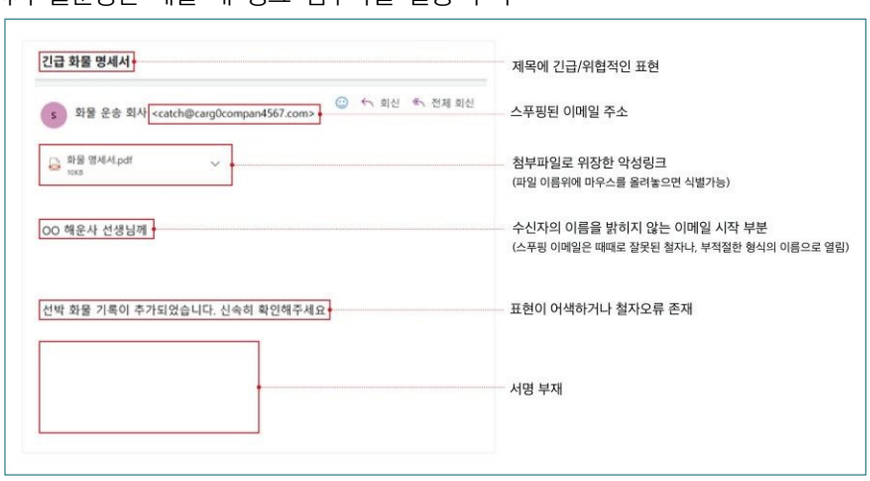
[그림 84] 선박사이버 공격 시나리오

■ 모의해킹 대상:

- 컴퓨터, 네트워크(사무용PC, 서버, 와이파이)
- OT/제어 시스템(엔진제어 시스템, 통신장비 등)

■ 대응 방법:

- 비밀번호 관리
- 출처가 불분명한 메일 내 링크·첨부파일 실행 주의



[그림 85] 이메일 열람시 주의 사항 예시

통제항목	C.1.3 보안설정 점검 및 모의해킹	Advanced
	• 출처가 불분명한 이메일은 열람 주의 - 첨부파일 실행, URL 클릭 주의 - 이메일을 보낸 사람에게 전화나 메신저로 메일 진위여부 확인 - 제목이나 내용에 긴급과 같은 위협적인 표현이 있는 메일 주의 - 표현이 어색하거나, 서명이 없는 메일 주의 - 이메일로 민감 정보가 유출되지 않도록 관리 - 이메일 및 웹 브라우저에서 악성 스크립트 실행 차단 - 이메일 전송 시 zip 또는 암호화 파일 권장 - 이메일 시스템에서는 하이퍼링크 비활성화 권장 - 일반 이메일 주소 사용 지양, 사용자 계정 설정 확인 • USB/외부 장치 사용 주의(개인 USB 사용 금지) • 정기 점검 협조	
비고		

D. 사이버 사고 대응

D.1 사이버보안 모니터링

통제항목	D.1.1 사이버 위협 모니터링	Advanced
점검목적	선박 내 IT시스템의 보안 위협을 실시간으로 탐지하고, 발생한 보안 이벤트를 분석하여 사이버 공격을 예방 및 대응하여 피해를 최소화 합니다.	
점검내용	침입 탐지 및 모니터링 체계를 구축하여 선박 내 IT시스템의 보안 위협을 실시간으로 대응하고, 보안 로그를 수집 및 분석하여 침입 탐지 및 대응을 수행합니다.	
점검기준	**양호 :** 침입 탐지 및 모니터링 체계가 구축 되어 있을 경우 **취약 :** 침입 탐지 및 모니터링 체계가 구축 되어 있지 않을 경우	
레퍼런스	[IMO 3.5.3.3 보호(protect)] [IMO 3.5.4 탐지(Detect)] [IMO 3.5.4.1 탐지(Detect)] [UR E26 4.3 탐지] [UR E26 4.3.1.3 세부 요구사항] [BIMCO 8.1 탐지, 차단 및 경고] [DCSA 2.4.3 구현] [DCSA 3.2.2 설명] [DCSA 3.2.3 구현] [DCSA 3.3.2 설명] [DCSA 3.3.3 구현] [DCSA 2.6.2 설명] [DCSA 2.6.3 구현] [DCSA 4.3.3 구현]	
증적자료	로그 분석 결과 보고서, 경보 발생 내역	
조치방법	**1. 침입 탐지 및 모니터링 체계 구축** ■ 선박의 네트워크 및 시스템에서 발생하는 보안 이벤트의 실시간 탐지·분석하는 지속적 모니터링 전략 수립: • 모니터링 대상 정의	

통제항목	D.1.1 사이버 위협 모니터링	Advanced

[표 15] 모니터링 대상 유형

모니터링 대상 유형	모니터링 대상	설명
네트워크/경계 장비	방화벽·IDS/IPS·UTM	허용되지 않은 트래픽, 포트 스캔, DoS/DDoS 징후 탐지
	VSAT·Inmarsat·FleetBroadband	위성 통신 채널의 비정상 접속, 과도한 데이터 전송 모니터링
	선내 WiFi·무선 AP	WPA3 인증 실패, MAC 스푸핑, 비인가 AP 접속 시도
핵심 운항·제어 시스템	ECDIS / RADAR / AIS	항로·위치 데이터 위·변조, 비인가 설정 변경 탐지
	IAS(Integrated Automation System)	엔진·보일러·발전기 제어 명령의 이상 동작 감시
	GMDSS / NAVTEX	긴급 통신 장애, 주파수 변조·재전송 공격
	BWMS, Cargo Control, Propulsion Control	밸러스트·화물 펌프 제어 신호 변조, PLC 펌웨어 변경
서버·IT 인프라	선내 메인 서버 (Windows/Linux)	관리자 권한 상승, 비인가 원격 데스크톱 접속
	파일·백업 서버, NAS	대량 데이터 유출, 무단 암호화 시도
	가상화·컨테이너 환경	VM 스냅샷 무단 생성, 이미지 변조
사용자·계정 활동	선원·운항인력 계정 로그인	비정상 시간대 로그인, 반복 실패, 다중 지역 로그인 탐지
	이동식 매체 (USB, 외장 HDD)	승인되지 않은 매체 연결, 악성코드 유입
	원격지원·유지보수 접속	공급업체 원격 유지보수 계정의 불규칙 접속
물리·환경 센서	서버실·브리지 출입 통제 로그	서버실·브리지 출입 기록 이상 징후
	온도·연기·전력 센서	전원 차단, 화재·침수 경보 변조 또는 이상 감지

- 모니터링 지표(KPI)설정 (로그인 실패 횟수, 비인가 장치 접속 등)
- 데이터 수집 및 상관 분석
- 평가 및 대응
- 보고 및 기록
- 정기 점검과 최신화 업데이트
  - 외부 침해지표(IOC)를 SIEM에 통합

통제항목	D.1.1 사이버 위협 모니터링	Advanced

[표 16] IOC 예시

구분	유형	설명	침해정보 예시
네트워크 기반 IOC	IP 주소	악성 서버와 통신한 흔적을 확인할 수 있는 공격자 서버 IP	203.0.113.45
	도메인/URL	피싱 메일 등에서 사용되는 악성 도메인 및 악성 URL 주소	malicious-phish.example.com
	DNS 패턴	무작위 생성 도메인을 이용한 봇넷·랜섬웨어의 통신 패턴	*.abcd1234.com
파일 기반 IOC	파일 해시	악성코드를 식별하기 위한 고유 지문값 (SHA256, MD5 등)	d2b1a1f0…
	악성 파일명	사용자를 속이기 위해 정상 문서처럼 보이는 악성 실행 파일	invoice_update.scr
	파일 경로	감염 시 특정 경로에 생성되는 악성 파일 위치	C:\Users\Public\malware.exe
호스트 기반 IOC	레지스트리 키	윈도우 부팅 시 악성 프로그램을 자동 실행하도록 등록	HKLM\Software\...\Run\evil
	프로세스	정상 도구를 악용해 악성 스크립트를 실행하는 행위	powershell.exe -enc …
	로그 이벤트	무차별 대입 공격이나 계정 탈취 시도의 흔적	다수의 로그인 실패
이메일 기반 IOC	발신자 주소	신뢰받는 기관을 사칭한 스푸핑 메일 발신자	admin@fake-bank.com
	첨부파일	매크로를 포함해 실행 시 악성코드를 설치하는 첨부파일	report.xlsm
행위 기반 IOC	비정상 트래픽	내부 자산을 스캔하여 취약점을 찾는 공격 시도	짧은 주기의 대량 포트 스캔
	권한 상승	시스템 권한 탈취를 위한 관리자 권한 확인/획득 시도	whoami /priv
	데이터 유출	내부 데이터를 외부로 빼돌릴 때 나타나는 비정상 통신량	대량의 암호화된 아웃바운드 트래픽

■ 침입 탐지/방지 시스템(IDS/IPS), 보안정보 및 이벤트 관리(SIEM) 등 보안 솔루션을 활용하여 위협 식별·기록·보고·차단:

- 침입 탐지 시스템(IDS): 의심스러운 네트워크 트래픽을 수집, 분석하여 침입 활동을 탐지한 후 관리자에게 통보하는 기능을 수행하는 보안 시스템
- 침입 방지 시스템(IPS): 악성 네트워크 트래픽을 탐지한 후 격리,차단,제거 등 IDS와 다른 강력한 조치를 취하는 네트워크 보안 시스템
- 보안정보 및 이벤트 관리(SIEM): 정보시스템의 보안 정보 및 이벤트 관리를 통해 내부 및 외부 위협을 모니터링 함으로써, 내부·외부 정보유출을 방지하는 보안 솔루션

통제항목	D.1.1 사이버 위협 모니터링	Advanced
	 [그림 86] 관제 모니터링 이미지 **2. 로그 관리 및 이상 징후 분석** ■ 항해 장비, 통신 시스템, 엔진 제어 시스템 등 핵심 자산의 로그를 수집·보관 ■ 로그는 육상 관제센터 또는 외부 전문가와 공유·분석하여 조기 경보 체계 마련 ■ 보안/감사 관련 로그의 지속적인 최신화 **3. 지속적 모니터링 필요** ■ 선박 내 자산(항해 장비, ECDIS, 엔진 제어 시스템 등) 및 네트워크 장치에서 발생하는 이벤트·로그 상시 확인 ■ 최신 리스크 목록을 반영하여 모니터링 • 최신 리스크 목록: AI 악용, 랜섬웨어, 크리덴셜 스터핑(유출된 ID/PW목록을 다른 웹사이트에 무작위로 입력해 로그인 후 개인정보를 탈취하는 방식) 등	
비고		

4.3 Optimized

B. 사이버보안 통제

B.3 네트워크 접근 통제

통제항목	B.1.3 사이버 자산 변경관리	Optimized
점검목적	네트워크를 보안 구역별로 구분해 구역 간 통신을 엄격히 통제하고 불필요한 접근과 공격을 차단하여 네트워크 전반의 안전성을 확보하는 데 있습니다.	
점검내용	분리 대상 자산이 보안 구역별로 배치되어 있는지 확인하며 네트워크 통신 제어 현황을 확인합니다.	
점검기준	**양호 :** 보안구역별 네트워크 분리 구성도가 존재하는 경우 **취약 :** 보안구역별 네트워크 분리 구성도가 없는 경우	
레퍼런스	[UR E26 4.2.1.1 요구사항] [UR E26 4.2.1.2 타당성] [UR E26 4.2.1.3 세부 요구사항] [UR E26 4.2.5.3 세부 요구사항] [BIMCO 7.2 기술적 보호 조치] [BIMCO 7.3 절차적 보호 조치]	
증적자료	네트워크 분리 구성도	
조치방법	**1. 네트워크 분리 대상 시스템 및 자산**	

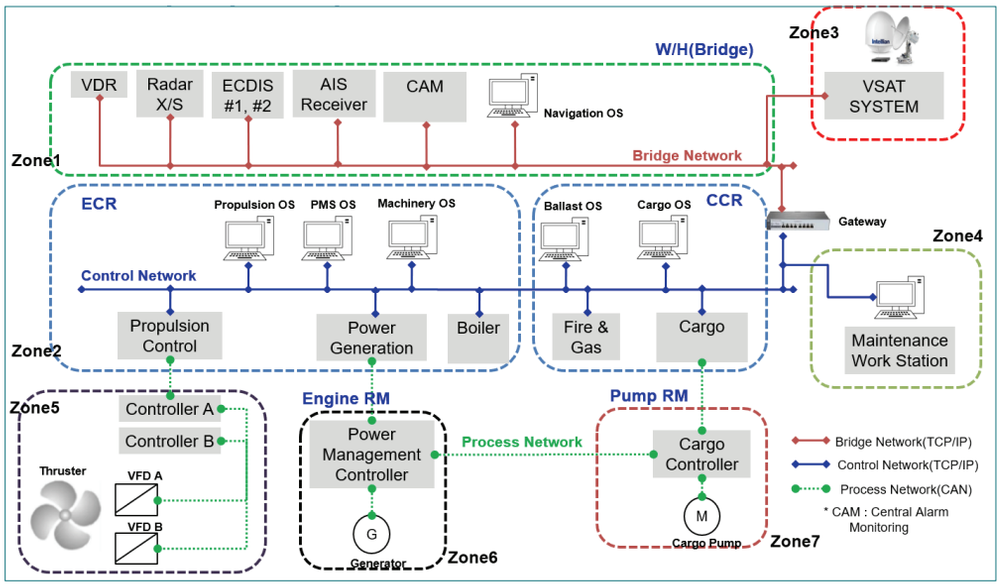
[표 17] 네트워크 분리 대상 자산 예시

보안구역	대표 자산(예시)
항해·통신 구역	ECDIS, GPS, AIS, GMDSS, 레이더 서버, VDR
기관·제어 구역	엔진제어 PLC, PMS, 발전기 제어, 추진·조타 제어 장비
화물·환경 구역	BWMS, 로딩컴퓨터, 밸브/펌프 제어, 탱크 레벨 측정
안전·감시 구역	VDR, CCTV/NVR, 화재경보 시스템, BNWAS, 침입감지 센서
OT·DMZ	패치 관리 서버, 원격정비 프록시, 데이터 다이오드 장비
IT·업무	서버, PC, ERP·메일, 프린터
승무원/복지, 게스트	개인 스마트폰·태블릿, 공유기
원격 접속 / 외부업체 구역	외부 정비업체 노트북, 서비스용 원격 VPN(가상사설망) 계정

- 안전 시스템(Safety System)을 제공하는 CBS(컴퓨터기반시스템)는 별도 보안 구역으로 그룹화
- 항해 및 통신 시스템은 기계류 또는 화물 시스템과 분리 필요
- 무선 장치 별도 분리 필요
  - 무선 네트워크는 별도의 구역으로 분리되며, 내부망과 외부망 동시에 연결 금지
  - 다른 중요 네트워크와 직접 연결 해제
- 신뢰할 수 없는 시스템, 네트워크, CBS(컴퓨터기반시스템)는 물리적으로 분리 필요
- 공급자를 위한 원격 접근이 요구되는 OT(운영 기술) 시스템 분리 필요

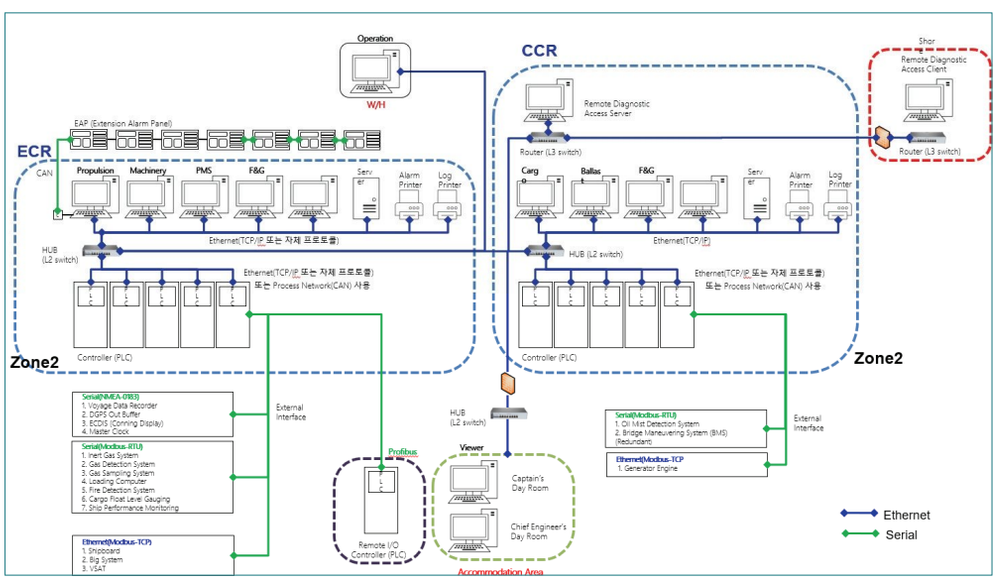
통제항목	B.1.3 사이버 자산 변경관리	Optimized

- 화물 적재 계획 및 선적 관리 시스템 분리 필요
- 게스트 액세스 네트워크 분리 필요
- 방문자용 컴퓨터 및 프린터 분리 필요



[그림 87] 네트워크 분리 구성도 예시 1

출처: 한국선급, '03. 사이버보안 현존선 인증 요구사항 해설'



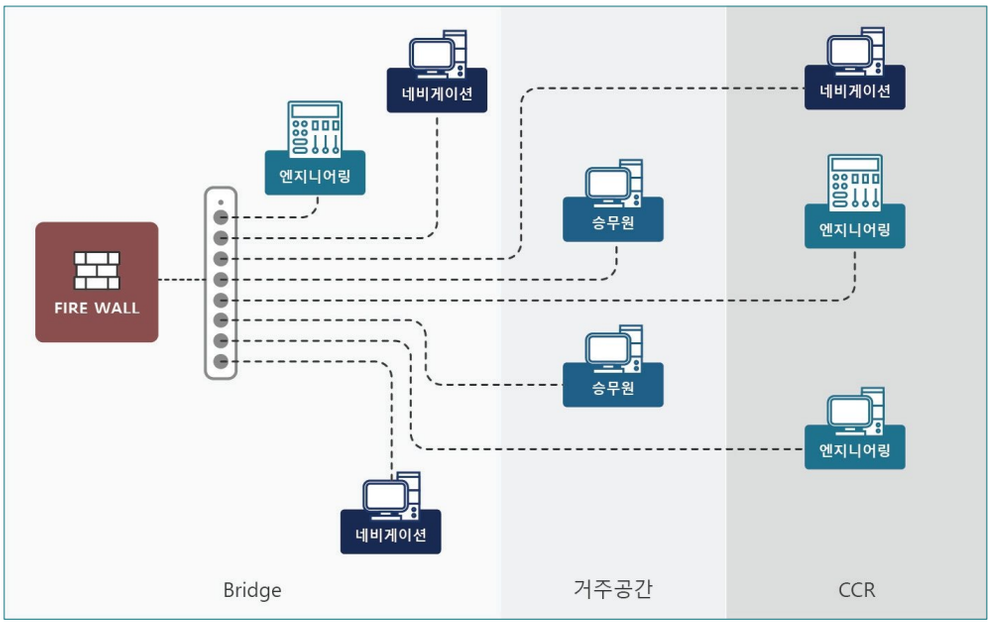
[그림 88] 네트워크 분리 구성도 예시 2

출처: 한국선급, '03. 사이버보안 현존선 인증 요구사항 해설'

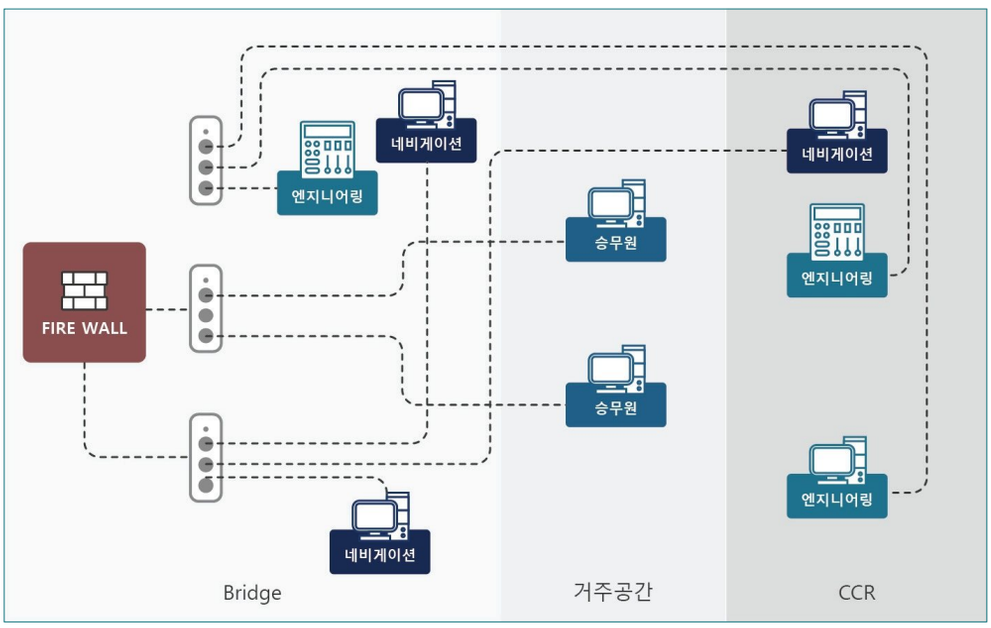
통제항목	B.1.3 사이버 자산 변경관리	Optimized

2. 네트워크 분리 방법

- 시스템은 보안 구역(Security Zones)으로 나눠야 하며, 구역 간 통신은 방화벽, 라우터, 보안 게이트웨이 등으로 엄격하게 제어
- 물리적 분리 우선, 불가 시 VLAN(가상 랜)·보안 게이트웨이로 논리적 분리 진행

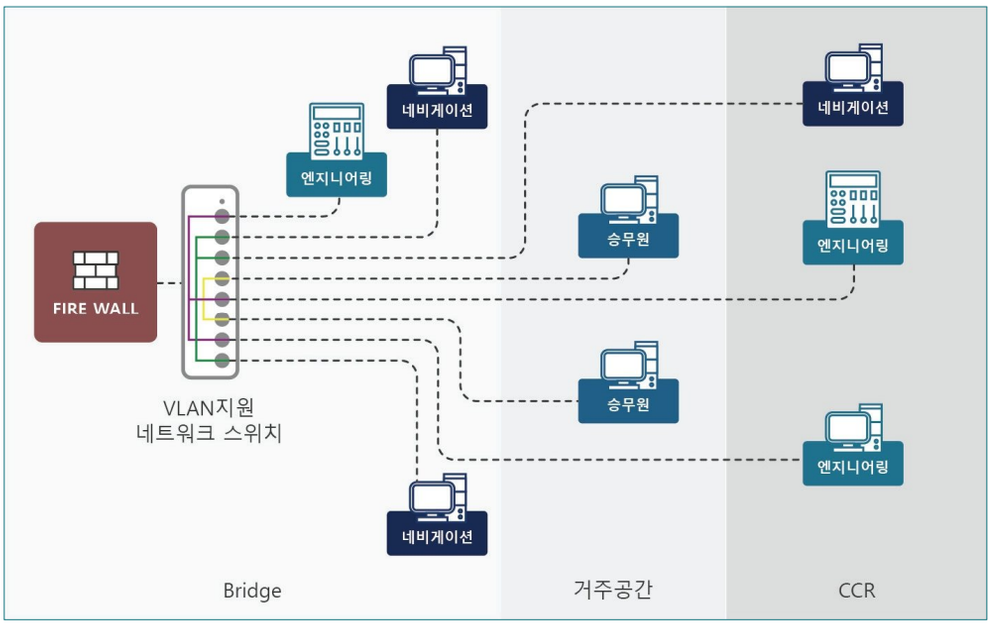


[그림 89] 분리되지 않은 네트워크



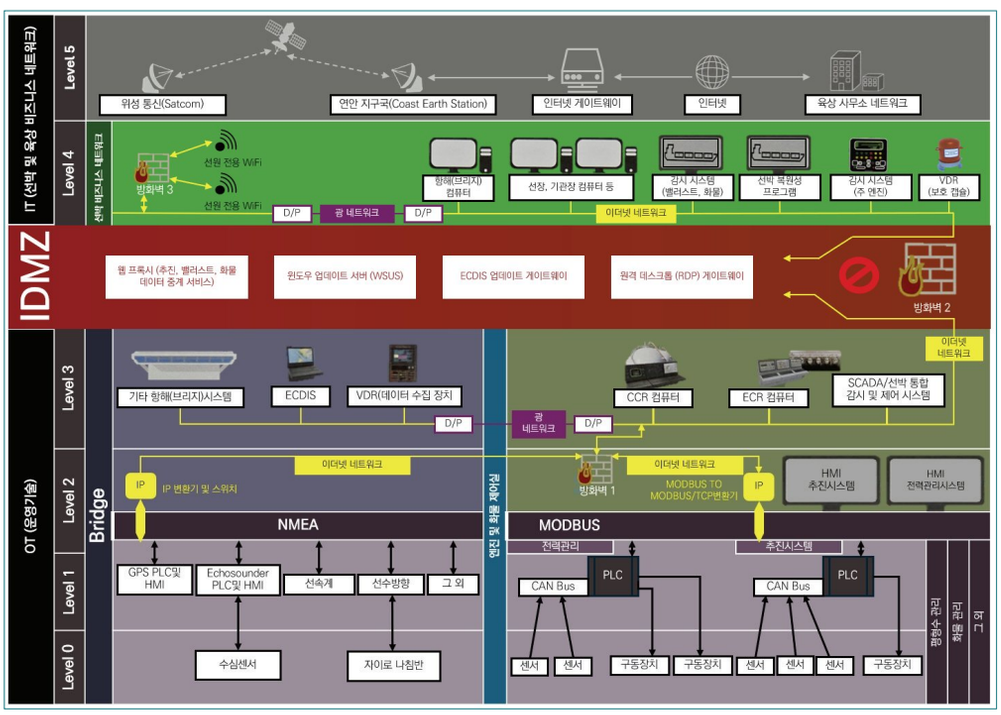
[그림 90] 물리적으로 분리된 네트워크

통제항목	B.1.3 사이버 자산 변경관리	Optimized



[그림 91] VLAN을 활용한 네트워크 분리

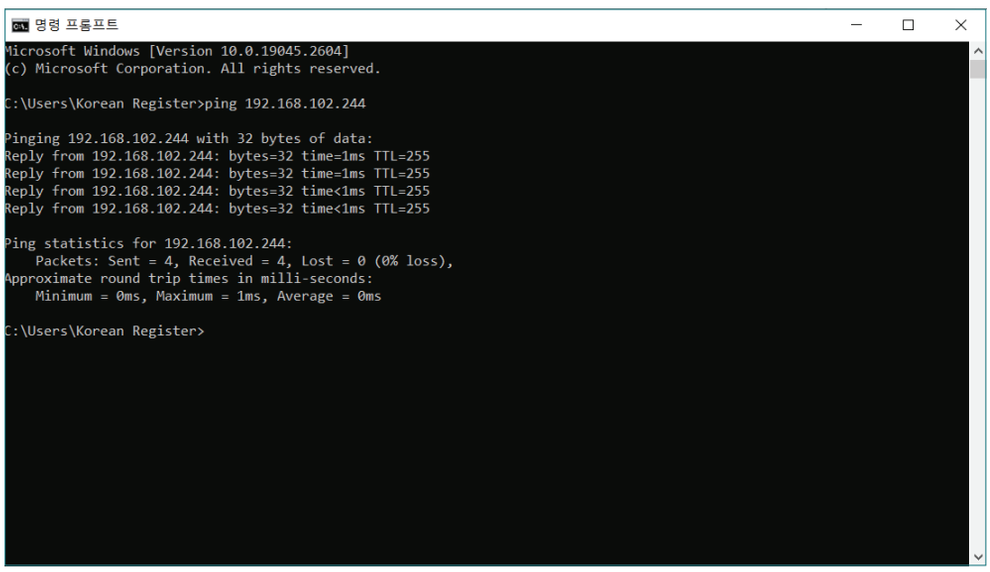
- 신뢰되지 않는 네트워크와의 통신을 제어하기 위해서 DMZ(Demilitarized Zone) 구축 혹은 기타 네트워크 아키텍처 메커니즘 구현



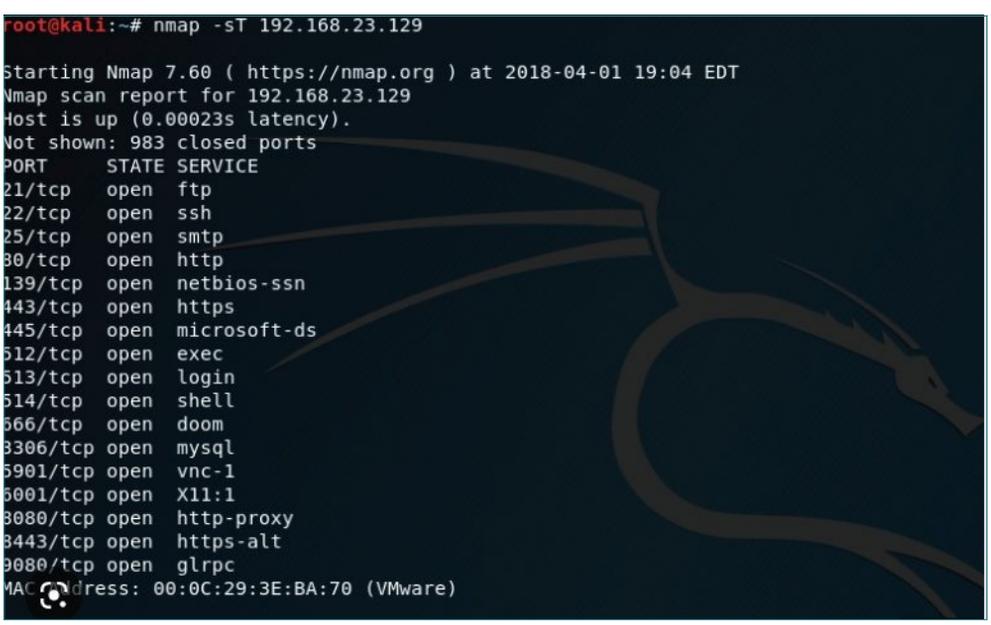
[그림 92] 윈도우기반 시스템에서 IDMZ가 설치된 선박 아키텍처 예시

통제항목	B.1.3 사이버 자산 변경관리	Optimized

■ Ping Test를 통해 IT시스템과 OT시스템의 네트워크 분할 여부 확인



[그림 93] Ping Test로 네트워크 분할 여부 확인 예시



[그림 94] 열려있는 네트워크 포트 확인 예시

비고	

C. 사이버 리스크 관리

C.2 사이버 리스크 평가

통제항목	C.2.4 사이버 리스크 평가 예외	Optimized
점검목적	사이버 리스크 평가 절차가 CBS(컴퓨터기반시스템)의 요구사항 적용 예외를 합리적으로 입증하고, 선박 운영 안전에 미치는 영향을 최소화하는지 확인하는 데 있습니다.	
점검내용	CBS(컴퓨터기반시스템) 일부가 사이버보안 요구사항 적용에서 제외될 경우, 시스템 통합자가 해당 CBS에 대해 체계적인 리스크 평가를 수행하고 허용 가능한 리스크 수준을 입증하는지 확인합니다. 선주는 운영 중 새로운 취약점과 사이버 위협 변화를 반영해 리스크 평가를 갱신하며, 임계값 초과 시 선급협회에 신속히 통지하는 절차를 이행하는지 점검합니다.	
점검기준	**양호 :** 사이버보안 요구사항 적용이 제외된 CBS(컴퓨터기반시스템)가 리스크 평가 결과 허용 가능한 리스크 수준으로 확인된 경우 **취약 :** 사이버보안 요구사항 적용이 제외된 CBS(컴퓨터기반시스템)가 리스크 평가 결과 허용 가능한 리스크 수준으로 확인되지 않은 경우	
레퍼런스	[UR E26 6 CBS(컴퓨터기반시스템)를 요구사항의 적용에서 제외하는 경우의 리스크 평가] [UR E26 6.1 요구사항] [UR E26 6.2 타당성 근거] [UR E26 6.3 세부 요구사항] [UR E26 6.4 수용 기준]	
증적자료	CBS(컴퓨터기반시스템) 리스크 평가 결과서	
조치방법	**1. 예외 적용 시 리스크 평가 필수** ■ CBS(컴퓨터기반시스템)일부가 요구사항 적용에서 제외되는 경우, 반드시 허용 가능한 리스크 수준을 입증하는 리스크 평가 수행 **2. 제외 사유 및 문서화** ■ 보안 요구사항을 적용하지 못하는 경우, 반드시 정당한 사유(기술적 제한, 안전성 고려 등)를 명확히 기록 ■ 해당 예외 사유와 리스크 평가 결과를 문서로 작성하여 보관하고, 필요 시 선급협회에 제출: • 문서화: 예외사유, 리스크 평가 결과(수치/등급 포함), 보완 대책, 책임자 승인 내역 ■ 리스크 평가 결과가 허용 가능한 수준(임계값 이하)일 때만 예외 인정	

리스크평가 결과서

작 성	검 토	승 인
/	/	/

부서명				작성일자				Page	/
자산/시스템	위협 시나리오	취약점	영향도(1~5)	발생 가능성(1~5)	리스크 값	리스크 등급	보완 조치	예외 사유	비고
ECDIS	악성코드 감염	OS 패치 미적용	5	4	20	High	네트워크 분리, USB 차단, 백신 강화	운항 중 시스템 업데이트 불가	선급 보고 필요

[그림 95] CBS(컴퓨터기반시스템) 리스크평가 결과서 예시

통제항목	C.2.4 사이버 리스크 평가 예외	Optimized
	3. 리스크 평가 수행 기준 ■ 유사 설계 지식과 경험, CBS(컴퓨터기반시스템) 범주, 연결성, 기능 요구사항 및 사양 고려 ■ 내부 및 외부 출처로부터 사이버 위협 정보 수집, 위협 발생 가능성과 영향 이해 심화 **4. 리스크 평가 갱신 및 관리** ■ 선주는 새로운 취약점에 따라 리스크 평가 갱신 ■ 허용 임계값 초과 시 선급협회에 통지하고 갱신 평가 제출 ■ 리스크 평가는 인명, 선박 안전, 해양 환경 영향까지 분석하며, CBS(컴퓨터기반시스템) 분류 및 공격 표면 고려 **5. 제외 수용 기준** ■ CBS(컴퓨터기반시스템)는 네트워크로부터 고립되어야 하며 IP 연결 없는 상태 ■ 물리적 인터페이스 포트 비활성화 또는 미보유 ■ 물리적 접근 통제된 장소 내 위치 ■ 복수의 선박 기능을 제공하는 통합 제어 시스템이 아닌 경우 ■ Category III 선박 기능 제공 금지 • 예: 추진 제어 시스템, 조타기 제어 시스템, 전력시스템(전력관리시스템 포함) ■ 알려진 취약점, 위협, 사고 영향 충분히 고려된 리스크 평가 수행 ■ 공격 표면 최소화 및 물리적·논리적 접근 지점 관리 **6. 문서 제출 및 근거 자료** ■ 합리적 설명과 근거 자료 제출 ■ 선급협회의 추가 문서 요구 가능성 존재	
비고		

C.4 사이버 복원력 검사

통제항목	C.4.1 사이버 복원력 검사	Optimized
점검목적	선박의 사이버 복원력 검사 절차가 UR 요구사항에 따라 설계, 제출, 승인, 시험 및 문서화되어 선박 사이버보안이 효과적으로 검증되고 유지되는지 확인합니다.	
점검내용	사이버 복원력 검사 준비에 필요한 서류들을 준비하고, 사이버 복원력 준수를 위한 본 가이드의 점검 항목을 준수하고 있는지 확인합니다.	
점검기준	**양호 :** 사이버 복원력 검사 절차를 주기적으로 관리하고 있을 경우 **취약 :** 사이버 복원력 검사 절차가 준비되어 있지 않을 경우	
레퍼런스	[UR E26 5.3 선박 운항 기간 동안] [UR E26 5.3.1 최초 연차 검사] [UR E26 5.3.2 후속 연차 검사] [UR E26 5.3.3 특별 검사] [UR E26 4.1.1.3 세부 요구사항] [UR E26 4.1.1.3 세부 요구사항] [UR E26 4.1.1.3.1 하드웨어] [UR E26 4.1.1.3.2 소프트웨어] [UR E26 4.1.1.4.4 운영 단계] [UR E26 4.2.1.4.4 운영 단계] [UR E26 4.2.3.4.4 운영 단계] [UR E26 4.2.4.4.4 운영 단계] [UR E26 4.2.6.4.4 운영 단계] [UR E26 4.2.7.4.4 운영 단계] [UR E26 4.3.1.4.4 운영 단계] [UR E26 4.3.2.4.4 운영 단계] [UR E26 4.4.1.4.4 운영 단계] [UR E26 4.5.1.4.4 운영 단계]	
증적자료	선박 사이버 복원력 시험 절차서, 복원력 프로그램 이행 증빙자료	
조치방법	**1. 사이버 복원력 검사 준비 사항** ■ 선주 준비 사항 • 선박 사이버 복원력 시험절차서를 최신 상태로 유지 • 선박 사이버 복원력 검사 결과의 사본 선내에 보관 • 업데이트된 선박 사이버 복원력 시험절차서를 선내에 보관 ■ 연차 검사 • 검사 전(최초 검사의 경우 가능한 6개월 전)까지 선박 사이버 복원력 프로그램을 문서화하여 선급협회 제출 • 검사를 위한 사이버 복원력 이행 입증 자료 준비 • 선박 관리회사 변경 후 선급협회의 요구사항에 따라 새로운 승인 추가 요구 가능 ■ 후속 연차 검사 • 선급협회 요청 시 선박 사이버복원력 프로그램의 이행 여부 입증	

통제항목	C.4.1 사이버 복원력 검사	Optimized

■ 정기검사
- 선박 선급 증서의 갱신 시 진행
- 선급협회의 입회하에 선박 사이버 복원력 시험 절차서에 따라 시험을 실시

2. 사이버복원력 준수 입증을 위한 점검 항목

[표 18] 사이버복원력 준수 입증을 위한 점검 항목

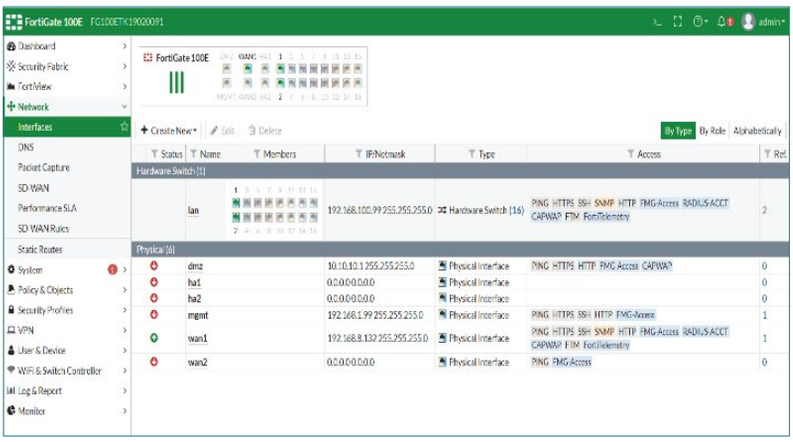
점검 항목	준수 입증을 위한 통제항목(본 가이드)
변경 관리	B.1.3 사이버 자산 변경 관리
소프트웨어 업데이트 관리	C.1.2 패치 관리
방화벽 관리	B.3.2 네트워크 접근 통제, C.1.2 패치 관리
멀웨어 보호 관리	C.1.1 악성코드 방지
접근 통제 관리	B.3.2 네트워크 접근 통제
기밀 정보 관리	B.1.1 자산목록 관리, B.2.1 계정 및 권한 관리, B.2.2 비밀번호 관리
원격 접근 관리	B.3.2 네트워크 접근 통제의 2항
모바일 및 휴대용 장치 관리	B.4.1 기기 반출입 통제
보안 이상징후 탐지	D.1.1 사이버 위협 모니터링
보안 기능의 검증	C.1.1 악성코드 방지, C.1.2 패치 관리
사고 대응 계획	D.2.1 사이버 사고 대응 절차
복구 계획	D.3.2 사이버 복구 계획

비고	

D. 사이버 사고 대응

D.1 사이버보안 모니터링

통제항목	D.1.2 네트워크 운영 모니터링	Optimized
점검목적	네트워크의 성능 저하나 장애를 조기에 탐지하고, 사이버 공격으로 인한 비정상 트래픽을 식별하여, 사고 발생 시 빠른 대응과 원인 분석을 가능하게 합니다.	
점검내용	네트워크 운영 모니터링이 지속적으로 실행되는지 확인하고, 장애 또는 용량 저하 발생시 경보를 울린 기록이 있는지 확인합니다.	
점검기준	**양호 :** 네트워크 운영 모니터링이 실시간으로 운영되는 경우 **취약 :** 네트워크 운영 모니터링이 실시간으로 운영되지 않는 경우	
레퍼런스	[UR E26 4.3.1.1 요구사항] [UR E26 4.3.1.2 근거] [UR E26 4.3.1.3 세부 요구사항]	
증적자료	네트워크 모니터링 정책서, 실시간 모니터링 UI 화면 캡처, 이상징후 탐지 로그	
조치방법	**1. 네트워크 운영 모니터링 대상** 네트워크는 지속적으로 모니터링되어 장애 또는 용량 저하/감소가 발생할 경우 경보가 생성되어야 합니다. ■ 과도한 트래픽에 대한 모니터링 및 보호: • 예시: 네트워크 트래픽이 평상시 평균보다 30% 이상 증가하면 경보 알림 ■ 네트워크 연결 상태 모니터링: • 예시: 스위치, 라우터, 서버 연결 상태 주기적 확인 ■ 장치 관리 활동 모니터링 및 기록: • 예시: 관리자 계정 로그인/로그아웃 기록 자동 저장 ■ 비인가 장치 연결에 대한 보호: • 예시: 새 장치 연결 시 포트 자동 비활성화 후 관리자 승인 필요 ■ 네트워크 대역폭의 사용률이 공급자가 정의한 비정상 기준치를 초과할 경우 경보 생성: • 예시: 네트워크 대역폭 모니터링 툴로 실시간 알람 발생 **2. 이상징후 탐지 기록 확인** ■ 이상징후 경보 기록 확인: • 예시: 비정상 포트 스캔 감지 시 즉시 경보 및 기록 저장 ■ 과도한 트래픽에 대한 로그 기록 확인: • 주간 트래픽 로그 분석 후 패턴 이상 시 보고서 작성	

통제항목	D.1.2 네트워크 운영 모니터링	Optimized
	 [그림 96] 네트워크 운영 모니터링 대시보드 이미지 출처: 한국선급, '03. 사이버보안 현존선 인증 요구사항 해설'	
비고		

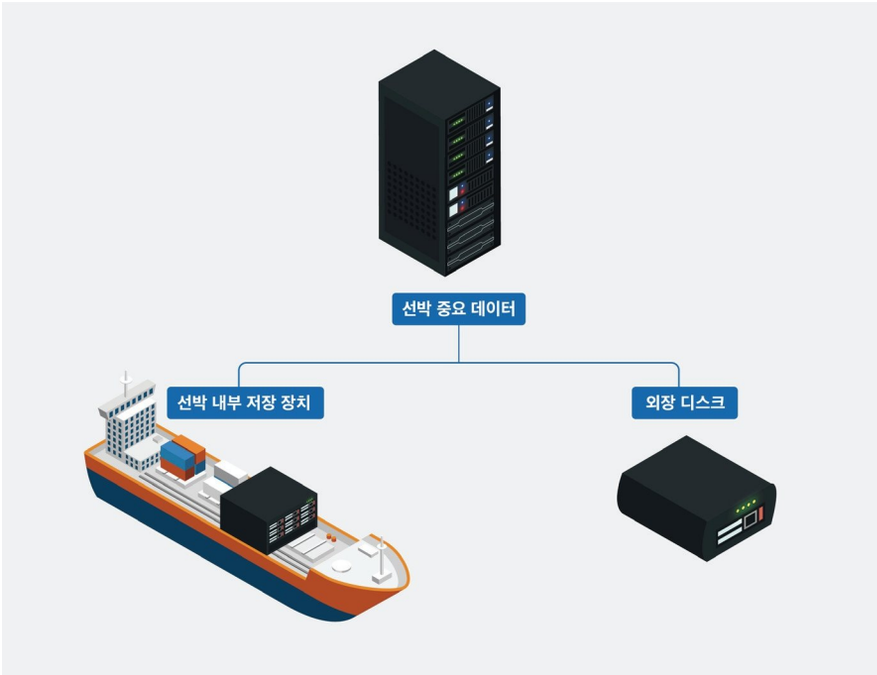
D.3 사이버 복구 계획

통제항목	D.3.1 사이버 백업 관리	Optimized
점검목적	백업은 정기적으로 유지·관리되고 테스트되어, 실제 복구 상황에서 신뢰할 수 있는 수단이 되어야 합니다. 사이버 사고 시 핵심 시스템과 데이터를 신속하고 안전하게 복원하여 선박의 항해·운항 연속성을 확보하고, 업무 중단과 피해를 최소화하는 효과를 기대합니다.	
점검내용	CBS(컴퓨터기반시스템) 및 네트워크가 정의된 백업 대상과 범위를 포함한 백업·복원 기능을 갖추고, 온라인·오프라인 병행 백업과 보안·무결성 절차를 통해 관리되며, 정기 스케줄과 복구 테스트 등 운영·개선 활동이 실제 수행되는지를 점검합니다.	
점검기준	**양호 :** 데이터가 백업되어 있는 경우 **취약 :** 데이터가 백업되어 있지 않은 경우	
레퍼런스	[IMO 3.5.3.7 보호] [UR E26 4.5.2.2 근거] [UR E26 4.5.2.3.1 복원 기능] [UR E26 4.5.2.3.2 백업] [OCIMF SIRE 2.0 7.5 사이버보안] [BIMCO 10.3 복구 계획] [BIMCO 10.4 데이터 복구 기능] [DCSA 2.4.3 구현] [DCSA 5.1.2 설명] [DCSA 5.1.3 구현]	
증적자료	백업 기록	
조치방법	**1. 백업 대상** ■ CBS(컴퓨터기반시스템) 및 네트워크 ■ OT 핵심 시스템 백업 • 항해 시스템: ECDIS로그, GPS 위치 데이터 매일 백업 • 통신 시스템: 위성 통신 로그, 무선 데이터 교환 기록 주간 백업 • 기계 시스템: 엔진 데이터(온도, 압력, 연료량 등) 자동 로그 저장 및 백업 • 화물 관리 시스템: 적재/하역 기록, 화물 상태 모니터링 데이터 백업 ■ 네트워크 장비(라우터, 스위치, 방화벽 등)의 설정 정보: • 라우터, 스위치, 방화벽 설정값 변경 시 즉시 백업 ■ 업무 데이터(문서, 로그, 기록 등): • 선상 보고 문서, 로그, 이메일 기록 등 주기적 백업 ■ 각 CBS(컴퓨터기반시스템)에서 생성되는 운영 데이터: • 사이버보안 장치(방화벽/IDS)에서 생성되는 보안 이벤트 기록 • 선상 보고 문서, 로그, 이메일 기록 등 주기적 백업	

통제항목	D.3.1 사이버 백업 관리	Optimized

2. 백업 방법

- 선박 내부 저장장치(NAS 등), 외장디스크와 같은 두 군데 이상의 매체로 백업 수행



[그림 97] 백업 방법 예시

- 중요 데이터(항해 로그, ECDIS 데이터, 엔진제어 설정 등)는 반드시 서비스 망과 분리하여 백업
- 백업 자료 선상과 육상에 분리 보관
- 시스템 수준 데이터(운영체제, 애플리케이션, 라이선스, 설정 등)와 사용자 수준 데이터(업무 파일, 로그, DB 등)를 구분하여 백업
- 백업 및 복구용 데이터베이스 환경 구성
- 백업 장치 파일은 암호화를 통해 승인된 인원만 열람하도록 제한

통제항목	D.3.1 사이버 백업 관리	Optimized

■ 랜섬웨어 대응을 위한 데이터백업 8대 보안수칙 적용

[그림 98] 랜섬웨어 대응을 위한 데이터백업 8대 보안수칙 이미지

출처: KISA, '2025년 상반기 사이버 위협 동향 보고서'

3. 백업 주기

자산의 중요도가 높은 자산일수록 더 빈번한 다중 위치 보관 백업을 수행해야합니다.

■ 백업 주기는 시스템의 중요도 및 복구 시나리오 따라 차등 설정

- 안전 운항에 필수적인 OT 시스템은 단기 주기(예: 일일 백업)로 관리
- 최소 주 1회 이상 전체 백업

■ 장기 보관 데이터는 주기적 무결성 검증 및 필요 시 폐기 및 정리(Clean-Up) 수행

비고	

통제항목	D.3.3 사이버 보험	Optimized
점검목적	사이버 사고 보험에 가입하여 사이버 사고로 인한 재무적 손실과 운영 중단 리스크를 최소화 합니다.	
점검내용	사이버 사고 보장이 되어있는 보험에 가입되어 있는지 확인하며, 사이버 사고 대응 준비를 증명할 수 있는 증적을 가지고 있는지 확인합니다.	
점검기준	**양호 :** 사이버 사고 보험에 가입한 경우 **취약 :** 사이버 사고 보험에 가입하지 않은 경우	
레퍼런스	BIMCO 10.6 사이버 사고로 인한 손실	
증적자료	선박 보험 가입증명서 사본, P&I보장 확인서	
조치방법	**1. 보험 가입증명서 확인** 보험가입증명서 피보험자 ABC Shipping Co. Ltd. 123 Maritime Ave., Seoul, Korea 선박정보 OCEAN EXPLORER IMO 9876543 Call Sign: D4EF7 보험정보 Marine Insurance Co. Tel. /-44 20 700 000 Cortificate Number INS-12345667 Protection & Indemnity 유효기간 2024년 1월 1일 2025년 1월 1일 약관 Bunker Convention 2001 보증 This certificate confirms that insurance or other financial security satisfying the requirements of Article 7 of the Bunker Convention 2001 is in force. 발급 기관 정보 서명 Marine Insurance Co. 2024년 1월 1일 [그림 99] 보험가입증명서 예시	

통제항목	D.3.3 사이버 보험	Optimized

2. 보험 보장 범위 내 사이버 사고 보장 포함 확인

(별지 제1호)

보험검사신청서

※ [ ]에는 해당되는 곳에 √표를 합니다.

접수번호	접수일자	처리기간

검사종류	[ ] 한국해운조합 P&I공제 Condition Survey [ ] 한국해운조합 P&I공제 Towing Survey [ ] 한국해운조합 P&I공제 Risk Survey [ ] 한국해운조합 선박공제 Condition Survey [ ] 한국해운조합 선박공제 Towing Survey [ ] 손해보험사 선박보험 Condition Survey [ ] 손해보험사 선박보험 Towing Survey [ ] KP&I P&I보험 Condition Survey [ ] 확인검사 [ ] 계선검사

소 유 자	성명(법인명)	생년월일 (법인등록번호)
	주 소 (Fax :)(전화번호)(전자우편 :)	
선 박	선박의 명칭	선박번호
	수검요청일자	수검장소
비 고		

위와 같이 선박의 보험검사를 받기 위해 신청합니다.

선 결	지사장		담당자		20 년 월 일
처리기한			접수구분		신청인 : (서명 또는 인)
수 수 료					
출장여비			합계 (부가세포함)		한국해양교통안전공단이사장 귀하

(주) 다음의 해당사항을 추가로 적으십시오.

선박내역	선 적 항		선 종	[ ]기선 [ ]범선 [ ]부선 [ ]그 밖의 선종
	선 질	[ ]강 [ ]목 [ ]FRP [ ]그 밖의 선질	선박의 용도	
	총 톤 수	톤	배의 길이	미터
	추진기관	[kW] [PS] [대]		

첨부서류	1. 선박국적증서(가 선박국적증서를 포함합니다) 2. 선박검사증서 3. 기타 필요하다고 인정하는 서류 4. 1 ~ 3. 에도 불구하고 외국으로부터 도입하는 선박에 대하여는 가선박국적증서, 선원명부 및 해기사면허 등에 관한 서류만을 확인할 수 있습니다.	수수료 한국해양교통안전공단의 수수료 기준에 따름

[그림 100] 보험검사신청서 사진

- 보험사/브로커와 보유 중인 보험 증권의 보장 범위에 실제로 사이버 사고가 포함되는지 사전 확인
- CL380, American Institute Cyber Exclusion Clause 등 사이버 배제 조항 적용 여부 확인
- 필요한 경우, 사이버 사고 보장 Buy-Back(재포함) 솔루션 검토 (추가 보험료 필요)
- 독립형 랜섬웨어 보험, 데이터 복구 비용 보장 상품 등 대체 보험 검토

3. 보험사 보장 심사 대비 사이버 리스크 관리 입증을 위한 증적 준비 권고

- 사이버 리스크 평가 보고서
- 사이버 사고 대응 계획(Cyber Response Plan)
- 사이버 인식 교육 이수 기록

통제항목	D.3.3 사이버 보험	Optimized
	4. P&I 클럽 관련 조치 권고 ■ P&I 클럽과 협의하여 사이버 사고 시 제3자 책임 보장 범위 확인 ■ 랜섬웨어 금전 손실, 데이터 복구 비용 등 비보장 영역 식별 ■ 전쟁 리스크 배제 조항(War Risk Exclusion) 적용 확인 P&I 가입신청서 1. 신청인 정보 회사명(Shipowner/Operator) : _____ 담당자 성명 / 연락처(전화·이메일) : _____ 2. 선박 정보 선명(Vessel Name) : _____ IMO 번호 : _____ 선박 종류 : _____ 총톤수(GT) : _____ 국적(Flag) : _____ 3. 운항 정보 주요 운항 구역 : _____ 4. 기존 보험 및 클레임 이력 기존 P&I 가입 여부 : □ 예 □ 아니오 최근 5년 내 사고/클레임 : _____ 5. 신청인 확인 본인은 위 기재 사항이 사실임을 확인하며 P&I 가입 심사에 필요한 정보 제공에 동의합니다. 신청인(서명) : _____ 날짜 : _____년 ___월 ___일 [그림 101] P&I 가입신청서 예시	
비고		

해운사 보안 요구사항
대응 가이드

5

결 론

5 결 론

5.1 요약

성숙도	참조문서	설명
Basic	IMO, SIRE 2.0, RIGHTSHIP	보안 목표를 달성하기 위해 구현되는 최소한의 보안 조치를 의미합니다. 조직은 기본적인 보안 활동을 수행합니다.
Advanced	IACS UR E26	식별된 표준과 모범 사례에 부합하는 보다 지속적인 보안 역량에 해당합니다. 조직은 정의된 목표와 운영 적합성에 따라 보안 체계를 구현, 관리, 모니터링합니다.
Optimized	BIMCO, DCSA	계획, 시험, 정책에 근거하고, 반복 가능한 활동 및 보안 역량에 해당합니다. 정기적인 감독과 검토를 받아 효과성을 확인하여, 지속적으로 보안 조치를 개선합니다.

Ⓐ 사이버보안 관리체계 → Ⓑ 사이버보안 통제 → Ⓒ 사이버 리스크 관리 → Ⓓ 사고대응

영역	상세
A. 사이버보안 관리체계	조직 전반의 보안 거버넌스를 정립하여 정책·조직·교육의 일관된 운영을 보장합니다. 경영진 승인과 정기 검토로 정책의 유효성을 확보하며, 전담 조직과 위원회 운영을 통해 의사결정과 책임 소재를 명확히 합니다. 역할기반 교육과 모의훈련을 통해 임직원과 선원의 보안 역량을 내재화하고, 결과 지표를 통해 효과성을 개선합니다.
A.1 사이버보안 정책	조직의 보안 목표, 범위, 준거 기준, 예외 처리, 검토 주기를 정의합니다. 정책은 상위 문서로서 각 절차 및 표준의 근거가 되며, 경영진 승인과 연 1회 이상 검토를 통해 최신성을 유지합니다. 임직원·협력사를 포함한 준수 대상과 위반 시 조치 기준을 명확히 합니다.
A.2 사이버보안 조직	조직 전반의 사이버 리스크 대응 능력이 강화되고, 책임성과 통제가 확보되어 보안 사고 발생 가능성이 감소하는 것을 목적으로 합니다.
A.2.2 사이버보안 외부업체 관리	외부 서비스 제공업체, 공급업체, 대리점 등과의 계약 및 협력 과정에서 사이버보안 요건이 반영되고 있는지를 확인하여, 외부업체의 보안 취약점이 선사의 IT·OT 시스템으로 전이되는 것을 예방하고, 공급망 전반의 보안 수준을 확보하는 것을 목적으로 합니다.
A.3 사이버보안 교육 및 훈련	직무·권한 수준에 따른 역할기반 커리큘럼을 운영하고, 피싱 모의훈련·테이블탑 연습을 포함합니다. 이수율, 평가 점수, 훈련 후 개선 조치 등 측정 가능한 KPI를 관리하여 교육의 실효성을 보장합니다.

Ⓐ 사이버보안 관리체계 Ⓑ 사이버보안 통제 Ⓒ 사이버 리스크 관리 Ⓓ 사고대응

영역	상세
B. 사이버보안 통제	자산·계정·네트워크·물리 영역에 걸친 실무 통제를 통해 IT/OT 위험 노출을 최소화합니다. 최신 인벤토리와 네트워크 구성도를 기반으로 접근 권한을 최소화하고, 세그멘테이션과 경계보호를 적용합니다. 이동식 매체와 중요 구역 출입을 관리하여 기술적·물리적 취약점을 동시 차단합니다.
B.1 사이버 자산 관리	전 자산의 식별·분류·중요도·소유자 정보를 관리하고, IP/VLAN·펌웨어 버전 등 운영 속성을 포함합니다. 네트워크 구성도와 1:1 매핑하여 변경관리와 감사 대응을 용이하게 합니다.
B.2 계정 관리	Join/Move/Leave(JML) 프로세스를 표준화하고 최소 권한·권한 검토·관리자 계정 분리를 시행합니다. 비정상 로그인과 특권 사용을 모니터링하며, 퇴사 시 계정과 접근 권한을 즉시 해지합니다.
B.3 네트워크 접근 통제	보안 존과 세그멘테이션, 방화벽·ACL·VPN·MFA를 적용하여 트래픽을 허용 기반으로 제한합니다. 외부 접점과 원격지원 경로를 명확히 문서화하고, NAC·IDS/IPS와 연동하여 비인가·비준수 단말을 차단합니다.
B.4 기기 및 출입 통제	이동식 매체의 승인·검사·로깅을 실시하고, 중요 설비실·브리지 등 물리 구역의 이중 인증·CCTV·로그 보존을 운영합니다. 반출입 절차와 자산 대장을 연계하여 무단 반출 위험을 통제합니다.

Ⓐ 사이버보안 관리체계 Ⓑ 사이버보안 통제 Ⓒ 사이버 리스크 관리 Ⓓ 사고대응

영역	상세
C. 사이버 리스크 관리	취약점·위협·리스크를 체계적으로 식별·평가하고, 우선순위에 따른 조치와 복원력 점검으로 잔여위험을 관리합니다. 정기 스캔과 패치, 시나리오 기반 평가·훈련을 통해 실제 운영 환경의 회복탄력성을 검증합니다.
C.1 사이버 취약점 진단	EDR/AV 탐지, 구성 점검, 주기 스캔을 통해 취약점을 발견하고 SLA에 따라 조치합니다. 패치 창구와 롤백 계획을 마련하여 가용성과 보안을 균형 있게 유지합니다.
C.2 사이버 리스크 평가	자산 중요도·위협·가능도/영향 기반의 매트릭스로 정량·정성 평가를 수행합니다. 잔여리스크에 대해 경영 승인과 수용 근거를 문서화하고, 외부 감사·심사에 대비합니다.
C.3 사이버 리스크 조치 계획	저감·회피·전가·수용의 전략을 선택하고 일정·예산·책임을 명확히 합니다. 대시보드로 이행 상황을 추적하여 마감 준수율과 위험 감소 추세를 관리합니다.
C.4 사이버 복원력 검사	테이블탑·페일오버·침투 모의 등 다양한 훈련을 통해 탐지·전환·복구 절차의 실행력을 검증합니다. 교훈 학습(LL)을 문서·구성에 반영하여 지속적 개선을 추진합니다.

Ⓐ 사이버보안 관리체계 | Ⓑ 사이버보안 통제 | Ⓒ 사이버 리스크 관리 | Ⓓ 사고대응

영역	상세
D. 사이버 사고대응	조기 탐지, 신속 대응, 안정적 복구를 목표로 모니터링·IR·백업·보험 체계를 통합합니다. 네트워크·위협 가시화를 기반으로 경보 우선순위를 최적화하고, 표준 대응 절차와 온콜 조직을 통해 중단 시간을 최소화합니다. 백업·복구 시험과 보험 체계를 통해 재무·운영 리스크를 동시에 완화합니다.
D.1 사이버보안 모니터링	네트워크 가용성과 이상 트래픽, SIEM/IDS/EDR 경보를 상관 분석하여 탐지 품질을 높입니다. 우선순위 기준과 MTTR 목표를 운영하여 대응 효율을 관리합니다.
D.2 사이버 사고 대응 계획	탐지-분류-격리-조치-보고-복구의 플레이북을 표준화하고, 구조적 커뮤니케이션 라인을 유지합니다. 비상 연락망과 권한 위임 체계를 검증하여 24×7 대응 역량을 확보합니다.
D.3 사이버 복구 계획	RTO/RPO 기준과 우선순위 복구 절차를 정의하고, 주기적인 복원 테스트로 실효성을 검증합니다. 3-2-1 원칙·오프라인/불변 백업을 적용하며, 보험 담보 범위와 통지 절차를 명확히 합니다.

5.2 기대효과

① 다양하고 복잡한 해사 사이버보안 규제 및 가이드를 통합함으로서 해운사는 국제 사이버보안 요구사항에 효과적으로 대응할 수 있는 사이버보안 관리체계를 수립할 수 있고, 관리체계의 유지와 개선을 통해 기본적인 사이버보안 수준을 확보할 수 있습니다.

② 해운사 및 선박 담당자에 사이버보안 업무를 할당하고 이에 대한 성과를 평가할 때 활용될 수 있고, 채용시에도 어떠한 사이버보안 역량이 필요한지 참고할 수 있습니다.

③ 사이버보안 담당자 및 선원을 대상으로 사이버보안 개념 및 실무에 필요한 교육을 수행하는데 활용될 수 있고, 이를 통해 사이버보안에 대한 인식제고와 사이버 사고에 대한 초동조치를 효과적으로 수행할 수 있습니다.

④ 통제 항목을 Basic에서 Advanced, Optimized로 단계별 적용함으로써 조직은 자원을 효율적으로 활용하면서 점진적으로 보안 성숙도를 향상시켜 사이버 복원력과 규제 대응력을 강화할 수 있습니다.

6

용 어

과학기술정보통신부
KISA 한국인터넷진흥원
KR KOREAN REGISTER

6 용 어

A

- APT (Advanced Persistent Threat, 지능형 지속 위협): 특정 조직·기관·기업·국가를 목표로 오랜 기간 은밀히 침투해 지속적으로 공격을 이어가는 고도화된 사이버 공격
- ARP (Address Resolution Protocol): 네트워크 계층(IP 주소)와 데이터링크 계층(MAC 주소)을 연결하기 위해 사용되는 TCP/IP 프로토콜

C

- CAT I: 고장이 인명안전, 선박안전 및/또는 환경에 위협이 되는 위험한 상황으로 귀결되지 않는 시스템
- CAT II: 고장이 인명안전, 선박안전 및/또는 환경에 위협이 되는 위험한 상황으로 궁극적으로 귀결될 수 있는 시스템
- CAT III: 고장이 인명안전, 선박안전 및/또는 환경에 위협이 되는 위험하거나 치명적인 상황으로 즉시 귀결될 수 있는 시스템
- CBS (Computer Based System, 컴퓨터기반시스템): 정보의 수집·처리·유지보수·사용·공유·배포·폐기 등 하나 이상의 지정된 목적을 달성하기 위해 구성된 프로그래머블 전자 장치 또는 상호 운용 가능한 프로그래머블 전자 장치 집합. 선내 CBS(컴퓨터기반시스템)에는 IT 및 OT 시스템이 포함되며, 네트워크를 통해 연결된 하위 시스템의 조합일 수 있음, 또한 선내 CBS(컴퓨터기반시스템)는 직접 연결하거나 공용 통신 수단(예: 인터넷)을 통해 육상 CBS(컴퓨터기반시스템), 다른 선박의 CBS(컴퓨터기반시스템) 및 기타 시설과 연결될 수 있는 시스템.
- CCSO (Company Cyber Security Officer): 선사 사이버보안 책임자
- CSA (Cyber Security Assessment): 조직이나 선박의 정보 운영 기술 환경을 대상으로 사이버 위협과 취약점을 평가하고, 리스크 완화를 위한 개선 대책을 마련하는 사이버보안 평가 절차
- CySO (Cyber Security Officer): 사이버보안 책임자

D

- DNS (Domain Name System): 사용자에게 친숙한 도메인 이름(예: www.naver.com)을 컴퓨터가 네트워크에서 서로를 식별하는데 사용하는 인터넷 프로토콜(IP) 주소로 변환하는 인터넷 표준 프로토콜
- DNS Relay 설정 조작: 올바른 DNS 서버 대신 공격자가 만든 가짜 DNS 서버로 요청이 전달되어, 피싱 사이트 접속 유도, 개인정보 탈취 등이 발생
- DOC (Document Of Compliance, 안전관리적합증서): ISM Code의 요건에 적합한 사업장에 발급하는 문서를 의미
- DPA (Designated Person Ashore, 지정 육상 담당자): 각 선박의 안전운항을 보장하고 사업장과 선박직원 간의 연계를 확보하기 위하여 최고경영자에게 직접 보고할 수 있는 자

E

- ETC (Estimated Time of Completion): 선박의 하역, 정비, 수리 등 특정 작업·공정이 완료될 것으로 예상되는 시간을 나타내는 표준 해운 약어

F

- Firewall – 방화벽: 미리 정의된 보안 규칙에 기반한, 들어오고 나가는 네트워크 트래픽을 모니터링하고 제어하는 네트워크 보안 시스템
- Firmware – 펌웨어: 하드웨어 장치의 기본적인 구동 및 제어를 담당하는 소프트웨어
- Forensic – 포렌식: 증거로 사용될 수 있도록 과학적인 방법으로 데이터를 수집·분석·보존하는 조사 기법

G

- GDPR (General Data Protection Regulation – 일반 데이터 보호 규정): 유럽 연합(EU)의 법률로, 자연인(Natural person)에 관한 기본권과 자유(특히 개인정보보호에 대한 권리)를 보호하고, EU 역내에서 개인정보의 자유로운 이동을 보장

H

- Hooking – 후킹: 각종 소프트웨어 구성 요소 간에 발생하는 함수 호출, 메시지 등을 중간에서 가로채는 명령, 방법, 기술이나 행위
- HTTP (HyperText Transfer Protocol – 하이퍼텍스트 전송 프로토콜): 웹 브라우저와 웹 서버가 데이터를 주고받기 위해 사용하는 통신 규약
- HTTPS (Hypertext Transfer Protocol Secure): 웹 브라우저와 웹 서버 간의 통신을 암호화하여 안전한 연결을 제공하는 프로토콜

I

- IAS (Integtatred Automation System – 통합 자동화 시스템): 선박 설비에서 사용되는 통합 제어 및 감시 시스템
- IDS (Intrusion Detection System – 침입탐지시스템): 네트워크나 시스템에서 발생하는 비정상적인 활동, 악의적인 공격, 보안 정책 위반 등을 탐지하고 관리자에게 경고
- IPS (Intrusion Prevention System – 침입방지시스템): IDS와 마찬가지로 위협을 탐지하며, 더 나아가 탐지된 위협을 실시간으로 차단하고 방어하는 능동적인 역할 수행
- ISM Code (International Safety Management Code – 국제안전관리규약): 국제해사기구(IMO)에서 선박의 안전운항과 환경보호를 위해 총회결의 741호로 채택된 규약
- ISPS Code (International Ship and Port Facility Security Code – 2002년 12월 12일 1974 SOLAS 협약의 당사국 정부회의에서 결의서 2호로 채택한 A편(강제사항)과 B편(권고사항)으로 구성된 선박과 항만시설의 보안을 위한 국제 규칙을 말하며 향후 개정 가능
- IT(Information Technology – 정보기술): 정보를 생성, 저장, 전송, 처리, 관리하는 데 사용되는 모든 기술과 시스템(물류·보고 시스템, 데이터베이스 시스템)

L

- LNK (악성 LNK): 바로가기 파일을 위장해 사용자가 무심코 실행하도록 유도하는 공격 기법

M

- MITM (Man-in-the-Middle, 중간자 공격): 해커가 사용자와 웹 애플리케이션과 같은 두 온라인 대상 간의 통신을 도청하여 민감한 정보를 훔치는 사이버 공격
- Modbus: 주로 PLC, 센서, 계측기, 제어 장치 등과 데이터를 주고받는 통신 프로토콜(규약)

N

- NAC (Network Access Control – 네트워크 접근 제어): 인증된 사용자와 장치만 네트워크에 접근하도록 제어하여 네트워크 보안을 강화하는 시스템
- 망분리: 회사 업무를 볼 수 있는 업무망과 인터넷에 접속할 수 있는 인터넷망을 분리

O

- Onboard Network – 선상 네트워크: 선박에 설치된 각종 IT와 OT를 연결해주는 네트워크 인프라
- OT (Operational Technology – 운영기술): 물리적인 프로세스나 장비를 제어하고 모니터링하기 위해 사용되는 하드웨어 및 소프트웨어(ECDIS, 발전기, 밸브)

P

- Phishing – 피싱: 개인정보(Private data)를 낚는다(Fishing)라는 의미의 합성어로 전기통신수단을 이용해 이용자의 개인정보나 금융정보를 빼낸 후, 타인의 재산을 갈취하는 사기 수법
- Pivoting – 피보팅: 공격자가 침해한 한 지점을 발판으로 삼아 내부망의 다른 시스템으로 이동하는 기술
- PLC (Programmable Logic Controller): 자동화 시스템에서 사용되는 컴퓨터 기반의 전자장치, 산업용 컴퓨터

R

- RCA (Root Cause Analysis – 근본 원인 분석): 문제 또는 사건이 발생한 후 근본 원인을 확인하는 품질 관리 프로세스
- Read Holding Registers: 장치(센서, PLC) 내부에 있는 Holding Register라는 메모리 공간을 읽어오는 기능. 이 레지스터에는 보통 센서값(온도, 압력, 속도 등), 상태 정보, 제어 파라미터가 저장
- Risk – 리스크: 예상되는 위협에 의하여 자산에 발생할 가능성이 있는 손실의 기대치
- Router – 라우터: 네트워크와 네트워크 간의 경로(Route)를 설정하고 가장 빠른 길로 트래픽을 이끌어 주는 네트워크 장비
- RPO (Recovery Point Objective – 복구 시점 목표): 장애 발생 시 비즈니스 연속을 위해 어느 시점으로 백업할 지 결정하게 될 지표
- RTO (Recovery Time Objective – 목표 복구 시간): 장애 발생 시 시스템을 원 상태로 복원하는데 소요되는 시간

S

- SCSO (Ship Cyber Security Officer): 선박 사이버보안 책임자(선장)
- SIEM (Security Information and Event Management – 보안 정보 및 이벤트 관리): 잠재적인 보안 위협과 취약성이 비즈니스 운영을 침해하기 전에 이를 인식하고 해결하는데 도움을 주는 보안 솔루션
- SMC (Safety Management Certificate – 선박안전관리증서): 사업장과 선박이 승인된 안전관리체제에 따라 운영되고 있음이 증명된 선박에 발급하는 문서
- SMS (Safety Management System – 안전관리시스템): 사업장의 구성원들이 사업장의 안전과 환경보호 정책을 효과적으로 수행할 수 있도록 구성화되고 문서화된 체제
- SSH (Secure Shell): 원격 컴퓨터에 안전하게 접속하고 관리하기 위한 암호화된 네트워크 프로토콜
- SSP (Ship Security Plan – 선박보안계획서): 선박 보안관련 업무에 대한 절차서. 파트A와 B 두개로 나뉘어져 있으며, B는 기밀문서 이므로 SSO의 허가 없이 공개 불가

S

- STCW 협약: 국제해사기구(IMO)가 제정한 협약으로, 선원의 교육(Training), 자격증명(Certification), 당직근무(Watchkeeping) 기준을 국제적으로 통일하여 해상 안전과 해양 환경 보호를 보장하는 국제 조약
- Switch – 스위치: 컴퓨터와 같은 2개 이상의 IT디바이스가 서로 통신하도록 허용하는 장비
- SYBAss (Superyacht Builders Association): 세계적인 슈퍼요트 건조 조선소들이 회원으로 참여하여, 대형 요트의 건조 산업을 대표하고, 규제·기술·품질·지속가능성 관련 표준과 정책을 국제 무대에서 조율·개선하기 위해 설립된 비영리 산업 협회
- Shodan – 쇼단: 인터넷에 연결된 서버, 네트워크 장비, 산업제어시스템(ICS), IoT 기기 등 네트워크에 노출된 장치와 서비스를 검색·수집·분석하는 전문 검색 엔진

T

- TCP (Transmission Control Protocol – 전송 제어 프로토콜): 데이터가 손실 없이, 순서대로, 정확히 전달되도록 보장하는 기능
- Telnet: 네트워크 상에서 다른 컴퓨터에 원격 로그인하거나 원격으로 명령을 실행하기 위한 프로토콜
- Threat – 위협: 자산에 손실을 발생시키는 원인이나 행위
- TLS (Transport Layer Security – 전송 계층 보안): 온라인 통신을 암호화하여 데이터의 무결성을 보장하는 보안 프로토콜

V

- VLAN (Virtual LAN – 가상랜): 물리적인 네트워크를 논리적으로 구분지어 분할한 네트워크
- VPN (Virtual Private Network – 가상사설망): 공중 네트워크를 통해 회사나 단체가 내용을 바깥 사람에게 드러내지 않고 통신할 목적으로 쓰이는 사설 통신망
- Vulnerability – 취약점: 위협에 의하여 손실이 발생하게 되는 자산의 약점

W

- Winsock DLL (Windows Sockets Dynamic Link Library): Windows에서 네트워크 통신을 담당하는 핵심 라이브러리
- WSC (World Shipping Council): 세계 컨테이너 해운사를 대표하여 정책·규제·환경·보안과 관련된 국제 이슈를 다루는 비영리 해운 산업 협회

해운사 보안 요구사항
대응 가이드

7

부 록

과학기술정보통신부
KISA 한국인터넷진흥원
KR KOREAN REGISTER

7 부 록

1. 해운사 사이버보안 체크리스트

해운사 보안 요구사항 대응 가이드 점검 체크리스트											
				점검 일시		점검자		결재	기안	실의	결정
									/	/	/
분류	코드	성숙도	점검항목	점검내용						점검결과	증적자료
A. 사이버 보안 관리체계	A.1.1	B	사이버보안 정책	사이버보안 정책이 SMS(안전관리시스템)에 반영되어 있습니까?							
	A.2.1	B	사이버보안 조직	사이버보안 조직의 역할과 책임이 정의되어 있습니까?							
	A.2.2	A	사이버보안 외부업체 관리	작성된 외부 업체 보안 서약서가 있습니까?							
	A.3.1	B	사이버보안 교육 및 훈련	사이버보안 교육과 훈련을 매년 각 1회 이상 실시하고 있습니까?							
B. 사이버 보안 통제	B.1.1	B	사이버 자산 목록	선박 내 모든 사이버 자산 목록을 최신 버전으로 문서화하여 관리하고 있습니까?							
	B.1.2	A	네트워크 구성도	네트워크 연결 구성도를 최신 버전으로 관리하고 있습니까?							
	B.1.3	A	사이버 자산 변경관리	사이버 자산 목록 변경 이력을 기록하고 있습니까?							
	B.2.1	B	계정 및 권한 관리	사용자 계정이 절차에 따라 생성, 삭제되고 있습니까?							
	B.2.2	B	비밀번호 관리	복잡한 비밀번호 규칙을 사용하고 있습니까?							
	B.3.1	O	네트워크 분리	보안구역별 네트워크 분리 구성도가 존재하고 있습니까?							
	B.3.2	A	네트워크 접근 통제	주요 시스템에 대한 네트워크 접근 통제가 이루어지고 있습니까?							
	B.4.1	B	기기 반출입 통제	이동식 매체 사용의 통제가 이루어지고 있습니까?							
	B.4.2	A	인원 출입 통제	제한구역에 대한 물리적 접근이 승인된 절차에 따라 관리되고 있습니까?							
C. 사이버 리스크 관리	C.1.1	B	악성코드 방지	최신 악성코드 방지 소프트웨어가 설치되어 있습니까?							
	C.1.2	B	패치 관리	적절한 승인 절차에 따라 최신 패치가 적용 되어있습니까?							
	C.1.3	A	보안설정 점검 및 모의해킹	주요 자산에 대한 취약점 점검이 정기적으로 이루어지고 있습니까?							
	C.2.1	B	사이버 영향도 평가	영향도 평가를 진행하고 있습니까?							
	C.2.2	B	사이버 발생빈도 평가	발생빈도를 평가하고 있습니까?							
	C.2.3	B	사이버 리스크 평가	연 1회 이상 리스크 평가를 수행하고 있습니까?							
	C.2.4	O	사이버 리스크 평가 예외	리스크 평가 예외 시 허용 가능한 리스크 수준입니까?							
	C.3.1	B	사이버 리스크 조치 계획	리스크 관리 체계가 이행되어 리스크 감소가 이루어지고 있습니까?							
	C.4.1	O	사이버 복원력 검사	사이버 복원력 검사 절차를 주기적으로 관리하고 있습니까?							
D. 사이버 사고 대응	D.1.1	A	네트워크 운영 모니터링	침입 탐지 및 모니터링 체계가 구축되어 있습니까?							
	D.1.2	O	사이버 위협 모니터링	네트워크 운영 모니터링이 실시간으로 운영되고 있습니까?							
	D.2.1	B	사이버 사고 대응 절차	사고 대응 절차가 수립되어 있습니까?							
	D.3.1	O	사이버 백업 관리	데이터가 백업되어 있습니까?							
	D.3.2	B	사이버 복구 계획	필수 시스템에 대한 사이버 복구 계획이 관리되고 있습니까?							
	D.3.3	O	사이버 보험	사이버 사고 보험에 가입되어 있습니까?							

2. 사이버 사고 사례

“
사이버사고 발생하면
PC를 사용하지 못하는 것인가?
PC없어도 괜찮은데?
”

“
하지만 PC에 발생한 피해가
ECDIS에 전파된다면?
잘못 된 위치로 좌초 된다면?
”

선박사고예상피해

✓ 매출 손실 ✓ 선체 손실 ✓ 화물 손실 ✓ 인명 피해 ✓ 환경 오염

국가 재난 급 피해

천문학적 경제손실

선박 대상			
DNW, 선박관리 시스템	랜섬웨어	고객사 70곳, 선박 100척 영향	2023.01
영국 구축함	AIS 스푸핑	외교문제 유발	2021.06
현대 글로비스 자동차 운반선	랜섬웨어	내부 시스템 삭제	2019.03
미국 이지스함	사이버 공격	선박충돌	2017.08
선사 대상			
Voyager Worldwide (싱가포르)	랜섬웨어	IT 시스템 중단	2022.12
HMM (대한민국)	바이러스	이메일 중단	2021.06
COSCO (중국)	해킹공격	IT시스템 중단	2020.03
Maersk (덴마크)	랜섬웨어	3주간 시스템 마비, 약 3000억 손실	2017.06
항만 대상			
시애틀 항구	데이터 유출	운영 중단	2024.08
호주_DP월드	사이버 공격	운영 중단	2023.11
Lisbon 항구	랜섬웨어	기밀정보 유출	2022.12
이란 샤히드항	이스라엘 공격	항만시스템 중단(수일간)	2020.05

출처: 데일리시큐. “선박 ICT 공급망 사이버 공격 위협 증가”

'17년 6월 세계 최대 해운회사 AP 묄러-머스크(AP Møller-Maersk) 랜섬웨어감염

- 세계적으로 창궐한 악성 프로그램(Malware) 낫페트야(NotPetya)에 감염되어 우리 돈 **2272억~3400억**규모의 피해가 발생함
- 낫페트야는 머스크의 우크라이나 지사에서 세금 환급에 쓰는 회계 프로그램인 미독(MEDoc)을 통해 퍼졌는데, 미독의 자동 업데이트 기능에 사용자의 네트워크에 몰래 들어갈 수 있는 백도어가 있었고 이를 통해 내부 네트워크에 접속된 컴퓨터가 악성 프로그램을 내려받게함

- 머스크는범죄 조직이 요구한 돈을 지불하지 않고 **45,000대의 PC**와 **4,000대 규모의 서버**를 **재설치** 했으며 머스크해운 관련 계열사 세 곳을 포함하여 시스템 안정화 작업을 하여 서비스를 원상복구 하는 한편 보안 대책도 강화함
- 머스크는 "낫페트야는 전례가 없던 악성 프로그램 종류"라며 윈도우 시스템과 바이러스 백신 업데이트와 패치 모두 이번 사태는 예방할 수 없었다며 이와 같은 사태를 예방하기 위해 내부 시스템을 계속 재검증하는 한편 추가 예방 조치를 도입했다고 밝힘

출처: NAKED DENMARK. 머스크 "해킹으로 최대 3400억 손해 봐"

선박 랜섬웨어 사고 사례

'19년 3월 29일 현대 글로비스자동차운반선 수척 랜섬웨어피해

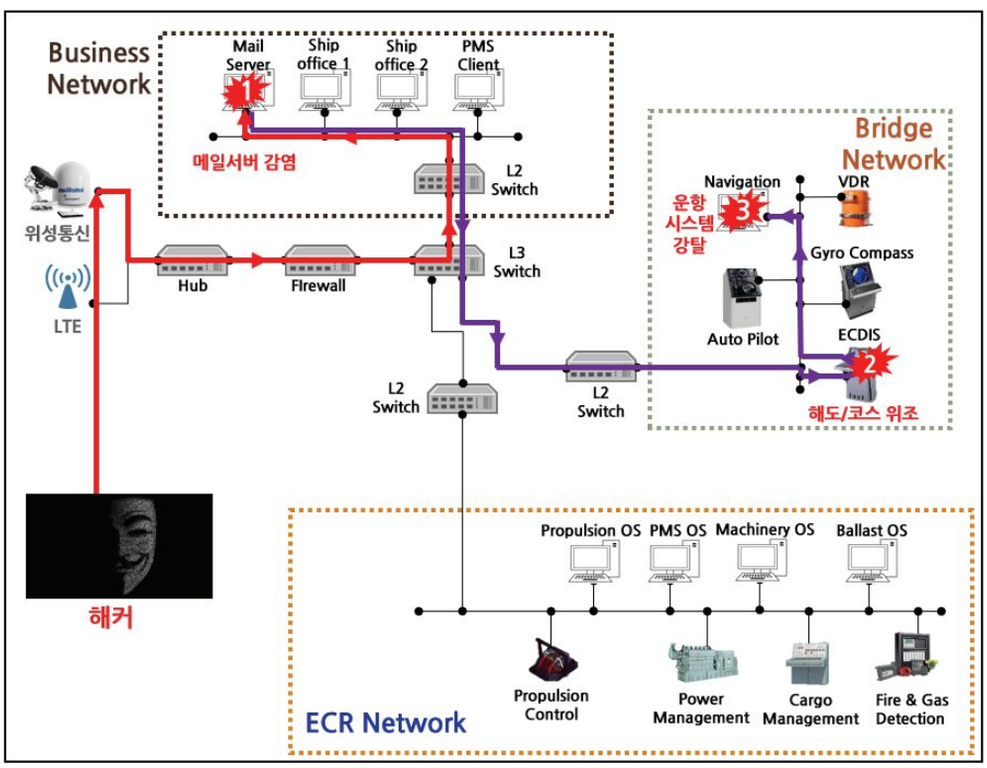
- 현대 글로비스선단 소속 일부 선박이 랜섬웨어에 감염돼 선내 메인 컴퓨터가 잠기는 피해가 발생함
- 감염된 컴퓨터는 파일복원이 불가능해 포맷 후 업무에 필요한 서류를 새로 만들어야 하는상태로 파악됐으며 배포된 메일은 경찰청을 사칭하여 첨부된 파일을 받아 열면 감염이 진행되는 것으로 확인됨

대응 및 향후 전망

- 감염된 선박들은 해당 컴퓨터를 포맷하고 손실된 자료를 다시 만들고 있는 것으로 알려졌으나 인터넷에 접속된 메인 컴퓨터에는 선박이 입항할 해당국가 관청과 오가는 수속서류를 포함, 운항에 필요한 각종 자료가 들어있어 손실이 적지만은 않을 것으로 확인됨
- 현대 글로비스는 수일이 지나도록 피해 현황을 확인하지 못함

출처: 파이낸셜뉴스. "한국 유명선사 선박 수척 랜섬웨어 피해…사이버보안 경각심 가져야"

선박 사이버공격 시나리오



선박 GPS스푸핑 사고 사례

'17년 6월 22일 "20척 이상 선박의 GPS가 내륙 공항으로 오인 위치 표시"

- 흑해에서 최소 20척 이상의 선박이 내륙 공항으로 위치가 이동한 것처럼 표시됨
- 한 탱커선은 실제 해상 위치에서 약 25~30마일 떨어진 공항으로 표시되어, 전문가들은 단순 오작동이 아닌 의도적인 GPS 스푸핑공격으로 판단함
- 선박 항행 오류, AIS오류, '유령 선박' 표시 등 피해가 일어남

대응 및 향후 전망

- 미국 해사청은 GPS 간섭 주의보를 발령해 선박들에게 경계할 것을 요청함
- GPS 의존 위험성을 제기하여 보완 대책을 검토하도록 권고
- 항해 다중 신호 수신기, 관성항법시스템, 레이더 기반 보조 시스템 등을 활용

출처: CISOMAG. "BlackSea incident: New frontier in cyberwarfare
출처: maritime administration. "2017-005A-Black Sea-GPS Interference

항만 해킹사례

'23년 7월 4일 "일본 나고야항 해킹 공격 받아 컨테이너 하역 중단"

- 일본 나고야항 컨테이너 하역과 운반을 관리하는 전산 시스템에 장애가 발생 확인결과 랜섬웨어에 감염됨
- 컨테이너 하역이 약 이틀 반 동안 중단되어 약 15,000개 컨테이너 이동이 지연, 항만 내 트레일러 정체 발생
- 나고야항은 일본 전체 무역량의 약 10%를 담당하여 주요 수출입 연계 기업들(Toyota 등)도 일시적 작업 차질
- 일본 내 첫 "국가 기간 항만 마비 사이버 공격"으로 분류

- 랜섬메시지가 프린터로 출력되었으며, 공격자(러시아계 랜섬웨어조직 LockBit)는 금전을 요구 했으나 항만측은 비용을 지급하지 않음
- 백업 데이터 활용 및 시스템 정비를 통해 7월 6일 오후부터 정상 운영 시작
- 국토교통성은 항만 터미널 정보 보안 강화 검토를 위한 정보보안대책 검토위원회를 구성

출처: ZDNET Korea. "日최대 항만 나고야항, 랜섬웨어공격으로 마비"
출처: KBS뉴스. "일본 나고야항 해킹 공격 받아 컨테이너 하역 중단"

3. 레퍼런스 상세

통제항목 상세 – Basic

A. 사이버보안 관리체계

A.1 사이버보안 정책

통제항목	A.1.1 사이버보안 정책		Basic
레퍼런스 상세	IMO	사이버 리스크 관리 전략, 기대사항 및 정책을 수립·모니터링합니다. 인력의 역할과 책임을 정의합니다. 백업 관리, 재해 복구, 위기 관리 등 비즈니스 연속성을 보장합니다. **[IMO 3.5.1 거버넌스(Govern)]** 식별된 중요 시스템 및 자산에 대한 소프트웨어·하드웨어 공급망 보안 통제 정책을 수립합니다. **[IMO 3.5.3.8 보호(protect)]** 감사와 같은 사이버 리스크 관리 조치의 효과를 평가하고, 이러한 조치를 정기적으로 검토하고 업데이트하기 위한 정책과 절차를 수립합니다. **[IMO 3.5.3.9 보호(protect)]**	
	IACS UR E26	공격자는 선박 내, 회사 내부, 또는 인터넷을 통한 원격 연결을 이용하여 선박의 시스템 및 데이터에 접근을 시도할 수 있습니다. 따라서 사이버 자산, 네트워크 등에 대한 물리적 및 논리적 접근 제어는 선박 및 화물의 안전을 보장하기 위해 구현되어야 합니다. 물리적 위협과 이에 대한 대응 조치는 ISPS 코드에서 고려됩니다. 유사하게, ISM 코드에서는 선박의 안전 운항과 환경 보호를 위한 지침을 제공합니다. ISPS 및 ISM 코드의 이행은 Ship Security Plan (SSP) 및 Safety Management System (SMS)에 접근 제어에 대한 지침과 절차를 포함하도록 요구할 수 있습니다. **[UR E26 4.2.4.2 타당성]**	
	OCIMF SIRE 2.0	7.5. 사이버 보안 (Cyber Security) 7.5.1. 선장과 선원이 회사의 사이버 보안 리스크 관리 절차에 익숙하며, 이 절차들이 완전히 이행되었습니까? 짧은 질문 텍스트 사이버 보안 리스크 관리. 적용 선종 유조선, 케미컬, LPG, LNG ROVIQ 순서 문서, 브리지, 화물 제어실, 기관 제어실 출판물 ■ OCIMF/ICS: International Safety Guide for Oil Tankers and Terminals. Sixth Edition.	

통제항목	A.1.1 사이버보안 정책	Basic

- IMO: ISM Code
- IMO: MSC-FAL.1/Circ.3 Guidelines on maritime cyber risk management
- Industry: The Guidelines on Cyber Security Onboard Ships Version 4
- IMO: Resolution MSC.428(98) Maritime cyber risk management in safety management systems

목적
사이버 사고에 대비하고 운영의 연속성을 보장하기 위하여, 선박이 효과적인 기술적·절차적 보호조치를 마련하고 있는지를 확인합니다.

산업 지침
OCIMF/ICS: International Safety Guide for Oil Tankers and Terminals. Sixth Edition

6.4 사이버 안전 및 보안
사이버 보안은 정보기술(IT), 운영기술(OT), 정보 및 데이터를 무단 접근, 조작, 방해로부터 보호하는 것과 관련이 있습니다. 사이버 안전은 중요 데이터 및 OT의 가용성 또는 무결성 상실에 대한 리스크를 다룹니다.

IMO: MSC-FAL.1/Circ.3 해상 사이버 리스크 관리 지침
[OCIMF SIRE 2.0 7.5 사이버보안]

2.1.2
정보기술 시스템과 운영기술 시스템의 구분을 고려해야 합니다.
정보기술 시스템은 데이터를 정보로 사용하는 것에 초점을 둔다고 볼 수 있습니다.
운영기술 시스템은 물리적 프로세스를 제어하거나 모니터링하기 위해 데이터를 사용하는 것에 초점을 둔다고 볼 수 있습니다.
또한, 이러한 시스템 간 정보와 데이터 교환의 보호도 고려해야 합니다.
산업: The Guidelines on Cyber Security Onboard Ships Version 4

1.1 해운 산업의 사이버 보안 특성
…사이버 리스크 관리는 다음을 수행해야 합니다:
- 사용자, 핵심 인력, 육상 및 선상 경영진의 역할과 책임을 식별할 것.
- 교란 시 선박의 운영과 안전에 리스크를 초래할 수 있는 시스템, 자산, 데이터 및 역량을 식별할 것.
- 사이버 사고에 대비하여 기술적·절차적 보호조치를 이행하고, 사고의 신속한 탐지 및 운영의 연속성을 보장할 것.
- 정기적으로 시행되는 비상계획(contingency plan)을 마련할 것.

TMSA KPI 13.1.2
회사는 선박의 항해 구역 및 육상 기반 위치에 적용되는 보안 위협을 식별하기 위한 문서화된 절차를 마련해야 합니다. 보안 위협에는 다음이 포함될 수 있습니다:
사이버 위협
식별된 위협은 상황 변화에 따라 필요 시 검토되어야 합니다.

통제항목	A.1.1 사이버보안 정책	Basic

	IMO: ISM Code 8.1 회사는 잠재적인 비상 선내 상황을 식별, 설명 및 대응하기 위한 절차를 수립해야 합니다. IMO: Resolution MSC.428(98) 안전관리시스템 내 해상 사이버 리스크 관리 해사안전위원회(The Maritime Safety Committee)는, 1. 승인된 안전관리시스템은 ISM Code의 목적과 기능적 요건에 따라 사이버 리스크 관리를 고려해야 한다는 것을 확인합니다. 2. 행정당국은 사이버 리스크가 안전관리시스템 내에서 적절하게 다루어지도록 보장해야 하며, 이는 2021년 1월 1일 이후 최초의 회사 적합성 증서(DOC) 유효성 검증 시점까지 이루어져야 함을 권고합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]** 선박 보안 계획은 기국(flag state)의 승인을 받아야 하며, 선장이 선박 보안 계획 및 기타 보안 관련 계획이 기밀이라고 통보한 경우, 검사관은 전면 표지를 확인하여 존재 여부만 확인해야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]**
RIGHTS HIP	사이버보안 정책 및 절차가 SMS(안전관리시스템)에 통합되어 있으며, 사이버보안 관리 시스템이 평가 및 인증되었습니까? **[RIGHTSHIP 12.7]** 회사의 2021년 1월 1일 이후 최초의 DOC 연례 검증 시점까지 선박의 SMS(안전관리시스템)에 사이버보안 관리가 포함되지 않은 경우, 해당 사실을 기록합니다. 사이버보안 관리는 다음을 수행하여야 합니다. • 육상 및 선상에서 사용자, 핵심 인력 및 경영진의 역할과 책임을 식별합니다. • 선박의 운영 및 안전에 리스크를 초래할 수 있는 시스템, 자산, 데이터 및 기능을 식별합니다. • 사이버 사고를 방지하고 운영의 연속성을 보장하기 위해 보호하는 기술적 조치를 구현합니다. 여기에는 네트워크 구성, 네트워크 및 시스템에 대한 접근 통제, 통신 및 경계 방어, 보호 및 탐지 소프트웨어 사용이 포함될 수 있습니다. • 사이버 사고에 대한 회복력을 제공하기 위한 절차적 보호 조치를 포함한 활동 및 계획을 구현합니다. 여기에는 교육 및 인식, 소프트웨어 유지보수, 원격 및 로컬 접근, 접근 권한, 이동식 미디어 및 장비 폐기 관리가 포함될 수 있습니다. • 사이버 사고에 대비하고 대응하기 위한 활동을 수행합니다. (The Guidelines on Cyber Onboard Ships, 2017) **[RIGHTSHIP 12.7]** IMO는 회원국 정부 및 기국 행정기관의 요구사항과 함께, 관련 국제 및 산업 표준과 모범 사례를 참조할 것을 해운업계에 권고하였습니다. 이는 사이버 리스크 관리에 대한 세부 지침을 제공하기 위함입니다. 추가적인 지침 및 표준에는 다음이 포함되나, 이에 제한되지 않습니다. 1. ICS, IUMI, BIMCO, OCIMF, INTERTANKO, INTERCARGO, InterManager, WSC, SYBAss가 제작·지원한 The Guidelines on Cyber

통제항목	A.1.1 사이버보안 정책	Basic

	Onboard Ships 2. Consolidated IACS Recommendation on cyber resilience(Rec 166) 3. ISO/IEC 27001 standard on information technology – Security techniques –Informaion security management systems – Requirement. 국제표준화기구(ISO)와 국제전기기술위원회(IEC)가 공동 출판 4. United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity(the Nist Framework) 참고문헌은 항상 가장 최신 버전을 사용하여야 합니다. (추가 지침 및 표준 목록은 사용자 참고용으로, 발행기관이 발행한 공식문서는 아니며 사용 여부는 이용자의 재량에 따릅니다.) **(IMO Guidelines on Maritime Cyber Risk Management 2021))** **[RIGHTSHIP 12.7]** 컴퓨터 기술이 발전함에 따라 디지털 공격의 성격은 지속적으로 진화할 것입니다. 디지털 인프라의 안전을 확보하기 위해 해운회사는 규제 준수를 넘어 보다 적극적인 사이버 리스크 관리 접근 방식을 시행할 것을 강력히 권장합니다. RightShip은 선박 관리자에게 강력한 사이버보안 관리 시스템을 구축하여 사이버 위협을 예방하고 완화할 것을 권장합니다. 이 시스템은 운영적, 기술적, 물리적 평가를 거쳐야 하며, 산업 표준에 따라 평가를 진행하고, 전문가 사이버보안 회사의 인증을 받아야 합니다. 전문가 사이버보안 회사의 예로는 선급이나 해당 분야 전문 업체가 있습니다. '사이버보안 전문가 회사'란 외부 및 내부 위협으로부터 기업의 민감한 데이터를 보호하기 위해 기술, 기술 전문성, 교육을 활용하는 회사를 의미합니다. **[RIGHTSHIP 12.7]**
BIMCO	회사의 경우, IMO에서 요구하는 절차를 정리하는 간단한 방법은 다음 사항을 SSP(선박보안계획서)에 반영하거나, 아니면 동일한 내용을 SMS(안전관리시스템)의 해당 부분에 포함시키는 것일 수 있습니다. : • IT 및 OT 시스템에 대한 물리적 접근과 관련된 절차 • SMS(안전관리시스템)의 사이버보안 절차에 대한 언급, 이 언급은 절차 변경 시마다 업데이트하지 않도록, 수정 없이 그대로 유지 가능한 형태로 작성하는 것이 바람직합니다. 이러한 변경은 일반적으로 기국(Flag State)이나 인증기관의 승인을 요할 수 있습니다. **[BIMCO 1.5 계획 및 절차]** 나머지 사이버 리스크 관리 관련 절차는 시스템 문서(3.2. IT and OT systems' documentation절 참조)에 기재된 민감한 정보는 제외한 채 SMS(안전관리시스템)에 반영되어야 합니다. 이러한 민감한 정보는 외부의 악의적 행위자가 악용할 수 있습니다. SMS(안전관리시스템)에는 이미 사고나 리스크 상황 발생 시 보고 절차 및 의사결정 권한 수준이 명시되어 있습니다. 필요하다면, 사이버 사고 시 의사소통 및 권한 체계를 반영하기 위해 해당 절차를 수정할 수 있습니다. 선장은 사이버 사고 발생 시 참조할

통제항목	A.1.1 사이버보안 정책	Basic

수 있는 명확한 대응 계획을 보유해야 하며, SMS(안전관리시스템)는 사이버 사고를 위한 구체적인 대응 계획을 포함해야 합니다 (9장 참고).
회사의 SMS(안전관리시스템)에 사이버 리스크 관리를 통합하는 방법에 대한 추가 지침은 본 가이드라인 부속서 2(Cyber risk management and the safety management system)에서 확인할 수 있습니다.
SMS(안전관리시스템) 절차는 선박 내 IT 및 OT 사용으로 인해 발생할 수 있는 리스크를 고려해야 하며, 관련 코드, 지침, 권장 기준들을 반영해야 합니다. 상업적 리스크와 같은 절차는 별도 문서보다 SMS(안전관리시스템) 내에 포함되는 것이 바람직합니다.
회사는 다음을 고려해야 합니다:
선박 또는 선박군이 각각의 IT/OT 설정에 따라 고유하게 구성된 경우, 해당 선박에 특화된 리스크 평가 절차가 필요한지 여부입니다. 고려할 요소는 다음과 같습니다:

- IT 및 OT 시스템의 선박 내 사용 범위
- 시스템 통합의 복잡성
- 운영의 성격

또한, SMS(안전관리시스템) 내 절차가 회사 전체 선대(fleet)를 포괄할 수 있는지, 아니면 선박별로 별도의 절차가 필요한지도 고려해야 합니다.
사이버 리스크 평가 및 3.2절(IT and OT systems' documentation)에서 설명된 IT 및 OT 시스템 문서는 민감한 정보로 간주됩니다. 이를 어떻게 보관해야 하는지에 대한 명확한 규정은 없으나, 권장사항은 이를 선박보안평가서(SSA) 및 SSP(선박보안계획서)과 유사한 방식으로 저장 및 관리하는 것입니다.
[BIMCO 1.5 계획 및 절차]

이러한 요소들은 고려되어야 하며, 관련 정책은 회사의 사이버보안 정책 및 SMS(안전관리시스템)에 통합되어야 합니다. 종합적인 데이터 분석과 스마트 선박, "산업용 사물인터넷(IIoT)"의 확대는 위협 행위자가 이용할 수 있는 정보의 양을 증가시켜 사이버 공격의 표면을 확대시킬 수 있습니다. 따라서 강력한 사이버 리스크 관리 접근이 필요합니다. IMO 결의안 MSC.428(98)은 사이버 리스크 위협과 취약점에 대한 인식을 제고하여 안전하고 보안이 유지되는 해운을 지원할 필요성을 강조하고 있습니다. 이는 사이버 리스크에 대해 운영적으로 회복탄력성이 있는 해운을 목표로 합니다. 따라서 모든 해운 관련 이해관계자는 현재와 새로운 사이버 위협과 취약점으로부터 해운을 보호하기 위해 노력해야 합니다. 해당 결의안은 또한, SMS(안전관리시스템)은 ISM 코드의 목적 및 기능 요건에 따라 사이버 리스크 관리를 고려해야 한다고 명시하고 있습니다.
[BIMCO 1.5 계획 및 절차]

IMO 해사안전위원회(MSC)의 제101차 회의(MSC 101/24 문서에 해당 회의 내용 수록)에서는 다음과 같은 내용에 합의했습니다: "사이버보안 관리의 일부 측면, 특히 물리적 보안 측면은 ISPS 코드에 따라 SSP(선박보안계획서)에서 다뤄져야 하며, 이는 회사를 별도의 사이버보안 시스템으로 운영하라는 의미는 아니다. 대신 기존의 회사 SMS(안전관리시스템)와 병행하여 운영되는 것이 바람직하다."
[BIMCO 1.5 계획 및 절차]

통제항목	A.1.1 사이버보안 정책	Basic
		같은 회의에서 IMO는 다음과 같이 재확인하였습니다: “해사 사이버 리스크 관리를 위한MSC.428(98) 결의안은, 사이버 리스크가 기존 SMS(ISM 코드에 정의됨) 내에 적절히 반영되었는지를 행정당국이 확인할 수 있도록 하기 위한 IMO의 요구사항을 설정하였습니다. 이러한 확인은 인증된 적합성증서(DOC) 및 안전관리증서(SMC)에 의해 이루어져야 하며, SSP(선박보안계획서)에서도 관련 절차에 대해 언급되어야 합니다.” **[BIMCO 1.5 계획 및 절차]**
	DCSA	선박은 조직 운영, 자산, 인원, 기타 조직, 안전에 대한 정보 보안 및 그에 따른 리스크를 고려하여 임무/비즈니스 프로세스를 정의하는 프로세스에 포함되어야 합니다. **[DCSA 1.2.3 구현]** 이 프로세스는 정의된 임무/비즈니스 프로세스에서 발생하는 정보 보호 요구사항을 규명하고, 보호 및 안전 요구사항이 달성될 때까지 필요에 따라 해당 프로세스를 수정해야 합니다. **[DCSA 1.2.3 구현]** 선박의 안전 정책은 선박 내에서의 안전하고 건강한 환경, 승무원을 위한 안전한 작업 조건, 장비 및 시스템의 안전성을 제공하는 동시에, 사이버 리스크가 식별되고 완화되도록 보장해야 합니다. • 선박 내 안전하고 건강한 작업 환경 보장 • 식별된 모든 리스크에 대한 보호 조치 수립 • 선박 장비의 성능과 안전을 정기적으로 모니터링하는 절차 포함 • 해상 인력의 성과 및 훈련 수준을 모니터링하는 절차 포함 • 선박과 승무원이 비즈니스 환경 내에서 안전하게 운영될 수 있도록 필요한 자원, 정보, 교육, 감독 제공 **[DCSA 1.2.3 구현]** 품질, 보건, 안전 및 환경 보호 정책은 다음 사항을 반영하도록 갱신되어야 합니다: • 사이버 리스크 관리에 대한 확고한 의지 • OT, IT, 네트워크로 인해 유입되는 안전 리스크 관리의 중요성 이해 • 적절한 통제 조치 없이 OT는 선박의 안전한 운항과 환경 보호에 영향을 미치는 장애에 취약하다는 이해 **[DCSA 1.2.3 구현]** 적절한 기술적 및 절차적 리스크 보호 통제 조치와 승무원의 긴밀한 협력이 없다면, 보건, 안전, 환경 보호는 향상될 수 없습니다. IT와 OT 모두 중단(disruption)에 취약해질 수 있습니다. 따라서 회사는 선박에 승선 중인 선원이 다음과 같은 절차를 준수하기를 기대합니다. PPE 착용, 필요한 안전 예방 조치 이행, 부서 책임자 및 선장과 협력, 선박과 승무원의 안전에 위협이 될 수 있는 사항 보고. 다가오는 사이버보안 계획(Cyber Security Plan, IMO 결의안 MSC.428(98) 참조)에 대한 내용도 승무원에게 전달되어야 합니다. **[DCSA 1.2.3 구현]**

통제항목	A.1.1 사이버보안 정책	Basic
		선박 내 정보 시스템과 자산 보호를 관리하기 위해 유지되고 사용되는 적절한 보안 정책, 프로세스, 절차가 마련되어야 합니다. **[DCSA 2.4.2 설명]** 회사 내에 이미 프로세스와 절차를 자세히 설명하는 정책 계층 구조가 존재할 수 있지만, 선박 내에서의 주요 프로세스와 절차를 식별하는 것은 기밀성, 무결성, 가용성 및 안전성의 원하는 수준을 보장하기 위한 사이버보안 프레임워크의 중요한 요소입니다. **[DCSA 2.4.2 설명]** IT 및 OT를 보호하는 적절한 정책이 마련되어야 합니다. 선박 내 IT/OT의 특정 환경과 그들이 직면한 고유한 리스크를 다루기 위해 “선박 사이버보안” 정책을 수립하는 것이 효과적인 방법일 수 있습니다. **[DCSA 2.4.3 구현]** 물리적 보안은 선박 내 사이버보안의 중요한 요소로, 핵심 시스템 및 네트워크 인프라 접근 제한과 무단 접근 방지를 다룹니다. ISPS(국제 선박 및 항만 보안) 코드에 따라 SSP(선박보안계획서)는 제한 구역의 식별과 예방 조치를 명시하며, 이러한 핵심 시스템 및 네트워크 접근을 제한해야 합니다. SSP(선박보안계획서)에는 사이버 리스크 관리 장(SMS 내)의 참조도 포함되어야 합니다. **[DCSA 2.4.3 구현]**
비고		

A.2 사이버보안 조직 및 외부업체 관리

통제항목	A.2.1 사이버보안 조직		Basic
레퍼런스 상세	IMO	사이버보안 활동의 기획, 자원 조달 및 실행에 책임 있는 개인 또는 기관을 지정합니다. **[IMO 3.5.1.1 거버넌스(Govern)]** 지정된 개인 또는 기관이 직무를 수행하는 데 필요한 권한과 지원을 부여하며, 사이버 리스크 관리에 대한 충분한 지식과 전문성을 갖추도록 합니다. **[IMO 3.5.1.2 거버넌스(Govern)]**	
	OCIMF SIRE 2.0	검사 지침 (Inspection Guidance) 선박 운영자는 사이버 리스크 관리에 대한 절차를 개발해야 하며, 그 내용은 다음을 포함해야 합니다: ■ 사용자, 핵심 인력, 육상 및 선상 경영진의 역할과 책임 식별 • 선상에서 사이버 리스크 관리 책임을 가진 담당자 • 선내 네트워크에서 사용자 프로필 및 비밀번호를 관리하는 담당자 **[OCIMF SIRE 2.0 7.5 사이버보안]**	
	BIMCO	다음 질문에 대한 답변은 경영진에게 선박 내 사이버 리스크 관리의 중요성을 알리는 데 활용할 수 있습니다. **[BIMCO 1.2 고위 경영진의 참여]** • 회사의 위험 허용 수준은 어떻습니까? 손실 수준(예: 규모)은 얼마이며 수용 가능합니까? • 어떤 자산이 리스크에 놓여 있습니까? • 사이버 사고가 비즈니스, 고객, 파트너 및 이해관계자에게 미칠 잠재적 영향은 무엇입니까? • 사이버 리스크 관리에 대한 최종 책임은 누구에게 있습니까? • OT 시스템과 그 작업 환경은 무단 접근 및 변경으로부터 보호되고 있습니까? • 외부로부터 OT 시스템에 접근할 수 있나요? 그렇다면 어떻게 모니터링하고 보호할 수 있습니까? • IT 시스템이 보호되고 있으며 접근이 모니터링 및 관리되고 있습니까? • 사이버 리스크 관리 관련 모범 사례가 사용되고 있습니까? • IT 및 OT 보안에 할당된 직원은 어떤 교육 수준을 이수했습니까? 답변을 바탕으로, 회사는 필요한 권한을 적절히 부여하고, 리스크 평가 결과를 고려하여 적절한 솔루션을 개발하고 유지 보수하는 데 필요한 자원을 할당해야 합니다. **[BIMCO 1.2 고위 경영진의 참여]** 사이버 리스크 관리는 예를 들어, 선박 보안 담당자나 IT 관리자 같은 특정 부서에만 국한되지 않고, 회사의 고위 경영진도 지속적으로 참여해야 합니다. 여기에는 여러 가지 이유가 있습니다. **[BIMCO 1.2 고위 경영진의 참여]** 일부 사이버 리스크는 직원과 환경의 안전은 물론 회사의 성과와 평판에도 광범위한 파괴적 잠재력을 가지고 있습니다. 따라서 사이버 리스크는 단순한 보안 문제가 아니라 경영진의 참여가 필요한 비즈니스 문제입니다. **[BIMCO 1.2 고위 경영진의 참여]**	

통제항목	A.2.1 사이버보안 조직	Basic

사이버보안 및 안전을 강화하기 위한 발의는 표준 비즈니스 절차와 운영에 더 많은 시간 또는 비용을 초래할 수 있습니다. 따라서 리스크 완화를 위해 필요한 자원을 허용 가능한 잔여 리스크 수준까지 평가하고 할당하는 것은 고위 경영진의 결정입니다.

[BIMCO 1.2 고위 경영진의 참여]

사이버 인식을 높이는 이니셔티브는 회사가 노조, 고객, 공급업체 및 관계당국과 상호 작용하는 방식을 변화시키고 당사자 간의 협력에 새로운 요건을 부과할 수 있습니다. 이러한 관계 변화를 주도하거나 그렇게 하는 최선의 방법은 고위 경영진의 결정입니다.

[BIMCO 1.2 고위 경영진의 참여]

효과적인 사이버 리스크 관리는 회사 내 책임과 업무의 명확한 배분에 달려 있습니다. 사이버 리스크 관리는 선박 관리와 선박 운영의 필수적인 부분이며, 직원마다 역할, 책임, 업무가 다릅니다. 또한 일부 기업에서는 일부 역할, 책임, 업무를 제3자에게 아웃소싱하기도 합니다.

[BIMCO 1.3 역할, 책임, 그리고 업무]

다양한 책임과 업무는 SMS(안전관리시스템)에 있는 업무 설명 및/또는 역할 설명에 매핑되어야 합니다. 사이버 리스크 관리 계획 및 실행은 회사 전체를 포함하므로 매번 각각에서 누가 책임자인지, 누가 그 사람을 지원해야 하는지 명확히 하는 것이 유용할 수 있습니다. 예를 들어, 선박 IT 관리자는 선박 내 사이버 리스크 관리의 책임자가 될 수 있지만, 보안 담당자, 안전담당자, 교육담당자, 조타수, 해상 인사 직원, 승무원을 둔 회사 전체의 다른 관리자와 직원의 지원에 의존합니다.

[BIMCO 1.3 역할, 책임, 그리고 업무]

종종 책임과 업무의 부여는 일반적인 지휘 체계와 일치하는 경우 가장 잘 작동합니다. 예를 들어, 선박 내 사이버 리스크 관련 절차 준수에 대한 책임을 할당할 때는 선장이나 기관장을 임명하는 것이 합리적인 경우가 많습니다.

[BIMCO 1.3 역할, 책임, 그리고 업무]

업무 직책/인사	사이버 안전/보안 정책	선박 OT시스템 사이버 리스크 평가	선박 IT 시스템 사이버 리스크 평가	선박 IT 인프라 관리	승무원 사이버 리스크 관리 교육
임원	책임				
회사 IT 담당자	지원		지원		
선박 IT 담당자	지원	책임	책임	책임	
안전 담당자	지원	지원	지원	지원	지원
구매 담당자	지원			지원	
선대 기술 담당자		지원	지원	지원	지원
훈련 담당자			지원	지원	지원
해상 인사 담당자			지원		책임

통제항목	A.2.1 사이버보안 조직	Basic
		그림 3: 역할, 책임, 작업을 매트릭스로 매핑한 예시 (포괄적이지 않음). 직책과 관련된 직무 범위 및 책임은 회사마다 다를 수 있습니다. IT 및 OT 담당자는 회사의 사이버 리스크 관리 전략을 조정하고 일치시킬 필요가 있습니다. **[BIMCO 1.3 역할, 책임, 그리고 업무]**
	DCSA	대부분의 선박은 이미 안전 확보 및 운영 지속이라는 비즈니스 목적에 부합하는 관리 구조 하에 있을 것으로 예상됩니다. 그러나 선박에 사이버보안을 도입하는 과정에서는, 추가적인 역할과 책임과 같은 새로운 관리 구조 요소들을 고려해야 할 수도 있습니다. 기존의 관리 구조에 이러한 요소들을 매핑하는 것은 원활한 전환을 돕는 데 효과적일 수 있으며, 그 예로는 사이버보안 책임자(CySO) 역할을 신설하고 이를 선박 보안 책임자(SSO) 역할에 통합하는 방식이 있습니다. **[DCSA 1.3.2 설명]** 해사 보안 규정은 SOLAS 협약 적용 선박의 소유 회사에게 회사 보안 책임자(CSO)를 지정하도록 법적 요구사항을 부과하고 있습니다. CSO는 회사를 대신하여 SSA(선박 보안 평가서) 및 CSA(사이버보안 평가 절차)를 작성할 책임을 지며, ISPS 코드 제8절은 SSA가 선박의 무선 통신 및 정보통신 시스템(컴퓨터 시스템 및 네트워크 포함)을 포함해야 한다고 규정합니다. 회사는 CSO 및 CySO의 역할과 직무가 적절하게 정의되고, 이들이 기존의 지배 구조에 반영되도록 보장해야 합니다. **[DCSA 1.3.2 설명]** DCSA 가이드라인은 이러한 역할과 책임을 추가로 설명하되, 조직 구조보다는 기능적 측면에 초점을 둡니다. 이로 인해 각 회사는 자사에 적합한 형태로 해당 역할과 책임을 배치할 수 있으며, 이는 선박 수, 자원 분포, 규모 등 다양한 요소들을 고려한 유연한 적용을 가능하게 합니다. **[DCSA 1.3.2 설명]** 각 선박에는 그 선박 내 사이버보안에 대한 책임을 지는 명확한 역할이 정의되어야 합니다. 이 통제 항목에서 언급된 보안 책임자(Security Officer)는 조직 내 공식적인 직책이며, 해당 역할은 명확한 책임 목록과 함께 정식으로 정의되어야 하며, 역할 수행을 위한 교육 및 자원이 갖춰져야 합니다. **[DCSA 1.3.3 구현]** 선사는 이러한 지침을 이행할 수 있도록 적절한 자격을 갖춘 역할 또는 인력을 지정해야 합니다. 이들은 사이버보안의 취약점, 이행 요구사항 및 의존성을 식별할 수 있어야 하며, 이를 지원할 수 있는 기존 프로세스에 대한 이해도 필요합니다. 자본 계획 및 투자 통제 절차와 관련된 보안 측면도 함께 고려되어야 합니다. **[DCSA 1.3.3 구현]** 사이버보안 정책, 표준 또는 프로세스가 기존 거버넌스 체계에 통합되도록 하는 강력한 지배 구조가 구축되어야 합니다. 이를 통해 기존 시스템과의 연계성을 보장하고, 보안 노력이 고립되지 않도록 해야 합니다. **[DCSA 1.3.3 구현]**

통제항목	A.2.1 사이버보안 조직	Basic

선사에게는 "선박 내 사이버보안" 검토 팀(Cyber Security on-board Vessels Review Team)을 구성하는 것도 바람직합니다. 이는 안전 및 운항에 미치는 영향, 그리고 선박 내 복잡한 기술 환경 및 선박과 육상 조직 간 사이버보안 책임의 경계 모호성 등을 고려할 때 필요합니다. 안전, 기업 리스크, 해상 운용, IT 운영, 컴플라이언스 등 다양한 분야의 이해관계자가 초기 단계부터 이 검토 기능에 참여하는 것이 선사에 도움이 될 수 있습니다.

[DCSA 1.3.3 구현]

지정 육상 담당자 (DPA, Designated Person Ashore)

DPA는 일반적으로 선사의 사이버보안 책임자(Cyber Security Lead Officer) 역할을 수행하며, CISO와 협력합니다.

이들은 함대 전체의 사이버보안 프레임워크를 구현하고 유지하는 데 책임이 있으며, 선박 내 사이버보안 역할에 대한 기능적 책임을 집니다.

[DCSA 1.3.4 기능적 역할 및 책임]

주요 책임 (Key Responsibilities)

- 산업 표준과 같은 BIMCO에 따라 사이버보안 프로그램을 개발하고 관리
- 고위 경영진과의 소통 지원
- 정책 및 기준 관련 분쟁 조정
- 사이버보안 인식 교육 및 인식 제고 활동 주도
- 고위 경영진에게 관련 보고 제공
- 연간 DOC(Document of Compliance) 검토 주관

만약 이 DPA가 CSO(Company Security Officer) 역할도 겸한다면, ISPS 규정 준수 또한 그의 책임입니다.

회사에서 계약직 인력을 광범위하게 활용하는 경우, CSO는 계약 인력의 안전한 채용을 위한 적절한 절차(예: 신원조회 등)를 마련해야 합니다. 이 절차는 다른 채용 방식에도 적용되어야 합니다.

[DCSA 1.3.4 기능적 역할 및 책임]

사이버보안 책임자 (CySO, Cyber Security Officer)

선박 또는 함대의 규모와 특성에 따라 CySO는 선박에 직접 탑승하거나, 육상에서 역할을 수행할 수 있습니다. 예를 들어, 원양 항해를 수행하는 선박의 경우 선박 내 CySO를 둘 수 있으며,

정해진 항로를 오가거나 국제 수역에서만 운항하는 선박의 경우, 육상에 CySO를 배치하는 것이 일반적입니다. 또한, 선박 내에 적절한 인력이나 자원이 부족한 경우에도 육상 CySO 운영이 필요할 수 있습니다.다CySO는 선박 내 사이버 기반 시스템(IT, OT, 통신 시스템 등)의 보안 전반에 대한 관리 책임을 집니다.

참고: 선박이 국내 수역과 공해를 포함한 외국 수역을 모두 운항하는 경우, CySO는 법 집행, 사이버 사고 대응 등과 관련된 관할권 이슈에 대한 이해가 필요합니다. 해사 사이버보안 사고는 법적 해석과 대응 범위가 복잡하므로,

사고 발생 시에는 전문 법률 자문을 받는 것이 권장됩니다.

또한, 조직 내부에는 사고 발생 시 보고 체계가 마련되어 있어야 합니다.

[DCSA 1.3.5 기능적 역할 및 책임]

통제항목	A.2.1 사이버보안 조직	Basic
	주요 책임 (Key Responsibilities) • 물리적 보안, 인적 보안, 절차적 보안과 관련하여 회사 보안 책임자(CSO)와 협력 • 사이버보안 평가(CSA) 및 계획(CSP)의 수립, 정기 검토 및 유지 • 사이버보안 계획(CSP)의 실행 및 적용 CySO가 특정 사이버보안 분야나 기술적 해결방안에 대해 충분한 지식이 없을 경우, 외부 전문가의 자문을 받도록 합니다. 이러한 전문 자문은 회사 내부 자원으로 제공될 수도 있고, 회사가 별도로 체결한 전문 지원 계약을 통해 제공될 수도 있습니다. CySO는 선박 자산의 보안에 영향을 미칠 수 있는 관련 법령 및 규제의 변화에 대해 지속적으로 인지하고 있어야 하며, 필요 시 내부 정책, 절차, 대응 방안을 해당 변화에 맞춰 적절히 조정해야 합니다. 참고: 법령 및 규제 변화에 대한 정보는 회사가 자체적으로 수집하여 제공할 수 있으며, 외부 전문 업체와의 계약을 통해 정기 업데이트 형식으로 CySO에게 전달될 수도 있습니다. **[DCSA 1.3.5 기능적 역할 및 책임]** 업무 분리(Separation of duties)는 승인된 권한의 오남용 가능성을 줄이고, 공모 없이 악의적 활동의 리스크를 낮추는 데 기여합니다. 선박에서는 이러한 업무 분리가 제한적일 수 있으나, 여러 역할로 나눌 수 있는 경우 분리를 권장합니다. 예를 들어, 접근 통제 기능을 관리하는 보안 담당자가 감사를 수행하지 않도록 해야 합니다. **[DCSA 2.3.3 구현]** IT 및 OT 시스템에 대한 선박 내 유지보수 활동 및 절차는 다음과 같은 과정을 포함해야 합니다: a. 제조업체 또는 공급업체의 사양 및/또는 조직 요구사항에 따라 정보 시스템 구성요소의 유지보수 및 수리에 대한 일정을 수립, 수행, 문서화하고 기록을 검토합니다. b. 장비가 현장에서 유지보수되든 원격으로 유지보수되든, 또는 다른 장소로 이동되어 유지보수되든 관계없이 모든 유지보수 활동을 승인하고 모니터링합니다. c. 정보 시스템 또는 시스템 구성요소를 조직 시설 외부로 이동하여 유지보수하거나 수리하기 위해서는 명확한 승인 절차가 있어야 함을 요구합니다. d. 장비를 조직 시설 외부로 이동시키기 전에 관련 매체로부터 모든 정보를 제거(소거)하는 절차를 수행합니다. e. 유지보수 또는 수리 이후에도 보안 통제가 여전히 제대로 작동하는지 확인하기 위해 모든 영향을 받았을 가능성이 있는 보안 통제를 점검합니다. f. 조직의 유지보수 기록에 대한 업데이트를 포함합니다. **[DCSA 2.5.3 구현]**	
비고		

A.3 사이버보안 교육 및 훈련

통제항목	A.3.1 사이버보안 교육 및 훈련		Basic
레퍼런스 상세	IMO	모든 직원을 대상으로 매년 기본 사이버보안 교육을 의무화하고, OT 사용자를 대상으로 OT 관련 사이버보안 교육을 의무화하며, 모든 승무원이 승선 시 사이버보안을 숙지하도록 합니다. 모든 직원과 OT 사용자를 위한 이 교육에는 사이버 위생, 진행 중인 사이버 사고의 인식 및 탐지, 그리고 대응 및 복구에 대한 내용이 포함되어야 합니다. 사이버보안에 대한 지식은 훈련 및 연습 등을 통해 수시로 검증되어야 합니다. **[IMO 3.5.3.6 보호(protect)]** 모든 직원을 대상으로 하는 연례 기본 사이버보안 교육에는 진행 중인 사이버 사고를 인식하고 탐지하는 방법에 대한 교육이 포함되어야 합니다 **[IMO 3.5.4.2 탐지(detect)]** 모든 직원을 대상으로 하는 연례 기본 사이버보안 교육에는 사이버 사고 대응 교육이 포함되어야 합니다. **[IMO 3.5.5.3 대응(Respond)]** 전 직원 대상 연간 기본 교육에 사이버 사건 복구 훈련을 포함합니다. **[IMO 3.5.6.2 복구(Recover)]**	
	IACS UR E26	선주는 운영 절차를 준비 및 실행하고, 관련 선원 및 육상 관계자를 대상으로 교육 훈련과 반복 연습(drill)을 수행하여야 하며, 이를 통해 선박 내 CBS(컴퓨터기반시스템)와 해당 시스템들을 상호 연결하는 네트워크에 대한 이해를 높이고, 이들을 다른 CBS(컴퓨터기반시스템) 또는 선박 외부 시스템(예: 육상)과 연결하는 네트워크를 숙지할 수 있도록 해야 합니다. 또한 요구사항을 이행하기 위한 조치를 적절히 관리할 수 있도록 하여야 합니다. **[UR E26 5.3 선박 운항 기간]**	
	OCIMF SIRE 2.0	승무원은 각자의 책임과 직무에 맞는 사이버보안 교육을 받아야 합니다. 사이버보안 인식은 선내에서 적극적으로 제고되어야 하며, 예를 들어 포스터, CBT(컴퓨터 기반 교육) 또는 온라인 과정 등을 통해 홍보할 수 있습니다. **[OCIMF SIRE 2.0 7.5 사이버보안]**	
	BIMCO	교육 및 인식 교육과 인식은 이 지침에서 설명한 효과적인 사이버 리스크 관리 접근 방식의 핵심 지원 요소입니다. 내부 사이버 위협도 고려되어야 합니다. 인원은 IT 및 OT 시스템을 보호하는 데 핵심적인 역할을 하며, 또한 부주의할 수도 있습니다. 예를 들어, 이동식 미디어를 사용하여 시스템 간 데이터를 전송하면서 악성코드 전파 방지를 위한 조치를 취하지 않을 경우가 그렇습니다. **[BIMCO 7.3 절차적 보호 조치]** 교육과 인식은 다음과 같은 대상의 적절한 수준에 맞게 조정되어야 합니다: • 선장을 포함한 선상 인원, 항해사, 승무원 • 관리, 하역, 적재 및 운영을 지원하는 육상 인원 **[BIMCO 7.3 절차적 보호 조치]**	

통제항목	A.3.1 사이버보안 교육 및 훈련	Basic

STCW 협약은 선원이 "[…] 모든 선상 배치, 설치, 장비, 절차 및 선박 특성에 친숙해져야 한다"고 요구합니다. 이는 "[…] 선원들이 안전, 오염 방지 또는 완화에 중요한 기능을 수행할 수 있도록 효과적으로 활동을 조정할 수 있도록" 하기 위함입니다. 적절한 경우, 사이버 리스크 관리 역시 STCW 협약의 범위 내에 포함됩니다.

[BIMCO 7.3 절차적 보호 조치]

STCW 협약에 따라 요구되는 승무원 대상의 숙지 교육 외에도, 모든 선상 인원이 자신의 역할에 따라 다음을 포함한 내용을 다루는 인식 프로그램을 갖추어야 합니다:

- 이메일과 안전한 방식으로 행동하는 것과 관련된 리스크. 예로는 사용자가 악성 사이트로 연결되는 링크를 클릭하거나 악성 첨부파일을 열 때 발생하는 피싱 공격이 있습니다. 이러한 측면에 대한 교육의 한 방법은 피싱 시뮬레이션 테스트를 포함한 특별히 제작된 캠페인을 통해 이루어지며, 이는 인식을 높이고 헌신 수준을 자극하는 검증된 방법입니다.
- 인터넷 사용과 관련된 리스크. 여기에는 소셜 미디어, 채팅 포럼 및 데이터 이동이 덜 통제되고 모니터링되는 클라우드 기반 파일 저장소가 포함됩니다.
- 인원 및 선박의 공개된 위치 정보(geolocation data)와 관련된 리스크.
- 개인 기기 사용과 관련된 리스크. 이러한 기기는 보안 패치와 통제(예: 백신 프로그램)가 적용되지 않았을 수 있으며, 연결된 환경으로 리스크를 전이시킬 수 있습니다.
- 회사 하드웨어에 소프트웨어를 설치 및 유지관리하는 과정에서 감염된 하드웨어(이동식 매체) 또는 소프트웨어(감염된 패키지)를 사용하는 것과 관련된 리스크.
- 소프트웨어 및 데이터 보안 관행이 부실하여 백신 검사나 진위 확인이 수행되지 않는 경우와 관련된 리스크.
- 사용자 정보, 비밀번호 및 디지털 인증서를 보호하는 것과 관련된 리스크.
- 비소속 인원의 물리적 존재와 관련된 사이버 리스크. 예를 들어, 제3자 기술자가 감독 없이 장비에서 작업하는 경우.
- 의심스러운 활동이나 장치를 탐지하고 잠재적인 사이버 사건을 보고하는 방법과 관련된 리스크. 이에 대한 예로는 시스템의 무작위 재부팅, 보통은 보이지 않는 이상한 연결, 또는 누군가가 알 수 없는 장치를 선박 네트워크에 연결하는 경우가 있습니다.
- 사이버 사건이 선박의 안전 및 운영에 미치는 결과 또는 영향에 대한 인식과 관련된 리스크.
- 백신 및 안티멀웨어, 패치, 백업 및 사고 대응 계획과 테스트와 같은 예방적 유지관리 절차를 구현하는 방법에 대한 이해와 관련된 리스크.
- 선박 시스템에 연결하기 전에 서비스 제공자의 이동식 매체로부터 발생하는 리스크로부터 보호하기 위한 절차.
- OT 장비에서의 원격 유지관리 세션을 처리하는 방법과 관련된 교육 및 숙지, 그리고 관련된 리스크 및 영향.

[BIMCO 7.3 절차적 보호 조치]

게다가, 직원은 악성코드 방지 소프트웨어가 존재하더라도 견고한 보안 절차의 필요성이 사라지지 않음을 인식해야 합니다. 예시: 모든 이동식 미디어에 대한 통제 유지.

[BIMCO 7.3 절차적 보호 조치]

통제항목	A.3.1 사이버보안 교육 및 훈련	Basic
	더 나아가, 관련 인원은 컴퓨터가 침해되었을 경우의 징후를 알아야 합니다. 다음과 같은 예가 있습니다: • 응답이 없거나 반응 속도가 느려짐 • 예기치 않은 비밀번호 변경 또는 사용자 잠김 • 프로그램 오류 또는 비정상적인 실행 • 디스크 공간이나 메모리의 예기치 않은 변화 • 이메일 반송 • 네트워크 연결 문제 • 빈번한 시스템 다운 • 비정상적인 하드 드라이브 또는 CPU 활동 • 브라우저, 소프트웨어, 사용자 설정 등의 예기치 않은 변경 **[BIMCO 7.3 절차적 보호 조치]** 지정된 인원은 침입 탐지 시스템(IDS)이 사용되는 경우 해당 보고서를 이해할 수 있어야 합니다. 이 목록은 모든 것을 포괄하는 것은 아니며, 잠재적인 사이버 사고 징후에 대한 인식을 높이기 위한 것입니다. **[BIMCO 7.3 절차적 보호 조치]** 사용자 인식 교육과 절차 강화를 위해 사이버보안 중심 시나리오를 보안 훈련 및 연습에 통합해야 합니다. 선장과 선임 항해사는 선내 사이버 사고 발생 시 적절히 대응할 수 있도록 숙달해야 하며, 이러한 훈련과 연습은 대응 역량을 강화하고 향상하는 데 기여합니다. **[BIMCO 7.3 절차적 보호 조치]** 이 지침은 공급망의 주요 이해관계자(용선자, 선급, 서비스 제공자 등)도 자체 사이버 보안 보호 및 교육을 수행해야 함을 전제로 합니다. 선주 및 운영자는 외부 공급자(해상 터미널, 하역업체 포함)의 보안 상태를 확인하는 것이 좋습니다. **[BIMCO 7.3 절차적 보호 조치]** 7.3(Procedural protection measures)절에서 설명했듯이, 훈련과 인식 제고는 효과적인 사이버 리스크 관리 접근법의 핵심 요소입니다. 따라서, 선박과 육상의 관련 인원이 정기적으로 사이버보안 훈련을 수행할 수 있도록 하는 것이 중요합니다. **[BIMCO 10.2 사고 대응의 네 가지 단계]**	
	DCSA	선박에 승선한 선원들의 교육 및 인식 요구사항을 정의하기 위한 정식 절차가 마련되어야 합니다. 이에는 다음과 같은 다양한 단계가 포함되어야 합니다: 새로운 역할을 맡았을 때, 역할에 변화가 생겼을 때, 주기적인 재교육, 또는 개인의 개선이 필요한 경우 시행되는 교정 교육 등입니다. IT 및 OT 자산에 대해 예상되는 노출 수준이 다른 그룹이 서로 다른 교육 및 인식 커리큘럼을 갖는 것이 바람직할 수 있습니다. 예시로는 다음과 같은 그룹 분류가 있습니다: • Group 1 – 정보 보안 전담 역할을 수행하는 전문가 (예: 사고 대응자, 관리자 수준 접근 권한 보유자 등). 보안 업무를 맡은 선원은 STCW 협약(국제 해상인력 교육, 훈련, 자격증명 및 당직 기준에 관한 국제협약) Table A-VI/6-2(Specifications of minimum standard of competence for

통제항목	A.3.1 사이버보안 교육 및 훈련	Basic
		seafarers with designated security duties)의 요건을 충족하는 보안 교육을 이수해야 합니다. • Group 2 – 중요한 시스템에 접근할 수 있는 일반 사용자. 모든 선원은 승인된 보안 인식 교육 또는 지침을 선상이나 육상에서 이수해야 하며, 이는 선박에 특화되지 않고 1회만 이수하면 됩니다. • Group 3 – 그 외 모든 승무원. 모든 해상 근무자 또는 고용된 인원은 선박보안책임자(SSO) 또는 자격을 갖춘 다른 담당자가 시행하는 보안 관련 기본 교육을 받아야 합니다. **[DCSA 2.2.3 구현]** STCW 협약 준수는 지정된 사이버보안 업무 요건을 충족하기 위해 필요합니다. **[DCSA 2.2.3 구현]** 교육은 선박 내에서 두 가지 핵심 영역으로 나뉘어 진행될 수 있습니다: 1. 리스크를 회피하는 방법에 대한 인식 및 교육 2. 리스크 현실화에 따른 조치 및 인식 및 교육 **[DCSA 2.2.3 구현]** 선박에 가해질 수 있는 리스크 유형에 대한 일반적인 인식은 선원에게 전달되어야 하며, 이러한 리스크를 피하기 위한 예방 조치도 함께 전달되어야 합니다. 예를 들어, 피싱 이메일을 인지하거나 USB 드라이브 사용의 리스크 등을 설명할 수 있습니다. **[DCSA 2.2.3 구현]** 사고 대응 교육은 적절한 승무원 또는 팀에게 제공되어야 하며 기존의 사고 대응 계획과 일치해야 합니다. 예를 들어, 일부 선원은 누구에게 연락할지 또는 정보 시스템에서 사고를 인지하는 방법만 알고 있어도 충분할 수 있습니다. 시스템 관리자 등은 사고 억제, 대응, 복구, 시스템 복원 및 복구 등의 보다 구체적인 교육이 필요할 수 있으며, 이는 내부 및 외부 출처로부터의 사고 모두를 포함합니다. **[DCSA 2.2.3 구현]** 교차훈련 강화 (Maximize cross-training) 사이버 사고 대응에는 선박 내(On-vessel) 팀과 육상(On-shore) 팀 두 조직이 관여할 수 있으므로, 지속적인 교차훈련이 필수적입니다. 교차훈련은 다음을 목표로 해야 합니다: • 모든 책임자가 사고 대응 과정에서 자신의 역할을 명확히 이해하도록 함 • 각 참여자의 지원 역할에 대한 이해를 증진시킴 • 주요 통신 시스템이 공격으로 영향을 받을 경우를 대비하여 보조 통신 수단 및 커뮤니케이션을 명확히 하고 숙지시킴 **[DCSA 4.1.4 선박 내 사고 대응을 위한 주요 권고사항]**
비고		

B. 사이버보안 통제

B.1 사이버 자산 관리

통제항목	B.1.1 사이버 자산 목록		Basic
레퍼런스 상세	IMO	주요 시스템 간 상호 의존성을 포함하여, 중단 시 선박, 인명 안전 또는 환경에 위협을 가하는 시스템, 자산, 서비스, 데이터 및 역량을 식별합니다. 소프트웨어·하드웨어 공급망 관련 요소도 포함합니다. **[IMO 3.5.2.1 식별(Identify)]**	
	IACS UR E26	본 UR의 적용 범위에 해당하는 CBS(컴퓨터기반시스템) 및 해당 시스템들 간 또는 타 CBS(컴퓨터기반시스템)와의 연결을 구성하는 네트워크의 하드웨어 및 소프트웨어(응용 프로그램, 운영 체제, 펌웨어 및 기타 소프트웨어 구성요소 포함)에 대한 목록을 제공하고, 선박의 전체 수명 기간 동안 최신 상태로 유지하여야 합니다. **[UR E26 4.1.1.1 요구사항]** 선박 자산 목록에는, 탑재되어 있는 경우, 1.3.2(Systems in scope)절에 명시된 CBS(컴퓨터기반시스템)가 최소한 포함되어야 합니다. 해당 목록은 선박의 전체 수명 기간 동안 최신 상태로 유지되어야 합니다. 새로운 취약점을 유발하거나 기능적 종속성 또는 시스템 간 연결을 변경할 수 있는 소프트웨어 및 하드웨어 변경 사항은 자산 목록에 기록되어야 합니다. 만약 자산 목록에 기밀 정보(예: IP 주소, 프로토콜, 포트 번호 등)가 포함되는 경우, 해당 정보에 대한 접근은 권한이 부여된 사람에게만 제한되도록 특별한 조치를 취해야 합니다. **[UR E26 4.1.1.3 세부 요구사항]** 본 UR의 적용 범위에 해당하는 모든 하드웨어 장치에 대해, 선박 자산 목록에는 UR E27의 3.1.1(CBS asset inventory)절에 명시된 정보를 최소한 포함해야 합니다. 또한, 자산 목록에는 해당 CBS(컴퓨터기반시스템)와 관련된 시스템 분류 및 보안 영역(Security Zone)을 명시할 수 있습니다. **[UR E26 4.1.1.3.1 하드웨어]** 본 UR의 적용 범위에 해당하는 모든 소프트웨어(예: 응용 프로그램, 운영체제, 펌웨어 등)에 대해, 선박 자산 목록에는 UR E27의 3.1.1절(CBS asset inventory)에 명시된 정보를 최소한 포함해야 합니다. **[UR E26 4.1.1.3.2 소프트웨어]**	
	OCIMF SIRE 2.0	검사 지침 (Inspection Guidance) 선박 운영자는 사이버 리스크 관리에 대한 절차를 개발해야 하며, 그 내용은 다음을 포함해야 합니다: ■ 선박에서 리스크에 노출된 IT(정보기술) 및 OT(운영기술) 시스템 식별 • 화물 관리 시스템 • 브리지 시스템 • 추진 및 기계 관리, 전력 제어 시스템 • 접근 제어 시스템	

통제항목	B.1.1 사이버 자산 목록	Basic
	• 행정 및 승무원 복지 시스템 • 통신 시스템 **[OCIMF SIRE 2.0 7.5 사이버보안]**	
	BIMCO	리스크 평가의 모든 단계를 지원하기 위해 IT 및 OT 시스템은 자산 등록부 내에 문서화된 거버넌스 및 소유권 책임과 함께 명확하게 식별되어야 하며, 이는 적절하게 업데이트되어야 합니다. 자산 등록부에는 자산 가치 평가, 자산 원가 및 자산 유지 관리 비용이 포함되어야 합니다. IACS 통합 요건 E26 및 E27은 신조선에만 적용되지만, 다음을 포함하는 문서 개발 지침으로 활용할 수 있습니다: ■ 통신 장치의 목록(Inventory of communicating devices) ■ 네트워크 통신 장비의 목록(Inventory network communication devices) • OT-OT 및 OT-IT 장비 간 인터페이스를 보여주는 네트워크 토폴로지 도면 • 장비 기능 설계 사양 • 스위치/방화벽 구성 ■ 네트워크의 논리적 구성도(logical map of networks): • IP 주소 • 비-IP 주소 • 비이더넷 공유기 • 엔드포인트 • 커넥터 및 통신용 필드 장치 ■ 버전 정보를 포함한 소프트웨어 인벤토리(어떤 경우에는 이 인벤토리가 선박 소프트웨어 로깅 시스템의 일부임) ■ 각 장비의 네트워크 서비스 목록(Inventory of network services) IT 시스템 인벤토리를 처리하는 데 사용할 수 있는 도구가 있지만 OT 시스템 인벤토리에는 권장되지 않습니다. OT 시스템의 무결성이 손상될 수 있기 때문입니다.(자격을 갖춘 전문가가 마스터, 수석 엔지니어 등과 긴밀히 협의하여 처리하지 않는 한) **[BIMCO 3.2 IT와 OT 시스템 문서화]** 사고: 항해 중 항법 컴퓨터 오류 선박이 도선 중일 때, ECDIS와 항해 성능 모니터링 컴퓨터가 동시에 다운되었습니다. 도선사가 브리지에 있었고, 해당 오류는 당직자에게 일시적인 혼란을 초래했습니다. 하지만 도선사와 선장은 함께 협력하여 브리지 팀이 시각적인 수단 및 레이더를 이용해 안전 운항에 집중할 수 있도록 했습니다. 컴퓨터를 재부팅했을 때, 운영 체제가 노후되었고 더 이상 지원되지 않는 시스템임이 명백해졌습니다. 선장은 해당 컴퓨터 문제가 자주 발생했으며("그렘린"이라 불림), 선주에게 반복적으로 유지보수를 요청했지만 무시당했다고 보고했습니다. 이는 경영진의 간단한 서비스와 선박에 대한 관심이 얼마나 사고를 예방할 수 있는지를 보여주는 분명한 사례입니다. **[BIMCO 3.7 시스템 및 소프트웨어 유지관리]** 선박은 디지털 통신을 통해 비즈니스 수행, 운영 관리, 본사와의 연락 유지 등을 가능하게 하면서 육상 운영과 점점 더 통합되고 있습니다. 더 나아가, 항해 안전,

통제항목	B.1.1 사이버 자산 목록	Basic
		전력, 화물 관리에 필수적인 핵심 선박 시스템들은 점차 디지털화되고 인터넷에 연결되어 다음과 같은 다양한 합법적 기능들을 수행할 수 있게 되었습니다: • 엔진 성능 모니터링 • 원격 진단 • 온도 모니터링(예: 냉동고, LNG 등) • 유지보수 및 예비 부품 관리 • 화물 및 컨테이너 추적과 관리, 선적 및 하역, 적재 계획 • 크레인 및 펌프 관리 • 환경 규제 및 보고 요구사항 준수를 위한 시스템 모니터링 • 항해 성능 모니터링 위 목록은 이 인터페이스의 예시일 뿐이며, 포괄적인 내용은 아닙니다. 이러한 시스템은 데이터를 처리하고 교환하는 기능을 가지며, 이는 사이버 범죄자들이 악용할 수 있는 대상이 될 수 있습니다. **[BIMCO 3.4 선박-육상 간 인터페이스]**
	DCSA	선박 내 조직에서 사용되는 모든 중요 하드웨어 장치가 자산 목록화되었는지 확인해야 합니다 (BIMCO 5.1(Hardware inventory) 참조). **[DCSA 1.1.3 구현]** 이 절차는 자산 수명주기 관리 프로세스의 일부로, 자산의 조달 또는 생성, 처리, 저장, 전송, 삭제 및 폐기 활동을 문서화해야 합니다. 이러한 수명주기는 자산 등록부에 문서화되어야 하며, 예시는 1.1.4(Asset List) 항목에 나와 있습니다. **[DCSA 1.1.3 구현]** 자산 목록(inventory)은 정확하고 최신 상태를 유지해야 하며, 자산 목록과 실제 자산이 일치하는지 검토하는 절차가 있어야 합니다. 이 검토는 정기적으로 수행되어야 하며, SMS(안전관리시스템)에 통합되어야 합니다. **[DCSA 1.1.3 구현]** 자산 목록에는 모든 정보 자산도 포함되어야 합니다. 자산의 버전 정보가 기록되는 것도 중요합니다. 정확하고 최신 상태의 구성 관리 데이터베이스(CMDB)는 이의 좋은 예입니다. 자산 목록에 포함될 수 있는 항목 예시는 다음과 같습니다. [DCSA 1.1.3 구현] • 일련 번호 (Serial number) • 자산 유형 (하드웨어/소프트웨어) • 자산 이름 • 자산 소유자 • 버전 번호 • 위치 • 마지막 검토 날짜 • 중요도 (낮음, 보통, 높음, 안전 관련 중요 등) **[DCSA 1.1.3 구현]** 회사가 통제하는 소프트웨어가 업데이트되거나 변경될 때 이 자산 목록이 유지되도록

통제항목	B.1.1 사이버 자산 목록	Basic

하는 절차가 존재하는지 확인해야 합니다 (BIMCO V3 5.2.2(maintaning this inventory when software controlled by the company is updated or changed) 참조). 이는 자산 목록/CMDB가 자산 인벤토리 절차에 대한 책임을 가진 역할(role)에게 관리되도록 함으로써 달성할 수 있습니다. 이러한 모든 사항은 기존의 선박 설비 유지보수 계획 내에 포함되어야 하며, 이는 다음의 3대 국제 협약에 따라 구성됩니다:
SOLAS(해상 인명 안전에 관한 국제협약),
STCW(해기사 교육, 훈련 및 자격증에 관한 국제기준),
MARPOL(해양 오염 방지 협약).

[DCSA 1.1.3 구현]

이 페이지는 자산 목록의 예시를 보여줍니다. 사이버 리스크로부터 보호가 필요한 모든 자산이 식별되고, 기록되며, 관리되도록 하기 위해 아래의 항목들을 사용하는 것을 권장합니다. 이는 회사의 선호도에 따라 기존 자산 인벤토리의 일부로, 또는 병행하여 수행될 수 있습니다.

dcsa

자산 목록

SMS 내의 기존 영향 평가를 기반으로 유형(하드웨어/소프트웨어), 소유자(욕상), 관리자(선박) 및 중요도를 포함한 중요 자산 목록을 제공 수 있는 예시 자산 목록입니다.

자산 일련번호	자산.	유형 / 설명	버전	주인	관리인	위치	마지막 점검 일자	업정성
1	셀 인스피론 17 노트북	하드웨어	윈도우 10	J. 도	스미스	다리	01/11/2019	보통
2								
3								
4								
5								
6								
7								
8								
9								
10								

[DCSA 1.1.4 자산 목록]

데이터 보안은 의도적 또는 우발적인 파괴, 수정 또는 공개로부터 데이터를 보호하는 일련의 표준 및 기술입니다. 데이터 보안은 관리적 통제, 물리적 보안, 논리적 통제, 조직 표준 및 무단 또는 악의적인 사용자 또는 프로세스의 접근을 제한하는 기타 보호 기술을 포함한 다양한 기법과 기술을 통해 적용될 수 있습니다.

[DCSA 2.3.2 설명]

왜 데이터 보안이 중요한가?

- 오늘날 모든 비즈니스는 데이터를 다룹니다. 대량의 개인 및 금융 데이터를 처리하는 대형 은행부터, 고객의 연락처 정보를 휴대폰에 저장하는 소규모 자영업자에 이르기까지, 모든 규모의 기업에서 데이터는 핵심입니다.

데이터 보안의 주요 목적은 조직이 수집, 저장, 생성, 수신 또는 전송하는 데이터를 보호하는 것입니다. 컴플라이언스(규정 준수)도 중요한 고려사항입니다. 어떤 장치, 기술, 프로세스를 사용하든 데이터를 관리, 저장 또는 수집하는 데 사용된다면, 반드시 보호되어야 합니다.
데이터 유출은 소송과 막대한 벌금으로 이어질 수 있으며, 회사의 평판에도 심각한 손상을 줄 수 있습니다. 공격자들의 수법이 점점 정교해짐에 따라 보안 위협으로부터 데이터를 보호하는 것은 그 어느 때보다 중요해졌습니다.

[DCSA 2.3.2 설명]

소프트웨어 및 펌웨어의 비인가 변경 방지를 위한 절차가 있어야 합니다. 모든 변경

통제항목	B.1.1 사이버 자산 목록	Basic
		사항은 승인 및 문서화되어야 하며, 변경이 보안에 미치는 영향 또는 리스크 프로파일 변경에 대한 이해와 평가, 수용 또는 처리(해당 시)가 사전에 이루어져야 합니다. 선상 인력의 안전, 선박 조종 및 환경 보호와 관련된 주요 작업 절차는 이미 SMS(안전관리시스템)에 포함되어 있어야 하며, 데이터 보안은 중요한 시스템에 대한 장애 발생이 의심될 경우 취해야 할 조치 지침 개발에 중점을 두고 있습니다. **[DCSA 2.3.3 구현]** 정보 흐름 통제(Information flow control)는 데이터 보안 리스크가 있는 시스템에 구현되어야 합니다. 흐름 통제의 제한 사항에는 다음이 포함됩니다: • 수출 통제 정보가 인터넷을 통해 명시되지 않은 상태로 전송되지 않도록 함 • 조직 내부에서 온 것처럼 보이는 외부 트래픽 차단 • 내부 웹 프록시 서버가 아닌 인터넷에 대한 웹 요청 제한 • 데이터 구조 및 내용에 기반하여 조직 간 정보 전송 제한 **[DCSA 2.3.3 구현]** 모든 IT/OT 시스템 변경 사항에 대해 보안 영향을 사전에 분석하기 위해 변경 관리 프로세스(Change Management Process)를 수립해야 합니다. **[DCSA 2.4.3 구현]**
비고		

B.2 계정 관리

통제항목	B.2.1 계정 및 권한 관리		Basic
레퍼런스 상세	IMO	모든 사용자에게 고유 자격 증명을 부여하고, 사용자 및 관리자 계정을 구분하며, 퇴사자 또는 사용자 계정을 비활성화합니다. **[IMO 3.5.3.1 보호]**	
	IACS UR E26	CBS(컴퓨터기반시스템) 및 관련 정보는 파일 시스템, 네트워크, 응용 프로그램 또는 데이터베이스 수준의 접근 통제 목록(ACL: Access Control Lists)을 통해 보호되어야 합니다. 선상 및 육상 인력의 계정은 역할 및 책임에 따라 제한된 기간 동안만 활성 상태로 유지되어야 하며, 필요하지 않을 경우 삭제되어야 합니다. **[UR E26 4.2.4.3.5 사용자 인증정보 관리]** 주의: CBS(컴퓨터기반시스템)는 UR E27 표 1의 항목 No.1(Human user identification and authentication)에 따라 사람 사용자를 식별 및 인증해야 하나, 모든 사용자를 "고유하게" 식별 및 인증할 필요는 없습니다. **[UR E26 4.2.4.3.5 사용자 인증정보 관리]** 관리자 권한은 접근 통제 정책에 따라 관리되어야 하며, 회사 또는 선박 내에서 해당 역할을 수행하는 공인되고 적절히 교육받은 인력만이 CBS(컴퓨터기반시스템)에 전체 접근 권한을 갖고 로그인할 수 있어야 합니다. **[UR E26 4.2.4.3.5 사용자 인증정보 관리]** CBS(컴퓨터기반시스템) 및 네트워크에 접근할 수 있는 모든 사용자는 해당 기능을 수행하는 데 필요한 최소한의 권한만을 부여받아야 합니다. **[UR E26 4.2.4.3.6 최소 권한 원칙]** 모든 신규 계정의 기본 설정으로는 가능한 한 최소 권한이 부여되도록 설정되어야 합니다. 권한은 가능한 경우에만 필요한 시점에 제한적으로 부여되어야 하며, 일회성 사용 또는 세션 기반 권한처럼 만료되거나 자동으로 종료되는 방식이 바람직합니다. 관리자 권한의 영구적 부여는 피해야 하며, 예를 들어 시간 제한 사용자 계정을 사용해야 합니다. **[UR E26 4.2.4.3.6 최소 권한 원칙]**	
	OCIMF SIRE 2.0	관리자 프로필 및 사용자 프로필 유지 책임은 고위 간부(선장, 기관장 및 일등 항해서, 일등 기관사 등)에게만 부여되어야 하며, 그 책임은 명확히 규정되어야 합니다. 사용자 프로필은 작업용 워크스테이션 등 본래의 목적에 맞게 사용하도록만 허용되어야 합니다. 사용자 프로필은 신중히 관리되어야 하며, 불필요한 프로필은 삭제해야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]**	
	BIMCO	관리자 권한 사용 정보 접근은 관련된 권한이 있는 인원에게만 허용되어야 합니다. 관리자 권한은 시스템 구성 설정 및 모든 데이터에 대한 전체 접근을 허용합니다. 관리자로 시스템에 로그인할 경우 기존의 취약점이 더 쉽게 악용될 수 있습니다. 관리자 권한은 회사 또는 선상에서 해당 역할을 수행하는 적절히 훈련된 인원에게만 부여되어야 하며, 해당 인원이 해당 권한을 사용하는 경우 시스템에 로그인할 필요가	

통제항목	B.2.1 계정 및 권한 관리	Basic
		있습니다. 어떠한 경우에도 관리자 권한 사용은 해당 기능 수행에 필요한 범위로 제한되어야 합니다. 이상적으로는 해당 사용자가 더 이상 승선하지 않을 때 사용자 권한을 제거하는 것이 좋습니다. 사용자 계정을 일반적인 사용자 이름을 사용하여 한 사용자에서 다른 사용자로 이전해서는 안 됩니다. 사용자가 역할을 변경하여 더 이상 접근할 필요가 없을 때, 선박 시스템에 원격으로 접근할 수 있는 육상 직원에게도 유사한 규칙을 적용해야 합니다. 선박과 같은 비즈니스 환경에서는 다양한 이해관계자에게 시스템 접근 권한이 부여됩니다. 공급자 및 계약자는 회사 운영 및 시스템에 대해 깊은 이해를 바탕으로 접근 권한이 있으므로 특히 높은 보안 리스크를 초래할 수 있습니다. **[BIMCO 7.3 절차적 보호 조치]**
	DCSA	선박 내에서 계정 관리 및 접근 통제가 적용되어야 하는 시스템의 예시는 다음과 같습니다: • 최종 사용자 장치 (예: 회사 노트북) • 네트워크 인프라 (예: 무선 공유기) • OT 시스템 **[DCSA 2.1.2 설명]** 자산 관리 목록에 등재된 모든 자산을 포함하는 접근 통제 정책(Access Control Policy)이 수립되어야 하며, 리스크 관리는 접근 통제 요구사항의 선정 및 우선순위 결정에 유용한 기준을 제공해야 합니다. **[DCSA 2.1.3 구현]** 선박 내 계정 관리 및 접근 통제가 필요한 자산은 사용자/그룹에 대한 명확한 접근 요구사항을 갖추어야 하며, 이는 자산 관리자(Asset Owner)가 승인해야 합니다 (자산 관리 목록에 명시된 담당자). **[DCSA 2.1.3 구현]** 사용자 계정, 관리자 계정 등 다양한 승인 절차와 필요 시 그 외의 속성에 대한 프로세스가 마련되어야 합니다. **[DCSA 2.1.3 구현]** 선박 내 자산은 계정 접근 및 관리 라이프사이클에 포함되어야 하며, 계정이 승인, 생성, 모니터링 및 삭제되는 절차가 적절히 적용되어야 합니다. **[DCSA 2.1.3 구현]**
비고		

통제항목	B.2.2 비밀번호 관리	Basic
레퍼런스 상세		
	IMO	모든 기기의 기본 비밀번호를 변경하고, 강력한 비밀번호 정책을 시행하며, 무차별 대입 공격, 피싱 등의 악의적인 시도로부터 보호하기 위해 다른 사용자 계정 접근 제어 관리 조치를 수립하는 것을 고려해야 합니다. 필요한 경우, 다중 인증 또는 지속적 인증 솔루션, 보안 음성, 영상 및 문자 통신, 그리고 기업 내 보안 비상 통신 시스템을 사용해야 합니다. **[IMO 3.5.3.2 보호(protect)]**
	IACS UR E26	선박 내 CBS(컴퓨터기반시스템)에는 보안 구역 정책에 적합하면서도 주요 기능을 저해하지 않는 적절한 접근 통제가 제공되어야 합니다. 높은 수준의 접근 보안이 요구되는 경우에는 강력한 암호화 키 또는 MFA(다중인증)을 사용하여 보호되어야 합니다. **[UR E26 4.2.4.3.5 사용자 인증정보 관리]**
	OCIMF SIRE 2.0	일반 사용자 프로필 및 비밀번호는 승무원 교대 과정에서 공유되어서는 안 되며, 비밀번호는 정기적으로 변경해야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]**
	BIMCO	MFA(다중인증) 및 비밀번호 기밀 데이터 및 중요 시스템에 대한 접근을 보호하기 위해, MFA(다중인증)과 함께 견고한 비밀번호 정책이 개발되어야 합니다. MFA(다중인증)는 가능한 한 광범위하게 사용되어야 하며, 각 사용자 수준에 적합하게 적용되어야 합니다. 무차별 대입 공격(Brute-force attack)의 가능성을 줄이기 위해, 비밀번호는 강력하고 사용자 또는 시스템에서 생성된 것이어야 합니다. 회사 정책은 너무 복잡해서 자주 변경해야 하며, 종이에 적어두거나 컴퓨터 근처에 두게 되는 비밀번호 사용의 리스크를 고려해야 합니다. 비밀번호는 MFA(다중인증)와 함께 사용되어야 하며, MFA(다중인증)는 사용자의 소유(예: 토큰 또는 장치)와 사용자 자신(예: 지문, 얼굴 인식 등)을 기반으로 합니다. MFA(다중인증)가 구현되면, 공격자가 비밀번호를 확보하더라도 토큰이나 장치가 없으면 접근할 수 없어 보안이 강화됩니다. 예를 들어, 복잡한 비밀번호보다 기억하기 쉬운 혼합 단어 시퀀스인 암호문구를 사용하는 것이 좋습니다. 관리 시스템의 비밀번호 또는 암호문구는 토큰이나 장치와 같은 사용자가 소유한 것과 비밀번호와 휴대폰의 지문 암호와 같은 사용자가 알고 있는 것을 기반으로 하는 MFA(다중 인증)를 사용하여 보완해야 합니다. MFA(다중인증)를 구현하면 암호를 획득하는 위협 행위자가 토큰이나 장치를 소유하지 않으므로 침해 위험이 크게 줄어듭니다. 선원과 사무직 직원에게 시스템 비밀번호를 공공 장소에 게시해서는 안 된다는 경고를 포함해야 합니다. **[BIMCO 7.3 절차적 보호 조치]**
	DCSA	선박 내 사용자 계정 및 비밀번호를 관리하는 책임 있는 역할이 지정되어야 하며, 기본 비밀번호 사용을 방지하고 사용되지 않거나 불필요한 계정을 제거하기 위한 정기적인 점검이 수행되어야 합니다. **[DCSA 2.1.3 구현]**
비고		

B.4 기기 및 출입통제

통제항목	B.4.1 기기 반출입 통제		Basic
레퍼런스 상세	IMO	무단 이동식 저장매체 사용을 방지하는 통제를 수립합니다. **[IMO 3.5.3.5 보호]**	
	IACS UR E26	이동식 미디어 장치의 사용에 대한 정책이 수립되어야 하며, 해당 정책에는 선박 시스템에 파일을 업로드하거나 선박 시스템에서 다운로드하기 전에 디지털 서명, 워터마크, 바이러스 검사 등을 통해 이동식 미디어를 검사하고 정품 소프트웨어임을 검증하는 절차가 포함되어야 합니다. 4.2.7(Use of Mobile and Portable Devices) 절도 참조하십시오. **[UR E26 4.2.4.3.4 이동식 미디어 통제]**	
	OCIMF SIRE 2.0	휴대용 매체 사용은 엄격히 제한되어야 하며, 불가피하게 사용할 경우 선박 제어 네트워크와 연결되지 않은 컴퓨터에서 악성코드 검사를 실시해야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]** 민감한 IT 또는 OT 제어 장비가 포함된 공간은 반드시 안전하게 잠가야 합니다. 민감한 사용자 장비(예: 브리지 시스템의 노출된 USB 포트, Wi-Fi 허브 포트 등)에 대한 물리적 접근은 보호되거나 비활성화되어야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]** 조사관, 기술자 등 방문자의 컴퓨터 접근은 제한되어야 하며, 민감한 OT 컴퓨터에 대한 무단 접근은 금지되어야 합니다. 민감한 네트워크 접근(원격 접근 포함)에 대한 승인 절차가 마련되어야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]**	
	RIGHTSHIP	선박 내 컴퓨터에서 USB 메모리 스틱, CD, DVD, 디스켓 등의 이동식 미디어 사용을 통제하기 위한 조치가 마련되어 있습니까? **[RIGHTSHIP 12.8]** 이동식 미디어(removable media)는 컴퓨터 간 데이터 저장 및 전송을 위한 모든 방식을 통칭합니다. 여기에는 노트북, USB 메모리 스틱, CD, DVD, 디스켓이 포함됩니다. 통제되지 않은 시스템에서 통제된 시스템으로 데이터를 전송하는 것은 악성코드 유입의 주요 리스크 요인입니다. 이동식 미디어는 방어 계층을 우회하는 데 사용될 수 있으며, 인터넷에 연결되어 있지 않은 시스템을 공격하는 데도 이용될 수 있습니다. 이러한 미디어 장치 사용에 대한 명확한 정책은 필수적이며, 미디어 장치가 일반적으로 통제되지 않은 시스템과 통제된 시스템 간의 정보 전송에 사용되지 않도록 보장해야 합니다. **[RIGHTSHIP 12.8]** 무단 접근을 방지하기 위해, 이동식 미디어 차단 장치는 물리적으로 접근 가능한 모든 컴퓨터 및 네트워크 포트에 설치해야 합니다. (The Guidelines on Cyber Security on board Ships, 2017) **[RIGHTSHIP 12.8]** ECDIS와 같은 중요 장비는 악성코드 및 바이러스 공격으로부터 보호되어야 합니다.	

통제항목	B.4.1 기기 반출입 통제		Basic
		USB 및 RJ-45 포트에 대한 접근은 통제되어야 하며, 즉 포트를 비활성화하거나 잠가야 합니다. **[RIGHTSHIP 12.8]**	
	DCSA	이동식 매체의 사용 제한 이동식 외부 장치는 고유한 보안 위협을 초래할 수 있으므로, 다음과 같은 보안 기술을 적용해야 합니다. (사용 기록 로깅, 저장된 데이터에 대한 접근 통제, 암호화 요구사항 적용) 또한, 네트워크 측면에서는 자동 실행 및 자동 재생 기능을 비활성화하고, USB 포트 사용을 원천 차단하는 방안을 도입할 수 있습니다. **[DCSA 2.6.2 설명]**	
비고			

C. 사이버 리스크 관리

C.1 사이버 취약점 진단

통제항목	C.1.1 악성코드 방지		Basic
레퍼런스 상세	IMO	인터넷이나 회사 인트라넷에 접속하거나 제3자 또는 육상 네트워크 및 정보 시스템(특히 선박/항만 인터페이스)과 상호 작용하는 모든 선박 디지털 시스템 및 장치에 대한 보안 조치(방화벽 또는 바이러스 백신 등)를 시행하며, 암호화 사용에 대한 정책을 구현합니다. **[IMO 3.5.3.4 보호]**	
	IACS UR E26	CBS(컴퓨터기반시스템)에 악성코드가 침입하는 일반적인 경로로는 전자메일, 이메일 첨부파일, 웹사이트, 이동식 미디어(예: USB 장치, 디스켓, CD 등), PDF 문서, 웹서비스, 네트워크 연결, 감염된 노트북 등이 있습니다. **[UR E26 4.2.3.2 타당성]** CBS(컴퓨터기반시스템)에 대한 악성코드 보호는 본 UR의 적용 범위 내에서 구현되어야 합니다. 운영체제를 탑재한 CBS(컴퓨터기반시스템)의 경우, 산업 표준의 안티바이러스 및 안티멀웨어 소프트웨어가 설치되어야 하며, 이를 최신 상태로 유지하고 정기적으로 업데이트해야 합니다. 단, 해당 소프트웨어의 설치가 CBS(컴퓨터기반시스템)의 기능 또는 요구되는 서비스 수준 제공에 영향을 줄 경우(예: 실시간 작업이 필요한 Cat.II 및 Cat.III CBS의 경우), 설치 여부는 제한될 수 있습니다. CBS(컴퓨터기반시스템)에 안티바이러스 및 안티멀웨어 소프트웨어 설치가 불가능한 경우에는, 악성코드 보호는 시스템 설계, 운영 절차, 승인된 미디어 사용, 디지털 서명, 백신 검증 절차 등을 통해 달성되어야 합니다. **[UR E26 4.2.3.3 세부 요구사항]**	
	OCIMF SIRE 2.0	모든 선내 컴퓨터는 안티바이러스 소프트웨어로 보호되어야 하며, 이는 항상 최신 상태로 유지되어야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]**	
	BIMCO	**이메일 및 웹 브라우저 보호** 이메일과 웹 브라우저는 다음 사항을 충족하는 방식으로 보호되어야 합니다: • 육상 및 선박의 인력을 사회공학 공격으로부터 보호해야 합니다. • 이메일이 민감한 정보를 얻기 위한 수단으로 악용되지 않도록 방지해야 합니다. • 이메일이나 음성을 통한 민감 정보의 교환은 기밀성과 무결성을 확보할 수 있도록 적절히 보호되어야 합니다 (예: 암호화 적용). • 웹 브라우저와 이메일 클라이언트가 악성 스크립트를 실행하지 않도록 해야 합니다. 안전한 이메일 전송을 위한 모범 사례는 다음과 같습니다: 이메일은 필요시 zip 또는 암호화 파일 형식으로 전송합니다. 이메일 시스템에서는 하이퍼링크를 비활성화하는 것이 좋습니다. 일반적인 이메일 주소 사용은 피하고, 사용자 계정이 제대로 설정되어 있는지 확인합니다.	

통제항목	C.1.1 악성코드 방지	Basic
		또한, 발신자 정책 프레임워크(SPF), 도메인 키 식별 메일(DKIM), 도메인 기반 메시지 인증 보고 및 준수(DMARC) 보안 제어를 구현하면 이메일의 유효성을 인증하고 피싱 공격으로부터 보호하는 데 도움이 됩니다. 기업은 피싱 공격으로부터 더욱 안전하게 보호할 수 있는 이메일 보안 도구와 서비스 활용도 고려해야 합니다. 인터넷 접속이 합법적으로 요구되는 선박 시스템의 웹 브라우저에 쉽게 구현할 수 있는 몇 가지 보안 제어 기능이 있습니다. 첫째, 브라우저를 더욱 안전한 설정으로 쉽게 구성하여 기능을 제한하고 더욱 안전한 환경을 조성할 수 있습니다. 여기에는 팝업 창 및 플러그인 차단, JavaScript 및 쿠키 비활성화, 브라우저 프로세스를 샌드박스 환경에서 실행되도록 격리하는 것이 포함됩니다. 또한, 온보드 컴퓨터의 다른 소프트웨어 취약성 관리 노력의 일환으로 브라우저를 정기적으로 패치해야 합니다. **[BIMCO 7.2 기술적 보호 조치]** 피싱: 가장 흔히 보고되는 사이버 공격 피싱은 비용이 저렴하고 실행이 쉬우며 위험도가 낮기 때문에 앞서 언급한 다양한 공격자들이 사용하는 가장 일반적인 사이버 공격입니다. 많은 중요 인프라 관계자들이 받는 피싱 캠페인에는 온라인 쇼핑 판매, 경품 지급, 계정 검증 요건 사칭(예: Microsoft, Amazon 등) 등이 포함됩니다. 또한, 해운 산업을 표적으로 하는 피싱 캠페인도 빈번하게 발생합니다. 일반적인 캠페인 유형은 선장이나 선박 사관에게 보내는 이메일에서 항만국 통제국을 사칭하거나, 반대로 육상 직원에게 보내는 이메일에서 선원을 발신자로 위장하는 것입니다. 이는 모든 기업이 이메일 보안에 집중해야 함을 보여줍니다. **[BIMCO 7.2 기술적 보호 조치]** 선상 시스템에서 악성코드의 존재를 자동으로 탐지하고 대응할 수 있는 스캐닝 소프트웨어는 최신 상태로 유지되고 적절히 관리되어야 합니다. 일반적인 지침으로서, 선박 내 컴퓨터는 육상 사무실 컴퓨터와 동일한 수준으로 보호되어야 합니다. 모든 개인용 및 업무용 선상 컴퓨터에는 백신 소프트웨어와 악성코드 방지 소프트웨어가 설치되고, 유지 관리되며, 최신 상태로 업데이트되어야 합니다. 이는 이러한 컴퓨터들이 선박 네트워크의 서버나 다른 컴퓨터에 대한 공격 벡터로 작용할 리스크를 줄여줍니다. 스캐닝 소프트웨어가 얼마나 자주 업데이트되는지를 고려하는 것은 이러한 방어 방법에 의존할지를 결정할 때 반드시 고려되어야 합니다. **[BIMCO 8.2 악성코드 탐지]**
비고		

통제항목	C.1.2 패치 관리	Basic
레퍼런스 상세	OCIMF SIRE 2.0	애플리케이션 소프트웨어는 정기적으로 보안 패치 및 업그레이드로 최신화되어야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]**
	BIMCO	하드웨어 및 소프트웨어의 보안 구성 선박에서 사용되는 모든 엔드포인트(서버, 워크스테이션, 노트북, 회사에서 지급한 모바일 기기 포함)는 운영체제 및 기타 소프트웨어에 대해 안전한 기준 구성을 갖춘 후 운영 상태에 배치되어야 합니다. 운영에 들어간 이후에는 기준 구성 변경이 변경 관리 절차를 따라야 하며, 취약점 관리 프로그램의 일환으로 이러한 시스템에 대한 정기적인 패치가 수행되어야 합니다. 함대 전체에 걸쳐 표준화된 기준 구성이 마련되어 있으면 이러한 시스템을 보다 쉽게 모니터링할 수 있고, 의심스러운 또는 비정상적인 활동이 발생했을 때 이를 식별하기가 용이해집니다. 사용자 프로파일은 오직 컴퓨터, 워크스테이션 또는 서버가 지정된 목적에 맞게 사용되도록 제한되어야 합니다. **[BIMCO 7.2 기술적 보호 조치]** 애플리케이션 소프트웨어 보안(패치 관리) 선상 시스템에 보안 업데이트를 제공해야 하며, 소프트웨어 및 하드웨어 패치 계획을 수립하는 것이 좋습니다. 보안 패치는 정기적인 유지 관리 주기에 포함되어야 하며, 가상 네트워크 분리(VLAN) 및 방화벽 구축에 사용되는 장비에 특히 주의를 기울이는 것이 좋습니다. 이러한 업데이트 또는 패치는 반드시 적용해야 합니다. 시스템의 취약점이 악용되어 해커에게 노출되기 전에 해당 취약점을 해결할 수 있도록 권한이 있는 직원만 적시에 패치를 적용해야 합니다. 선박 내 IT 시스템 패치는 정기적(예: 월 1회)으로 적용해야 합니다. 일부 OT 시스템에 패치를 적용하는 것은 복잡하고 비용이 많이 들 수 있습니다. 모든 소프트웨어와 하드웨어 펌웨어를 정렬하고 설치 후 무결성을 검증하기 위해 철저한 테스트를 수행해야 하며, 클래스에서 나중에 시스템을 인증해야 할 수도 있기 때문입니다. 다른 경우에는, 시스템 하드웨어를 일부 또는 전체적으로 업그레이드하지 않으면 보안 패치가 적용되지 않을 수 있습니다. 이러한 이유로 OT 시스템은 자주 업데이트되지 않거나 전혀 업데이트되지 않습니다. 따라서 패치를 설치하기 전에 OT 시스템의 호환성과 잠재적 운영 영향을 평가하는 것이 중요합니다. 중요한 패치를 설치할 수 없는 경우, 취약점이 대규모 IT 네트워크 또는 궁극적으로 인터넷에 노출되지 않도록 대체 방안을 검토해야 합니다. 이는 물리적 보호, 네트워크 접근 제한, 그리고 가상 패치 기술 구현을 병행하는 것이 될 수 있습니다. **[BIMCO 7.2 기술적 보호 조치]** 업그레이드 및 소프트웨어 유지관리 제조사나 소프트웨어 개발자가 더 이상 지원하지 않는 하드웨어 또는 소프트웨어는 잠재적 취약점을 수정하기 위한 업데이트를 받지 못합니다. 따라서 이러한 장비와 소프트웨어의 사용은 회사의 사이버 리스크 평가의 일환으로 신중히 평가되어야 합니다. 선박에 설치된 관련 하드웨어 및 소프트웨어는 적절한 보안 수준을 유지하기 위해

통제항목	C.1.2 패치 관리	Basic
		업데이트되어야 합니다. 소프트웨어의 시기적절한 업데이트를 위한 절차는 선박의 유형, 인터넷 연결 속도, 항해 시간 등 다양한 요소를 고려하여 수립되어야 합니다. 소프트웨어에는 컴퓨터 운영 체제가 포함되며, 이것도 최신 상태로 유지되어야 합니다. 또한, 다양한 라우터, 스위치, 방화벽, OT 장치들은 각각 자체 펌웨어를 실행하게 되므로 정기적인 업데이트가 요구되며, 이는 절차적 요구사항에 반영되어야 합니다. 소프트웨어 유지관리의 효율성은 전체 소프트웨어 생명주기 전반에 걸쳐 유지관리 활동을 지원하는 데 필요한 식별, 계획, 실행 조치에 달려 있습니다. 업계 표준이 개발되어 선박 장비 및 통합 시스템의 소프트웨어 유지보수를 위한 이해관계자 요구사항을 규정하고 있습니다. 이 표준은 선박, 육상 및 원격 소프트웨어 유지보수를 모두 포괄합니다. **[BIMCO 7.3 절차적 보호 조치]**
	DCSA	소프트웨어 유지보수는 운영 유지보수 절차의 일부로 포함되어야 합니다. 이러한 절차는 보안 패치를 포함한 소프트웨어 업데이트의 적용이 숙련된 인력에 의해 적시에 적용 및 테스트되도록 보장해야 합니다. 유지보수 및 패치 주기는 한 달을 초과하지 않는 주기로 수행하는 것이 권장됩니다. **[DCSA 2.5.2 설명]** 또한, IT 또는 OT 자산과 관련된 유지보수 활동은 패치 적용, 업데이트, 하드닝 또는 소프트웨어/하드웨어/펌웨어의 수정 등의 작업이 사이버보안 또는 안전 리스크를 유발하지 않도록, CySO(사이버보안 책임자)와 같은 역할에 의해 검증 및 승인되어야 합니다. **[DCSA 2.5.3 구현]**
비고		

C.2 사이버 리스크 평가

<table>
<tr><th>통제항목</th><th colspan="2">C.2.1 사이버 영향도 평가</th><th>Basic</th></tr>
<tr><td rowspan="2">레퍼런스 상세</td><td>BIMCO</td><td colspan="2">회사는 선박의 OT 및 IT 시스템이 어떻게 육상 시스템과 연결되고 통합되는지, 그리고 이러한 시스템들이 관계당국, 해상 터미널, 하역업자 등과 어떻게 연결되는지를 완전히 이해하고 적절히 문서화하는 것이 권장됩니다. 이를 위해서는 선박 내 모든 컴퓨터 기반 시스템과 이들이 안전, 운영, 비즈니스(화물 및 하역 관리 포함)에 어떤 영향을 미칠 수 있는지에 대한 충분한 이해가 필요합니다. 이는 사이버 사고로 인해 시스템이 손상될 수 있기 때문입니다.
[BIMCO 3.4 선박-육상 간 인터페이스]

기밀성, 무결성, 가용성을 의미하는 CIA 모델은 다음과 같은 영향을 평가하기 위한 프레임워크를 제공합니다:
• 정보의 기밀성 상실: 예를 들어, 시스템에 대한 무단 접근 및 공개, 선박, 승무원, 화물 및 승객에 대한 정보 또는 데이터
• 무결성 상실: 선박의 안전하고 효율적인 운항 및 관리를 위한 정보와 데이터를 변경하거나 조작하는 경우
• 가용성 상실: 정보와 데이터의 파괴, 또는 선박 시스템의 서비스/운영 중단으로 인한 접근 불가 상태
[BIMCO 5.1 CIA 모델]

기밀성, 무결성, 가용성의 상대적 중요성은 시스템, 정보 또는 데이터의 사용 목적과 IT 시스템인지 OT 시스템인지에 따라 달라집니다. IT 시스템은 일반적으로 기밀성을 더 중시하는 반면, 선박 내 OT 시스템, 특히 안전에 중요한 시스템을 평가할 때는 가용성과/또는 무결성이 더 중요한 요소로 고려될 수 있습니다.
[BIMCO 5.1 CIA 모델]

SMS(안전관리시스템)에는 일반적으로 리스크 평가 매트릭스가 포함되어 있으며, 특정 사건의 영향은 5단계 척도로 측정됩니다. 이 5단계 척도는 인명 안전, 환경 안전, 화물 안전, 자산 안전, 사업 연속성, 재무적 영향, 회사 평판 등 다양한 범주에 미치는 영향의 심각도가 점차 증가하는 구조입니다.
SMS(안전관리시스템)의 기존 영향 척도를 사용하여 사이버 관련 리스크를 설명하면 회사 전체의 이해도를 높일 수 있습니다. 마찬가지로, 회사가 사업 영향 분석(BIA) 모델을 사용하는 경우에도 이 모델을 적용할 수 있으며, 다양한 사업부에서 쉽게 채택할 수 있어야 합니다. 두 모델 중 어느 것도 사이버 위험으로 인한 영향을 설명하는 데 사용되지 않은 경우, 각 영향 수준에 대한 구두 설명을 수정해야 합니다. 이러한 척도를 사용하면 회사는 회사 전체 활동에 대한 중요도에 따라 함대 내 여러 선박을 구분할 수 있습니다. 이러한 척도의 예는 다음과 같습니다.
[BIMCO 5.2 영향 정량화]
<table>
<tr><th>Level</th><th>영향도</th></tr>
<tr><td>1</td><td>건강상 영향이나 부상 없음. 운영, 환경, 자산, 재정, 회사 평판에 대한 피해 없음</td></tr>
</table></td></tr>
</table>

통제항목	C.2.1 사이버 영향도 평가	Basic

2	건강상 매우 경미한 영향 또는 부상, 운영, 환경, 자산, 재정, 회사 평판에 대한 매우 경미한 피해
3	어느 정도 건강상 영향 또는 경미한 부상. 운영, 환경, 자산, 재정, 회사 평판에 대한 매우 경미한 피해
4	중대한 건강상 영향/상대적으로 심각한 부상. 운영, 환경, 자산, 재정, 회사 평판에 대한 국지적이지만 중대한 피해
5	사망 또는 영구적인 장애. 운영, 환경, 자산, 재정, 회사 평판에 대한 광범위하고 심각한 피해

그림 6: SMS(안전관리시스템)에서 영향 수준을 구두로 설명한 예시.

[BIMCO 5.2 영향 정량화]

또한 규모를 정의하는데 도움이 될 수 있는 몇가지 다른 평가 방법론도 있습니다.

잠재적 영향	정의	실제 적용 예시
낮음	기밀성, 무결성 또는 가용성의 손실은 회사 및 선박, 조직 자산 또는 개인에게 제한적인 부정적 영향을 미칠 것으로 예상됨	제한된 부정적 영향이란 다음과 같은 보안 침해가 발생할 가능성이 있음을 의미함: (i) 개인에게 경미한 피해를 입힘 (ii) 경미한 재정 손실 초래함 (iii) 조직 자산에 경미한 피해 (iv) 조직이 기본적인 기능을 수행할 수 있는 정도와 기간까지 선박 운영의 저하를 일으키지만, 해당 기능의 효과는 눈에 띄게 감소한 경우
중간	기밀성, 무결성 또는 가용성의 손실은 회사 및 선박, 자산 또는 개인에게 상당한 부정적 영향을 미칠 것으로 예상됨	중대한 부정적 영향이란 다음과 같은 보안 침해가 발생할 가능성이 있음을 의미함: (i) 목숨을 잃거나 생명에 위협을 주는 부상과 관련 없이 개인에게 상당한 피해를 입힘 (ii) 상당한 재정 손실을 초래함 (iii) 조직의 자산에 중대한 피해를 입힐 수 있음 (iv) 조직이 기본적인 기능을 수행할 수 있는 정도와 기간까지 선박 운영에 중대한 저하를 일으키지만, 기능의 효율성은 상당히 감소하는 수준
높음	기밀성, 무결성 또는 가용성의 손실은 회사 및 선박 운영, 자산, 환경 또는 개인에게 심각하거나 치명적인 부정적	중대하거나 치명적인 부정적 영양이란 다음과 같은 보안 침해가 발생할 가능성이 있음을 의미함: (i) 인명에 지장을 주거나 심각한 위협적 부상을 입히는 심각한 결과를 초래하는 경우

통제항목	C.2.1 사이버 영향도 평가	Basic

	영향을 미칠 것으로 예상됨	(ii) 중대한 재정 손실을 초래함 (iii) 환경 및/또는 조직의 주요 자산에 중대한 피해를 초래하는 결과를 가져옴 (iv) 선박 운영의 심각한 저하 또는 손실로 인해 조직이 기본 기능 중 하나 이상을 수행할 수 없는 정도와 기간으로 이어짐.

그림 7: CIA모델을 사용할 경우 잠재적 영향 수준.

[BIMCO 5.2 영향 정량화]

선박에 탑재된 모든 시스템에 대해 영향 평가가 수행되어야 합니다. OT 시스템의 경우, 이러한 영향 평가는 장비 및 기술 시스템 목록의 일부로 간주되며, 해당 시스템의 갑작스러운 작동 실패는 크든 작든 리스크한 상황으로 이어질 수 있습니다. 이는 ISM 코드 10.4항에서 요구하는 사항으로, 흔히 "중요한(Critical)" 장비 및 기술 시스템이라고도 불립니다.

[BIMCO 5.3 "중요" 장비 및 기술 시스템]

IT 시스템의 잠재적 영향 또한 평가되어야 하며, 일반적으로 주요 사용자들의 의견이 필요합니다. 시스템의 기능에 따라 이는 화물 적재 담당자, 운영 인력, 상업 및 재무 담당자 등이 될 수 있습니다. IT 시스템의 성능 저하 또는 손실은 선박의 운영, 규제 준수, 심지어 안전 성과에 매우 큰 지장을 줄 수 있으므로 과소평가되어서는 안 됩니다.

[BIMCO 5.3 "중요" 장비 및 기술 시스템]

예시

한 선박에는 복잡한 전력 관리 시스템이 설치되어 있습니다. 이 시스템은 자동 부하 분산, 전력 제어 및 동기화를 위한 스위치보드와 발전기 제어 시스템으로 구성됩니다. 전력 관리 시스템 상위에는 SCADA(감시 제어 및 데이터 수집) 시스템이 있으며, 이 시스템은 출력값을 제공하고 선원들이 선박 내 전력 분배를 제어할 수 있도록 합니다.

전력 관리는 승무원, 선박, 화물의 안전에 매우 중요합니다. 또한 환경적·재정적 영향도 명확합니다. 주 발전기(축 발전기) 또는 보조 엔진의 사용을 통해 전력이 생성되기 때문입니다. 따라서 사이버 사고로 인해 전력 관리 시스템이 작동하지 않거나 오작동할 경우 선박의 작동 및 안전에 영향을 줄 수 있습니다. 이러한 리스크를 줄이기 위해, 회사는 해당 사이버 사고 가능성을 최소화할 수 있는 보호 조치를 추가해야 합니다.

SCADA 시스템은 전력 관리를 위해 선박 내에서 사용되는 실시간 센서 데이터를 포함하며, 선박 회사의 행정 목적을 위해 사용되는 전력 소비 통계 데이터도 생성합니다. 정보 또는 데이터가 침해되었을 때의 잠재적 영향을 판단하기 위해 CIA 모델을 활용할 수 있습니다. 따라서 선사는 SCADA 시스템에서 처리되거나 전송되는 가장 민감한 정보에 대한 잠재적 영향을 평가해야 합니다.

CIA 모델을 활용하면 선사는 다음과 같은 결론을 도출할 수 있습니다:

- SCADA 시스템에서 획득한 센서 데이터의 기밀성이 손실되는 경우는 그 정보가

통제항목	C.2.1 사이버 영향도 평가	Basic

선박 내에 공개적으로 표시되기 때문에 낮은 영향으로 평가됩니다. 그러나 안전성 관점에서는 센서가 전송하는 정보를 신뢰할 수 있어야 하므로 무결성 상의 높은 영향이 존재할 수 있습니다. 만약 정보를 읽을 수 없다면 가용성 손실로 인한 안전상의 문제가 발생할 수 있으므로 가용성에도 높은 영향이 있습니다.

- 전력 소비 통계 정보가 외부에 전송되는 것과 관련된 기밀성 손실은 잠재적인 낮은 영향으로 평가됩니다. 해당 데이터는 사내 용도로만 사용되므로 무결성 및 가용성 손실에 대한 영향도 낮게 평가됩니다.

다음 그림은 평가 결과를 보여줍니다.

SCADA 시스템	기밀성	무결성	가용성	종합 영향
센서 데이터	높음	높음	높음	높음
통계 데이터	낮음	낮음	낮음	낮음

그림 8: SCADA 시스템에 대한 CIA 평가 결과.

[BIMCO 5.3 “중요” 장비 및 기술 시스템]

비고	

통제항목	C.2.2 사이버 발생빈도 평가	Basic

레퍼런스 상세

BIMCO

IT 시스템이 데이터를 관리하고 비즈니스 기능을 지원하는 반면, OT는 물리적 장치와 프로세스를 직접 모니터링/제어하는 하드웨어 및 소프트웨어로, 선박의 필수 구성 요소이며 선내 IT 시스템과 독립적으로 작동해야 합니다. 그러나 이러한 시스템은 성능 모니터링, 원격 지원 등을 위해 IT 네트워크에 연결될 수 있습니다. 이러한 시스템을 산업용 사물 인터넷(IIOT)이라고도 합니다. 이러한 경우, 인터페이스는 최소한 방화벽으로 충분히 보호되어야 하며, OT 시스템의 잠재적 취약점이 IT 네트워크에 노출되지 않도록 해야 합니다. 이는 OT 시스템에 적절한 패치 수준을 적용하는 것이 항상 가능하거나 실현 가능한 것은 아니기 때문에 중요합니다.

[BIMCO 1.4 IT와 OT 시스템의 차이점]

위협을 식별할 때 기업은 잠재적 위협 행위자의 역량, 기회, 그리고 공격 의도 등 구체적인 측면을 고려해야 합니다. 위협이 식별되면, 식별된 취약성과 함께 위협을 고려하여 공격이나 사고의 발생빈도를 평가해야 합니다. 특정 사건의 영향과 함께, 사고의 발생빈도에 따라 위험 요소가 생성됩니다.

[BIMCO 2.1 위협 행위자]

조직이나 개인은 의도적 또는 비의도적인 방식으로 선원, 환경, 선박의 안전과 보안에 위협이 될 수 있습니다. 다음 그림은 다양한 위협 행위자 유형과 그들의 동기 및 목적을 예시로 제시합니다.

이 목록은 포괄적이지 않으며, 이러한 위협 행위자들은 각기 다른 수준의 기술과 자원을 가지고 있어, 선박과 기업의 안전, 보안, 그리고 비즈니스 운영 능력에 위협을 가할 수 있습니다.

[BIMCO 2.1 위협 행위자]

그룹	범행동기
우연한 행위자	악의적인 동기는 없지만, 감염된 USB를 선내 IT, OT 시스템에 삽입하는 등 불운, 지식 부족 또는 관리 부족으로 인해 의도치 않게 피해를 입히는 경우
내부자	정치적인 복수 운영중단 언론의 관심 명예훼손
범죄자	재무적 이득 상업적 스파이 행위 산업 스파이 행위
기회주의자	도전 평판 향상 재정적 이득

통제항목	C.2.2 사이버 발생빈도 평가	Basic

그룹	범행동기
국가/국가 지원 단체	정치적/이념적 이득 예: 경제 및 중요 국가 기반시설에 대한 (통제되지 않은) 방해 간첩 활동 혼란 재정적 이득 상업 스파이 활동 산업 스파이 상업적 이득
테러리스트	정치적인 재정적인 혼란 인식/미디어의 관심

[BIMCO 2.1 위협 행위자]

일반적으로, 기업과 선박에 영향을 미칠 수 있는 사이버 위협은 두 가지 범주로 나눌 수 있습니다:

- 특정 기업이나 선박의 시스템 및 데이터가 여러 잠재적 표적 중 하나이거나, 의도치 않은 피해자 또는 부수적 피해를 유발하는 비표적 공격(예: NotPetya의 영향을 받은 선박은 표적 피해자가 아님). 비표적 공격은 인터넷에서 이용 가능한 도구와 기술을 사용할 가능성이 높으며, 이를 통해 기업 및 선박에 존재할 수 있는 광범위한 취약점을 찾아내고, 발견하여 악용할 수 있습니다.
- 특정 회사 또는 선박의 시스템 및 데이터가 의도된 공격 대상이거나 여러 대상 중 하나인 표적 공격. 표적 공격은 더욱 정교할 수 있으며, 소셜 미디어나 웹페이지 등을 통한 사전 정찰이 필요할 수 있으며, 특정 회사나 선박을 표적으로 삼도록 특별히 개발된 도구와 기술을 사용합니다.

[BIMCO 2.2 사이버 위협의 유형]

이러한 상황에서 사용할 수 있는 도구와 기술의 예는 다음과 같습니다:

- 맬웨어. 소유자 모르게 컴퓨터에 접근하거나 손상시키도록 설계된 악성 소프트웨어입니다. 트로이 목마, 랜섬웨어, 스파이웨어, 바이러스, 웜 등 다양한 유형의 맬웨어가 있습니다. 랜섬웨어는 몸값을 지불할 때까지 시스템의 데이터를 암호화합니다. 맬웨어는 또한 오래되었거나 패치되지 않은 비즈니스 소프트웨어의 알려진 결함과 문제점을 악용할 수 있습니다. "악용"이라는 용어는 일반적으로 다른 컴퓨터의 소프트웨어 또는 하드웨어의 문제점을 악용하고 조작하도록 설계된 소프트웨어 또는 코드의 사용을 의미합니다. 이러한 문제는 예를 들어 코드 버그, 시스템 취약성, 부적절한 설계, 하드웨어 오작동 및/또는 프로토콜 구현 오류일 수 있습니다. 경우에 따라 스파이웨어는 관리자 사용자 자격 증명을 식별하여 악의적인 공격자가 관리자 사용자로 로그인하여 시스템 기능을 조작할 수 있도록 허용합니다. 이러한 취약점은 원격으로 악용되거나 로컬에서 트리거될 수 있습니다. 예를 들어, 악성 코드는 종종 사용자가 실행할 수 있으며, 때로는 이메일

통제항목	C.2.2 사이버 발생빈도 평가	Basic

첨부 파일로 배포된 링크나 악성 웹사이트를 통해 실행될 수 있습니다.

- 워터홀링(Water holing). 가짜 웹사이트를 만들거나 진짜 웹사이트를 해킹하여 악용하는 행위로, 아무것도 모르는 방문객들을 착취당하게 합니다.
- 스캐닝. 인터넷의 광범위한 부분을 무작위로 검색하여 잠재적인 취약점을 찾아내는 작업입니다.
- 타이포스쿼팅(Typosquatting). URL 하이재킹 또는 가짜 URL이라고도 합니다. 인터넷 사용자가 웹 브라우저에 웹사이트 주소를 입력할 때 오타를 내거나, 얼핏 보면 익숙한 웹사이트처럼 보이는 링크를 클릭하도록 유도하는 등의 실수를 이용합니다. 사용자가 실수로 잘못된 웹사이트 주소를 입력할 경우, 악성 웹사이트로 연결될 수 있습니다.
- 사회 공학. 잠재적 사이버 공격자가 내부자를 조종하여 보안 절차를 위반하도록 하는 비기술적 기법으로, 일반적으로 이메일, 소셜 미디어, 전화 통화 또는 대면 접촉을 통해 이루어지나, 이에 국한되지는 않습니다.
- 무차별 대입 공격. 여러 개의 비밀번호를 시도하여 결국 정답을 맞히려는 공격입니다. 공격자는 올바른 비밀번호를 찾을 때까지 가능한 모든 비밀번호를 체계적으로 확인합니다.
- 자격 증명 스터핑. 이전에 손상된 자격 증명이나 일반적으로 사용되는 특정 자격 증명을 사용하는 행위로, 시스템이나 애플리케이션에 대한 무단 액세스를 시도하기 위한 비밀번호를 사용하는 것입니다.

위협 식별

- 서비스 거부(DoS) 공격은 일반적으로 네트워크에 데이터를 대량으로 공급하여 합법적이고 권한이 있는 사용자가 정보에 접근하지 못하도록 차단합니다. 분산 서비스 거부(DDoS) 공격은 여러 컴퓨터 및/또는 서버를 제어하여 DoS 공격을 실행합니다.
- 피싱. 다수의 잠재적 대상에게 이메일을 발송하여 특정 민감 정보나 기밀 정보를 요구하는 행위입니다. 이메일에는 악성 첨부 파일이 포함되어 있거나, 이메일에 포함된 하이퍼링크를 통해 가짜 웹사이트를 방문하도록 유도할 수도 있습니다.
- 스피어피싱. 피싱과 유사하지만, 개인 이메일을 통해 개인을 표적으로 삼는 방식으로, 악성 소프트웨어나 악성 소프트웨어를 자동으로 다운로드하는 링크가 포함된 경우가 많습니다. 경우에 따라 SAT-C 메시지를 통해 악의적인 발신자의 이메일 주소를 인지하는 데 사용되기도 했습니다.
- 공급망을 파괴합니다. 장비를 손상시켜 회사나 선박에 제공되는 소프트웨어나 지원 서비스를 공격합니다.

위의 예시는 모든 것을 포괄하는 것은 아닙니다. 사이버 공격에 사용되는 도구와 기술의 수와 정교함은 끊임없이 진화하고 있으며, 이를 개발하는 조직과 개인의 독창성에 의해서만 제한될 뿐입니다.

[BIMCO 2.2 사이버 위협의 유형]

일반 고려사항

위협(threat)은 위협 행위자의 능력(capability), 기회(opportunity), 의도(intent)의 곱으로 정의됩니다. 위협을 정량화하는 목적은 발생빈도(likelihood)을 수치화하는

통제항목	C.2.2 사이버 발생빈도 평가	Basic

데 있으며, 이는 리스크(risk)을 계산할 때 핵심 요소인 발생빈도와 영향 중 하나입니다. 즉, 위협 행위자의 능력, 기회 또는 의도가 0 또는 0에 가까운 경우, 그에 따른 리스크는 작거나 무시할 수 있을 정도로 낮습니다.

[BIMCO 2.4 위협의 정량화]

역사적 증거가 있는 다른 안전 및 보안 분야와 달리, 사이버 위험 관리는 사고와 그 영향에 대한 통계가 부족하여 더욱 어렵습니다. OT 시스템을 특별히 표적으로 삼은 공격이 증가하고 있지만 여전히 그러한 공격이 지속되고 있다는 징후가 있습니다. IT 시스템에 대한 공격에 비해 덜 흔하며, 많은 경우 공개되지 않습니다. 그 이유는 다음과 같습니다.

- 해양 산업의 많은 OT 시스템은 여전히 외부 네트워크에 연결되지 않았습니다. 접근성, 즉 위협 노출이 낮고 사이버 범죄자가 공격할 기회가 없습니다. 그러나 예외도 있습니다. 예를 들어, 많은 모니터링 장치(예: 엔진 성능 모니터링 장치)는 인터넷에 연결되어 있으며, 특히 다른 IT 또는 OT 시스템에 비해 최소한의 사이버 보안 제어만 갖추고 있습니다. 이러한 IIOT 시스템은 선박 내 통합이 더욱 강화되어 원격 모니터링 및 시스템 연결을 통해 운영 자동화 및 효율성을 높이고 있습니다. 위협 행위자는 이러한 시스템을 스캔하여 선박 네트워크 침투의 초기 지점으로 활용할 수 있으며, 앞서 설명한 바와 같이 이를 기반으로 공격을 전개할 수 있습니다. 따라서 이러한 시스템에 대한 위험은 평가하는 것이 중요하며 간과해서는 안 됩니다.
- OT 시스템을 공격하면 피해자에게 안전 위험이 초래되며, 이는 일부 사이버 범죄자에게는 억제력이 될 수도 있습니다.
- OT 및 IIoT 시스템에서는 기본적인 위협 정보와 비정상적인 활동을 모니터링하는 기능을 IT 시스템과 달리 쉽게 사용할 수 없으므로 침해를 감지, 분석하고 대응하는 것이 어렵습니다.

위의 내용에도 불구하고, 운영 시스템(OT)에 대한 위험을 과소평가해서는 안 됩니다. 온라인 또는 USB 메모리와 같은 수동 프로세스를 통해 소프트웨어 업데이트를 통해 유입되는 맬웨어나 승무원의 규제되지 않거나 허가받지 않은 접근을 통해 발생하는 위협은 여전히 발생할 수 있으며, 운영 중단 및 다운타임을 유발하는 것으로 알려져 있습니다.

[BIMCO 2.4 위협의 정량화]

IT 시스템에 대한 위협

IT 시스템에 대한 위협은 일반적으로 정량화하기가 더 쉽습니다. 그 이유는 일반적인 산업뿐만 아니라 해운 산업에서도 사고 관련 증거와 통계가 많기 때문입니다. 보통 IT 시스템의 중단은 인명, 환경, 자산, 화물 등에 직접적인 리스크 요소로 간주되지 않습니다. 그러나 IT 시스템에 대한 위협도 절대 과소평가해서는 안 됩니다. 최근 정기선 산업 사례에서는 사이버 사고가 선박 운영 및 화물 관리에 막대한 혼란을 초래하고, 이는 심각한 재정 손실로 이어질 수 있다는 점을 보여주었습니다. 또한, 이러한 사고는 인명, 환경, 자산, 화물의 안전에 연쇄적 영향을 미칠 수 있으며, 예를 들어 IT 시스템 장애로 인해 부패성 화물 또는 리스크물의 통제를 상실하는 사태로 이어질 수 있습니다.

통제항목	C.2.2 사이버 발생빈도 평가	Basic

[BIMCO 2.4 위협의 정량화]

다음은 기존 선박에서 발견될 수 있는 일반적인 사이버 취약점입니다(참고로, 새로 건조된 선박은 IACS 통합 요구 사항 E26 및 E27에 명시된 요구 사항을 준수해야 합니다).

- 더 이상 지원되지 않는 운영 체제입니다.
- 패치되지 않은 시스템 소프트웨어
- 오래되었거나 누락된 바이러스 백신 소프트웨어 및 맬웨어 방지 기능
- 비효율적인 네트워크를 포함한 부적절한 보안 구성 및 모범 사례 관리, 이동식 미디어의 불충분한 검사 및 기본 관리자 계정과 암호 사용(때로는 모든 사람이 볼 수 있도록 게시됨)
- 약하고 일반적이거나 쉽게 추측할 수 있는 비밀번호
- 공유 계정 및 다중 요소 인증 부족
- 경계 보호 조치 및 세분화가 부족한 선박 컴퓨터 네트워크
- 안전에 중요한 장비 또는 시스템은 항상 해안 측과 연결됩니다.
- 제3자를 포함한 사이버 자산, 네트워크 등에 대한 부적절한 액세스(계약자 및 서비스 제공자)
- 사이버 위험을 관리하는 데 필요한 교육 및/또는 기술이 부족한 직원
- 누락, 부적절 또는 테스트되지 않은 비상 및 사고 대응 계획 및 절차
- 자산 수명 주기에 정의된 대로 해체 및 폐기 활동을 완료하지 못함(정책 및 절차)
- 검색이나 스트리밍과 같은 개인 활동을 위한 비즈니스 네트워크 사용
- 컴퓨터가 유휴 상태일 때 잠기지 않습니다.

[BIMCO 3.1 공개적인 취약점]

취약점 식별은 어플리케이션, 시스템, 절차를 분석하여 위협 행위자가 악용할 수 있는 약점을 찾아내는 과정을 포함합니다. 이 과정은 내부 전문가 또는 해운 산업과 주요 프로세스에 대한 이해를 가진 외부 전문가의 지원을 통해 수행될 수 있습니다.

[BIMCO 3.3 일반적인 취약 시스템]

선박의 네트워크 및 시스템 평가의 핵심 목표는 시스템, 네트워크 또는 선박 전체의 기밀성, 무결성 또는 가용성을 위협할 수 있는 취약점 및 약점을 식별하는 것입니다. 이러한 취약점은 다음과 같은 범주에 해당할 수 있습니다:

- 소프트웨어 결함, 구식 또는 패치되지 않은 시스템 등 일시적 노출
- 접근 관리, 미관리된 네트워크 연결 등 설계상의 결함
- 방화벽이 잘못 구성되었거나 불필요한 방화벽을 비활성화하지 못한 경우와 같은 구현 오류(컴퓨터의 소프트웨어)
- 절차적 또는 기타 사용자 오류(예: 암호 보호 및 인증 부족 프로세스)

[BIMCO 3.3 일반적인 취약 시스템]

독립형 시스템은 외부 사이버 사고에 덜 취약하지만, 인터넷 또는 무방비 네트워크와 연결된 경우 더 큰 리스크에 노출됩니다. 많은 사고가 인적 요인에 의해 발생하므로, 사용자의 행동도 반드시 고려되어야 합니다. 다음은 리스크에 노출될 수 있는 선박 내 시스템 예시입니다:

- 화물 및 적재 관리 시스템: 리스크 화물을 포함한 화물 적재/관리 디지털 시스템은

통제항목	C.2.2 사이버 발생빈도 평가	Basic

항만, 해상 터미널, 도선사와 연동될 수 있습니다. 이들은 인터넷 기반 화물 추적 시스템과 인터페이스되며, 적재 명세서 및 화물 리스트가 사이버 위협에 노출될 수 있습니다.

- 브리지 시스템: 디지털 내비게이션 시스템의 활용이 증가하면서, 업데이트 및 서비스 제공을 위해 육상 시스템과의 연결이 요구됩니다. 독립형 시스템이 아닌 경우, 이동식 저장장치(USB 등)를 통해 업데이트되며, 이로 인해 외부 또는 통제되지 않은 네트워크를 통한 감염 리스크가 존재합니다.
- 기관 및 전원 제어 시스템: 디지털 시스템은 엔진, 추진, 전력 제어를 위한 장치에 적용됩니다. 이 시스템들이 네트워크로 통합될 경우 리스크가 증가할 수 있으며, 특히 무단 접근 시 시스템 마비가 발생할 수 있습니다.
- 출입 통제 시스템: 선박 보안, 감시, 접근 통제 등을 위한 디지털 시스템은 중요한 물리적 보안을 담당하므로, 사이버 사고에 매우 민감합니다.
- 여객 서비스 및 관리 시스템: 승선/하선, 자산관리, 출입통제 등과 관련된 디지털 시스템은 수집된 데이터를 타 시스템으로 전달하게 되어 공격 벡터가 될 수 있습니다.
- 여객용 공용 네트워크: 엔터테인먼트 목적 등으로 탑재된 고정/무선 네트워크는 안전 시스템과 분리되어야 하며, 별도로 관리되어야 합니다.
- 행정 및 복지 시스템: 선내 이메일, 인터넷 접근 등은 사이버 공격자의 진입 경로가 될 수 있으며, 이 시스템은 안전 관련 시스템과 분리되어야 합니다.
- 통신 시스템: 위성 또는 무선 통신은 선박의 보안에 취약점을 증가시킵니다. VSAT 등은 저비용 제품을 통한 악용 리스크가 존재하며, 암호화, 인증, 접근통제 정책이 엄격히 적용되어야 합니다. 또한, 컨테이너 부착 장비, 데이터 로거 등도 취약점이 될 수 있습니다.

[BIMCO 3.3 일반적인 취약 시스템]

위 시스템들은 잠재적으로 취약한 장비로 간주되어 평가 시 반드시 점검되어야 합니다. 각 시스템의 취약점 평가는 아래와 같은 질문을 통해 보완할 수 있습니다:

- 이 시스템은 독립형인가, 다른 시스템과 연결되어 있는가?
- 이 시스템은 외부 또는 다른 시스템과 연결되어 있는가?
- 이 시스템은 자체적인 보안 조치를 갖추고 있는가? (예: 암호화)
- 이 시스템은 정기적인 소프트웨어 업데이트가 필요한가?
- 이 시스템은 외부 진단 장비 연결을 필요로 하는가?
- 이 시스템은 중요한가?

[BIMCO 3.3 일반적인 취약 시스템]

리스크를 평가할 때, 흔히 잠재적 영향과 기존의 취약성만을 기준으로 판단하는 경향이 있습니다. 하지만 앞서 설명했듯이, 사이버보안 사고가 발생빈도는 위협과 취약성의 곱으로 나타낼 수 있습니다. 이는 두 요소 중 하나라도 거의 존재하지 않거나 0에 가깝다면, 발생빈도 또한 낮거나 거의 없다는 것을 의미합니다. 따라서 발생빈도를 정량화할 때 이 점을 반드시 고려해야 합니다.

[BIMCO 4.1 위협과 취약성의 곱으로서의 발생빈도]

회사의 SMS(안전관리시스템)에는 일반적으로 특정 사건의 발생 가능성을 5단계

통제항목	C.2.2 사이버 발생빈도 평가	Basic

척도로 측정하는 위험 평가 매트릭스가 포함됩니다. SMS(안전관리시스템)의 기존 발생 가능성 척도를 사용하는 것이 유리할 수 있습니다. 사이버 관련 위험을 설명하는 데 기존 언어와 개념을 사용하면 회사 전체의 효율 측정 및 이해도를 높일 수 있기 때문입니다. 위험 평가 결과에 기반한 효과적인 사이버 위험 관리 전략에 대한 고위 경영진의 지원을 확보하기 위해서는 전사적 위험 관리 전략과 이에 대한 이해가 일치되어야 합니다. 이러한 척도의 한 예는 다음과 같습니다.

[BIMCO 4.2 발생빈도의 정량화]

Level	발생 빈도 설명
1	업계에서 들어본 적도 없는 사건, 상상할 수 없을 정도로 드문 수준
2	업계에서는 들어본 적 있지만, 극히 드물고 불운한 사건들이 연쇄적으로 일어났을 때 발생
3	자사 내에서 발생한 적 있는 사건, 보통 장비 결함이나 인적 실수로 인한 경우
4	자사 내에서 가끔 발생, 보통 장비 문제 또는 승선 중 종종 일어나는 인적 실수로 인한 경우
5	해당 작업을 수행할 때 자주 발생

그림 5: SMS(안전관리시스템)에서 사용된 발생빈도 척도의 예시

[BIMCO 4.2 발생빈도의 정량화]

이상적인 상황에서는, 해당 부문을 겨냥한 식별된 위협 활동과 사고 보고서를 기반으로 한 해운 산업별 위협 인텔리전스에 대한 접근을 통해 발생빈도를 정량화할 수 있을 것입니다. 이러한 위협 인텔리전스는 국제 해운 시스템 정보 공유 및 분석 센터(MTS-ISAC)나 NORMA Cyber, France Cyber Maritime 등 국가 차원의 노력을 통해 확보할 수 있습니다. 이러한 출처는 기업에 상황 인식을 제공할 수 있습니다. 예를 들어, 어떤 위협 행위자가 해당 부문을 적극적으로 표적으로 삼고 있는지, 현재 진행 중인 캠페인의 위협 지표, 표적으로 삼은 취약성 등을 파악하여 사이버 공격의 가능성과 잠재적 영향을 판단하는 데 도움이 됩니다. 더욱이 위협 요인의 역량, 기회, 그리고 의도를 면밀히 살펴보는 것이 종종 도움이 될 것입니다. 특히 의도를 살펴보는 것이 유용할 수 있는데, 의도가 전혀 없다면 주어진 잠재적 위협이 이론적인 것으로 정량화될 뿐이며, 따라서 취약점과 병치되거나 또는 그 위협과 곱해졌을 때 발생 가능성이 매우 낮기 때문입니다.

[BIMCO 4.2 발생빈도의 정량화]

비고	

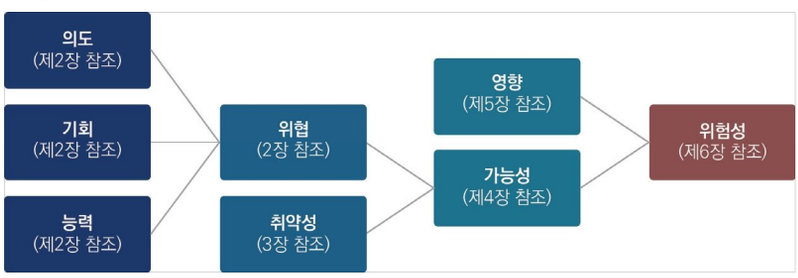
통제항목	C.2.3 사이버 리스크 평가		Basic
레퍼런스 상세	IMO	선박 및 선박/항구 인터페이스에 대한 현재 사이버 리스크를 파악합니다. **[IMO 3.5.2 식별]** 선박 운항에 필수적인 시스템, 서비스, 자산, 데이터 및 역량에 대한 리스크 평가를 수행합니다. 갑작스러운 운영 중단으로 인해 위험한 상황이 발생할 수 있습니다. 사이버 관련 위협을 식별합니다. 시스템, 서비스, 자산, 데이터 및 역량의 취약성을 식별합니다. 사이버 사고 발생 가능성과 해당 요소의 안전, 가용성, 무결성 및 기밀성에 미치는 영향을 평가합니다. **[IMO 3.5.2.3 식별]**	
	BIMCO	그림 1(가이드라인에 명시된 사이버 위험 관리 접근 방식)의 접근 방식에 따라 사이버 위험 관리 프로그램을 개발, 구현 및 유지하는 것은 결코 간단한 작업이 아닙니다. 따라서 보호 및 비상 계획의 균형을 유지하고 위험을 허용 가능한 한도 내에서 관리하기 위해 고위 경영진이 프로세스 전반에 걸쳐 지속적으로 참여하는 것이 중요합니다. 악의적인 행위자의 영향, 발생 가능성, 취약성, 위협, 역량, 기회 및 의도와 같은 요소는 서로 연관되어 있으며(아래 그림 참조), 모두 위험 평가에 중요한 역할을 합니다. 따라서 다음 중 하나가 해당되는 경우 요인 중 낮은 수준 또는 0%라도 결국 위험에는 동일한 사항이 적용됩니다. 위험 평가는 일회성 활동이 아니라는 점을 강조하는 것이 중요합니다. 위협, 취약성, 발생 가능성, 영향 및 위험이 변화했는지, 그리고 통제 조치가 여전히 적절한지 평가하기 위해 정기적으로 반복해야 합니다. **[BIMCO 1.1 해운 산업의 사이버보안 특성]** IT 시스템은 데이터를 관리하고 비즈니스 기능을 지원하는 반면, OT는 물리적 장치와 프로세스를 직접 모니터링 및 통제하는 하드웨어 및 소프트웨어로, 선박의 통제계 구성 요소이며 선상 IT 시스템과 독립적으로 작동해야 합니다. 그러나 시스템은 성능 모니터링, 원격 지원 등을 위해 IT 네트워크에 연결될 수 있으며, 이러한 시스템은 때때로 산업용 사물인터넷(IIoT)에 속한다고 일컬어집니다. 이러한 경우 인터페이스가 최소한 방책적으로 충분히 보호되고 잠재적인 리스크가 있는지를 확인해야 합니다. **[BIMCO 1.4 IT와 OT 시스템의 차이점]** IT는 소프트웨어, 하드웨어 및 통신 기술을 포함하여 정보 처리를 위한 기술 전반을 포괄합니다. 전통적으로 OT와 IT는 분리되어 왔으나, 인터넷의 등장으로 인해 과거에는 독립적으로 운영되던 시스템들이 통합되면서 OT와 IT는 점점 더 가까워지고 있습니다. OT 시스템의 운영이 중단되면 선내 인원의 안전, 화물, 해양 환경에 피해를 줄 수 있으며 선박 운항에도 지장을 초래할 수 있습니다. 마찬가지로, 특정 IT 시스템이 실패할 경우(예: 위험물 적하목록에 즉시 접근할 수 없는 상황), 위험한 상황이 발생할 수도 있습니다. 예를 들어, 선박에 실린 컨테이너에서 화재가 발생했을 때 인접한 컨테이너의 적재 내용에 대한 정보는 올바른 소방 활동을 위해 매우 중요합니다. **[BIMCO 1.4 IT와 OT 시스템의 차이점]** OT 시스템과 선박의 IT 시스템 구매 및 관리를 담당하는 사람 간에도 중요한 차이가 있을 수 있습니다. IT 관리자는 일반적으로 OT 시스템 구매에 관여하지 않으며 사이버보안에 대한 깊이 있는 이해가 있을 수도 있고 없을 수도 있습니다. 이러한 시스템 구매에는 선내 시스템에 미치는 영향에 대해 잘 알고 있지만 소프트웨어	

통제항목	C.2.3 사이버 리스크 평가	Basic

및 사이버 위험 관리에 대한 지식은 제한적일 가능성이 높은 사람이 참여해야 합니다. 따라서 OT 구매 과정에서 사이버 위험을 고려하기 위해 사이버보안에 대한 지식이 있는 사람과 상담하는 것이 중요합니다. OT 소프트웨어 업데이트는 제조업체에서 수행하는 경우가 많으며, 일반적으로 정기적으로 업데이트되는 IT 소프트웨어와 달리 사이버보안 고려 사항, 철저한 호환성 검사 및 등급 승인을 포함한 변경 관리가 필요합니다. 잠재적인 과제를 파악하고 소프트웨어 유지 관리에 필요한 정책 및 절차를 수립하기 위해 선박의 사이버보안 담당자가 OT 시스템 목록을 보유하는 것이 유리할 수 있습니다.

[BIMCO 1.4 IT와 OT 시스템의 차이점]

위협(의도, 역량, 기회), 취약점, 영향 및 발생빈도에 대한 개요가 수립된 이후에야 비로소 리스크 평가를 수행할 수 있습니다. 리스크 평가는 일회성 활동이 아니며, 지속적이고 사전 예방적인 위험 관리 접근 방식의 일부입니다. 이는 위험을 정기적으로 재평가하고 적절하고 최신 완화책을 구현하는 것을 의미합니다.



[BIMCO 6.1 리스크에 영향을 미치는 요소 간의 관계]

그림 9: 리스크에 영향을 미치는 다양한 요인들 간의 관계. 선은 곱셈을 나타내며, "발생빈도"와 "영향"을 곱하여 "리스크"를 생성합니다.

[BIMCO 6.1 리스크에 영향을 미치는 요소 간의 관계]

1단계: 사전 평가 활동

리스크 평가는 기존 선박, 신조선 및 중고선에 적용되며, 함대에 새로 도입되는 중고선에는 특별한 주의를 기울여야 합니다. 사이버 리스크 평가는 복잡한 작업으로, 사이버 리스크 관리에 대한 상세한 지식이 필요하며, 리스크 평가 과정에 제3자의 지원이 필요할 가능성이 높습니다.

선상에서 사이버 리스크 평가를 시작하기 전에 다음과 같은 활동을 수행해야 합니다.:

- 3.2에 설명된 IT 및 OT 시스템 문서를 검토하고, 예를 들어 CIA 모델(5.1 참조) 등을 사용하여 잠재적 영향 수준을 평가합니다.
- 주요 선박 내 IT 및 OT 장비의 주요 제조업체를 파악합니다. (이 식별 과정에서는 리스크 기반 접근법을 사용하는 것이 좋습니다.)
- 주요한 제조사와의 사이버보안 연락처를 파악하고 협력 관계를 구축합니다.
- IT 및 OT 시스템의 유지보수 및 지원에 대한 상세한 문서를 검토합니다.
- 선주/선박 운영자가 선박 내 네트워크 및 장비의 유지보수와 지원에 대해 갖는 계약상 요구사항과 의무를 수립합니다.

[BIMCO 6.2 리스크 평가의 네 가지 단계]

통제항목	C.2.3 사이버 리스크 평가	Basic

2단계: 선박 평가

모든 위협 요소(위협, 취약점, 발생 빈도, 영향 등)가 평가되면, 리스크 평가 및 이에 따른 리스크 저감 조치를 수행할 수 있습니다. 리스크 평가는 관련 리스크 요소에 대한 체계적인 고려과정을 의미합니다.

[BIMCO 6.2 리스크 평가의 네 가지 단계]

리스크 평가는 시스템별로 수행되며, 따라서 5.2절에 설명된 시스템 문서화에 기반하여 진행됩니다. 정확하게 평가하기 위해서는, 각 시스템의 기능, 데이터 흐름, 그리고 시스템 간 연결 방식(유선 또는 무선) 에 대한 이해가 필요합니다. 이러한 이유로, 리스크 평가는 회사 내부의 다양한 직원, 장비 제조업체, 필요 시 외부 사이버보안 전문가의 폭넓은 의견 수렴이 요구될 가능성이 높습니다. 모든 연결 지점은 잠재적인 취약점이 될 수 있습니다. 예를 들어, 인터넷에 연결된 공유 네트워크 프린터는 사이버 범죄자가 해당 프린터를 경유해 연결된 다른 시스템에 침입할 수 있는 경로가 될 수 있습니다.

[BIMCO 6.2 리스크 평가의 네 가지 단계]

리스크 평가에 기반한 완화 조치의 식별 및 실행은 ISM 코드와 회사 SMS(안전관리시스템)를 통해 모든 선박에서 확립되어 있습니다. 그러나 사이버 리스크 평가는 SMS(안전관리시스템)에 따라 승무원이 일반적으로 수행하는 운영 위험 평가와 혼동되어서는 안 됩니다. 사이버 리스크 평가에는 다양한 지식과 경험이 필요하며, 복잡성 수준에 따라 사무 직원은 물론, 제3자 컨설턴트의 참여가 필요할 수도 있습니다.

[BIMCO 6.2 리스크 평가의 네 가지 단계]

특정 시스템의 리스크를 평가하려면, 발생빈도(likelihood)와 영향도(impact) 를 함께 고려해야 합니다.

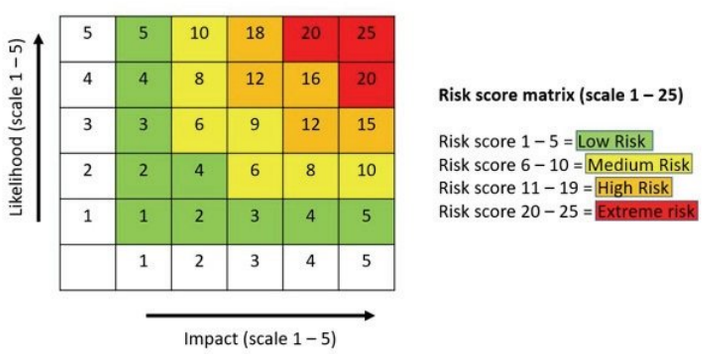


그림 10: 회사의 리스크 점수 행렬의 예시

[BIMCO 6.2 리스크 평가의 네 가지 단계]

회사의 리스크 수용 기준에 따라, 특정 시스템에 대한 계산된 초기 리스크가 허용 가능한 수준을 초과할 경우, 잔존 리스크가 허용 가능한 수준에 도달하도록 완화 조치를 적용해야 합니다 (아래 예시 참조):

통제항목	C.2.3 사이버 리스크 평가	Basic

시스템	영향	발생 빈도	초기 리스크	완화 조치	잔존 리스크
ECDIS	점수 5, 좌초 및 충돌과 같은 치명적인 사고의 리스크로 인하여	점수 4	리스크 = 5X4=20	비밀번호 보호 및 ECDIS 전용으로만 PC 사용 제한	리스크 =5X3=15
				관리 네트워크 연결 차단	리스크 = 5X2=10
				USB 포트 물리적 차단	리스크 =5X1=5

그림 11: 리스크 평가 및 완화 조치 식별 예시

[BIMCO 6.2 리스크 평가의 네 가지 단계]

시스템별로 수행되지만, 선박 리스크 평가는 하나의 시스템에 대해 제안된 잠재적 리스크 완화 조치가 종종 연결된 다른 시스템의 리스크 평가와 물론 비용 효율성에 영향을 미칠 수 있다는 사실을 인지하는 전체적인 접근 방식을 필요로 합니다. 다양한 리스크 완화 조치는 본 지침의 다음 장에서 더 자세히 설명합니다.

평가 과정에서 수행되는 활동에는 필요한 기능과 서비스가 회사 표준에 맞게 구성되어 있는지 확인하기 위해 모든 컴퓨터, 서버, 라우터 및 방화벽을 포함한 사이버보안 기술의 구성을 검토하는 것이 포함될 수 있습니다. 또한, 연결된 IT 및 OT 시스템과 장치에 대한 모든 사이버보안 문서 및 절차를 검토하는 것도 포함될 수 있습니다.

선상 평가의 한 측면은 모든 직급의 승무원, 특히 선장, 기관장, 사관의 참여입니다. 이 과정은 승무원들이 선상 IT 및 OT 시스템의 구현 방식을 이해하고, 이러한 시스템이 명시된 설계 문서와 어떻게 다를 수 있는지, 그리고 선원들에게 제공될 사이버 교육 수준을 이해하는 데 도움이 됩니다.

완화 조치의 선택은 가용 자원과 리스크의 특성에 따라 달라집니다. 절차적 변경을 포함한 일부 완화 조치는 사건 발생 가능성, 빈도 또는 영향을 줄임으로써 값비싼 기술 솔루션만큼 효과적일 수 있습니다. 특히 기존 시스템을 사용하는 기존 선박의 경우, 기술 솔루션을 구현하는 데 어려움이 있고 비용도 많이 들 수 있습니다.

다양한 리스크 완화 조치의 효과를 평가하는 것은 리스크 평가 및 변경 관리 프로세스의 필수적인 부분이어야 합니다. 또한 다양한 리스크 완화 조치를 분류할 때도 이를 고려할 수 있으므로, 어떤 통제 수단을 어디에서 사용해야 하는지에 대한 지침을 제공하고 이해하기가 더 쉬워집니다.

[BIMCO 6.2 리스크 평가의 네 가지 단계]

3단계: 보고 및 브리핑

ISM 코드의 요구사항을 충족하기 위해, 리스크 평가는 체계적이고 최신 상태의 문서로 작성되어야 하며, 해당 문서에는 리스크가 어떻게 평가되고 완화되었는지가 반영되어야 합니다. 이러한 리스크 평가 문서는 다양한 완화 조치들을 서로 다른 조합으로 고려한 후, 가장 최적의 조합을 결정하는 반복적과정을 거쳐 작성됩니다.

통제항목	C.2.3 사이버 리스크 평가	Basic

리스크 완화 조치의 구성은 법적 요구사항, 리스크 수용 수준, 발생빈도, 효과성, 비용 등의 기준에 따라 평가되어야 합니다.

[BIMCO 6.2 리스크 평가의 네 가지 단계]

외부 전문가(예: 사내에 충분한 전문 역량이 없는 경우)에 의해 리스크 평가가 수행되는 경우, 외부 기관의 최초 보고서는 위험에 대한 중간 보고서가 될 가능성이 높으며, 이때 권고 사항이 함께 제시됩니다. 해당 권고 사항이 충분히 검토되고 최종 결정이 내려지면, 이는 최종 리스크 평가 문서에 반영되어야 합니다.

[BIMCO 6.2 리스크 평가의 네 가지 단계]

초기 외부 사이버 리스크 평가는 다음과 같은 항목을 포함할 수 있습니다:

- **요약 보고:** 결과 요약, 권고 사항, 평가 대상 선박의 전반적인 보안 상태에 대한 고수준 요약
- **기술적 발견 사항:** 발견된 취약점에 대한 세부 분석, 악용 가능성, 금전적 피해 가능성, 선원·선박·환경에 미치는 영향, 그리고 적절한 기술적 대응 및 완화 조치에 대한 제언
- **우선 조치 목록:** 우선순위는 조치의 효과성, 비용, 적용 가능성 등을 기준으로 설정되어야 하며, 이 목록은 이용 가능한 전체 조치 옵션을 망라해야 하며, 제3자가 판매를 목적으로 제시하는 서비스나 제품 목록이 되어서는 안 됨
- **보조 자료:** 주요 발견 사항의 기술적 세부 정보와 심각한 결함에 대한 종합 분석을 포함한 부속 문서 또한, 침투 테스트 중에 확보된 데이터 샘플(있는 경우)도 포함되어야 하며, 이는 중대한 또는 고리스크 취약점에 대한 것일 수 있음
- **부록:** 사이버 리스크 평가팀이 수행한 활동의 기록과 사용한 도구 목록

[BIMCO 6.2 리스크 평가의 네 가지 단계]

4단계: 제조사 브리핑

선주가 조사 결과를 검토하고 논의하며 평가할 기회를 가진 후에는, 해당 결과의 일부를 관련 시스템 제조업체에 전달해야 할 수도 있습니다. 이는 리스크를 줄이거나 완화하기 위한 목적입니다. 예를 들어, 중요 시스템 또는 구성요소의 공장 출하시 기본 설정에서 발견된 사이버 취약점과 같은 항목은, 외부 전문가의 지원을 받아 추가 분석이 이루어질 수 있습니다. 이 전문가들은 제조업체의 사이버보안 담당자와 협력하여 문제에 대한 완전한 리스크 및 기술적 이해가 확보되도록 해야 합니다. 이러한 지원 활동은, 제조업체가 수립한 개선 계획이 충분히 포괄적이며, 식별된 취약점을 정확히 해결할 수 있는 적절한 해결책을 포함하도록 보장하기 위한 것입니다.

[BIMCO 6.2 리스크 평가의 네 가지 단계]

회사가 정확한 리스크 평가를 수행할 수 있는 역량에 따라, 외부 제3자의 지원을 고려할 수 있습니다.

[BIMCO 6.3 제3자 리스크 평가]

제3자 리스크 평가는 중요 IT 및 OT 인프라에 대한 침투 테스트를 포함할 수 있으며, 이는 실제 방어 수준이 회사의 사이버보안 전략에서 설정한 목표 수준과 일치하는지를 판단하기 위해 수행됩니다. 이러한 테스트는 IT 시스템, 사회공학 기법, 필요 시에는 물리적 보안 경계 침투 시나리오까지 포함할 수 있습니다. 이러한 테스트는 시스템에

통제항목	C.2.3 사이버 리스크 평가	Basic

	접근하고 소프트웨어를 삽입할 가능성이 있기 때문에 "능동 테스트" 라고 불립니다. 이러한 접근 방식은 일반적으로 IT 시스템에 적합합니다. 반면, OT 시스템의 경우 침투 테스트 중단이 허용되지 않는 상황이라면, 수동 테스트 방식을 고려해야 합니다. 수동 방식은 시스템에서 전송되는 데이터를 스캔하여 취약점을 식별하는 방식으로, 시스템에 직접 접근하거나 소프트웨어를 삽입하지 않습니다. **[BIMCO 6.3 제3자 리스크 평가]** 제3자 리스크 평가는 전문 기술 및 현장 경험을 통합하여 사이버 리스크를 관리하고 완화하는 전체 과정에서 다양한 업무를 수행할 수 있는 효과적인 방법입니다. 이러한 평가는 인력 자원이 부족한 회사에게도 객관적이고 투명한 리스크 평가를 수행할 수 있게 해줍니다. 또한, 제3자를 참여시킴으로써 다양한 관점을 학습하고, 신중한 검토를 통해 정보에 기반한 자신 있는 의사결정을 내릴 수 있는 기회를 제공합니다. **[BIMCO 6.3 제3자 리스크 평가]** 침투 테스트는 네트워크와 시스템이 침해되었는지를 판단하는 수단으로 널리 인식되어 있지만, 자체 조직이나 선대 환경에 대한 이해의 토대를 구축하는 데에는 그 외에도 다양한 방법이 있습니다. 이러한 서비스에는 선주와 운영자가 무엇이, 어디에, 누구와 연결되어 있는지 파악하도록 지원하는 네트워크 자산 검색 및 목록 작성이 포함될 수 있습니다. 제3자는 네트워크 아키텍처 검토 및 설계를 수행하여 현재 설계를 이해하고 감사하며, 수동 네트워크 스캐닝까지 포함할 수 있습니다. 침투 테스트는 침투적이고, 더 큰 리스크를 수반하며, 비용이 훨씬 더 많이 들고, 네트워크 및 목록 자산에 대한 이해가 필요합니다. 침투 테스트는 보다 구체적인 상황과 기술적 조치에 국한되어야합니다. 다른 모든 서비스와 마찬가지로, 안전 목적을 위해 관련 업무를 감독할 선박 책임자 및 육상 인력과 협력하는 것이 중요하며, 선대 운영 경험을 갖춘 제3자 서비스를 선택하는 것이 바람직합니다. **[BIMCO 6.3 제3자 리스크 평가]**
DCSA	1.4.5(Example information security risk assessment)에 있는 사이버보안 리스크 평가 수행을 위한 예시 템플릿 **[DCSA 1.4.2 설명]** 우선, 회사는 리스크 평가의 범위, 사용될 메트릭, 적용할 거버넌스 모델을 명확히 이해하기 위해 컨텍스트 수립(context establishment)을 수행해야 합니다. 다음 항목들이 반드시 다루어져야 합니다: • 사이버 리스크 평가에 포함될 선박의 자산은 무엇인가? • 누가 무엇을 하는가? 각 선박에 대해 개별적으로 리스크 평가를 수행할 것인가, 아니면 선박의 입력을 반영한 그룹 또는 클래스 단위로 육상에서 수행할 것인가? • 식별된 위협 목록을 결정한다. • 식별된 취약점 목록을 정의한다. • 리스크 평가를 수행하기 위한 프로세스, 인력, 도구, 시간 등을 확인한다. **[DCSA 1.4.3 구현]** 사이버 리스크의 컨텍스트가 수립되면, 회사는 다음을 통해 리스크를 분석할 수 있습니다:

통제항목	C.2.3 사이버 리스크 평가	Basic

- 지정된 자산 내의 취약점을 활용할 수 있는 위협이 있는지를 확인합니다 (예: 1.4.5(Example information security risk assessment)에 있는 리스크 평가 문서 참조).
- 리스크 점수 매트릭스를 사용하여 식별된 각 리스크에 점수를 부여할 수 있습니다.
- 이후 해당 리스크를 수용, 회피, 처리 또는 이전의 대상으로 분류할 수 있습니다 (예: 1.4.7 Risk treatment options 참조).

[DCSA 1.4.3 구현]

리스크는 리스크 관리 프로세스의 모든 단계에서 모니터링되어야 하며, 리스크에 대한 통제 조치의 효과성도 평가되어야 합니다. 위협이나 취약점에 변화가 생긴 경우에는 구현된 보안 통제 조치의 개선이 필요한지 여부도 검토해야 합니다.

[DCSA 1.4.3 구현]

선박에 탑재된 자산에 대해 정확한 리스크 평가를 수행하기 위해, 다음과 같은 문서가 준비되어야 합니다:

a) 회사 고유의 가이드라인 문서 – 이는 회사의 정책 및 거버넌스에 따라 직원들이 리스크 평가를 수행하는 데 도움을 줄 수 있습니다.
b) 완전한 자산 목록 (1.1 Asset Management 참조)
c) 사이버 위협 보고 – 사이버 위협 행위자, 동기 및 목적에 대한 목록을 작성합니다.
d) 모든 위협이 외부에서 발생하는 것은 아니므로, 내부 위협도 반드시 식별되어야 합니다. 이는 사고 이후 보고, 익명 보고, 과거 또는 기업 차원의 리스크 평가 등을 통해 확인할 수 있습니다.
e) 커뮤니티 보고
f) 자산 내 취약점 목록 – 이는 취약점 스캔, 공급업체 정보, 리스크 보고 등 여러 출처를 통해 확보될 수 있습니다.
g) 각 자산에 대한 영향 평가 – 자산 손실로 인한 영향을 이해하기 위해 필요하며, 이는 손실을 유발한 행위와는 무관하게 수행되어야 합니다.

[DCSA 1.4.4 문서화]

아래 표는 선박의 IT 및 OT 자산에 사용하도록 수정된 사이버보안 리스크 평가의 예를 보여줍니다. 이는 1.1의 자산 재고 내용과 연결되어야 합니다.

[DCSA 1.4.5 정보 보안 리스크 평가 예시]

자산에 대한 위협 및 취약점은 분석 및 리스크 평가를 위해 여기에 입력되는 정의된 위협을 초래하여 리스크 평가 및 추후 리스크 결정을 지원합니다. (치료, 이전, 수락 또는 회피)를 수행합니다.

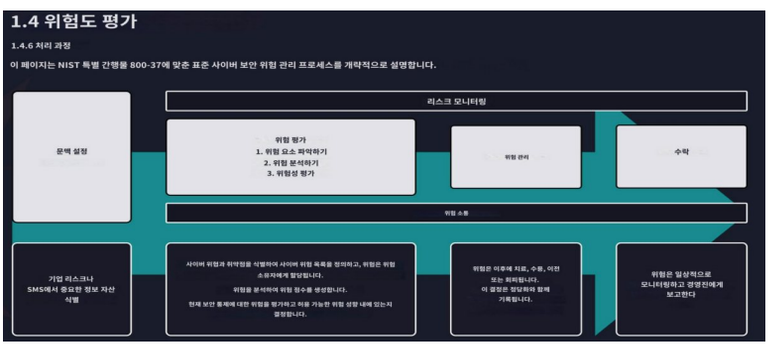
[DCSA 1.4.5 정보 보안 리스크 평가 예시]

dcsa **Assess Risks**

Formally identified and owned risks are initially assessed as inherent, this is because the control landscape may change over time so there should be a base level of the risk to re-assess against. The inherent impact and likelihood is assessed against the CIA triad to generate the inherent score. Current controls are then put against the risk to generate the residual risk. If this residual risk is higher than defined risk appetite, then the risk is put forward to risk treatment.

Risk ID	Risk description	Inherent Impact / risk category				Impact score	Likelihood score	Inherent risk score	Risk Owner	Controls	Residual Impact / Risk category				Impact score	Likelihood score	Residual risk score	Risk decision
		C	I	A	S						C	I	A	S				
DGRG#201	**Unauthorised access by breached or stolen credentials** – The risk of unauthorised individuals obtained access to the environment	x	x	x		4	4	Very High	Captain	Two factor authentication	x	x	x		4	2	Medium	Treat
DGRG#202																		
DGRG#203																		
DGRG#204																		
DGRG#205																		
DGRG#206																		
DGRG#207																		
DGRG#208																		
DGRG#209																		
DGRG#210																		

리스크/영향 범주 범례:

통제항목	C.2.3 사이버 리스크 평가	Basic
	C: 기밀성 I: 무결성 A: 가용성 S: 안전성 **[DCSA 1.4.5 정보 보안 리스크 평가 예시]**  **[DCSA 1.4.6 처리 과정]** **[DCSA 1.4.7 리스크 조치 방법]**	
비고		

C.3 사이버 리스크 조치 계획

통제항목	C.3.1 사이버 리스크 조치계획	Basic
레퍼런스 상세	**IMO**	본 지침의 목적상, 사이버 리스크 관리(cyber risk management)란 이해관계자가 사이버 관련 리스크를 식별, 분석, 평가 및 전달하며, 해당 리스크를 수용, 종료, 이전 또는 수용 가능한 수준으로 완화하는 과정을 의미하며, 이때 조치의 비용과 편익을 고려합니다. **[IMO 3.1 사이버 리스크 관리 요소]** 해사 사이버 리스크 관리의 목표는 사이버 위협과 리스크에 대해 운영적으로 회복력이 있는 안전하고 보안이 확보된 선박 운영을 지원하는 것입니다. 선박과 선박-항만 간 인터페이스 시스템을 신규 위협으로부터 보호하기 위해서는 지속적으로 진화하는 다양한 통제 조치가 필요합니다. 따라서, 선박 장비 및 시스템의 설계, 제조, 통합, 운영 및 유지관리 단계에서 사이버 회복력 있는 보안 기능이 포함되어야 합니다. **[IMO 3.2 사이버 리스크 관리 요소]** 효과적인 사이버 리스크 관리는 고위 경영진 수준에서 시작해야 합니다. 고위 경영진은 관련 교육을 이수하고, 조직 전반에 사이버 리스크 인식 문화를 심어야 하며, 조직의 모든 수준에서 전방위적이고 유연한 사이버 리스크 관리 체계를 지속적으로 운영·평가하기 위해 효과적인 피드백 메커니즘을 갖추어야 합니다. **[IMO 3.3 사이버 리스크 관리 요소]** 이를 달성하는 한 가지 인정된 접근 방식은 조직의 현재 및 목표로 하는 사이버 리스크 관리 상태를 포괄적으로 평가·비교하는 것입니다. 이러한 비교는 CBS(컴퓨터 기반시스템) 내 사이버보안 격차를 드러낼 수 있으며, 리스크 기반 접근법을 통해 사이버 회복력 목표를 달성하는 데 활용될 수 있습니다. 이 접근법은 선박 유형, 운항 프로파일, 선박 내 시스템의 복잡성과 연결성을 고려하여 사이버 리스크를 평가하며, 이를 통해 조직은 가장 비용 효과적이고 효율적인 방식으로 자원을 배분할 수 있습니다. **[IMO 3.4 사이버 리스크 관리 요소]** 본 지침은 효과적인 사이버 리스크 관리를 지원하는 기능적 요소를 제시합니다. 이 기능적 요소들은 순차적이지 않으며, 실제 운영에서는 동시에 적용되고, 리스크 관리 체계에 적절히 통합되어야 합니다. 아래에 명시된 기능적/기술적 사이버보안 통제는 반드시 이행해야 하는 최소 통제를 나타냅니다. 식별된 사이버 리스크 평가에 따라 추가적인 사이버보안 통제를 고려할 수 있습니다. **[IMO 3.5 사이버 리스크 관리 요소]** 이러한 기능적 요소들은 해사 운영과 해양 환경 보호에 영향을 미치는 핵심 시스템 전반에 걸쳐 효과적인 사이버 리스크 관리의 활동과 결과를 포괄하며, 지속적인 운영과 효과적인 피드백 메커니즘을 포함합니다. 모든 관련 문서는 무단 접근, 삭제, 파괴 또는 수정 방지를 위한 절차로 보호되어야 합니다. **[IMO 3.6 사이버 리스크 관리 요소]** 효과적인 사이버 리스크 관리는 조직 전반에 걸친 적절한 인식 수준을 보장해야 하며, 인식 수준과 준비 상태는 역할과 책임에 적합해야 합니다. **[IMO 3.7 사이버 리스크 관리 요소]**

통제항목	C.3.1 사이버 리스크 조치계획	Basic

	사이버 회복력 있는 장비 및 시스템의 구현은 국제 표준과 지침에 따라 설계·시험되어야 하며, 이를 통해 선박의 회복력을 보장해야 합니다. **[IMO 3.8 사이버 리스크 관리 요소]**
OCIMF SIRE 2.0	검사 지침 (Inspection Guidance) 선박 운영자는 사이버 리스크 관리에 대한 절차를 개발해야 하며, 그 내용은 다음을 포함해야 합니다: ■ 사용자, 핵심 인력, 육상 및 선상 경영진의 역할과 책임 식별 • 선상에서 사이버 리스크 관리 책임을 가진 담당자 • 선내 네트워크에서 사용자 프로필 및 비밀번호를 관리하는 담당자 ■ 선박에서 리스크에 노출된 IT(정보기술) 및 OT(운영기술) 시스템 식별 • 화물 관리 시스템 • 브리지 시스템 • 추진 및 기계 관리, 전력 제어 시스템 • 접근 제어 시스템 • 행정 및 승무원 복지 시스템 • 통신 시스템 ■ 사이버 사고로부터 보호하기 위한 기술적 보호 조치 명시 • 네트워크 구성요소의 물리적 보안 • 안티바이러스 소프트웨어 • 애플리케이션 소프트웨어 관리 • 백업 설비 • 승무원 인터넷 접근 통제 • 관리자 프로필, 사용자 프로필 및 비밀번호의 관리 통제 ■ 사이버 사고로부터 보호하기 위한 절차적 보호 조치 명시 • 승무원 대상 사이버보안 교육 및 인식 제고 • IT 및 OT 시스템에 대한 로컬 및 원격 접근 통제 • 선상에서 개인용 장치 사용 통제 • 데이터 삭제를 포함한 장비 폐기 • 잠재적 사이버 사고에 대비한 비상계획(contingency plans) 제안된 검사관 행동 (Suggested Inspector Actions) ■ 선상에서 사이버 리스크 관리 책임이 있는 담당자를 인터뷰하여 다음의 존재 여부를 확인해야 합니다: • 회사의 사이버 리스크 관리 절차 • 선내 장착된 민감한 IT/OT 시스템의 목록/등록부 • 민감한 IT/OT 시스템에 대한 외부 로컬 또는 원격 접근 승인 기록 • 운영자의 IT 부서 또는 외부 IT 계약업체의 기술 지원 연락처 • 사이버보안 교육 기록 • 사이버 비상계획의 하드 카피(Hard Copy) ■ 선박 순회 중 장비를 검사하여 실제 사이버보안 조치가 시행되고 있는지 확인해야

통제항목	C.3.1 사이버 리스크 조치계획	Basic

합니다.

기대되는 증거 (Expected Evidence)

- 회사의 사이버 리스크 관리 절차
- 선내 장착된 민감한 IT/OT 시스템의 목록/등록부
- 민감한 IT/OT 시스템에 대한 외부 로컬 또는 원격 접근 승인 기록
- 사이버 비상계획의 하드 카피(Hard Copy)
- 운영자의 IT 부서 또는 외부 IT 계약업체의 기술 지원 연락처
- 사이버보안 교육 기록

검사관은 위의 문서 및 기록 중 기밀로 간주되는 항목을 검토 요청해서는 안 됩니다.

부정적 관찰의 잠재적 근거 (Potential Grounds for a Negative Observation)

- 회사에 다음이 포함된 사이버 리스크 관리 절차가 없었던 경우:
  - 사용자, 핵심 인력, 육상 및 선상 경영진의 역할과 책임 식별
  - 선내 리스크에 노출된 IT 및 OT 시스템 식별
  - 사이버 사고로부터 보호하기 위한 기술적 보호 조치 설명
  - 사이버 사고로부터 보호하기 위한 절차적 보호 조치 설명
- 동반 사관이 회사의 사이버 리스크 관리 절차에 친숙하지 않았던 경우
- 민감한 IT 또는 OT 제어 장비가 있는 공간이 안전하게 잠겨 있지 않았던 경우
- 선내 장착된 민감한 IT/OT 시스템의 목록/등록부가 없었던 경우
- 민감한 사용자 장비(예: 브리지 시스템의 노출된 USB 포트 등)가 안전하게 보호되거나 비활성화되지 않았던 경우
- 회사 절차에서 누가 관리자 프로필을 가져야 하는지, 또는 누가 사용자 프로필을 관리해야 하는지 지정하지 않았던 경우
- 백업 설비가 없거나 사용되지 않았던 경우
- 선박의 항해 및 추진에 중요한 OT 시스템의 백업 체계에 대해 선원들이 친숙하지 않았던 경우
- ECDIS 등 민감한 장비에 대한 기술자의 선내 접근에 대한 공식 승인 증거가 없었던 경우
- 사용 중인 휴대용 매체가 선박 제어 네트워크와 연결되지 않은 컴퓨터에서 악성코드 검사를 받았다는 증거가 없었던 경우
- 확인된 경우:
  - 선내 컴퓨터가 안티바이러스 소프트웨어로 보호되지 않았음
  - 안티바이러스 소프트웨어가 정기적으로 업데이트되지 않았음
  - 애플리케이션 소프트웨어가 업그레이드 및 보안 패치로 정기적으로 업데이트되지 않았음
  - 선임 사관이 아닌 승무원이 관리자 프로필을 가지고 있었음
  - 사용자 프로필이 작업용 워크스테이션을 본래 의도와 다르게 사용하도록 허용했음
  - 사용자 프로필이 적극적으로 관리되지 않았음

통제항목	C.3.1 사이버 리스크 조치계획	Basic

	• 일반 사용자 프로필 및 비밀번호가 승무원 교대 시 전달되었음 • 동반 사관이 자신의 책임과 직무에 맞는 사이버보안 교육을 받지 않았음 • 사용자 이름과 비밀번호가 워크스테이션에 게시되어 있었음 • 워크스테이션 접근에 비밀번호가 요구되지 않았음 • 선내에서 사이버보안 인식이 적극적으로 홍보되고 있다는 증거가 없었음 • 사이버 비상계획이 다음의 상실을 다루지 않았음: - 항해 장비의 기능 또는 신뢰성 (예: ECDIS) - GNSS와 같은 외부 데이터 소스의 가용성 또는 무결성 - GMDSS 통신을 포함한 육상과의 연결성 - 추진, 조타 등과 같은 중요 시스템 제어 시스템 ■ 사이버 비상계획의 하드 카피(Hard Copy)가 없었음 ■ 운영자의 IT 부서 또는 외부 IT 계약업체의 기술 지원 연락처 정보가 적절히 준비되어 있지 않았음 **[OCIMF SIRE 2.0 7.5 사이버보안]**
BIMCO	**심층 방어** 중요 시스템과 데이터를 보호하기 위해 인적 요소, 절차, 기술의 역할을 고려한 다중 보호 계층을 적용하는 것이 중요합니다. 이러한 접근은 다음과 같은 목적을 가집니다: • 사이버 사고가 탐지될 가능성을 높인다. • IT 및 OT 시스템의 기밀성, 무결성, 가용성을 보호하기 위해 필요한 자원을 최대한 효과적으로 활용한다. • 시스템을 무단으로 사용하는 것을 방지하기 위해 시스템을 추가로 격리하고 보호하는 체계적 조치를 수립하다. **[BIMCO 7.1 심층 방어와 광역 방어]** 선박 내 연결된 OT 시스템은 하나 이상의 기술적 및/또는 절차적 보호 조치가 요구되어야 합니다. 방화벽과 같은 경계 방어는 시스템에 대한 무단 접근을 방지하는 데 중요하지만 내부 위협에 대응하기에는 불충분할 수 있습니다. **[BIMCO 7.1 심층 방어와 광역 방어]** 이러한 심층 방어 접근은 다음과 같은 요소들의 조합을 권장합니다: • SSP(선박보안계획서)에 따른 선박의 물리적 보안 • 네트워크 보호, 효과적인 분할 포함 • 침입 탐지 • 방화벽의 사용 • 정기적인 취약점 스캔 및 테스트 • 화이트리스트 방식의 소프트웨어 실행 제어 • 접근 및 사용자 통제 • 구성 및 변경 관리 통제 • 이동식 미디어와 비밀번호 정책 사용에 관한 적절한 절차 • 직원의 사이버보안 인식과 산업 및 자신에게 미치는 리스크에 대한 이해 • 사건 대응을 포함한 적절한 절차에 대한 이해 및 숙지 **[BIMCO 7.1 심층 방어와 광역 방어]**

통제항목	C.3.1 사이버 리스크 조치계획	Basic

회사의 정책과 절차는 사이버보안이 안전 및 보안 리스크 관리의 전체 접근 방식 내에서 고려되도록 보장해야 합니다. 사이버 위협의 복잡성과 지속 가능성을 고려할 때, '심층 방어' 접근 방식은 반드시 고려되어야 합니다. 보호 계층으로 구성된 장비 및 데이터는 사이버 사고에 대해 더 탄력적으로 대응할 수 있습니다.

[BIMCO 7.1 심층 방어와 광역 방어]

광역 방어

시스템 간 통합을 개발할 때는 신뢰 경계(trust boundary) 모델을 고려해야 하며, 이는 다음과 같은 원칙에 기반합니다: 시스템 간의 신뢰가 암묵적인 경우(예: 사용자 워크스테이션 간)와 신뢰가 명시적으로 설정되어야 하는 경우(예: 조타실 컴퓨터와 회사 네트워크 간)를 구분합니다. 대규모 또는 복잡한 네트워크에서는 위협 모델링을 통해 시스템 간 어디에 기술적 통제가 구현되어야 하는지 파악함으로써 광역 방어 접근을 지원할 수 있습니다.

[BIMCO 7.1 심층 방어와 광역 방어]

하지만, 선박 내에서는 IT와 OT 시스템 간 통합 수준이 높은 경우가 많으며, 기술적 및 절차적 보호 조치가 모든 통합된 취약 시스템에 걸쳐 계층적으로 적용되는 경우에만 심층 방어가 효과적입니다. 이것이 '광역 방어' 접근입니다. 이를 통해 한 시스템의 취약점이 우회 공격 통로로 사용되는 것을 방지할 수 있습니다.

[BIMCO 7.1 심층 방어와 광역 방어]

사이버 리스크 보호 조치는 기술적일 수 있으며, 선내 시스템이 사이버 사고에 강인하도록 설계되고 구성되었는지를 보장하는 데 중점을 둡니다. 특히 기존 선박의 경우, 실용적이고 비용 효율적인 기술적 통제를 구현하는 것이 중요합니다. 기술 통제 조치의 구현은 일회성 활동이 아니며, 일단 구현되면 실패 리스크를 방지하기 위해 최신 상태로 유지되어야 합니다.

[BIMCO 7.2 기술적 보호 조치]

인터넷 보안 센터(CIS)는 사이버보안 취약점을 해결하는 데 사용할 수 있는 조치들에 대한 지침을 제공합니다. 보호 조치는 핵심 보안 통제(CSC) 목록이며, 이는 우선순위가 매겨지고 검토되어 기업들이 자산을 보호하고 방어를 향상시키는 효과적인 접근 방식을 제공하는 데 도움이 됩니다. CSC는 기술적 및 절차적 측면을 모두 포함합니다.

[BIMCO 7.2 기술적 보호 조치]

아래에 언급된 CSC의 예시는 선박 내 장비 및 데이터와 특히 관련성이 높은 항목으로 선택되었습니다.

[BIMCO 7.2 기술적 보호 조치]

사고: 해상 IT 및 OT의 웜 감염 사고

한 선박에는 전력 관리 시스템이 장착되어 있었으며, 이 시스템은 소프트웨어 업데이트 및 패치, 원격 진단, 데이터 수집, 원격 운영을 위해 인터넷에 연결될 수 있었습니다. 해당 선박은 최근에 건조되었으며, 이 시스템은 설계상 인터넷에 연결되어 있지 않았습니다.

회사의 IT 부서는 시스템이 감염 증상을 보이는지 확인하고 연결이 안전한지를 결정하기 위해 선박을 방문하여 취약점 스캔을 수행하기로 결정했습니다. 팀은 시스템이

통제항목	C.3.1 사이버 리스크 조치계획	Basic

인터넷에 연결되었을 때 활성화될 수 있는 잠복 웜(worm)을 발견했으며, 이로 인해 심각한 결과가 발생했을 수 있었습니다. 이 사고는 에어갭 시스템조차도 손상될 수 있으며, 사전 예방적 사이버 리스크 관리의 중요성을 강조합니다.
선주사는 이 웜의 발견 사실을 제조사에 통보하고, 웜을 삭제하는 절차에 대한 지침을 요청했습니다. 선주는 이 사고 이전에 기술자가 선박에 승선했던 점을 언급했으며, 이 감염이 기술자로부터 발생했을 가능성이 있다고 판단했습니다.
해당 웜은 USB 장치를 통해 메모리로 로드되는 실행 프로세스를 통해 확산되었으며, 이 프로그램은 명령 및 제어 서버와 통신하여 다음 명령을 받아 실행하도록 설계되었습니다. 또한 파일 및 폴더를 생성할 수 있는 기능도 있었습니다.
회사는 사이버보안 전문가에게 포렌식 분석 및 복구를 의뢰했습니다. 분석 결과, 장비에 연결된 모든 서버가 감염되었으며, 이 바이러스는 무려 875일 동안 탐지되지 않은 채 존재해왔습니다. 스캐닝 도구를 통해 웜이 제거되었으며, 분석 결과 서비스 공급자가 웜의 근원이었고, USB 드라이브를 통한 소프트웨어 설치 중 선박 시스템에 맬웨어를 주입했다는 사실이 확인되었습니다.
추가 분석 결과, 이 웜은 시스템 메모리에서 실행되며, 인터넷에 연결된 서버로 실제로 호출을 전송했다는 사실이 드러났습니다. 웜이 메모리에 로드된 이후, 서버의 성능과 인터넷 연결된 시스템에 영향을 줄 수 있었던 것입니다.

[BIMCO 7.2 기술적 보호 조치]

보호 조치는 절차적일 수도 있으며 회사의 정책, 안전 관리 절차, 보안 절차 및 접근 통제에 의해 다루어져야 합니다. 다른 모든 통제 수단과 마찬가지로, 실용적이고 비용 효율적인 절차적 통제만이 구현되어야 합니다. 절차적 통제는 승무원이 선상 시스템을 어떻게 사용하는지에 초점을 맞춥니다. 민감한 정보를 포함하는 계획 및 절차는 기밀로 유지되어야 하며 회사 정책에 따라 처리되어야 합니다. 절차적 조치의 예는 다음과 같습니다:

[BIMCO 7.3 절차적 보호 조치]

사고: 주요 애플리케이션 서버 랜섬웨어 감염

선박의 주요 애플리케이션 서버에서 발생한 랜섬웨어 감염으로 인해 IT 인프라 전체가 심각하게 마비되었습니다. 랜섬웨어는 서버 내 모든 중요 파일을 암호화하였고, 선박의 행정 운영에 필요한 애플리케이션을 사용할 수 없게 만들었습니다. 사건은 애플리케이션 서버 복구 이후에도 재발했습니다.

감염의 근본 원인은 공격자가 원격 관리 서비스에 무차별 대입 공격을 성공적으로 수행할 수 있도록 허용한 허술한 비밀번호 정책이었습니다. 회사 IT 부서는 문서화되지 않은 사용자 계정을 비활성화하고 시스템 내 강력한 비밀번호 정책을 적용하여 이를 해결하였습니다.

[BIMCO 7.3 절차적 보호 조치]

데이터 삭제 및 장비 폐기

폐기되는 장비에는 상업적으로 민감하거나 기밀인 데이터가 포함될 수 있습니다. 장비 폐기 전에 회사는 해당 장비에 저장된 데이터를 복구 불가능하도록 완전히 삭제하는 절차를 마련해야 하며, 예를 들어 탈자 장비(degaussing tool)를 사용하여 제조사 지침에 따라 완전히 제거해야 합니다.

통제항목	C.3.1 사이버 리스크 조치계획	Basic
	[BIMCO 7.3 절차적 보호 조치]	
DCSA	선박에서 대응이 필요한 리스크가 식별되면, 리스크 처리 계획(Risk Treatment Plan)을 작성해야 합니다. 이 계획은 리스크 등급을 낮추기 위해 어떤 통제 수단(논리적, 관리적 또는 물리적)이 사용될 수 있는지를 검토하며, 실행 방식, 소요 비용, 추가 자원 등도 포함해야 합니다. 이 계획은 해당 리스크 소유자에게 제출되어 승인 후 실행됩니다. **[DCSA 1.4.3 구현]** 본 절은 사이버보안 리스크 완화와 관련하여 선박의 인적, 물리적, 절차적 및 기술적 측면에 적용할 수 있는 완화 조치 식별을 위한 지침을 제공합니다. **[DCSA 4.4.2 설명]** 또한, 선박 내에서 비적합 사항으로 선언될 수 있는 결과를 유발할 수 있는 요소들을 사전에 식별하고 완화하는 데 중점을 둠으로써, 사이버보안 리스크를 조기에 파악하고 사전 대응을 통해 이러한 상황을 예방할 수 있습니다. **[DCSA 4.4.2 설명]** 완화 조치를 선택할 때 다음과 같은 균형이 고려되어야 합니다: a) 완화 조치가 예상치 못한 새로운 리스크를 초래하지 않아야 함 b) 완화 조치가 인력, 운영 절차 또는 기술적 이점을 과도하게 제한함으로써 운영에 부정적 영향을 미치지 않아야 함 c) 완화 조치가 너무 과도하거나 복잡하여 무시되거나 우회되지 않도록 해야 함 **[DCSA 4.4.2 설명]** 완화 조치는 문서화되어야 하며, 이는 다음의 목적으로 활용됩니다. 효과성에 대한 모니터링 수행, 리스크관리 절차에 반영, 필요 시 업데이트 및 개선 조치 수행 **[DCSA 4.4.2 설명]** 또한, 완화 조치는 사이버 리스크 관리 프로세스 내에서 리스크처리 방안의 일환으로 생성될 수 있습니다. **[DCSA 4.4.2 설명]** 사람은 보안 시스템 또는 운영 체계에서 가장 약한 요소로 간주되므로, 선박 시스템과 사람 간의 상호작용을 명확히 이해할 필요가 있습니다. 이에 따라, 다음 질문들에 대한 답변을 확보하는 것이 적절하고 비례적인 완화 조치를 결정하는 첫 단계로 권장됩니다. **[DCSA 4.4.3 구현-인적요소]** (a) 누가 선박 데이터 및 시스템에 접근해야 하는가? **[DCSA 4.4.3 구현-인적요소]** (b) 어떤 종류의 접근이 필요한가? **[DCSA 4.4.3 구현-인적요소]** (c) 이 접근은 어떻게 제공되며, 선박 외부에서 원격으로 필요한가? [DCSA 4.4.3 구현-인적요소] (d) 어떤 접근 통제가 필요한가? (예: 개인이 선박 데이터를 생성, 읽기, 업데이트	

통제항목	C.3.1 사이버 리스크 조치계획	Basic

또는 삭제할 수 있는가? 그리고 어떤 수준의 통제권을 가지는가?)

[DCSA 4.4.3 구현-인적요소]

(e) 개인에게 요구되는 사이버보안 인식 수준 및 이해도는 어느 정도인가?

[DCSA 4.4.3 구현-인적요소]

(f) 계약직, 임시직 및 파견직원이 입사 시 사이버보안 인식 교육을 받는가?

[DCSA 4.4.3 구현-인적요소]

(g) 선박 운영자의 정책, 절차 및 시스템 생성·사용·유지보수에 관한 절차를 직원들이 이해하고 있는가?

[DCSA 4.4.3 구현-인적요소]

(h) 정책, 절차, 프로세스 변경 시 이를 갱신하여 직원에게 통보하는 절차가 수립되어 있는가?

[DCSA 4.4.3 구현-인적요소]

(i) 위협, 리스크, 필요한 보안 통제의 변화에 대해 적시에 브리핑이 이루어지고 있는가?

[DCSA 4.4.3 구현-인적요소]

위 질문 중 초기 4개에 대한 답변은 SSO(선박 보안 책임자)가 고리스크 직무를 식별하는 데 도움을 줍니다. 이러한 직무에 종사하는 인원은 적절한 채용 전·계약 전 보안 검증 및 확인 절차를 거쳐야 하며, 지속적인 모니터링이 병행되어야 합니다.

[DCSA 4.4.3 구현-인적요소]

주요 직무자(HRPs) 예시

(a) IT 및/또는 운영 시스템 관리 책임자

(b) 보안 담당자

(c) 정보관리 업무 담당자

(d) 구매, 조달, 계약 관리 담당자

(e) 인사 담당자 (예: 보안 위반 관련 징계 조치, 내부 위협 관련 관리 포함)

[DCSA 4.4.3 구현-인적요소]

사이버보안 수준을 향상시키기 위해서는 다음과 같은 물리적 보안 조치를 수립하고 유지하는 것이 필요합니다:

[DCSA 4.4.3 구현-물리적]

(a) 민감한 선박 시스템에 대한 무단 접근 방지, 예:
- IT 장비(정보 접근, 처리, 저장 장치)
- 안전 필수 기능을 수행하는 시스템
- 보안 및 제어 시스템

(b) 장비의 도난 또는 손상 방지, 예:
- IT 장비, 저장매체, 케이블 등
- 선박 데이터 (특히 안전하고 안정적인 선박 운항에 필요한 정보)

(c) 네트워크 및 통신 인프라 보호
- 우발적 손상
- 고의적/악의적 손상
- 서비스 거부 및 변조

통제항목	C.3.1 사이버 리스크 조치계획	Basic

(d) 유틸리티, 난방, 환기, 냉각 시스템 보호, 이는 다음의 기능을 위해 필수적임:
- 민감한 시스템의 작동 유지
- 네트워크 및 통신 인프라 운영
- 안전하고 보안된 작업 환경 유지

[DCSA 4.4.3 구현-물리적]

일부 선박 시스템은 주요 운영 공간과 동일한 수준의 물리적 보호가 필요할 수 있으며, 이 경우 보안 경계(perimeter)를 설정해 장비, 전력, 플랜트, 기계 등을 함께 보호해야 합니다. 이를 위해 다음을 파악할 필요가 있습니다:

[DCSA 4.4.3 구현-물리적]

(a) 선박 데이터를 생성, 접근, 처리, 저장하기 위한 물리적 및 전자적 인프라(통신 및 네트워크 포함)
(b) 시스템 운영 및 관련 서비스의 연속성을 보장하기 위해 중요한 인프라
(c) 해당 인프라가 타 주요 서비스나 인프라와의 의존관계 여부
(d) 해당 인프라가 선박 시스템에 전용인지, 또는 타 작업과 공유되는지 여부
(e) 제3자와의 공유 여부
(f) 사고 발생 시 외부 기관 및 구조기관의 도달 가능성 및 대응 능력

[DCSA 4.4.3 구현-물리적]

위 정보를 바탕으로, 어느 영역에 어떤 수준의 물리적 보안이 필요한지를 결정해야 합니다.
보안 경계가 필요하다고 판단되는 경우, 무단 접근 및 간섭을 방지할 수 있도록 설계되어야 하며, 경보 시스템 및 CCTV 감시를 통해 관리되어야 합니다. 보호 수준 및 형태를 설정할 때는 심층 방어(defense-in-depth) 접근법을 적용하는 것이 권장됩니다.

[DCSA 4.4.3 구현-물리적]

조직의 운영 문화를 반영하는 적절한 정책 및 이를 뒷받침하는 절차를 수립·유지하지 못할 경우, 해당 정책이 무시되거나 비공식적인 현장 관행이 채택될 수 있으며, 이는 선박 자산의 보안 또는 운용을 저해할 수 있습니다. 따라서 사이버보안에 특화된 절차를 최소한 다음 항목을 포함하여 수립해야 합니다:

[DCSA 4.4.3 구현-절차]

(a) 웹 기반 인터페이스를 사용하는 외부 호스팅 시스템 또는 비즈니스 포털의 사용
(b) 외부 호스팅 서비스 또는 항만·접안 시설 내 호스팅 서비스와의 통신 및 네트워크 연결
(c) 블루투스, Wi-Fi 등 무선 네트워크 및 통신 기술의 사용
(d) 방화벽, 악성코드 방지 제품, 침입 탐지/방지 소프트웨어 등 보호용 소프트웨어 구성
(e) 선박 IT 인프라에 새 컴퓨터, 모바일 장치, 또는 IT 제어 운영 장비 연결
(f) 선박 내 개인용 무전기(PMR: Personal Mobile Radios) 사용
(g) 사용자 및 시스템 계정 권한 설정 및 관리 (제3자 인력 포함), 예: 출입 통제, 보안 경계 제어, CCTV, 환기·냉방 등 선박 내 IT 시스템 또는 보안 시스템이 설치된 구역 접근 통제

통제항목	C.3.1 사이버 리스크 조치계획	Basic

(h) 개인 IT 장비 또는 이동식 저장매체를 선박 시스템에 연결하는 행위
(i) 업무 시스템(제어 시스템, 보안 시스템 등)에서 이메일, 메신저, 외부 웹사이트, 파일 공유 서비스에 접근하는 행위
(j) 긴급 상황 발생 시 모바일을 통한 데이터에 시간 제한적 접근. 다음과 같은 프로세스도 반드시 수립되어야 함:
- 개인의 직무 및 역할에 부합하는 접근 권한을 정기적으로 검토하는 절차
- 시스템 로그 및 이상 행위에 대한 정기적인 검토 및 분석 절차

[DCSA 4.4.3 구현-절차]

사이버보안 리스크를 해결하기 위한 기술적 완화 조치를 결정하기 위해서는 먼저 다음에 대한 이해가 선행되어야 합니다:
(a) 사용 중인 시스템
(b) 시스템, 센서 및 액추에이터 간 통신에 사용되는 채널
(c) 저장·처리되는 정보 및 데이터

[DCSA 4.4.3 구현-기술 I]

시스템은 선박 전체에서 작동할 수도 있고, 특정 영역에만 제한되어 있을 수도 있습니다. 또한 완전히 선박 내에 위치할 수도 있고, 회사가 호스팅하거나 원격으로 운영될 수도 있습니다.
예를 들어, 위성항법 신호 제공과 같은 경우가 이에 해당됩니다.

[DCSA 4.4.3 구현-기술 I]

사용 중인 시스템의 특성을 파악하기 위해 고려해야 할 질문:
(a) 어떤 선박 시스템이 선박 데이터의 생성, 사용, 유지관리, 저장 및 전송에 관여하는가?
(b) 이러한 시스템 각각은 단일 선박에 전용되어 있는가?
(c) 선박 시스템이 서로 다른 작업 간에 공유되고 있는가?
(d) 선박 내·육상 또는 타 선박에 있는 제3자가 해당 시스템에 접근 가능한가?
(e) 각 시스템의 일반적인 수명 주기는 얼마인가?
(f) 각 시스템이 언제쯤 지원이 중단되거나 노후화되어 교체가 필요한가? 시스템·센서·액추에이터 간 통신 채널은 공격 또는 간섭에 취약할 수 있음

[DCSA 4.4.3 구현-기술 I]

다음 사항에 대한 이해 또한 확보되어야 함:
(a) 선박 시스템 간 및 데이터 접근이 필요한 사용자 간 데이터를 공유하거나 통신하는데 사용되는 채널, 기술, 주파수 범위
(b) 선박 시스템의 제어 및 통합에 사용되는 전자기 스펙트럼의 채널, 기술, 구성요소
(c) 해당 통신이 선박 내에서 이루어지는지, 또는 원격 접속이나 외부 처리 등의 통신이 요구되는지 여부

[DCSA 4.4.3 구현-기술 I]

선박 시스템에서 생성, 사용 및/또는 처리되는 정보와 데이터에 대한 명확한 이해가 필요합니다. 이를 위해 아래 질문들에 대한 답변을 사전에 수립해야 합니다:

[DCSA 4.4.3 구현-기술 II]

통제항목	C.3.1 사이버 리스크 조치계획	Basic
	(a) 선박 시스템의 운영을 위해 필요한 정보 및 데이터(센서 데이터 포함)는 무엇인가? (b) 그 외 보유 중인 정보 및 데이터는 무엇인가? (예: 개인 식별 정보) (c) 보유 중인 정보 및 데이터에 대해 적용되는 법적 요구사항은 무엇인가? (d) 정보 및 데이터는 어떻게 인코딩되어 있는가? (e) 정보 및 데이터는 어디에, 어떻게 저장되는가? (f) 데이터가 저장(rest), 전송(transit), 사용 중(in use)일 때, 어떻게 보호할 것인가? (g) 정보 및 데이터가 유실되어 사용할 수 없게 되었을 경우 어떤 영향이 발생하는가? (h) 해당 정보 및 데이터의 소유자는 누구인가? (i) 정보 및 데이터는 어떻게 제공되고, 사용에 어떤 제한이 있는가? (j) 해당 정보 및 데이터는 얼마나 오래 보관되어야 하는가? (k) 더 이상 필요하지 않을 경우, 해당 정보 및 데이터는 어떻게 안전하게 제거해야 하는가? **[DCSA 4.4.3 구현-기술 II]** IT 기반 물리적 보안 시스템을 설계, 구매, 구현 및 운영할 때, SSO(선박보안책임자)는 사이버 공격이나 보안 사고로부터 시스템을 보호할 방안을 고려해야 합니다. 특히, 운영 데이터, 행정 데이터, 개인 메일 등이 동일한 네트워크를 공유하는 경우, 다음과 같은 조치를 회사가 확보하고 있어야 합니다: **[DCSA 4.4.3 구현-기술 II]** (a) 적절한 아키텍처가 적용된다. (b) 시스템 보안 및 성능 유지를 위해 선박의 엔지니어링 팀과 시스템 공급업체 모두로부터 적절한 관리, 지원 및 유지보수가 제공된다. (c) IT 제어 및 보안 시스템이 손상되지 않도록 적절한 보호가 제공된다. (d) 가능한 경우 핵심 보안 시스템은 분리된 인프라를 통해 운영된다 (e) 필요할 경우, 데이터/정보가 저장 중, 사용 중 또는 전송 중일 때 이를 보호하기 위해 적절한 암호화 기술이 사용되어야 한다. **[DCSA 4.4.3 구현-기술 II]**	
비고		

D. 사이버 사고 대응

D.2 사이버 사고 대응 계획

통제항목	D.2.1 사이버 사고 대응 절차		Basic
레퍼런스 상세	IMO	사이버 사건 발생 시 CBS(컴퓨터기반시스템)를 보호하고, 해사 운영, 인명, 선박 안전 및 환경 위협을 최소화하기 위해 리스크 통제 조치와 비상 계획을 이행합니다. **[IMO 3.5.3 보호(protect)]** 사이버 사고로 인해 손상된 해운 및 항만 운영 또는 서비스에 필요한 시스템을 복원하고 복원력을 확보하기 위한 활동 및 계획을 개발, 실행 및 실행하십시오. 탐지된 사이버 사고가 선박 시스템의 다른 부분에 미치는 영향을 최소화하기 위한 적절한 조치를 실행하십시오. **[IMO 3.5.5 대응(Respond)]** 행정부가 정한 요구 기간 내에 필요한 당사자에게 사고를 보고하십시오. **[IMO 3.5.5.1 대응(Respond)]** 사이버 사고 기록은 보관되어야 합니다. **[IMO 3.5.5.2 대응(Respond)]**	
	IACS UR E26	Respond 기능 요소에 대한 요구사항은 사이버 사고의 영향을 최소화하고, 선박 내 CBS(컴퓨터기반시스템) 및 네트워크의 기능 저하 확산을 통제할 수 있도록 하는 적절한 수단의 개발 및 이행에 중점을 둡니다. **[UR E26 4.4 대응]** 사고 대응 계획(Incident response plan)은 사이버보안 사고에 대응하는 방법과 관련된 비상 상황 및 절차를 포함하여 선박 소유자에 의해 수립되어야 합니다. 이 계획은 본 UR의 적용 범위 내의 CBS(컴퓨터기반시스템)에 대해 다음을 문서화하여야 합니다. 사고를 감지(detect), 대응(respond), 제한(limit)하기 위한 사전에 정해진 지침 또는 절차의 문서화, 사고 발생 시 그 결과를 완화하기 위한 조치 **[UR E26 4.4.1.1 요구사항]** 사고 대응 계획은 사이버보안 사고에 대응해야 하는 관계자가 효과적으로 대응할 수 있도록 돕는 도구입니다. 사고 대응 계획은 단순하고 신중하게 설계될수록 효과적입니다. 계획 수립 시에는 사이버 사고의 심각성을 이해하고, 대응 조치의 우선순위를 설정하는 것이 중요합니다. 가능한 한 선박의 기능 및 서비스 수준을 유지하기 위한 수단도 포함되어야 하며, 예를 들어 예비 시스템으로의 전환 등이 명시되어야 합니다. 또한, 지상에 위치한 지정된 대응 인력은 사고 발생 시 선박 내 시스템과 통합되어 있어야 합니다. **[UR E26 4.4.1.2 근거]** 사고 대응 계획에는 사이버 사고에 대응하기 위한 절차가 포함되어야 하며, 이는 다음을 포함합니다: • 적절한 관계당국에 통지 • 사고 증거의 보고 • 사이버 사고의 영향을 네트워크 세그먼트 내로 제한하기 위한 시의적절한 수정	

통제항목	D.2.1 사이버 사고 대응 절차	Basic

조치

[UR E26 4.4.1.3 세부 요구사항]

사고 대응 계획에는 최소한 다음 정보가 포함되어야 합니다:

- 침해된 시스템을 격리하기 위한 분리 지점(breakpoints)
- 진행 중인 사이버 이벤트 또는 비정상적인 징후를 식별하는 알람 및 지표에 대한 설명
- 사이버 사고로 인해 예상되는 주요 결과에 대한 설명
- 가능한 대응 방안 중 독립 또는 로컬 제어의 중단이나 전환을 필요로 하지 않는 옵션을 우선적으로 선택
- 사이버 사고로 인해 실패한 시스템으로부터 독립적으로 작동할 수 있도록 하는 정보 (해당되는 경우)

[UR E26 4.4.1.3 세부 요구사항]

사고 대응 계획은 전자 장비를 통한 접근이 불가능한 경우를 대비하여 인쇄본으로 보관되어야 합니다.

[UR E26 4.4.1.3 세부 요구사항]

보안 구역(Security zone)에서의 네트워크 기반 통신을 종료할 수 있어야 합니다.

[UR E26 4.4.3.1 요구사항]

보안 침해가 발생하고 탐지된 경우, 사고 대응 계획에는 사고의 추가 확산 및 영향을 방지하기 위한 조치가 포함될 가능성이 높습니다. 이러한 조치에는 네트워크 구간(segment) 또는 주요 기능을 지원하는 제어 시스템의 격리가 포함될 수 있습니다.

[UR E26 4.4.3.2 근거]

사고 대응 계획(Incident Response Plan)에서 네트워크 격리가 필요한 조치로 지시된 경우, 지정된 절차에 따라 보안 구역을 격리할 수 있어야 합니다. 예를 들어, 네트워크 장비에 있는 물리적 ON/OFF 스위치를 작동시키거나, 라우터/방화벽에 연결된 케이블을 분리하는 등의 유사한 방식으로 수행할 수 있습니다. 해당 장비에는 승무원이 네트워크를 효율적으로 격리할 수 있도록 명확한 표시와 지침이 제공되어야 합니다.

[UR E26 4.4.3.3 세부 요구사항]

각 개별 시스템의 데이터 종속성 중 기능적 또는 안전 운영에 영향을 미칠 수 있는 항목은 식별되어야 하며, 격리 시 보상을 필요로 하는 데이터 또는 기능적 입력 항목이 있는 시스템이 어디인지 명확히 표시되어야 합니다.

[UR E26 4.4.3.3 세부 요구사항]

이 UR의 적용 범위 내에 있는 CBS(컴퓨터기반시스템) 또는 네트워크가 사이버 사고로 인해 의도된 서비스를 제공할 수 없는 경우, 해당 시스템이나 네트워크는 최소 리스크 상태(minimal risk condition)로 전환되어야 합니다. 즉, 가능한 안전 문제의 리스크를 줄이기 위해 안정적이고 정지된 상태로 스스로를 전환하여야 합니다.

[UR E26 4.4.4.1 요구사항]

CBS(컴퓨터기반시스템) 및 통합 시스템이 하나 이상의 최소 리스크 조건으로 전환될 수 있는 능력은, 예상치 못했거나 통제가 어려운 고장이나 사건이 발생했을 때 도달할

통제항목	D.2.1 사이버 사고 대응 절차	Basic

	수 있는 상태를 제공함으로써 시스템을 일관되고, 알려진, 안전한 상태로 유지하기 위한 안전 조치입니다. 최소 리스크 상태로의 전환은 일반적으로 시스템이 현재의 운영을 중단하고, 지원이 필요하다는 신호를 보내는 기능을 포함합니다. 이는 선박의 항해 단계(예: 항만 입·출항 vs. 공해 항해), 환경 조건 및 사건의 특성에 따라 다를 수 있습니다. **[UR E26 4.4.4.2 근거]** CBS(컴퓨터기반시스템) 또는 네트워크에 영향을 주는 사이버 사고가 감지되어, 해당 시스템이 요구되는 의도된 서비스를 제공하는 기능이 손상된 경우, 시스템은 합리적으로 안전한 상태에 도달할 수 있는 조건으로 전환되어야 합니다. 전환 조치(fall-back actions)에는 다음과 같은 내용이 포함될 수 있습니다: • 시스템을 완전히 정지시키거나 다른 안전 상태로 전환하는 것 • 시스템을 해제(disengaging)하는 것 • 제어 권한을 다른 시스템 또는 인간 운영자에게 이전하는 것 • 기타 보완 조치 최소 리스크 조건으로의 전환은 시스템을 안전하게 유지할 수 있는 적절한 시간 내에 이루어져야 합니다. 시스템이 최소 리스크 상태로 전환하는 능력은 이 UR에서 요구하는 사이버 회복력 설계에서 검토되어야 합니다. **[UR E26 4.4.4.3 세부 요구사항]**
OCIMF SIRE 2.0	다음은 선내 비상대응 계획에서 다루어야 할 사이버 사고의 포괄적 예시 목록입니다. 이러한 사고들은 ISM Code 제8장(비상 대비)에서 요구하는 선내 비상 상황 대응 절차에도 포함될 수 있습니다: ■ 전자 항해 장비의 가용성 상실 또는 항해 관련 데이터 무결성 상실 ■ 외부 데이터 소스의 가용성 또는 무결성 상실 (GNSS 포함) ■ 육상과의 필수 통신 연결 상실 (GMDSS 통신 포함) ■ 추진, 보조 시스템 및 기타 중요 시스템을 포함한 산업 제어 시스템의 가용성 상실, 데이터 관리 및 제어 무결성 상실 ■ 랜섬웨어 또는 서비스 거부(DoS) 사고 발생 **[OCIMF SIRE 2.0 7.5 사이버보안]** 비상계획과 관련 정보에는 통신 및 보고 체계 관리가 포함되어야 하며, 이는 적절한 지원 체계에 접근할 수 있도록 하고, 일부 사이버 사고 유형(데이터 삭제, 통신 링크 차단 등)에서 전자적 수단이 사용 불가할 수 있으므로 비전자적 형태로도 제공되어야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]** 운영자의 IT 부서 또는 외부 IT 계약업체로부터 기술 지원을 받을 수 있도록 연락처 정보가 준비되어 있어야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]**

통제항목	D.2.1 사이버 사고 대응 절차	Basic
BIMCO	사이버 사고에 대비한 관련 비상 상황을 다루는 대응 계획이 수립되어야 하며, 모든 계획은 전자적 접근이 완전히 불가능해지는 경우를 대비하여 인쇄본으로도 보관되어야 합니다. 선박에 비상계획을 수립할 때는 사이버 사고의 중요성을 안전 문제로 인식하고, 이에 따른 대응 조치를 우선순위에 따라 설정하는 것이 중요합니다. 이는 육상 관리팀과 함께 수행되어야만 가능합니다. **[BIMCO 9 비상 계획 수립]** 모든 사이버 사고는 운영, 자산 등에 미치는 영향을 추정하기 위해 평가되어야 합니다. 대부분의 경우, 적재 계획 및 관리 시스템을 제외하고 선박 내 IT 시스템의 손실은 (기밀 정보의 유출을 포함하더라도) 일반적으로 사업 연속성 문제로 간주되며, 선박의 안전 운항에 즉각적이고 중대한 영향을 미치지는 않습니다. IT 시스템만 영향을 받는 사이버 사고의 경우, 우선순위는 지정된 인원에게 알리고, 즉각적인 대응보다는 사고 조사 및 복구 계획의 실행에 집중해야 할 수 있습니다. 이 지정된 인원은 해당 사고가 발생할 경우 선장이 접근할 수 있도록 준비되어 있어야 합니다. **[BIMCO 9 비상 계획 수립]** OT 시스템의 손실은 선박의 안전 운항에 중대하고 즉각적인 영향을 미칠 수 있습니다. 만약 사이버 사고로 인해 OT 시스템이 손실되거나 오작동이 발생한다면, 선원, 선박, 화물, 해양 환경의 즉각적인 안전을 보장하기 위한 효과적인 조치가 반드시 필요합니다. 일반적으로, 사이버 사고에 대한 적절한 비상계획에는 주요 시스템의 손실 및 운영 방식의 전환 필요성 등이 포함되어야 하며, 이는 SMS(안전관리시스템)에 포함된 관련 운영 및 비상 절차를 통해 다루어져야 합니다. 이상적으로는, 선박의 SMS(안전관리시스템) 내 기존 절차 중 일부가 이러한 사이버 사고를 이미 다루고 있어야 합니다. 그러나 사이버 사고는 여러 시스템의 동시 실패를 유발할 수 있으므로, 이러한 사안을 비상계획 수립 시 반드시 고려해야 합니다. **[BIMCO 9 비상 계획 수립]** 다음은 선박 비상계획에 포함되어야 할 수 있는 사이버 사고의 비포괄적인 예시 목록입니다. 실제로는 대부분이 ISM 코드 8장(비상사태 대비)에 따라 선박 내 비상사태를 처리하는 회사의 절차 내에서 이미 다루어지고 있을 가능성이 높습니다. • 전자 항해 장비의 이용 불가 또는 항해 관련 데이터 무결성 상실 • 외부 데이터 소스(예: GNSS 포함)의 이용 불가 또는 무결성 상실 • 육상과의 필수 연결성 상실 (예: GMDSS 통신 등) • 산업 제어 시스템의 이용 불가 (예: 추진, 보조 시스템 및 기타 중요 시스템 포함), 데이터 관리 및 통제 무결성 상실 포함 • 랜섬웨어 또는 서비스 거부(DoS) 사고 발생 **[BIMCO 9 비상 계획 수립]** 또한, 사이버 사고로 인해 장비나 신뢰할 수 있는 정보의 손실이 발생할 경우, 기존 비상 절차 및 계획이 무력화되지 않도록 주의해야 합니다. 비상계획과 관련된 정보는 통신 및 대응 관리 절차를 포함해야 하며, 육상 지원을 받을 수 있도록 관련 지원정보도 포함되어야 합니다. 이는 일부 사이버 사고가 데이터 삭제 및 통신 연결 중단 등을 동반할 수 있기 때문입니다. **[BIMCO 9 비상 계획 수립]**

통제항목	D.2.1 사이버 사고 대응 절차	Basic

비상계획은 신중하게 설계되어야 하며, 간단하고 명확하며, 지명된 육상 인원이 사이버 사고 발생 시 선박과 통합되어 대응할 수 있도록 구성되어야 합니다. 선장과 지정된 임원은 이 계획을 정기적으로 훈련하고 검토할 수 있도록 제공받아야 합니다.

[BIMCO 9 비상 계획 수립]

효과적인 대응을 위한 출발점은 관련된 예상치 못한 사태를 포괄하는 대응 계획입니다. 그러나 대응 계획이 사이버 사고 시나리오에 완벽하게 부합할 가능성은 낮습니다. 따라서 사고 대응 계획(IRP)은 발생 가능성이 높은 시나리오를 기반으로 악성코드, 데이터 유출, 서비스 거부(DoS), 시스템 장애 등에 대한 구체적인 플레이북을 통해 보완되어야 합니다.

따라서 대응 계획과 플레이북을 정기적으로 훈련하고, 위협, 취약성 및 영향에 대한 교훈을 바탕으로 비상 대책을 수립하는 것이 중요합니다. 선박의 경우, 비상 대책은 ISM 코드 1.4.5(procedures to prepare for and respond to emergency situations;and)에서 요구하는 비상 절차에 이미 포함되어 있어야 합니다.

[BIMCO 10.1 효과적인 대응]

사이버 사고 발생 시 선박 운항 재개를 위해서는 적극적인 대응이 필요합니다. 예를 들어 ECDIS가 악성코드에 감염된 경우, 백업 ECDIS를 가동하면 또 다른 사이버 사고가 발생할 수 있습니다. 따라서 역할과 책임, 통신 경로, 핵심 활동을 상세히 기술한 사고 대응 계획을 수립하고 정기적으로 연습하는 것이 좋습니다.

사이버 사고의 복잡성이나 심각성으로 인해 선내 또는 본사의 역량으로는 대응이 어려운 경우가 발생할 수 있습니다. 또한 보험사는 사고 대응의 일환으로 외부 서비스 제공업체를 이용하도록 요구할 수도 있습니다. 이러한 경우, 네트워크 활동, 연결된 장치의 비정상적인 동작 또는 재고가 없는 장치의 감지, 공급업체의 중요 시스템에 대한 승인되지 않거나 조정되지 않은 접근, 대응 및 복구 측면(예: 이벤트 후 법의학적 분석 및 정리) 등 여러 기능을 지원하기 위해 외부 전문가의 지원을 받을 수 있어야 합니다.

가능한 범위 내에서, 이전에 확인된 사이버 사고(자사 함대 및 다른 함대에서 발생한 사고)에 대한 지식을 활용하여 회사 함대에 속한 모든 선박의 대응 계획을 개선하고, 이러한 사고에 대한 정보 전략을 고려할 수 있습니다.

[BIMCO 10.1 효과적인 대응]

NIST에 따르면, 사고 대응에는 네 가지 주요 단계가 있습니다:

1. 준비 (Preparation)
2. 탐지 및 분석 (Detection and analysis)
3. 격리 및 제거 (Containment and eradication)
4. 사고 이후 복구 (Post-incident recovery)

[BIMCO 10.2 사고 대응의 네 가지 단계]

1단계, 준비 (Preparation):

이 가이드의 앞선 조언에 따라:

- 인력의 역할과 책임을 파악
- 선박의 주요 구성 요소를 식별하고, 그 우선순위와 위치를 파악
- 관련 모든 데이터를 정기적으로 백업

통제항목	D.2.1 사이버 사고 대응 절차	Basic

- 단일 실패 지점을 식별하고, 필요 시 우회 방안을 정의
- 사고 대응 계획을 수립하고 정기적으로 훈련. 이 계획은 선박 내 승무원과 육상 인원의 역할과 책임, 명확한 의사소통에 대한 지침을 포함해야 함. 또한, 필요 시 핵심 네트워크 및 데이터 복구 프로세스도 상세히 포함되어야 함.

[BIMCO 10.2 사고 대응의 네 가지 단계]

2단계, 탐지 및 분석 (Detection and analysis):
선박의 IT, OT, IoT 환경 모니터링은 사이버보안 사고를 조기에 탐지하는 데 필수적이며, 사이버 사고의 초기 징후를 사전에 식별하는 유일한 일관된 방법입니다. 예를 들어, 선내 시스템이 공격자의 명령 및 제어 서버와 통신하여 맬웨어 다운로드를 시도하는 것을 탐지하는 경우가 있습니다. 그렇지 않으면, 조직은 과거 ECDIS가 더 이상 작동하지 않았던 사례처럼 영향이 이미 드러난 후에야 사이버 사고를 인식하게 되는 경우가 많습니다.
따라서 선박의 다양한 로그를 적극적으로 수집하고 모니터링하여 보안 사고 징후를 파악하는 것이 중요합니다. 여기에는 다음이 포함됩니다.

- 시스템, 데이터 및/또는 네트워크에 대한 의심스러운 활동 또는 무단 액세스
- 의심스러운 활동 또는 시스템, 네트워크, 계정의 무단·부적절한 사용
- 변경 관리 또는 기타 보안 절차를 따르지 않은 행위
- 중요 시스템이나 데이터의 가용성 손실 또는 중단

적절한 대응을 보장하기 위해 대응팀은 감지된 보안 이벤트를 분류하고, 가능한 경우 다음 사항을 파악해야 합니다.

- 사건이 발생한 방법
- 어떤 IT 및/또는 OT 시스템이 영향을 받았으며, 그 영향의 구체적 형태
- 상업적 및/또는 운영 데이터가 어느 정도 영향을 받았는지
- IT 및 OT 시스템에 대한 위협이 여전히 남아 있는지 여부

[BIMCO 10.2 사고 대응의 네 가지 단계]

3단계, 격리 및 제거 (Containment and eradication):
사고 발생을 억제하는 것은 시간이 매우 중요한 활동입니다. 조직은 확립된 플레이북을 기반으로 체계적이고 효과적으로 상황을 억제할 수 있습니다.
IRP 및 플레이북에 따르면, 가능한 경우 장치를 네트워크에서 제거해야 합니다. 제거가 불가능한 경우에는 장치를 VLAN 또는 LAN에서 격리하고 네트워크 간 경계 제어가 정상적으로 작동하는지 확인하는 것이 중요합니다. 또한 IRP 및 플레이북에는 다음 단계가 포함되어야 합니다.

- 방화벽 규칙이 변경되지 않았는지 확인하십시오. 정교한 공격자는 네트워크 포트를 열 수 있습니다. 시스템이 인터넷/VSAT에 연결된 경우 원격 액세스 관리 포트를 차단하는 것이 좋습니다.
- 바이러스 백신 및 맬웨어 방지 정의가 최신 상태인지 확인하십시오.
- 영향을 받은 모든 시스템의 전체 디스크 이미지를 촬영하고, 육상 포렌식 조사를 위해 관리 연속성(Chain of Custody)에 따라 안전하게 보관해야 합니다. 이 과정에는 디스크 이미지의 식별, 라벨링, 기록, 취급, 운송, 접근 제어 및 안전한 보관이 포함됩니다.

통제항목	D.2.1 사이버 사고 대응 절차	Basic

- 포렌식 목적으로 메모리 덤프(RAM 이미지)를 확보하는 것도 고려해야 합니다. 단, 컴퓨터를 재시작하거나 전원을 차단하면 RAM과 같은 휘발성 데이터가 소실될 수 있으므로 전문가의 조언에 따라 진행해야 합니다.

사이버 사고가 복잡하여 IT 및/또는 OT 시스템을 정상 운영 상태로 복구할 수 없는 경우, 선상 비상 계획과 함께 별도의 복구 계획을 수립해야 할 수도 있습니다. 이때 대응팀은 선박에 다음과 같은 조언을 제공할 수 있어야 합니다.

- 데이터를 보호하기 위해 IT 또는 OT 시스템을 종료해야 하는지, 아니면 계속 실행해야 하는지 여부
- 해안 및 특정 선박 통신 링크를 차단해야 하는지 여부와 그 이유

이러한 조치의 의미는 다음과 같습니다.

- 사전 설치된 보안 소프트웨어에서 제공하는 복구 도구를 적절히 활용해야 한다는 것입니다.

[BIMCO 10.2 사고 대응의 네 가지 단계]

4단계, 사고 이후 복구 (Post-incident recovery):
사건이 봉쇄되고 복구 작업이 진행 중인 경우에도 다음을 포함한 추가 단계를 계속 진행해야 합니다.

- 시스템 및 데이터 복구: 사이버 사고에 대한 초기 평가 이후, IT 및 OT 시스템과 데이터는 위협을 제거하고 소프트웨어를 복원하여 가능한 한 원래 상태로 복구되어야 함. 복구 계획의 내용은 섹션 10.3(Recovery plan)에서 다룸.
- 사고 조사: 사이버 사고의 원인과 결과를 파악하기 위해, 필요시 외부 전문가의 지원을 받아 회사가 조사를 수행해야 함. 이 조사에서 얻어진 정보는 향후 재발 방지에 중요한 역할을 하게 됨. 사이버 사고 조사는 섹션 10.5에서 다룸.
- 재발 방지: 위의 조사 결과를 고려하여 기술적 및/또는 절차적 보호 조치의 부족한 점을 해결하기 위한 조치를 회사 절차에 따라 수행

[BIMCO 10.2 사고 대응의 네 가지 단계]

사이버 사고를 조사하는 것은 취약점이 어떻게 악용되었는지에 대한 귀중한 정보를 제공할 수 있습니다. 기업은 가능하면, 회사의 절차에 따라 선박 내 IT 및 OT에 영향을 미치는 사이버 사고를 조사해야 합니다. 정밀한 조사는 외부 전문가의 지원이 필요할 수 있습니다.

[BIMCO 10.5 사이버 사고 조사]

외부 지원이 필요한 경우, 격리 단계에서 촬영된 전체 디스크 이미지를 조사팀과 공유할 수 있습니다. 이때 관리 연속성(Chain of Custody)이 안전하게 유지되어야 하며, 이를 통해 수집된 모든 법의학적 증거가 법정에서 변조되지 않았음을 입증하는 절차로서 허용될 수 있습니다.
특히 중대한 사고가 발생한 경우, 사고 대응의 모범 사례는 법정 소송이 제기될 수 있으며 법적 증거가 필요할 것이라고 가정하는 것입니다.

[BIMCO 10.5 사이버 사고 조사]

조사에서 얻은 정보는 선박 내외에서의 기술적 및 절차적 보호 조치를 개선하는 데 활용될 수 있습니다. 또한, 더 넓은 해운 산업 전반에 걸쳐 해상 사이버 리스크에

통제항목	D.2.1 사이버 사고 대응 절차	Basic
	대한 이해도를 높이는 데에도 도움이 될 수 있습니다. 모든 조사는 다음의 결과로 이어져야 합니다: • 해운 산업이 직면한 잠재적인 사이버 리스크에 대한 더 나은 이해 (선박 내외 모두 포함) • 교훈의 도출, 이를 통한 인식 제고 및 교육 개선 • 재발 방지를 위한 기술적 및 절차적 보호 조치의 업데이트 **[BIMCO 10.5 사이버 사고 조사]** 사이버 사고 보고는 기업의 규제 및/또는 계약상 필수 요건으로 자리 잡고 있으며, 기국 및/또는 연안국 당국, 고객, 공급업체 및 기타 피해 당사자에게 보고하는 것을 포함할 수 있습니다. 보고 기한은 즉시 보고부터 2주 이내 보고까지 매우 다양하므로, 기업은 IRP에 구체적인 보고 요건을 담은 부록을 포함해야 합니다. 사고 발생 시 기업이 보고 요건을 준수하지 않을 경우, 다양한 처벌을 받을 수 있습니다. 또한 MTS-ISAC 또는 NORMA Cyber와 같은 국제 비정부 기구에 익명으로 사고를 보고하면 공격에 대한 조기 경고를 제공하는 데 도움이 될 수 있습니다. 이는 항만 당국, 선주, 터미널 운영자 등 잠재적으로 상호 의존적인 피해자들에게 사이버 공격에 대한 조기 경보를 제공함으로써 전 세계 해운 공급망 전반에 걸쳐 심각한 공격을 제한하는 데 기여할 수 있습니다. 더불어 MTS-ISAC 또는 NORMA Cyber는 이해관계자로부터 사이버 위협 활동에 대한 적시 알림을 받고, 사고 대응 시 신속한 정보 제공처 역할을 할 수 있습니다. **[BIMCO 10.7 사이버 사고 보고]**	
	DCSA 선박은 보안 사고 대응 계획(Security Incident Response Plan)을 개발하고 구현해야 합니다. 종합적인 대응 능력을 위해, 선박은 외부 조직과의 정보 공유 및 조율을 고려해야 하며, 예를 들어 외부 서비스 제공업체나 공급망 내 조직 등이 포함될 수 있습니다. **[DCSA 2.4.3 구현]** 조직의 SMS(안전관리시스템)가 사이버 사고의 탐지 및 보고, 그리고 조직의 보안 정책에 대한 비적합 예방과 관련된 절차를 포함하고 있는지 확인해야 합니다. 사이버 리스크 관리(CRM)를 SMS(안전관리시스템)에 통합하는 경우, 사이버 관련 사고를 포함하도록 사고 보고 요건을 업데이트해야 할 수 있습니다. **[DCSA 3.3.3 구현]** 다음은 일반적인 보안 사고 및 사이버 사고의 예시입니다: • 네트워크 인프라에 대한 무단 접근 • 관리자 권한의 무단 또는 부적절한 사용 • 의심스러운 네트워크 활동 • 중요 시스템에 대한 무단 접근 • 이동식 매체의 무단 사용 • 소프트웨어 유지보수 절차 미준수 • 악성코드 및 네트워크 보호 업데이트 미적용 • 중요 시스템이 요구하는 데이터의 가용성 손실 또는 장애 • 중요 시스템 자체의 가용성 손실 또는 장애	

통제항목	D.2.1 사이버 사고 대응 절차	Basic

근본 원인 분석(root-cause analysis)을 수행한 후, 시정 및 예방 조치는 문서화되어야 합니다.

[DCSA 3.3.3 구현]

사이버 사고 대응 계획은 각 사이버 사고가 보고되고, 조사되며, 격리 및 복구 조치가 이루어지도록 보장하는 절차입니다. 보안 사고가 발생한 경우, 비즈니스 연속성과 선박 안전성 측면에서 선박의 핵심 시스템이 중단 없이 정상적으로 운영되도록 하는 것이 필수적입니다.

[DCSA 4.1.2 설명]

사고 대응 계획을 수립할 때 다음과 같은 요소들을 고려하여야 합니다:

(a) 사이버보안 책임에 관한 정보와, 사이버보안 사고 발생 시 선박을 지원할 수 있는 조직(예: 전담 사고 대응팀, 보안 운영 센터 등)과의 연계 체계

(b) 선박 및 선박 승무원의 사이버보안 사고 대응 역량 강화를 위한 모의훈련 실시

(c) 사이버보안 관련 통신 체계 수립, 예를 들어:

- 보안 책임자 간의 정보 공유
- 기술 보안 담당자와 전체 보안 팀 간의 연계
- 선박 및 자산 관련 정보를 외부 제3자에게 제공하는 체계 등

기존의 비상/사고 대응 계획은 보안 사고 대응 절차 및 관련 커뮤니케이션 계획을 포함하도록 개정되어야 하며, 사이버 리스크 관리 역량을 갖춘 자원이 SMS(안전관리 시스템)에 의해 이미 구성된 비상 대응팀에 포함되어야 합니다.

[DCSA 4.1.3 구현]

보안 사고 대응 계획은 보안 사고에 대한 체계적이고 효과적인 대응을 위해 수립되어야 하며,

선박, 그 기능, 자산, 사고 시 승무원 및 제3자의 역할에 대한 리스크 평가를 기반으로 해야 합니다.

이 계획에는 다음 항목이 포함되어야 합니다:

a. 리스크 완화 조치
- 사고와 관련된 포렌식 정보를 법집행기관이 수집·활용할 수 있도록 하는 준비 조치
- 사고 원인에 대한 상세 분석 수행
- 보안 위반 또는 사고 발생 시(근접 사고 포함)의 대응 절차
- 시스템 장애 또는 불가용 상태 시 요구되는 비즈니스 연속성 유지 방안
- 중대한 장애 발생 시 재해 복구 또는 사고 복구 절차
- 사고 확산 방지 및 복구 절차

b. 사고 후 검토 절차
- SSO(선박 보안 책임자) 및 필요시 공급망 관련 기관이 수행하는 사고 리스크 및 대응 평가

c. 제3자로 인한 사고에 대한 계약 조항 반영
- 예: 자문기관, 협력업체, 공급업체로 인한 침해사고에 대한 조치 포함

d. 선박 내 조치와 기존 비즈니스 연속성 계획 간의 연계
- 선박에서 수행되는 조치가 기존 비상대응 및 연속성 계획과 연계되도록 구성

통제항목	D.2.1 사이버 사고 대응 절차	Basic

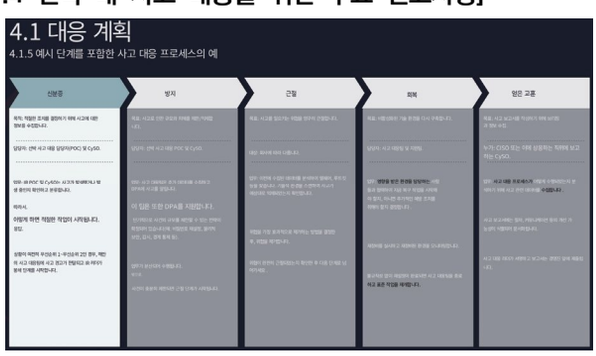
[DCSA 4.1.3 구현]

상황 평가 절차 도입 (Introduce a Situation Assessment Process)
SBAR(Situation, Background, Assessment, and Recommendation) 인계 프로토콜은 응급의료서비스(EMS) 팀에서 사용되는 명확하고 신속한 상황 전달 방식으로, 상황이 불분명하거나 긴급한 경우에도 효과적인 커뮤니케이션을 가능하게 합니다. 이 프로토콜은 팀 구성원 간 명확하고 정확한 의사소통을 촉진하며, 구두 및 서면으로 공유해야 할 중요 정보에 대한 공통의 이해 기반을 형성합니다. 선박 내에서 SBAR 플레이북을 보관하고 반복적으로 훈련하는 것을 권장합니다.

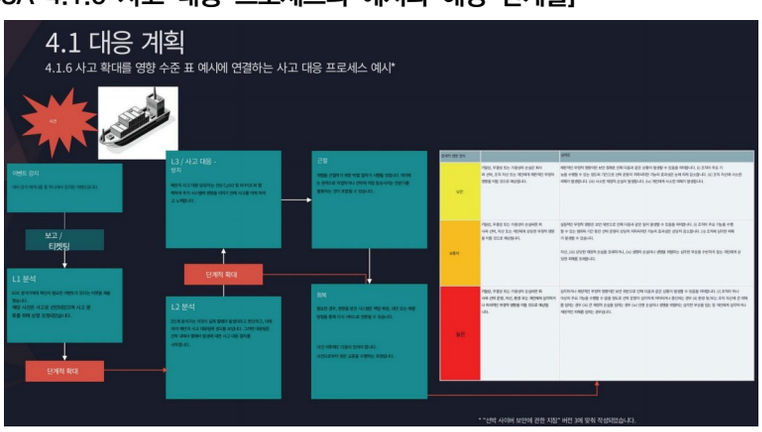
[DCSA 4.1.4 선박 내 사고 대응을 위한 주요 권고사항]

체크리스트 사용 (Use checklists)
사이버 사고 발생 시, 개인 또는 팀은 각자의 판단에 따라 최선의 방식으로 대응하려는 경향이 있습니다. 이는 상황 인식, 부서의 우선순위, 또는 조치를 하지 않으려는 두려움에 기반할 수 있습니다. 모든 논리적 절차가 빠짐없이 이행되도록 하기 위해, 체크리스트(또는 사고별 체크리스트)를 사전에 제작·훈련·활용하는 것이 필요합니다. 또한, 사고로 인해 IT 시스템에 접근이 제한될 수 있으므로 체크리스트는 하드카피(인쇄물) 형태로도 보관할 것을 권장합니다.

[DCSA 4.1.4 선박 내 사고 대응을 위한 주요 권고사항]



[DCSA 4.1.5 사고 대응 프로세스의 예시와 해당 단계들]



[DCSA 4.1.6 사고 확대를 영향 수준 표 예시에 연결하는 사고 대응 프로세스 예시]

커뮤니케이션 계획서에 최소한 포함되어야 할 권장 항목은 다음과 같습니다:

통제항목	D.2.1 사이버 사고 대응 절차	Basic

(a) 사이버보안 책임에 관한 정보 및 사이버보안 사고 발생 시 선박을 지원할 수 있는 외부 기관과의 연계 정보
(b) 커뮤니케이션의 시점 및 일정
(c) 대체 커뮤니케이션 수단
(d) 사이버보안 사고에 대한 선박 및 승무원의 대응 역량을 점검하기 위한 사이버보안 훈련의 실행
- 본사 참여가 요구되는 선박-육상 간 비상 훈련은 안전(ISM) 및 보안(ISPS)과 관련되어 있음
- 현재까지의 보안 훈련 항목에는 "해적", "폭탄 위협", "밀항자 발생" 등이 포함되며,
- "사이버보안 공격" 역시 하나의 시나리오로 포함되어야 함

(e) 사이버 관련 커뮤니케이션 사항 (예시):
- 보안 책임자 간의 커뮤니케이션
- 기술 보안 담당자와 전체 보안 팀 간의 커뮤니케이션
- 제3자에게 선박 및 자산에 대한 정보를 제공하는 커뮤니케이션

[DCSA 4.2.3 구현]

ISM 코드는 사고를 일반적으로 다음 두 가지 범주로 분류하고 있습니다:

(a) 관계당국에 보고되어야 할 만큼 심각한 사고

CSO(Company Security Officer, 회사 보안책임자)에 의해 관계당국에 보고되어야 할 사례로는 다음과 같습니다:
- 선박 내 민감한 시스템에 대한 무단 접근, 오용 또는 사기적 사용
- 민감한 선박 시스템의 정보에 대한 무단 변경 또는 손실
- 인명, 선박 또는 화물의 안전에 영향을 미치는 사이버 공격 시도 또는 성공 사례
- 사이버보안 침해가 의심되거나 명백히 사고에 기여한 선박 손상 사례
- 밀수 또는 불법·무단 운송을 위한 화물 적하 명세 조작 시도
- (예: 국제 조약에 따라 제한된 무기, 마약, 폭발물 등 통제 물품)
- 여객에게 영향을 주는 시도, 예: 개인정보 도용, 무단 접근을 통한 사기 발생, 또는 선박 내 금융 정보 처리 시스템의 침해

(b) 심각도는 낮지만 보고 및 조사가 필요한 사고

SSO(Ship Security Officer, 선박 보안책임자) 또는 사이버 사고의 경우 CySO(사이버보안책임자)에 의해 보고되고 조사되어야 하는 사례:
- 항목 (a)에 해당하지 않으나, 선박 및/또는 그 화물에 영향을 미치는 사이버보안 사고
- 선박과 관련 없는 시스템, 예: 승무원 개인 소유 장치에 영향을 주는 악성코드 사고, 이러한 사이버보안 사고는 일반적으로 무단 접근이나 다음과 같은 행위로 인해 발생할 수 있습니다:
  1. 자산(문서, 저장 매체 등)의 손실 또는 도난
  2. 데이터 또는 정보에 대한 무단 접근
  3. 데이터 또는 정보의 손상, 유출, 무단 조작 또는 변경
  4. 시스템과 연결된 선박 자산의 손실 또는 유출

통제항목	D.2.1 사이버 사고 대응 절차	Basic
		5. 버그 또는 기타 감시 장비의 설치 6. 악성 소프트웨어 삽입 **[DCSA 4.3.2 설명]** 선박은 다음 사항을 이해하고 기반으로 하는 보안 사고 관리 계획을 수립해야 합니다: (a) 사이버, 인적, 자연적 요인을 포함한 잠재적 혼란 원인 (b) 선박을 안전하게 운항하기 위해 필요한 핵심 시스템 (c) 사고 발생 시 운영 유지를 위해 사용할 수 있는 대체 운영 방안의 성격 및 실행 가능성 (d) 해당 대체 방안 하에 선박이 현실적으로 운영 가능한 수준의 역량 또한, 선박은 혼란을 야기하는 사건을 신속하게 탐지할 수 있는 시스템 및 절차를 갖추어야 하며, 이로 인해 보안 사고 관리 계획에 명시된 적절한 대응이 가능한 상태가 되어야 합니다. **[DCSA 5.1.3 구현]** 비상 대응 계획은 다음을 검증하기 위해 정기적으로 실시되어야 합니다. 통신, 협조, 자원 가용성, 절차 및 대응 역량. 훈련 형태는 다음 중 하나일 수 있습니다: (a) 전체 규모 훈련 또는 실제 훈련 (b) 테이블탑 시뮬레이션 또는 세미나 형식 훈련 (c) 비상 대응 등 다른 훈련과의 통합 훈련 **[DCSA 5.1.3 구현]**
비고		

D.3 사이버 복구 계획

통제항목	D.3.2 사이버 복구 계획		Basic
레퍼런스 상세	IMO	사이버 사고로 인해 영향을 받은 선박 운항에 필요한 네트워크를 포함하여 선상 CBS(컴퓨터기반시스템)를 복구하기 위한 조치를 파악하고 구현합니다. **[IMO 3.5.6 복구(Recover)]** 사이버 사고로 인해 영향을 받을 수 있는 필수 비즈니스 또는 임무 수행에 중요한 자산이나 시스템 복구 및 재가동 전략을 개발·유지·이행합니다 **[IMO 3.5.6.1 복구(Recover)]** 사이버 사고의 근본 원인을 분석하여, 기저 문제와 취약성을 해결하고 유사 사고의 재발을 방지합니다. **[IMO 3.5.6.3 복구(Recover)]**	
	IACS UR E26	선주는 사이버 사고 이후 CBS(컴퓨터기반시스템)를 작동 상태로 복원할 수 있도록 지원하는 복구 계획을 수립하여야 합니다. 이 계획은 이 UR의 적용 범위 내에서 사이버 사고로 인한 중단이나 고장이 발생한 후, 작동 가능한 상태로 복원할 수 있는 적절한 수단을 포함하여야 합니다. 가능한 지원 수단 및 복구 계획에 포함될 담당자가 명확히 정의되어야 합니다. **[UR E26 4.5.1.1 요구사항]** 사고 대응 절차는 시스템 복구의 필수적인 부분입니다. 책임 있는 인원은 복구 조치(예: 드라이브 삭제 등)의 결과를 신중히 고려하고 그 영향을 인지한 상태에서 이를 신중하게 수행하여야 합니다. 그러나 일부 복구 조치는 사고 원인에 대한 귀중한 정보를 제공할 수 있는 증거를 파괴할 수 있다는 점에 유의하여야 합니다. 필요한 경우, 외부 사이버 사고 대응 지원을 확보하여 운영 복구 능력을 회복하는 동안 증거를 보존할 수 있도록 해야 합니다. **[UR E26 4.5.1.2 근거]** 복구 계획은 선원 및 외부 인원이 쉽게 이해할 수 있도록 작성되어야 하며, 고장난 시스템의 복구를 위한 필수 지침과 절차, 그리고 육상 지원이 필요한 경우 이를 요청하는 방법을 포함하여야 합니다. 또한, 선박 내 복구에 필요한 소프트웨어 복구 매체 또는 도구도 비치되어야 합니다. **[UR E26 4.5.1.3 세부 요구사항]** 복구 계획을 개발할 때는 관련된 시스템 및 하위 시스템을 명확히 명시하여야 하며, 다음의 복구 목표 또한 정의되어야 합니다: • 시스템 복구: 통신 기능을 복구하기 위한 방법 및 절차는 복구 시간 목표(RTO, Recovery Time Objective) 기준으로 명시되어야 합니다. 이는 필요한 통신 링크와 처리 능력을 복구하는 데 걸리는 시간을 의미합니다. • 데이터 복구: OT 시스템의 안전 상태 및 선박의 안전 운항을 복구하기 위해 필요한 데이터를 복구하는 방법 및 절차는 복구 시점 목표(RPO, Recovery Point Objective) 기준으로 명시되어야 합니다. 이는 데이터가 존재하지 않아도 허용될 수 있는 최대 시간을 의미합니다. **[UR E26 4.5.1.3 세부 요구사항]**	

통제항목	D.3.2 사이버 복구 계획	Basic

복구 목표가 정의되면, 잠재적인 사이버 사고 목록이 작성되고, 복구 절차가 개발 및 기술되어야 합니다. 복구 계획에는 다음 정보가 포함되거나 이를 참조할 수 있어야 합니다:

- 고장난 시스템을 복구하기 위한 지침 및 절차, 이때 중복, 독립 또는 로컬 운영의 방해 없이 복구가 이루어져야 합니다.
- 정보 백업 및 안전한 저장을 위한 절차
- 완전하고 최신 상태의 논리적 네트워크 다이어그램
- 고장난 시스템 복구를 담당하는 인원 목록
- 외부 기술 지원을 위한 통신 절차 및 연락 인원 목록 (시스템 지원 벤더, 네트워크 관리자 등 포함)
- 모든 구성요소의 현재 설정 정보

[UR E26 4.5.1.3 세부 요구사항]

선박의 운항과 항해는 선박 내 인원의 안전을 보장하기 위해 복구 계획 내에서 우선순위가 부여되어야 합니다.

[UR E26 4.5.1.3 세부 요구사항]

복구 계획은 선박에 종사하는 인원이 현장에 보관하여야 하며, 사이버 사고 발생 시 신속한 접근이 가능해야 합니다.

[UR E26 4.5.1.3 세부 요구사항]

이 UR의 적용 범위 내에 있는 CBS(컴퓨터기반시스템)는 백업 및 복원 기능을 갖추어야 하며, 이를 통해 선박이 사이버 사고 이후 항해 및 운영 상태를 안전하게 회복할 수 있어야 합니다.

[UR E26 4.5.2.3.1 복원 기능]

데이터는 보안된 복사본 또는 이미지로부터 복원 가능하여야 합니다.

[UR E26 4.5.2.3.1 복원 기능]

이 UR의 적용 범위에 있는 CBS(컴퓨터기반시스템) 및 네트워크는 다음 기능을 수행할 수 있어야 합니다:

- 제어된 종료 (Controlled shutdown),
- 초기 상태로의 재설정 (Reset to an initial state),
- 안전 상태로의 롤백 (Roll-back to a safe state),
- 전원 차단 후 재시작 (Restart from a power-off condition)

이는 사이버 사고로 인한 손상 가능성으로부터 신속하고 안전한 복구를 가능하게 하기 위함입니다.

상기 작업들을 실행하는 방법에 대한 적절한 문서화 자료가 선박 승무원에게 제공되어야 합니다.

[UR E26 4.5.3.1 요구사항]

제어된 종료는 소프트웨어 기능을 통해 CBS(컴퓨터기반시스템) 또는 네트워크를 종료하는 것을 의미하며, 이 과정에서는 연결된 다른 시스템들이 보류 중인 트랜잭션을 완료/롤백하고, 프로세스를 종료하며, 연결을 닫고, 전체 통합 시스템을 안정적이고 알려진 상태로 남기는 작업이 수행됩니다. 이는 전원이 강제로 차단되어 컴퓨터가

통제항목	D.3.2 사이버 복구 계획	Basic

꺼지는 하드 종료(hard shutdown)와는 구별됩니다.

[UR E26 4.5.3.2 근거]

일부 사이버 사고의 경우 하드 종료가 안전 조치로 간주될 수 있으나, 통합 시스템의 경우에는 제어된 종료가 더 바람직합니다. 이러한 방식은 예측 가능한 동작으로 시스템을 일관되고 알려진 상태로 유지할 수 있기 때문입니다. 표준 종료 절차 없이 시스템이 종료될 경우 데이터 또는 프로그램, 운영 체제 파일의 손상이 발생할 수 있으며, 특히 OT 시스템에서는 불안정, 오작동, 기능 실패 등이 발생할 수 있습니다. 재설정(reset) 작업은 일반적으로 소프트 부트(soft boot)로 시작되며, 시스템이 종료, 메모리 정리, 장치 초기화 단계를 거치도록 지시합니다. 시스템에 따라 재설정의 동작은 다를 수 있습니다.

[UR E26 4.5.3.2 근거]

롤백(rollback)은 시스템을 이전의 안정적인 상태로 되돌리는 작업을 의미합니다. 이는 데이터 및 시스템 무결성을 유지하는 데 중요하며, 오류가 발생하더라도 정상 상태로 복구할 수 있는 능력을 제공합니다. 사이버 사고와 같은 충돌 상황에서의 복구에 핵심적인 기능입니다.

[UR E26 4.5.3.2 근거]

재시작(restart)는 소프트웨어 및 데이터를 읽기 전용 소스에서 다시 불러오는 작업으로,

롤백과 결합된 형태로 작동될 수 있으며, 예기치 않은 오류나 사이버 사고로부터 복구하는 효과적인 방법으로 여겨집니다. 재시작 후 결과는 일반적으로 한 구성 요소의 복구로는 충분하지 않은 통합 시스템의 복원 능력을 반영합니다.

[UR E26 4.5.3.2 근거]

이 UR의 적용 범위에 포함되는 CBS(컴퓨터기반시스템) 및 네트워크는 다음을 수행할 수 있어야 합니다:

- 제어된 종료(controlled shutdown)는 다른 연결된 시스템들이 보류 중인 트랜잭션을 완료하거나 롤백하고, 프로세스를 종료하며, 연결을 닫을 수 있도록 하여, 전체 통합 시스템이 안전하고 일관되며 알려진 상태에 있도록 합니다.
- 시스템 스스로를 리셋(reset)에서는 시스템이 종료, 메모리 정리 및 장치 초기화를 수행하도록 지시하는 과정이 포함됩니다.
- 이전 구성 또는 상태로의 롤백(roll-back)은 시스템 무결성과 일관성을 회복하기 위한 이전 구성 및/또는 상태로 되돌리는 작업입니다.
- 소프트웨어 및 데이터를 읽기 전용 소스에서 다시 불러와 새 이미지를 로드하는 재시작(restart)에서 (예: 롤백 작업 후) 재시작 시간은 시스템의 의도된 서비스와 호환되어야 하며,시스템이 포함된 다른 연결된 시스템이나 통합 시스템 전체를 불안정하거나 안전하지 않은 상태로 만들지 않아야 합니다.

사이버 사고로 영향을 받은 시스템에서 위에 언급된 작업을 수행하는 방법에 대한 문서가 선박 내 승무원에게 제공되어야 합니다.

[UR E26 4.5.3.3 세부 요구사항]

통제항목	D.3.2 사이버 복구 계획	Basic
	OCIMF SIRE 2.0	■ 확인된 경우: • 사이버 비상계획이 다음의 상실을 다루지 않았음: - 항해 장비의 기능 또는 신뢰성 (예: ECDIS) - GNSS와 같은 외부 데이터 소스의 가용성 또는 무결성 - GMDSS 통신을 포함한 육상과의 연결성 - 추진, 조타 등과 같은 중요 시스템 제어 시스템 ■ 사이버 비상계획의 하드 카피(Hard Copy)가 없었음 ■ 운영자의 IT 부서 또는 외부 IT 계약업체의 기술 지원 연락처 정보가 적절히 준비되어 있지 않았음 **[OCIMF SIRE 2.0 7.5 사이버보안]**
	BIMCO	사이버 사고가 복잡하여 IT 및/또는 OT 시스템이 정상 운영 상태로 복구되지 못하는 경우, 회복 계획은 선박 내 비상 대응 계획과 함께 실행되어야 할 수 있습니다. 이런 경우, 대응팀은 선박 측에 다음과 같은 조언을 제공할 수 있어야 합니다: • IT 또는 OT 시스템을 종료하거나 계속 운영할지 여부 • 육상과의 특정 통신 링크를 종료해야 할지 여부 및 그 영향 • 사전 설치된 보안 소프트웨어에서 제공하는 복구 도구의 적절한 사용 여부 • 사고가 기존 복구 계획의 범위를 초과하여 IT 또는 OT 시스템에 얼마나 영향을 미쳤는지 **[BIMCO 10.2 사고 대응의 네 가지 단계]**
	DCSA	사이버보안 복구 활동의 추가 목표에는 다음이 포함될 수 있습니다. 대체 방법을 활용한 정보 시스템 복구, 표준 운영 절차의 대체 실행, 백업 위치에서의 시스템 복구, 사고의 업무적 영향도에 따른 비상 대응 통제 조치(Contingency Controls) 적용 **[DCSA 5.1.2 설명]** 사이버 공격을 예방하는 것이 바람직하지만, NIST(National Institute of Standards and Technology)는 다음과 같이 명시합니다. “예방에만 의존하는 것은 아무런 준비가 없는 것과 마찬가지로 리스크하다.” 일부 사이버 공격은 완전히 방지할 수 없기 때문에, 복구에 대한 준비도 반드시 필요합니다. **[DCSA 5.1.2 설명]** 복구 계획은 선박 내외부에 하드카피(인쇄본) 형태로 보관되어야 하며, IT 및 OT 시스템의 복구를 위한 절차를 지원하는 것이 목적입니다. 선박의 운영 및 항해 기능을 담당하는 승무원의 안전 확보가 우선순위에 포함되어야 하며, 해당 계획은 사이버보안 담당자 및 관련 모든 기술 인력이 이해할 수 있도록 작성되어야 합니다. 복구 계획의 구체성은 선박 유형, 그리고 탑재된 IT, OT 및 기타 시스템에 따라 달라질 수 있습니다. **[DCSA 5.1.2 설명]**
비고		

통제항목 상세 – Advanced

A. 사이버보안 관리체계

A.2 사이버보안 조직 및 외부업체 관리

통제항목	A.2.2 사이버보안 외부업체 관리	Advanced
레퍼런스 상세	IACS UR E26	본 절에서는 3.1(Primary goal)에서 정의된 주요 목표를 달성하기 위해 충족되어야 하는 요구사항을 다루며, 이는 3.2(sub-goals per function element)절에서 식별된 다섯 가지 기능 요소에 따라 구성되어 있습니다. 요구사항은 선박의 설계, 건조 및 운항에 참여하는 이해관계자들에 의해 이행되어야 합니다. 이들 중 다음과 같은 이해관계자를 식별할 수 있습니다 (정의에 대해서는 2절(Definition) 참조): • 선주/회사 • 시스템 통합자 • 공급업체 • 선급협회 위의 요구사항들은 이러한 이해관계자들에 의해 이행될 수 있으나, 본 UR의 목적상 해당 요구사항을 이행할 책임은 선급협회와 계약을 체결한 이해관계자에게 있습니다. **[UR E26 4. 요구사항]**
	BIMCO	적합성 증서(DoC) 보유자는 선박 내 사이버 리스크 관리에 대한 최종 책임을 집니다. 만약 선박이 제3자에 의해 관리되고 있다면, 선박 관리자는 선주와의 합의를 권고받아야 합니다. **[BIMCO 1.6 선주와 선박 관리자 간의 관계]** 적합성 증서(DoC) 보유자는 선박 내 사이버 리스크 관리에 대한 최종 책임을 집니다. 만약 선박이 제3자에 의해 관리되고 있다면, 선박 관리자는 선주와의 합의를 권고받아야 합니다. **[BIMCO 1.6 선주와 선박 관리자 간의 관계]** 양 당사자는 책임 분담, 기대치의 일치, 관리자를 위한 구체적인 지침에 대한 합의, 그리고 구매 결정 및 예산 요건에 대한 참여 가능성에 대해 중점을 두어야 합니다. **[BIMCO 1.6 선주와 선박 관리자 간의 관계]** ISM 요구사항 외에도, 이러한 합의는 필요 시 EU 일반 데이터 보호 규정(GDPR), 기타 연안국의 특정 사이버보안 규정과 같은 추가적인 법령을 고려해야 합니다. 관리자와 선주는 이 가이드라인을 기반으로, 효과적인 사이버 리스크 관리 체계를 어떻게 구현할지에 대해 자유롭게 논의하는 출발점으로 삼는 것이 바람직합니다. **[BIMCO 1.6 선주와 선박 관리자 간의 관계]** 사이버 리스크 관리에 대한 선박 관리자와 선주 간의 모든 합의는 서면으로 작성되고 서명되어야 합니다. **[BIMCO 1.6 선주와 선박 관리자 간의 관계]** 이 관계의 중요성으로 인해, 선박 대리점은 이해관계자로 명시되며 선주, 운항자, 터미널, 항만 서비스 제공업체, 관계당국 등과 민감한 정보, 재무 정보, 항만 조정

통제항목	A.2.2 사이버보안 외부업체 관리	Advanced

정보 등을 동시에 지속적으로 교환하게 됩니다. 이 관계는 단순한 공급업체 이상의 의미를 가지며, 특히 부정기선(tramp trade)에서는 선주가 회사를 대리하는 현지 대표자(독립 선박 대리점)를 필요로 합니다.

[BIMCO 1.7 선주와 선박 대리점 간의 관계]

대리점의 품질 기준은 중요합니다. 왜냐하면 다른 비즈니스와 마찬가지로, 대리점 또한 사이버 범죄자의 표적이 될 수 있기 때문입니다. 예를 들어 IT 또는 OT 장비의 납품과 관련하여, 사이버 범죄자는 전자 송금 사기나 허위 선박 예약 등과 같은 범죄를 저지를 수 있으며, 랜섬웨어나 해킹과 같은 사이버 위협도 발생할 수 있습니다. 이에 따라 선주와 대리점 간에는 사이버 리스크를 줄이기 위한 공동의 사이버 전략 및 사이버 기반 협력이 요구됩니다.

[BIMCO 1.7 선주와 선박 대리점 간의 관계]

사고: 선박 대리인 및 선주 랜섬웨어 사건
한 선주가 회사 업무 네트워크가 피싱 이메일 첨부파일을 통해 랜섬웨어에 감염되었다고 신고했습니다. 랜섬웨어의 출처는 서로 다른 항구에 있는 두 명의 선박 요원이었으며, 이들은 각각 다른 시기에 감염된 것으로 보입니다. 선박들도 피해를 입었지만, 피해는 업무 네트워크에만 국한되었고 항해 및 선박 운항에는 영향을 미치지 않았습니다. 한 사례에서는 선주가 몸값을 지불했습니다.
이 사고의 중요성은 신뢰할 수 있는 비즈니스 파트너 및 제조업체와의 관계 전반에 걸쳐 조화로운 사이버보안이 공급망 전체에 매우 중요하다는 것입니다. 자신의 사업을 강화하기 위한 개별적인 노력은 용감하고 선의의 의도가 있을 수 있지만, 그것만으로는 충분하지 않을 수도 있습니다. 공급망의 모든 당사자는 사이버 위험을 완화하기 위해 협력하고 필요한 경우 정보를 공유해야 합니다. 피싱은 사이버 공격에 가장 흔히 사용되는 기법 중 하나이므로, 모든 직원을 대상으로 하는 필수 사이버보안 교육에 피싱을 식별하고 신고하는 방법에 대한 교육을 포함해야 합니다.

[BIMCO 1.7 선주와 선박 대리점 간의 관계]

기업은 서비스 제공자, 벤더 및 기타 외부 당사자(공공 기관 포함)와의 상호 작용에서 물리적 보안 및 사이버 위험 관리 프로세스를 평가해야 합니다.
공급업체, 벤더 또는 서비스 제공업체의 물리적 및/또는 사이버보안 부족은 기업 IT 시스템 침해 및/또는 선박 운영환경(OT)/IT 시스템 손상을 초래할 수 있습니다. 따라서 기업은 필요에 따라 사이버 관련 요구 사항 및 기대 사항을 정의하는 공급업체/벤더/서비스 제공업체 간 계약 및 계약 체결을 고려해야 합니다. 또한 신규 및 기존 계약 모두에 대한 사이버 위험 관리 프로세스를 평가해야 합니다. 널리 인정되는 표준(예: 서비스형 소프트웨어(SaaS) 애플리케이션용 서비스 조직 관리(SOC) 2 유형 2)이 존재하지만, 기업은 자체 표준을 정의할 수도 있습니다.
공급업체 검토 시 평가되며 계약 요건에 포함될 수 있는 프로세스는 다음과 같습니다:

- 하청업체 관리를 포함한 보안 관리
- 제조/운영 보안
- 소프트웨어 엔지니어링 및 아키텍처, 그리고 위협 개발 및 운영 체제 업데이트로 인해 발생하는 새로운 취약성을 지속적으로 해결할 수 있는 능력
- 자산 및 사이버 사고 관리

통제항목	A.2.2 사이버보안 외부업체 관리	Advanced

- 인사 보안
- 데이터 및 정보 보호
- 원격 서비스/접속

[BIMCO 1.8 공급업체 및 기타 외부 당사자와의 관계]

회사가 직접 계약을 맺고 있지 않은 서비스 제공업체를 평가하는 것은 도전적일 수 있으며, 특히 많은 공급업체가 있는 경우 더욱 그러합니다. 이러한 경우, 공급업체 리스크 데이터를 수집 및 관리하는 제3자 제공업체를 활용하는 것도 고려해볼 수 있습니다.

[BIMCO 1.8 공급업체 및 기타 외부 당사자와의 관계]

선박 및 선사의 공공기관과의 상호작용은 복잡하며, 선박 입항, 승무원 변동, 화물 서류 제출 등 다양한 이슈를 포함합니다. 이로 인해 사이버 리스크 관리와 관련된 문제가 발생할 수 있습니다. 이러한 문제는 상업적 관계와는 다른 방식으로 관리되어야 하며, 현재 및 향후 공공기관과의 커뮤니케이션 연결은 필수 정보 교환을 위해 회사의 사이버보안 전략의 일부로 평가되어야 합니다. 이러한 보안상의 우려 사항은 필요 시 관계당국에 보고되어야 하며, 일부 항목은 3.4절(ship to shore interface)에서 추가로 설명됩니다.

[BIMCO 1.8 공급업체 및 기타 외부 당사자와의 관계]

다음은 제조업체, 제3자(공급업체, 계약업체, 서비스 제공업체 포함)에 대해 고려해야 할 사항입니다:

- 제조업체 및 서비스 제공업체가 자사 제품 및 서비스에서 효과적이고 비용 효율적인 사이버보안 모범 사례를 구현할 수 있는 의지 및 능력 여부. 이는 예: CIRM 사이버보안 실천 강령 및 관련 구현 가이드라인을 따름으로써 입증될 수 있음.
- 제조업체 및 서비스 제공업체의 사이버 리스크 인식 및 관리 절차. 일부 업체는 자사 조직 내 사이버보안 인식 교육이나 거버넌스가 부족할 수 있으며, 이는 사이버 사고 발생 가능성을 높이는 취약점으로 작용할 수 있음. 제3자 공급업체와 협력업체는 위협 행위자의 주요 표적이 되어왔으며, 최근 몇 년간 다양한 사이버 사고에 연루된 바 있음. 따라서 이러한 업체들은 책임자의 승인을 받은 사이버 위험 관리 회사 정책을 정기적으로 검토하고 업데이트해야 하며, 접근 가능한 IT 및 OT 시스템에 대한 필수 사이버보안 교육 및 거버넌스 절차를 포함해야 합니다.
- 제3자의 사이버 위험 관리 절차의 성숙도: 선주는 다음을 수행해야 합니다. 사이버보안에 대한 내부 거버넌스를 점검하고 향후 계약 및 서비스 검토 시 사이버 위험 관리 보증을 확보해야 합니다. 선박이 지속적인 지원 및 유지보수를 위해 해상 터미널, 하역 회사 또는 OT 공급업체 등 제3자와 연동되는 경우, 네트워크 보안을 확보하는 것이 특히 중요합니다.

[BIMCO 1.8 공급업체 및 기타 외부 당사자와의 관계]

사고: ECDIS의 미확인 바이러스로 인해 항해 지연
신조 건화물선의 ECDIS가 바이러스에 감염되어 출항이 며칠 동안 지연되었습니다. 해당 선박은 종이 없는 항해를 위해 설계되었으며 종이 해도를 탑재하지 않았습니다. ECDIS 고장은 기술적인 문제로 보였으며, 선장과 항해사들은 이를 사이버 문제로

통제항목	A.2.2 사이버보안 외부업체 관리	Advanced
		인식하지 못했습니다. 제조사 기술자가 선박을 방문하여 상당한 시간 동안 문제 해결을 진행한 결과, 두 ECDIS 네트워크 모두 바이러스에 감염된 것을 발견했습니다. 바이러스는 격리되었고 ECDIS 컴퓨터는 복구되었습니다. 이 사건의 감염원과 감염 경로는 아직 밝혀지지 않았습니다. 항해 지연과 수리 비용은 총 수십만 달러(미화)에 달했습니다. **[BIMCO 1.8 공급업체 및 기타 외부 당사자와의 관계]**
비고		

B. 사이버보안 통제

B.1 사이버 자산 관리

통제항목	B.1.2 네트워크 구성도		Advanced
레퍼런스 상세	IMO	선박 내 디지털 자산 목록을 유지·관리하며, 2.2.1(Background)항에 명시된 시스템을 포함합니다. 내·외부 시스템 종속성과 네트워크 연결을 식별합니다. **[IMO 3.5.2.2 식별(Identify)]**	
	IACS UR E26	'식별' 기능 요소에 대한 요구 사항은 다음과 같습니다. 하나는 탑재된 CBS(컴퓨터기반시스템)와 이들의 상호 의존성 및 관련 정보 흐름을 식별하는 것을 목표로 하며, 다른 하나는 관리, 운영 및 거버넌스에 관련된 핵심 리소스, 역할 및 책임을 식별하는 것을 목표로 합니다. **[UR E26 4.1 식별]** Zones and conduit diagram은 본 UR의 적용 범위에 포함되는 CBS(컴퓨터기반시스템)들이 어떻게 보안 존(Security Zones)으로 그룹화되는지를 설명해야 하며, 다음의 정보를 포함해야 합니다: 각 보안 존을 명확하게 구분하여 표시합니다. 본 UR의 적용 범위에 포함되는 각 CBS(컴퓨터기반시스템)를 간략하게 도식화하고, 해당 CBS(컴퓨터기반시스템)가 배정된 보안 존을 명시하며, 해당 CBS(컴퓨터기반시스템)/장비의 물리적 위치도 함께 나타냅니다. 공급업체가 제공한 CBS(컴퓨터기반시스템)시스템 토폴로지 다이어그램(UR E27, 항목 3.1.2)의 승인된 버전 참조 정보를 포함합니다. 하나의 보안 존 내에서 시스템 간의 네트워크 통신 흐름을 도식화합니다. 서로 다른 보안 존 간의 시스템 간 네트워크 통신(conduits)을 도식화합니다. 보안 존 내 시스템과 신뢰되지 않은 네트워크(untrusted networks) 간의 통신 흐름(conduits)을 도식화합니다. **[UR E26 4.2.1.4.1 보안구역 네트워크 분리/설계]** SOLAS II-1 규칙 31에 따라 필요한 로컬 백업 통제를 위한 모든 CBS(컴퓨터기반시스템)는 기본 통제 시스템과 독립적이어야 합니다. 이는 효과적인 로컬 운영을 위해 필요한 인간-기계 인터페이스(HMI)를 포함합니다. **[UR E26 4.4.2.1 요구사항]** 로컬 제어 및 모니터링을 위한 CBS(컴퓨터기반시스템)는 독립적으로 구성되어야 하며, 의도된 운영을 위해 다른 CBS(컴퓨터기반시스템)와의 통신에 의존해서는 안 됩니다. **[UR E26 4.4.2.3 세부 요구사항]**	
비고			

통제항목	B.1.3 사이버 자산 변경이력	Optimized
레퍼런스 상세	IACS UR E26	선박 자산 목록에는, 탑재되어 있는 경우, 1.3.2(Systems in scope)절에 명시된 CBS(컴퓨터기반시스템)가 최소한 포함되어야 합니다. 해당 목록은 선박의 전체 수명 기간 동안 최신 상태로 유지되어야 합니다. 새로운 취약점을 유발하거나 기능적 종속성 또는 시스템 간 연결을 변경할 수 있는 소프트웨어 및 하드웨어 변경 사항은 자산 목록에 기록되어야 합니다. 만약 자산 목록에 기밀 정보(예: IP 주소, 프로토콜, 포트 번호 등)가 포함되는 경우, 해당 정보에 대한 접근은 권한이 부여된 사람에게만 제한되도록 특별한 조치를 취해야 합니다. **[UR E26 4.1.1.3 세부 요구사항]** 본 UR의 적용 범위에 해당하는 모든 하드웨어 장치에 대해, 선박 자산 목록에는 UR E27의 3.1.1(CBS asset inventory)절에 명시된 정보를 최소한 포함해야 합니다. 또한, 자산 목록에는 해당 CBS(컴퓨터기반시스템)와 관련된 시스템 분류 및 보안 영역(Security Zone)을 명시할 수 있습니다. **[UR E26 4.1.1.3.1 하드웨어]** 본 UR의 적용 범위에 해당하는 모든 소프트웨어(예: 응용 프로그램, 운영체제, 펌웨어 등)에 대해, 선박 자산 목록에는 UR E27의 3.1.1절(CBS asset inventory)에 명시된 정보를 최소한 포함해야 합니다. **[UR E26 4.1.1.3.2 소프트웨어]** 운영 단계에서의 일반적인 검사 요구사항에 대해서는 5.3(During the operational life of the ship)절을 참조합니다. 선주는 선박 사이버보안 및 회복력 프로그램(Ship cyber security and resilience program) 내에서, 본 UR의 적용 범위에 해당하는 CBS(컴퓨터기반시스템)에 대한 변경관리(MoC: Management of Change) 절차를 설명해야 하며, 다음 요구사항을 최소한 포함해야 합니다: • 변경관리 (5.3(During the operational life of the ship)절) • 하드웨어 및 소프트웨어 변경사항 (4.1.1.3(Requirement details)절) 또한 선주는 선박 사이버보안 및 회복력 프로그램 내에서 소프트웨어 업데이트 관리에 대해서도 설명해야 하며, 다음 요구사항을 최소한 포함해야 합니다: • 취약점 및 사이버 리스크 (4.1.1.2(Rationale)절 및 4.1.1.3(Requirement details)절) • 보안 패치 적용 (4.2.6.3.2(Additional requirements for remote maintenance)절) 최초 연차 검사 (First annual survey) 선주는 선박 사이버보안 및 회복력 프로그램이 이행되었음을 입증하는 문서화된 증빙자료 또는 기록을 선급협회에 제출해야 하며, 다음 사항을 포함해야 합니다: • 승인된 변경관리 절차가 준수되었음 • CBS(컴퓨터기반시스템) 내의 소프트웨어에 대해 알려진 취약점 및 기능적 종속성이 고려되었음

통제항목	B.1.3 사이버 자산 변경이력	Optimized
	• 선박 자산 목록이 최신 상태로 유지되었음 **[UR E26 4.1.1.4.4 운영 단계]**	
비고		

B.3 네트워크 접근 통제

통제항목	B.3.2 네트워크 접근 통제	Advanced
레퍼런스 상세	IACS UR E26	보안 구역은 4.2.1(Security Zones and Network Segmentation)절에 명시된 바와 같이 방화벽 또는 이에 상응하는 수단으로 보호되어야 합니다. 네트워크는 과도한 데이터 흐름률 또는 네트워크 자원의 서비스 품질을 저해할 수 있는 기타 사건 발생으로부터도 보호되어야 합니다. 본 UR의 적용 범위에 있는 CBS(컴퓨터기반시스템)는 최소 기능 원칙(Principle of Least Functionality)에 따라 구현되어야 합니다. 즉, 필수 기능만을 제공하도록 구성되어야 하며, 불필요한 기능, 포트, 프로토콜 및 서비스의 사용은 비활성화하거나 제한하거나 금지하여야 합니다. **[UR E26 4.2.2.1 요구사항]** 네트워크 보호는 네트워크의 무결성, 기밀성, 가용성을 보호하기 위해 설계된 다양한 기술, 규칙 및 구성요소를 포함합니다. 위협 환경은 지속적으로 변화하고 있으며, 공격자는 항상 취약점을 찾아내고 이를 악용하려고 시도합니다. **[UR E26 4.2.2.2 타당성]** 네트워크 보호를 다룰 때 고려해야 할 계층은 매우 많습니다. 공격은 네트워크 계층 모델의 어느 계층에서든 발생할 수 있으므로, 네트워크 하드웨어, 소프트웨어 및 정책은 각 계층을 대응할 수 있도록 설계되어야 합니다. **[UR E26 4.2.2.2 타당성]** 네트워크 설계에는 목표로 하는 데이터 흐름률을 달성할 수 있는 수단이 포함되어야 하며, 서비스 거부(DoS) 및 네트워크 폭주 또는 과도한 트래픽 발생 리스크를 최소화할 수 있어야 합니다. 데이터 흐름률의 추정치는 최소한 네트워크 용량, 데이터 사용 목적, 데이터 형식에 대한 요구사항을 충족해야 합니다. **[UR E26 4.2.2.3 세부 요구사항]** 본 UR의 적용 범위에 해당하는 CBS(컴퓨터기반시스템) 및 네트워크는 시스템 자체와의 통신, 상호작용, 정보 처리, 시스템이 포함하는 정보에 대한 접근, 시스템 구성요소 또는 기능 제어에 대한 권한을 제한하기 위해 물리적 및 논리적/디지털 조치를 제공하여야 합니다. 이러한 조치는 최소 권한 원칙(least privilege principle)에 따라 CBS(컴퓨터기반시스템)에 접근할 수 있는 권한을 부여받은 인원의 접근 능력을 방해하지 않도록 구성되어야 합니다. **[UR E26 4.2.4.1 요구사항]** 본 UR의 적용 범위에 해당하는 CBS(컴퓨터기반시스템) 및 네트워크와 이들에 저장된 모든 정보에 대한 접근은, 해당 정보에 대한 접근이 업무상 필요하거나 기능적으로 정당한 경우에 한해 권한 있는 인원에게만 허용되어야 합니다. **[UR E26 4.2.4.3 세부 요구사항]** 본 UR의 적용 범위에 포함된 무선 통신 네트워크는 다음 사항들을 보장할 수 있도록 설계되고, 구현되며, 유지되어야 합니다: • 사이버 사고가 다른 제어 시스템으로 전파되지 않도록 합니다. • 오직 인가된 사용자만이 무선 네트워크에 접근할 수 있도록 합니다.

통제항목	B.3.2 네트워크 접근 통제	Advanced

- 오직 인가된 프로세스 및 장치만이 무선 네트워크에서 통신할 수 있도록 합니다.
- 무선 네트워크를 통해 전송되는 정보는 조작되거나 유출될 수 없도록 합니다.

[UR E26 4.2.5.1 요구사항]

암호화 알고리즘과 키 길이 등 산업 표준 및 모범 사례에 부합하는 암호화 메커니즘을 적용하여, 무선 네트워크를 통해 전송되는 정보의 무결성과 기밀성이 보장되도록 해야 합니다.

[UR E26 4.2.5.3 세부 요구사항]

무선 공유기 및 네트워크 내의 다른 장비들은 네트워크 접근이 통제 가능하도록 설치 및 구성되어야 합니다.

[UR E26 4.2.5.3 세부 요구사항]

무선 통신을 사용하는 네트워크 장비 또는 시스템은 해당 통신에 참여하는 모든 사용자(사람, 소프트웨어 프로세스 또는 장치)를 식별하고 인증할 수 있는 기능을 제공해야 합니다.

[UR E26 4.2.5.3 세부 요구사항]

이 UR의 범위에 해당하는 CBS(컴퓨터기반시스템)는 신뢰되지 않은 네트워크로부터의 무단 접근 및 기타 사이버 위협으로부터 보호되어야 합니다.

[UR E26 4.2.6.1 요구사항]

선상 CBS(컴퓨터기반시스템)는 점점 더 디지털화되고 인터넷에 연결되어 다양한 합법적 기능을 수행하고 있습니다. 디지털 시스템을 사용하여 선상 CBS(컴퓨터기반시스템)를 모니터링하고 제어하는 것은 사이버 사고에 취약하게 만듭니다. 공격자는 인터넷 연결을 통해 선상 CBS(컴퓨터기반시스템)에 접근을 시도할 수 있으며, CBS(컴퓨터기반시스템) 운영에 영향을 미치는 변경 작업을 수행하거나 CBS(컴퓨터기반시스템)를 완전히 제어하거나 선박의 CBS(컴퓨터기반시스템)에서 정보를 다운로드하려고 시도할 수 있습니다. 또한, 더 이상 지원되지 않거나 오래된 운영 체제에 의존하는 기존 IT 및 OT 시스템을 사용하는 것은 사이버 복원력에 영향을 미치므로, 원격으로 시스템에 접근할 수 있는 경우 충분한 수준의 사이버 복원력을 유지할 수 있도록 선상 관련 하드웨어 및 소프트웨어 설치에 특별한 주의를 기울여야 합니다. 또한 모든 사이버 사고가 고의적인 공격으로 인한 것은 아니라는 점을 명심해야 합니다.

[UR E26 4.2.6.2 근거]

선박 내 IT 및 OT 시스템에 대한 원격 접근 통제에 관한 사용자 설명서를 제공해야 합니다. 명확한 지침에는 기능별 역할 및 권한이 식별되어야 합니다.

[UR E26 4.2.6.3 세부 요구사항]

본 UR의 적용 범위에 해당하는 CBS(컴퓨터기반시스템)에 대해서는, 신뢰되지 않은 네트워크에 IP 주소가 노출되어서는 안 됩니다.

[UR E26 4.2.6.3 세부 요구사항]

신뢰할 수 없는 네트워크와의 통신에는 엔드포인트 인증, 무결성 및 인증 보호, 그리고 네트워크 또는 전송 계층의 암호화를 갖춘 안전한 연결(예: 터널)이 필요합니다. 읽기 권한이 필요한 정보의 경우 기밀성이 보장되어야 합니다.

통제항목	B.3.2 네트워크 접근 통제	Advanced
	[UR E26 4.2.6.3 세부 요구사항] 이 UR의 적용 범위에 해당하는 CBS(컴퓨터기반시스템)는 다음 사항을 충족해야 합니다: • 선박 내 연결 엔드포인트에서 연결을 종료할 수 있는 기능을 갖추어야 합니다. • 원격 접속은 선박 내 해당 책임자가 명시적으로 수락하기 전까지는 가능하지 않아야 합니다. - OT 시스템의 안전한 기능이나 OT 시스템에서 사용하는 데이터의 무결성 및 가용성을 저해하지 않도록 원격 세션 중 중단을 관리할 수 있어야 합니다. - 모든 원격 접속 이벤트를 기록하고 사이버 사고 감지 후 등 원격 연결을 오프라인으로 검토하기에 충분한 기간 동안 보관하는 로깅 기능을 제공해야 합니다. **[UR E26 4.2.6.3.1 설계]** 원격 접속이 유지보수 목적으로 사용될 경우, 4.2.6.3.1(Design)의 요구사항 외에도 다음 요구사항을 준수해야 합니다: • 육상 측과의 연결 및 통합 방식을 보여주는 문서가 제공되어야 합니다. • 보안 패치 및 소프트웨어 업데이트는 설치 전에 반드시 테스트 및 평가되어야 하며, • 사이버 사고나 허용 불가능한 부작용이 발생하지 않도록 해야 합니다. • 원격 업데이트를 수행하기 전에, 상기 내용을 확인하는 소프트웨어 공급업체의 확인 보고서가 확보되어야 합니다. • 공급업체는 보안 업데이트 계획을 수립하고, 선주에게 이를 제공해야 합니다. (UR E27의 섹션 5.2(IEC 62443-4-1/SUM-2), 5.3(IEC 62443-4-1/SUM-3), 5.4(IEC 62443-4-1/SUM-4) 참조) • 원격 유지보수 중 언제든지, 권한을 부여받은 인원은 활동을 중단하거나 이전의 안정적인 CBS(컴퓨터기반시스템) 구성으로 되돌릴 수 있어야 합니다. • 신뢰되지 않은 네트워크로부터 CBS(컴퓨터기반시스템)에 접근하는 모든 사람은 다단계 인증을 거쳐야 합니다. • 구성 가능한 횟수만큼 원격 접근 시도가 실패한 경우, 이후 시도는 미리 정의된 시간 동안 차단되어야 합니다. • 원격 유지보수 중 통신이 일정 시간 이상 중단될 경우, 연결은 자동 종료되도록 설정되어야 합니다. **[UR E26 4.2.6.3.2 원격 유지보수를 위한 추가 요구사항]**	
	BIMCO	네트워크 포트, 프로토콜 및 서비스에 대한 제한 및 제어 네트워크 시스템 접근 목록은 회사의 보안 정책을 구현하는 데 사용될 수 있으며, 이를 통해 해당 네트워크 또는 서브넷의 제어 정책에 따라 적절한 트래픽만 제어된 네트워크 또는 서브넷을 통해 허용되도록 할 수 있습니다. 가장 흔한 공격은 일반적으로 웹 서버, 메일 서버, 파일 및 프린터 서버, 워크스테이션 등과 같은 호스트 시스템을 대상으로 발생합니다. 따라서 조직은 각 시스템에서 유효한 비즈니스 요구 사항이 있는 포트, 프로토콜 및 서비스만 열려 있거나 실행되도록 해야 합니다. 또한 관리형 라우터만 사용하고, 사용하지 않는 포트, 프로토콜 및 서비스를 비활성화하여 시스템이나 데이터에 대한 무단 접근을 방지하는 것이

통제항목	B.3.2 네트워크 접근 통제	Advanced

좋습니다.

[BIMCO 7.2 기술적 보호 조치]

무선 접근 통제

선박 내 네트워크에 대한 무선 접근은 승인된 장치로 제한되어야 하며, 강력한 암호화 키를 사용하여 보안이 유지되어야 합니다. 이 암호화 키는 정기적으로 변경하는 것이 좋습니다. 다음과 같은 방법을 통해 무선 접속을 통제할 수 있습니다:

- 비대칭 암호화를 사용하고 적절한 무선 공유기(예: 관리 네트워크와 분리된 게스트 네트워크)를 통해 네트워크를 분리하는 엔터프라이즈 인증 시스템 사용
- 무선 침입 방지 시스템(WIPS)과 같이 승인되지 않은 무선 공유기나 불법 장치를 차단할 수 있는 시스템 도입. 네트워크 접근 제어(NAC)를 사용하여 장치(기업용 및 개인용)를 프로파일링하고 무선 네트워크 접근을 제어하는 것은 접근 관리에 효과적입니다.
- 무선 접근 장치와 네트워크 간의 물리적 연결(예: 네트워크 플러그, 보안 네트워크 랙 등)을 보호하여 비인가 장치가 물리적으로 접근하지 못하도록 합니다.

[BIMCO 7.2 기술적 보호 조치]

위성 및 무선 통신

무선 및 위성 연결의 사이버보안은 서비스 제공업체와 협력하여 고려해야 합니다. 이와 관련하여, 선상 네트워크 보호 요건을 수립할 때 위성 링크의 사양을 고려해야 합니다.

위성 단말기에는 일반적으로 선박 네트워크에 연결하기 위한 보호되지 않은 LAN 포트가 있어 위협에 따라 다양한 보호 옵션이 제공됩니다. 암호화되지 않은 기기 통신을 사용할 경우 도청으로부터 보호하는 것은 일반적으로 VPN(가상사설망) 연결이나 암호화된 프로토콜을 통해 이루어집니다. 해킹, 침투 및 기타 유형의 공격으로부터 보호하는 것은 서비스 제공업체와의 보안 계약, 회사 소유의 해외 보안 서버를 통한 연결, 또는 선내 방화벽과 같은 다른 수단을 통해서도 가능합니다.

사이버보안의 중요한 측면 중 하나는 위성 단말기를 보이지 않게 하는 것입니다. 이는 단말기 설정 메뉴에서 "원격 관리 페이지" 및 "포트 포워딩"과 같은 기능을 비활성화하여 구현할 수 있습니다. 비활성화는 일반적으로 단말기 설정 메뉴에서 수행할 수 있습니다.

선박의 항해 및 제어 시스템을 육상 서비스 제공업체에 연결할 때는 불법적인 연결이 선내 시스템에 접근하는 것을 방지하는 방법을 고려해야 합니다. IP 주소는 공개되어 있지 않아야 하며, 인터넷에서 선박으로 직접 라우팅 가능한(즉, 공개) 주소로 설정해서는 안 됩니다. 인터넷 연결은 라우팅 및 접근 제어를 위해 육상 네트워크와 방화벽을 거쳐야 합니다. 두 번째 고려 사항은 선박 네트워크, 제어 네트워크 또는 제어 네트워크와 연결된 네트워크(즉, 역방향 터널 연결)에서 발생하는 아웃바운드 연결을 면밀히 모니터링하는 것입니다.

접속 상호 연결은 유통 파트너의 책임입니다. 인터넷 접속 지점에서 최종 목적지인 선상("라스트 마일")까지의 사용자 트래픽 최종 라우팅은 선주가 담당합니다. 사용자 트래픽은 통신 장비를 통해 선상에서 전송됩니다. 이 트래픽의 접속 지점에는 데이터

통제항목	B.3.2 네트워크 접근 통제	Advanced

	보안, 방화벽, 그리고 전용 "라스트 마일" 연결이 필요합니다. VPN(가상사설망)을 사용할 경우, 데이터 트래픽은 허용되는 가장 높은 국제 표준으로 암호화되어야 합니다. 또한, 네트워크에 연결된 서버와 컴퓨터(육상 및 선상) 앞에 방화벽을 구축해야 합니다. 유통 파트너는 특정 트래픽에 가장 적합한 라우팅 및 연결 유형에 대해 조언해야 합니다. 육상 트래픽 필터링(검사/차단) 또한 선주와 유통 파트너 간의 문제입니다. 육상 트래픽 필터링과 선박 내 방화벽/보안 검사/차단 게이트웨이는 모두 필요하며, 충분한 수준의 보호를 달성하기 위해 서로 보완적인 역할을 합니다. 위성 통신 단말기 및 기타 통신 장비 제조업체는 네트워크를 통해 접근 가능한 보안 제어 소프트웨어가 포함된 관리 인터페이스를 제공할 수 있습니다. 이는 주로 웹 기반 사용자 인터페이스 형태로 제공됩니다. 선박 설비의 보안을 평가할 때 이러한 인터페이스의 보호를 고려해야 합니다. 관리 인터페이스 보호의 예로는 웹 기반 인터페이스든 명령줄 인터페이스든 허용 목록에 추가하여 해당 인터페이스에 접근할 수 있는 네트워크를 제한하거나, 인터페이스를 완전히 비활성화하는 것이 있습니다. 초기 구성 시에만 사용되는 불필요한 인터페이스가 있습니다. 다른 시스템과 마찬가지로, 비밀번호는 적절하게 관리해야 합니다. 예를 들어 범죄자에게 잘 알려진 기본 비밀번호는 변경해야 합니다. MFA(다중인증)을 활용하여 보안을 더욱 강화할 수도 있습니다 **[BIMCO 7.2 기술적 보호 조치]** 방문자 컴퓨터 접근 관계당국, 기술자, 에이전트, 항만 및 터미널 직원, 선주 대표와 같은 방문자는 선상에서의 컴퓨터 접근이 제한되어야 합니다. 민감한 컴퓨터 접근은 금지되어야 합니다. 만약 방문자가 네트워크 접근이 필요하고 허용된 경우, 권한 수준이 제한되고 감독하에 수행되어야 합니다. 특정 네트워크 접근은 승인 및 회사/선박 운영자의 절차에 따라 조정되어야 합니다. 방문자가 컴퓨터와 프린터에 접속해야 하는 경우, 모든 통제된 네트워크에서 분리된 별도의 컴퓨터를 사용해야 합니다. 가능한 경우 문서 인쇄를 위해 WiFi Direct 또는 Wireless Direct 지원 프린터를 제공할 수 있습니다. WiFi Direct 또는 Wireless Direct를 사용하면 프린터가 액세스 포인트 역할을 하여 모바일 기기나 PC가 WiFi 공유기/라우터 없이 직접 연결됩니다. 무단 접근을 방지하기 위해 물리적으로 접근 가능한 다른 모든 컴퓨터와 네트워크 포트에는 이동식 미디어 차단기를 사용해야 합니다. **[BIMCO 7.3 절차적 보호 조치]**
DCSA	데이터 보안은 의도적 또는 우발적인 파괴, 수정 또는 공개로부터 데이터를 보호하는 일련의 표준 및 기술입니다. 데이터 보안은 관리적 통제, 물리적 보안, 논리적 통제, 조직 표준 및 무단 또는 악의적인 사용자 또는 프로세스의 접근을 제한하는 기타 보호 기술을 포함한 다양한 기법과 기술을 통해 적용될 수 있습니다. **[DCSA 2.3.2 설명]** 왜 데이터 보안이 중요한가?

통제항목	B.3.2 네트워크 접근 통제	Advanced
		• 오늘날 모든 비즈니스는 데이터를 다룹니다. 대량의 개인 및 금융 데이터를 처리하는 대형 은행부터, 고객의 연락처 정보를 휴대폰에 저장하는 소규모 자영업자에 이르기까지, 모든 규모의 기업에서 데이터는 핵심입니다. 정보 흐름 통제(Information flow control)는 데이터 보안 리스크가 있는 시스템에 구현되어야 합니다. 흐름 통제의 제한 사항에는 다음이 포함됩니다: • 수출 통제 정보가 인터넷을 통해 명시되지 않은 상태로 전송되지 않도록 함 • 조직 내부에서 온 것처럼 보이는 외부 트래픽 차단 • 내부 웹 프록시 서버가 아닌 인터넷에 대한 웹 요청 제한 • 데이터 구조 및 내용에 기반하여 조직 간 정보 전송 제한 **[DCSA 2.3.3 구현]** 또한, 선박 내·외부(육상) 간의 통신 인터페이스 역시 주요 리스크 요소로 작용할 수 있으므로, 외부 통신 연결이 가능한 자산에 대한 보호 조치가 필요합니다. **[DCSA 2.6.2 설명]** 통신 및 제어에 대한 집중 기술적 차원에서는 다음과 같은 보호 조치를 고려하여야 합니다: • 특정 장비 간의 외부 연결 및 인터페이스 제한 • 무선 접속 비활성화 • 권한 명령의 원격 실행 차단 • 엔드포인트의 지속적인 모니터링을 통한 공격 지표 탐지 및 대응 • 정교한 데이터 유출 방지 및 보호 솔루션을 활용하여 민감한 정보가 전송되는 것을 식별 및 사전 차단 • 업무 연속성을 위한 대체 통신 수단 구축 **[DCSA 2.6.2 설명]**
비고		

B.4 기기 및 출입 통제

통제항목	B.4.2 인원 출입 통제		Advanced
레퍼런스 상세	IACS UR E26	관계당국, 기술자, 대리점, 항만 및 터미널 관계자, 선주 대표 등 방문자는 선박에 탑승 중인 CBS(컴퓨터기반시스템)에 대한 접근이 제한되어야 하며, 예를 들어 감독하에 접근을 허용하는 방식으로 통제되어야 합니다. **[UR E26 4.2.4.3.2 방문자에 대한 물리적 접근 통제]** 모바일 및 휴대용 장치는 권한이 있는 인원만 사용할 수 있어야 합니다. CBS(컴퓨터기반시스템)에 연결할 수 있는 장치는 이러한 권한이 있는 장치에 한정되어야 하며, CBS(컴퓨터기반시스템) 내 악성코드 유입 리스크를 고려하여 선주의 모바일 및 휴대용 장치 사용 정책에 따라야 합니다. **[UR E26 4.2.7.3 세부 요구사항]**	
	BIMCO	제3자가 선박을 방문하여 선박 내 하나 이상의 컴퓨터에 연결해야 하는 경우, 이는 선박이 육상과 연결되는 결과를 초래할 수 있습니다. 기술자, 벤더, 항만 및 기타 관계자, 터미널 직원, 대리점, 도선사, 기타 기술자 등이 선박에 탑승하여 노트북이나 태블릿 등 장비를 연결하는 일이 흔하게 발생합니다. 일부 기술자는 이동식 저장장치를 사용하여 컴퓨터를 업데이트하거나 데이터를 다운로드하고 기타 작업을 수행해야 할 수도 있습니다. 또한, 세관 직원이나 항만국 통제관이 선박에 승선하여, 알 수 없는 이동식 저장장치를 삽입한 후 공식 문서를 출력하고자 컴퓨터 사용을 요청한 사례도 보고된 바 있습니다. **[BIMCO 3.5 선박 방문]** 물리적 보안 물리적 보안은 때때로 가장 간단하고 저렴하며 가장 명확한 사이버 방어 형태입니다. 이는 사이버 위험 관리의 핵심 요소이며, 효과적인 심층 방어 전략은 물리적 통제 조치를 우회할 수 없도록 보장하는 것을 목표로 해야 합니다. 민감한 운영기술(OT) 또는 정보기술(IT) 제어 구성 요소가 있는 구역은 안전하게 잠금되어야 합니다. 보안 및 안전에 중요한 장비와 케이블은 무단 접근으로부터 보호되어야 하며, 민감한 사용자 장비(예: 선교 시스템의 노출된 USB 포트)에 대한 물리적 접근은 보안되어야 합니다. 선박 보안 계획에서 이러한 구역은 ISPS 코드 A부 9.4.1절에서 요구하는 제한 구역으로 정의되며, 동 코드 B부의 지침을 참고해야 합니다. 이는 특히 선교와 같이 항내에서 일반적으로 무인으로 운영되는 장소와 관련이 있습니다. **[BIMCO 7.2 기술적 보호 조치]**	
비고			

C. 사이버 리스크 관리

C.1 사이버 취약점 진단

통제항목	C.1.3 보안설정 점검 및 모의해킹	Advanced
레퍼런스 상세	BIMCO	비표적 공격은 인터넷상에 존재하는 도구나 기술을 활용하여, 기업 또는 선박 내부에 존재할 수 있는 일반적인 취약점을 탐지, 발견, 악용하는 방식으로 발생할 가능성이 높습니다. 이러한 공격에 사용될 수 있는 도구 및 기술 예시는 다음과 같습니다: • 악성코드 (Malware): 소유자의 인지 없이 컴퓨터에 접근하거나 손상을 입히도록 설계된 악성 소프트웨어. 트로이목마, 랜섬웨어, 스파이웨어, 바이러스, 웜 등이 있으며, 시스템에 침투해 데이터를 암호화하고 몸값을 요구하기도 함. 보안 업데이트가 되지 않은 비즈니스 소프트웨어의 취약점을 악용하는 경우가 많음. "Exploit"은 일반적으로 취약한 소프트웨어나 코드, 또는 하드웨어 문제를 조작하기 위한 소프트웨어 또는 코드의 사용을 의미하며, 예: 코드 버그, 시스템 취약점, 설계 결함 등. 이러한 취약점은 원격 또는 로컬에서 실행될 수 있고, 악성 링크나 이메일 첨부파일을 통해 실행되기도 함. • 워터홀링 (Water holing): 가짜 웹사이트를 만들거나 진짜 웹사이트를 손상시켜, 방문자를 악용하는 방법. • 스캐닝 (Scanning): 인터넷의 광범위한 영역을 무작위로 검색하여 악용 가능한 취약점을 탐지. • 타이포스쿼팅 (Typosquatting): URL 탈취 또는 유사 도메인 활용. 사용자가 웹 주소를 오타로 입력했을 때 악성 웹사이트로 유도하는 수법. **[BIMCO 2.2 사이버 위협의 유형]** 표적 공격은 보다 정교하며, 특정 기업이나 선박을 대상으로 고안된 기술이나 도구를 사용합니다. 예시는 다음과 같습니다: • 사회공학 (Social engineering): 사이버 공격자가 내부 관계자를 조작하여 보안 절차를 우회하도록 유도하는 비기술적 기법. 보통 소셜미디어를 통해 접근함. • 무차별 대입 (Brute force): 가능한 모든 암호 조합을 시도하여 시스템에 침투하는 방식. • 자격 증명 채우기 (Credential stuffing): 이미 유출된 사용자 ID/비밀번호 또는 흔히 사용되는 조합을 활용해 시스템 접근을 시도. • 서비스 거부 공격 (DoS): 대량의 데이터를 네트워크에 전송해 정상적인 접근을 방해함. DDoS는 여러 시스템을 동시에 동원함. • 피싱 (Phishing): 많은 사용자에게 이메일을 보내 민감한 정보(예: 암호, 계좌 정보)를 탈취하거나 악성 첨부파일 또는 링크를 클릭하도록 유도. • 스피어 피싱 (Spear-phishing): 특정 대상에 대해 맞춤형으로 설계된 피싱 공격. 보통 기존의 이메일 양식을 위조하여 친숙한 사람으로 위장함. • 공급망 침해 (Subverting the supply chain): 선박이나 회사에 납품되는 장비, 소프트웨어, 지원 서비스 등을 손상시켜 침투하는 방식. **[BIMCO 2.2 사이버 위협의 유형]** 다음은 기존 선박 및 일부 신조선에서 발견될 수 있는 일반적인 사이버 취약점입니다: • 구식이거나 지원이 종료된 운영체제 [BIMCO 3.1 공개적인 취약점]

통제항목	C.1.3 보안설정 점검 및 모의해킹	Advanced
		• 보안 패치가 적용되지 않은 시스템 소프트웨어 [BIMCO 3.1 공개적인 취약점] • 오래되었거나 누락된 백신 소프트웨어 및 악성코드로부터의 보호 미비 [BIMCO 3.1 공개적인 취약점] • 비효율적인 네트워크 관리, 기본 관리자 계정과 비밀번호 사용 등 보안 설정 및 모범 사례 미준수 [BIMCO 3.1 공개적인 취약점] • 경계 보호 조치와 네트워크 분리가 부족한 선박 내 컴퓨터 네트워크 [BIMCO 3.1 공개적인 취약점] • 육상 시스템과 항상 연결된 중요 안전 장비 또는 시스템 [BIMCO 3.1 공개적인 취약점] • 계약업체 및 서비스 제공자를 포함한 제3자에 대한 사이버 자산 및 네트워크 접근 통제 미흡 [BIMCO 3.1 공개적인 취약점] • 사이버 리스크를 관리하기 위한 직원의 교육 부족 또는 기술 미비 [BIMCO 3.1 공개적인 취약점] • 부재하거나 불충분하거나 검증되지 않은 비상 대응 계획 및 절차 **[BIMCO 3.1 공개적인 취약점]**
비고		

D. 사이버 사고 대응

D.1 사이버보안 모니터링

통제항목	D.1.1 사이버 위협 모니터링	Advanced
레퍼런스 상세		
	IMO	인터넷에서 악용 가능한 서비스를 제한하고, 하드웨어 및 소프트웨어 승인 프로세스를 구축하고, 침입 탐지 및 사고 대응을 위한 로그를 수집하고 안전하게 저장하며, OT 장치 네트워크를 IT 네트워크와 분리합니다. 네트워크 및 정보 시스템 확보, 개발 및 유지 관리의 보안을 보장하고, 취약점 처리 및 공개를 포함합니다. **[IMO 3.5.3.3 보호(protect)]** 사이버 사건을 적시에 탐지하기 위한 활동을 개발·이행·실행합니다. CBS(컴퓨터기반시스템)에서 의도치 않은 활동을 탐지하고 사이버 사고를 적시에 식별하기 위한 적절한 조치를 구현합니다. **[IMO 3.5.4 탐지(Detect)]** 관련 위협, 위협행위자의 전술·기술·절차 목록을 유지 관리하고, 해당 위협에 대해 시스템을 적극적으로 모니터링합니다. **[IMO 3.5.4.1 탐지(Detect)]**
	IACS UR E26	탐지 기능 요소(Detect functional element)에 대한 요구사항은, CBS(컴퓨터기반시스템) 및 선박 내 네트워크에서 이상 행위를 식별하고 사이버 사건을 인식할 수 있도록 하는 적절한 수단의 개발 및 구현을 목적으로 합니다. **[UR E26 4.3 탐지]** 침입 탐지 시스템(IDS)은 다음의 조건을 만족하는 경우 구현할 수 있습니다: • IDS는 해당 CBS(컴퓨터기반시스템) 공급업체에 의해 적합성이 입증되어야 합니다. • IDS는 수동 모드로 동작하며, CBS(컴퓨터기반시스템)의 성능에 영향을 미칠 수 있는 보호 기능을 활성화해서는 안 됩니다. • 관련 인원은 IDS 사용을 위해 교육을 받고 자격을 갖추어야 합니다. **[UR E26 4.3.1.3 세부 요구사항]**
	BIMCO	침입 및 감염 탐지는 사이버 위험 관리의 핵심입니다. 시스템, 애플리케이션, 계정 및 네트워크 운영 기준과 사용자 및 시스템의 예상 데이터 흐름을 설정하고 관리하여 사이버 사고 경보 임계값을 설정해야 합니다. 이를 위해서는 선박 내 여러 로그 소스를 수집하고 정규화해야 합니다. 핵심은 탐지 역할과 책임을 정의하여 책임 소재를 명확히 하는 것입니다. 전담 보안 정보 및 이벤트 관리(SIEM) 시스템을 고려해야 합니다. SIEM 시스템은 가능한 모든 소스에서 로그를 수집하고 분석하며, 이를 통해 탐지되지 않을 수 있는 의심스러운 활동을 탐지할 수 있습니다. SIEM 시스템을 효과적으로 구축하는 것은 복잡한 작업이며, 일부 사이버보안 제공업체는 이를 서비스로 제공합니다. 또한 회사는 선박 통신 솔루션의 일부로 네트워크에 침입 탐지 시스템(IDS) 또는 침입 방지 시스템(IPS)을 통합하기로 선택할 수 있습니다. 또는 방화벽의 일부로 사용됩니다. 주요 기능 중 일부는 위협/악의적인 활동 및 코드를 식별하고, 로깅, 보고 및 활동 차단을 시도하는 것입니다. IDS 및 IPS에 대한 자세한 내용은 본 지침의 부록 3에서 확인할 수 있습니다. 관련 선상 또는

통제항목	D.1.1 사이버 위협 모니터링	Advanced
		육상 인력은 경보와 그 의미를 이해하고 합의된 대응 및 복구 활동을 수행할 수 있어야 합니다. 감지된 사고에 대한 정보는 이러한 유형의 경보에 대한 조치를 담당하는 개인 또는 서비스 제공업체에 전달해야 합니다. **[BIMCO 8.1 탐지, 차단 및 경고]**
	DCSA	조직은 지속적인 모니터링 전략을 개발하고, 보안 이벤트를 지속적으로 모니터링, 평가 및 보고하는 프로그램을 구현합니다. 이는 사후 검토, 이벤트 로그 리뷰, 보안 평가, 익명 보고 등의 활동을 통해 이루어질 수 있습니다. **[DCSA 2.4.3 구현]** 보안 및 지속적 모니터링은 여러 방식으로 수행될 수 있습니다. 예를 들어, 핵심 자산 및 네트워크 장치에서 생성되는 이벤트 로그를 모니터링하고, 이상 징후를 탐지하기 위해 보안 정보 및 이벤트 관리(SIEM) 플랫폼을 사용하는 것입니다. 또 다른 방법은 정기적으로 시스템 설정과 자산 구성을 검토하여 악의적인 변경이나 사고로 인한 변화가 없는지 확인하는 것입니다. **[DCSA 3.2.2 설명]** 조직의 IT 부서는 사이버 사고 발생 시 보안 담당자에게 경고를 줄 수 있는 특정 위협 탐지 시스템 또는 선박 보안 제품군 내의 추가 기능에 투자할 수 있습니다. 여기에는 네트워크 및 호스트 침입 사고를 탐지하고 경고하기 위한 침입 탐지 시스템(IDS)의 사용 또는 보안 정보 이벤트 관리(SIEM) 솔루션의 도입도 포함될 수 있습니다. 이 시스템은 이벤트 로그를 수집하고 상관 분석을 수행하며, 악의적인 활동이 탐지되었을 때 경보를 발생시킵니다. **[DCSA 3.2.3 구현]** 침입 탐지 시스템(IDS) 또는 침입 방지 시스템(IPS)과 같은 위협 탐지 시스템은 자산 등록부에 포함되어야 합니다. **[DCSA 3.2.3 구현]** 조직은 다양한 도구 간 상호운용성을 촉진하고 취약점 관리 프로세스의 일부를 자동화할 수 있는 취약점 스캐닝 도구 및 기술을 사용해야 합니다. 조직은 모든 정보 시스템 구성요소에 대해 필요한 취약점 스캐닝 주기를 결정하고, 네트워크 프린터, 스캐너, 복사기와 같이 취약점의 잠재적 원천이 될 수 있는 구성요소도 간과하지 않아야 합니다. **[DCSA 3.2.3 구현]** 위협 탐지 시스템에 의해 커버될 수도 있고 아닐 수도 있는, 사이버 사고 탐지의 다른 방법은 다음과 같습니다: • 이상한 비밀번호 활동에 주의: 예를 들어 부서 계정이나 승무원 계정이 잠기고 비밀번호 변경 요청이 들어오는 경우. 특히 사용자가 본인이 아닌 경우 이러한 요청이 의심됩니다. • 의심스러운 팝업 및 기타 애드웨어의 갑작스러운 등장에 주의: 특히 인터넷 브라우징 중에 나타날 경우, 이는 안전하지 않은 브라우징 활동을 나타낼 수 있습니다. • 시스템, 네트워크, 기타 서비스의 느려짐 또는 무반응 현상을 조사: 일반적인 속도보다 느려졌을 경우, 바이러스 검사 등 추가 조사를 실시하고 IT 부서에

통제항목	D.1.1 사이버 위협 모니터링	Advanced

보고되어야 합니다.

- 침해 사실이 확인되었을 때 대응: 예를 들어, 컴퓨터가 잠기고 랜섬 지불이 요구되거나, 키로거 또는 출처를 알 수 없는 물리적 장치가 노트북 같은 엔드 유저 장치에 연결된 경우. 랜섬웨어가 갑자기 나타났다면, 첫 조치는 항상 해당 컴퓨터를 네트워크에서 신속히 분리하는 것이 되어야 합니다. 이 지침은 바이러스나 감염이 의심되는 모든 경우에 해당되며, 해당 장치는 반드시 IT 부서의 확인 이후에만 다시 연결되어야 합니다.

[DCSA 3.2.3 구현]

보안 이벤트나 사고가 진행 중인지 탐지하는 방법에는 여러 가지가 있습니다. 경우에 따라 시스템이 작동을 멈추거나 잘못된 결과를 표시하거나, 속도가 느려지거나 사용자가 잠기는 등의 증상으로 쉽게 식별될 수도 있습니다. 그러나 사고가 탐지되지 않고 진행될 경우, 오히려 더 큰 리스크를 초래할 수 있습니다. 이는 특히 높은 무결성이 요구되는 시스템(예: 선박의 ECDIS 시스템)에 해당됩니다.

[DCSA 3.3.2 설명]

선박은 지속적인 모니터링 전략의 수립 및 유지에 포함되어야 하며, 다음을 포함하는 지속적 모니터링 프로그램을 구현해야 합니다:

- 모니터링 지표 및 그 빈도의 설정
- 조직의 지속 모니터링 전략에 따른 보안 통제의 지속적 평가
- 조직이 정의한 보안 상태 지표에 대한 지속적 모니터링
- 평가 및 모니터링을 통해 생성된 보안 관련 정보의 상관분석 및 해석
- 분석 결과에 따른 대응 조치 수행

위 내용은 ISM 코드에 따라 정기적으로 수행되는 안전관리 검토(Safety Management Review)에 포함되어야 합니다.

[DCSA 3.3.3 구현]

조직은 다음을 보장하기 위한 절차를 구현해야 합니다. 조직의 정보 시스템과 관련된 모니터링 활동에 대한 계획이 개발되고 유지되며, 리스크 기반 접근 방식으로 실행될 수 있도록 하는 것.

이 계획에는 조직 시스템이 초래할 수 있는 리스크를 식별하고, 사이버 정보 및 이벤트 모니터링 기능 등 보안 요구사항을 포함하는 내용이 포함되어야 합니다.

[DCSA 3.3.3 구현]

빅데이터의 활용

차세대 클라우드 기술을 활용할 경우, 이벤트 로그를 수집·저장·분석·상관관계 분석·공유·조치하는 것이 가능하며, 사용자 정의 응답 규칙과 결합하여 실시간 대응이 가능합니다. 이를 통해 조직은 전통적인 포렌식 및 감사 활동에 소요되는 시간을 줄이고, 거버넌스, 리스크관리 및 컴플라이언스 활동에 집중할 수 있습니다.

[DCSA 2.6.2 설명]

탐지 통제는 선박 시스템 내 자산을 보호하는 한 방법으로, 감사를 수행하고 로그를 분석하여 사건과 관련된 활동을 파악하는 데 활용됩니다. 탐지 통제가 마련되어 있다는 사실만으로도 악의적인 사용자가 중요 자산을 위협하는 행위를 시도하지

통제항목	D.1.1 사이버 위협 모니터링	Advanced
		않도록 억제하는 효과가 있습니다. **[DCSA 2.6.3 구현]** 조직은 지속적인 모니터링 전략을 수립하고 다음 사항을 포함하는 지속 모니터링 프로그램을 시행하여야 한다: a. 조직이 정의한 모니터링 대상 지표의 설정 b. 모니터링 수행 주기 및 해당 모니터링을 지원하는 평가 주기의 설정 c. 조직의 지속 모니터링 전략에 따른 보안 통제 평가의 지속적 수행 d. 조직이 정의한 지표에 따른 보안 상태의 지속적인 모니터링 e. 평가 및 모니터링을 통해 생성된 보안 관련 정보의 상관분석 및 해석 f. 분석 결과에 따른 대응 조치 수행 g. 조직 및 정보시스템의 보안 상태를 조직이 정한 담당자 또는 역할자에게 조직이 정한 보고 주기에 따라 보고 **[DCSA 4.3.3 구현]** 조직은 다음 사항을 수행하여야 한다: a. 조직이 정의한 기준에 따라 정보시스템 감사를 수행하고, 부적절하거나 비정상적인 활동 여부를 분석 b. 분석 결과를 조직이 지정한 담당자 또는 역할자에게 보고 c. 본사 대표가 선박에서 수행하는 안전 및 보안 관련 내부 감사에는 사이버보안 관련 서식, 절차 및 계획이 포함되어야 함 **[DCSA 4.3.3 구현]**
비고		

통제항목 상세 – Optimized

B. 사이버보안 통제

B.3 네트워크 접근 통제

통제항목	B.3.1 네트워크 분리		Optimized
레퍼런스 상세	IACS UR E26	원격 제어 시스템 또는 다른 CBS(컴퓨터기반시스템)와의 통신이 네트워크, 세분화 및 보호 수단(섹션 4.2.1(Security Zones and Network Segmentation) 및 4.2.2(Network protection safeguards)에 설명된 대로)을 통해 구성되는 경우, 로컬 제어 및 모니터링 시스템은 별도의 보안 구역으로 간주되어야 합니다. 단, 다양한 개념을 가진 CBS(컴퓨터기반시스템)에 대해서는 사례별로 특별한 고려가 가능함을 의미합니다. **[UR E26 4.4.2.3 세부 요구사항]** 본 UR의 적용 범위에 해당하는 모든 CBS(컴퓨터기반시스템)는 명확하게 정의된 보안 정책 및 보안 기능을 갖춘 보안 영역(Security Zones)으로 그룹화되어야 합니다. 보안 영역은 다음 중 하나로 구성되어야 합니다: 서로 완전히 격리된 상태(예: 에어 갭(air gapped))이거나, 다른 보안 영역 또는 네트워크와 연결되어 있으나, 그 사이의 데이터 통신이 적절히 제어되는 방식으로 연결된 경우 구역 간 통신 제어 방법에는 방화벽/라우터, 단방향 직렬 연결(simplex serial links), TCP/IP 다이오드, 건식 접점(dry contacts) 등이 포함될 수 있습니다. 명시적으로 허용된 트래픽만 보안 구역 경계를 통과할 수 있습니다. **[UR E26 4.2.1.1 요구사항]** 네트워크는 방화벽 경계로 보호되며, 침입 탐지 시스템(IDS) 또는 침입 방지 시스템(IPS)을 포함하여 들어오는 트래픽을 모니터링할 수 있지만, 이러한 경계를 우회당할 가능성은 항상 존재합니다. 네트워크 분리는 공격자가 전체 네트워크에 걸쳐 공격을 수행하는 것을 더 어렵게 만듭니다. 보안 구역 및 네트워크 분리의 주요 이점은 공격 표면을 줄이고, 공격자가 시스템을 통한 수평 이동을 수행하는 것을 방지하며, 네트워크 성능을 향상시키는 데 있습니다. CBS(컴퓨터기반시스템)를 보안 구역으로 할당하는 개념은 리스크 프로파일에 따라 CBS(컴퓨터기반시스템)를 그룹화할 수 있도록 합니다. **[UR E26 4.2.1.2 타당성]** 하나의 보안 구역은 여러 CBS(컴퓨터기반시스템)와 네트워크를 포함할 수 있으며, 이들 모두는 본 UR 및 UR E27에 명시된 해당 보안 요구사항을 준수해야 합니다. 보안 구역의 네트워크는 다른 구역 또는 네트워크와 논리적 또는 물리적으로 분리되어야 합니다. 4.2.6.3(Requirement details)절도 참조하십시오. 필수 안전 기능을 제공하는 CBS(컴퓨터기반시스템)는 별도의 보안 구역으로 그룹화되어야 하며, 다른 보안 구역과 물리적으로 분리되어야 합니다. 항해 및 통신 시스템은 기계류 또는 화물 시스템과 동일한 보안 구역에 포함되어서는 안 됩니다. 항해 및/또는 무선통신 시스템이 1.3.2(Systems in scope)절에 언급된 기타 동등한 기준에 따라 승인된 경우, 이 시스템들은 별도의 보안 구역에 포함되어야 합니다.	

통제항목	B.3.1 네트워크 분리	Optimized
		무선 장치는 전용 보안 구역에 있어야 합니다. 4.2.5(Wireless communication)절 참조하십시오. 본 UR의 적용 범위 외에 있는 시스템, 네트워크 또는 CBS(컴퓨터기반시스템)는 신뢰할 수 없는 네트워크로 간주되며, 본 UR이 요구하는 보안 구역 시스템과 물리적으로 분리되어야 합니다. 또는 이러한 시스템이 이 UR의 보안 구역의 일부로 간주되는 경우, 해당 OT 시스템은 UR에서 요구하는 동일한 조건을 충족해야 합니다. 보안 구역을 재설정하더라도 CBS(컴퓨터기반시스템)의 주요 기능에 영향을 주지 않고 이를 수행할 수 있어야 합니다. 4.4.3(Network isolation)절을 참조하십시오. **[UR E26 4.2.1.3 세부 요구사항]** 로컬 제어 및 모니터링용 CBS(컴퓨터기반시스템)는 이 UR의 요구사항을 준수하여야 합니다. **[UR E26 4.4.2.3 세부 요구사항]** 무선 네트워크 상의 장치는 오직 무선 네트워크 상에서만 통신해야 하며(즉, "듀얼 홈드(dual-homed)" 상태가 되어서는 안 됩니다). **[UR E26 4.2.5.3 세부 요구사항]** 무선 네트워크는 4.2.1(Security Zones and Network Segmentation)에 따라 별도의 세그먼트로 설계되어야 하며, 4.2.2(Network protection safeguards)에 따라 보호되어야 합니다. **[UR E26 4.2.5.3 세부 요구사항]**
	BIMCO	방화벽, 라우터 및 스위치와 같은 네트워크 장비의 구성 어떤 시스템이 제어 네트워크 또는 통제되지 않는 네트워크에 연결될 것인지 결정되어야 합니다. 제어 네트워크는 방화벽, 보안 게이트웨이, 라우터 및 스위치를 통해 연결된 장치들로부터의 보안 리스크를 방지하도록 설계되어 있습니다. 통제되지 않는 네트워크는 데이터 트래픽 제어의 부족으로 인해 리스크를 야기할 수 있으며, 직접적인 인터넷 연결로 인해 악성코드 침투에 매우 취약할 수 있습니다. 예를 들면: • 선박 자체의 운영에 중요도가 높은 네트워크는 통제되어야 합니다. 이러한 시스템은 높은 보안 수준을 갖춰야 합니다. • 항해 및 기타 OT 시스템 소프트웨어에 대한 원격 접근을 공급자에게 제공하는 네트워크는 통제되어야 합니다. 공급자가 시스템 업그레이드 또는 원격 정비를 수행해야 할 수도 있습니다. 육상 외부 접속 지점은 비인가 접근을 방지하도록 보호되어야 합니다. • 화물 적재 계획, 선적 및 적하물 관리 시스템은 제어되어야 합니다. 이들 시스템은 관계당국에 의무적인 선박 보고를 수행해야 하므로 중요합니다. • 게스트 액세스 네트워크와 같은 기타 네트워크는 통제되지 않는 상태일 수 있으며, 이는 예를 들어 여객 오락 활동이나 일반 인터넷 접근에 관련된 경우가 있습니다. 일반적으로 무선 네트워크는 통제되지 않는 것으로 간주됩니다. 접근 필요성과 신뢰 수준을 기반으로 한 효과적인 시스템 분리는 사이버 사고를 예방하는 가장 성공적인 전략 중 하나입니다. 효과적으로 분리된 네트워크는 공격자의 시스템 접근을 크게 제한할 수 있으며, 이는 맬웨어 확산 방지에 있어 가장 효과적인 기법 중 하나입니다. 선내 네트워크는 방화벽을 사용해 보호 구역으로 분할되어야

통제항목	B.3.1 네트워크 분리	Optimized
		하며, 방화벽 설정은 무단 변경을 탐지할 수 있도록 정기적으로 검토되어야 합니다. 통신 링크와 장치 수가 적을수록 해당 구역의 시스템과 데이터는 더욱 안전합니다. 기밀성과 안전성이 중요한 시스템은 가장 보호된 구역에 있어야 합니다. 자세한 내용은 부록 3의 선내 네트워크 가이드를 참고하고, ISO/IEC 62443 및 IACS 권고안 no.166 "Cyber Resilience"도 참조하십시오. **[BIMCO 7.2 기술적 보호 조치]** 방문자가 컴퓨터 또는 프린터 접근이 필요한 경우, 모든 제어 네트워크와 격리된 독립 컴퓨터를 사용해야 합니다. 무단 접근을 방지하기 위해 모든 물리적으로 접근 가능한 컴퓨터 및 네트워크 포트에는 이동식 미디어 차단 장치를 사용해야 합니다. **[BIMCO 7.3 절차적 보호 조치]**
비고		

C. 사이버 리스크 관리

C.2 사이버 리스크 평가

통제항목	C.2.4 사이버 리스크 평가 예외		Optimized
레퍼런스 상세	IACS UR E26	CBS(컴퓨터기반시스템)를 요구사항의 적용에서 제외하는 경우의 리스크 평가 **[UR E26 6 CBS(컴퓨터기반시스템)를 요구사항의 적용에서 제외하는 경우의 리스크 평가]** 본 UR의 적용 범위에 포함된 CBS(컴퓨터기반시스템) 중 일부가 관련 요구사항의 적용에서 제외되는 경우, 리스크 평가는 반드시 수행되어야 합니다. 리스크 평가는 해당 제외된 CBS(컴퓨터기반시스템)에 연관된 허용 가능한 리스크 수준을 입증하는 증거를 제공하여야 합니다. **[UR E26 6.1 요구사항]** 본 UR의 적용 범위에 포함된 CBS(컴퓨터기반시스템)를 관련 요구사항의 적용에서 제외하고자 할 경우, 그에 대한 정당한 사유가 필요하며 문서화되어야 합니다. 이러한 제외는 오직 해당 CBS(컴퓨터기반시스템)의 운영에 관련된 리스크 수준이 특정 리스크 평가 방법을 통해 허용 가능한 임계값 이하임이 입증될 경우에 한하여 선급협회가 수용할 수 있습니다. **[UR E26 6.2 타당성 근거]** 리스크 평가는 유사 설계에서의 지식 기반과 경험을 토대로 수행되어야 하며, 존재할 경우 CBS(컴퓨터기반시스템)의 범주, 연결성, 그리고 선박 및 CBS(컴퓨터기반시스템)의 기능 요구사항 및 사양을 고려하여야 합니다. 사이버 위협 정보는 내부 및 외부 출처 모두로부터 수집하여, 사이버보안 사건의 발생 가능성과 영향에 대한 이해를 심화하는 데 사용될 수 있습니다. **[UR E26 6.2 타당성 근거]** 선박의 운영하는 동안, 선주는 사이버 시나리오에서의 지속적인 변화와 선박 내 CBS(컴퓨터기반시스템)에서 식별된 새로운 취약점을 고려하여 리스크 평가를 갱신하여야 합니다. 새로운 리스크가 식별될 경우, 선주는 기존 리스크 평가를 갱신하거나 새로운 리스크 완화 조치를 구현하여야 합니다. **[UR E26 6.3 세부 요구사항]** 사이버 시나리오의 변화로 인해 해당 CBS(컴퓨터기반시스템)에 대해 허용 가능한 리스크 임계값을 초과하는 수준의 리스크가 발생할 경우, 선주는 선급협회에 이를 통지하고, 갱신된 리스크 평가를 제출하여 평가를 받아야 합니다. **[UR E26 6.3 세부 요구사항]** 검토 중인 CBS(컴퓨터기반시스템)에 대해 예상되는 운용 환경은 사이버 사고 발생 가능성과 그 사고가 인명 안전, 선박 안전 또는 해양 환경에 미칠 수 있는 영향을 파악하기 위한 리스크 평가에서 분석되어야 합니다. 이때 CBS(컴퓨터기반시스템)의 분류를 고려하여 분석이 수행되어야 합니다. 또한 공격 표면(Attack surface)은 CBS(컴퓨터기반시스템)의 연결성(Connectivity), 휴대용 장치용 인터페이스, 논리적 접근 제한 등과 같은 요소를 고려하여 분석되어야 합니다. **[UR E26 6.3 세부 요구사항]**	

통제항목	C.2.4 사이버 리스크 평가 예외	Optimized
	검토 중인 CBS(컴퓨터기반시스템)의 특정 구성과 관련된 새로운 리스크(emerging risk) 또한 식별되어야 합니다. 리스크 평가에서는 다음과 같은 요소들을 고려하여야 합니다: • 자산의 취약점 (Asset vulnerabilities) • 내부 및 외부 위협 (Threats, both internal and external) • 인명 안전, 선박의 안전 및/또는 환경에 미치는 사이버 사고의 잠재적 영향 • 시스템 간 통합 또는 시스템 간 인터페이스에 관련된 잠재적 영향 (예: 원격 접근이 제공되는 경우, 선박에 탑재되지 않은 시스템과의 연동 포함) **[UR E26 6.3 세부 요구사항]** 본 통합 요구사항(UR)의 적용 범위에 해당되는 CBS(컴퓨터기반시스템)가 관련 요구사항의 적용에서 제외되기 위해서는, 해당 CBS(컴퓨터기반시스템)의 운영이 사이버 리스크와 관련된 운영 안전에 영향을 미치지 않는다는 보장이 있어야 하며, 이 경우에 한하여 선급협회(Classification Society)은 이를 수용할 수 있습니다. 이러한 제외는 아래에 나열된 추가 기준을 완전히 충족하지 않더라도, 근거 자료와 함께 합리적인 설명이 제공되고, 그 내용이 선급협회에 의해 만족스럽다고 판단될 경우 수용될 수 있습니다. 선급협회는 이러한 제외를 고려하기 위해 추가적인 문서 제출을 요구할 수도 있습니다. **[UR E26 6.4 수용 기준]** 다음 기준은 본 UR의 적용 범위에서 시스템을 제외하기 위해 충족되어야 합니다: a) CBS(컴퓨터기반시스템)는 고립되어 있어야 합니다. (즉, 다른 시스템이나 네트워크와 IP 네트워크 연결이 없어야 합니다) b) CBS(컴퓨터기반시스템)는 접근 가능한 물리적 인터페이스 포트를 보유해서는 안 됩니다. 사용되지 않는 인터페이스는 논리적으로 비활성화되어야 하며, 승인되지 않은 장치를 CBS(컴퓨터기반시스템)에 연결할 수 없어야 합니다. c) CBS(컴퓨터기반시스템)는 물리적 접근이 통제되는 장소에 위치해야 합니다. d) CBS(컴퓨터기반시스템)는 본 UR의 적용 범위에서 정의된 바와 같이, 복수의 선박 기능을 제공하는 통합 제어 시스템이어서는 안 됩니다 (1.3(Scope of applicability)절 참조). 다음의 추가 기준은 리스크 수준 수용 가능성 평가 시 고려되어야 합니다: a) CBS(컴퓨터기반시스템)는 Category III에 해당하는 선박 기능을 제공해서는 안 됩니다. b) CBS(컴퓨터기반시스템)에 영향을 미치는 것으로 알려진 취약점, 위협, 사이버 사고로 인한 잠재적 영향이 리스크 평가에서 충분히 고려되어야 합니다. c) CBS(컴퓨터기반시스템)의 공격 표면은 최소화되어야 하며, 그 복잡성, 연결성, 물리적 및 논리적 접근 지점이(무선 공유기 포함)이 고려되어야 합니다. **[UR E26 6.4 수용 기준]**	
비고		

C.4 사이버 복원력 검사

통제항목	C.4.1 사이버 복원력 검사	Optimized
레퍼런스 상세	IACS UR E26	선박이 선주에게 인도된 이후, 선주는 본 UR에 명시된 바와 같이 기술적 및 조직적 보안 대응조치를 수립하고 구현함으로써 이를 관리해야 합니다. **[UR E26 5.3 선박 운항 기간 동안]** 본 UR의 적용 범위 내 CBS(컴퓨터기반시스템)에 대한 변경 사항은 UR E22의 변경 관리(Management of Change, MoC) 요구사항에 따라 수행되어야 합니다. 이는 CBS(컴퓨터기반시스템)에 대한 문서를 최신 상태로 유지하는 것을 포함합니다. **[UR E26 5.3 선박 운항 기간 동안]** 선주는 공급자의 지원을 받아, 선박에 탑재된 CBS(컴퓨터기반시스템) 및 이들 시스템을 상호 연결하는 네트워크, 그리고 이러한 시스템을 서로 및 선박 외부(CBS(컴퓨터기반시스템)가 탑재되지 않은, 예: 육상) 시스템과 연결하는 네트워크의 구성과 일치하도록, 선박 사이버 복원력 시험 절차를 최신 상태로 유지해야 합니다. 선주는 선박 내 CBS(컴퓨터기반시스템) 및 네트워크에서 발생한 변화, 이러한 변화에 수반되는 신흥 리스크, 새로운 위협, 신규 취약점 및 선박의 운항 환경 내 기타 변경사항 등을 고려하여 선박 사이버 복원력 시험 절차를 갱신해야 합니다. **[UR E26 5.3 선박 운항 기간 동안]** 선주는 공급자의 지원을 받아, 요구사항 이행을 위한 조치를 최신 상태로 유지하여야 하며, 예를 들어 선박 내 CBS(컴퓨터기반시스템)와 이를 연결하는 네트워크의 하드웨어 및 소프트웨어를 주기적으로 유지보수함으로써 이를 수행하여야 합니다. **[UR E26 5.3 선박 운항 기간 동안]** 선주는 시험 실행 결과의 사본과 최신 선박 사이버 복원력 시험 절차 문서를 선박에 비치하고, 선급협회(Classification Society)에 이를 제공할 수 있도록 하여야 합니다. **[UR E26 5.3 선박 운항 기간 동안]** 선박의 최초 연차 검사가 이루어지기 이전에 적절한 시점에, 선주는 본 UR의 적용 범위 내에 있는 CBS(컴퓨터기반시스템)의 사이버보안 및 사이버 복원력 관리 프로그램을 문서화한 선박 사이버보안 및 복원력 프로그램을 선급협회에 제출하여야 합니다. **[UR E26 5.3.1 최초 연차 검사]** 선박의 후속 연차 검사에서, 선주는 요청이 있을 경우 선급협회에 선박 사이버보안 및 복원력 프로그램의 이행을 입증하여야 합니다. **[UR E26 5.3.2 후속 연차 검사]** 선박의 선급(Classification) 인증 갱신 시, 선주는 선급협회가 승인한 선박 사이버 복원력 시험 절차에 따라 선급협회의 입회 하에 시험을 수행하여야 합니다. 특정 사이버보안 조치는 최초 특별 검사에서 입증되어야 하며, 다른

통제항목	C.4.1 사이버 복원력 검사	Optimized

특별 검사는 CBS(컴퓨터기반시스템)의 변경 사항이 발생한 경우 선급협회의 요청에 따라 수행되어야 하며, 본 UR의 제4절 "운영 단계(Operation phase)"에 명시된 조건에 따릅니다.

[UR E26 5.3.3 특별 검사]

선박 자산 목록에는, 탑재되어 있는 경우, 1.3.2(Systems in scope)절에 명시된 CBS(컴퓨터기반시스템)가 최소한 포함되어야 합니다.
해당 목록은 선박의 전체 수명 기간 동안 최신 상태로 유지되어야 합니다. 새로운 취약점을 유발하거나 기능적 종속성 또는 시스템 간 연결을 변경할 수 있는 소프트웨어 및 하드웨어 변경 사항은 자산 목록에 기록되어야 합니다.
만약 자산 목록에 기밀 정보(예: IP 주소, 프로토콜, 포트 번호 등)가 포함되는 경우, 해당 정보에 대한 접근은 권한이 부여된 사람에게만 제한되도록 특별한 조치를 취해야 합니다.

[UR E26 4.1.1.3 세부 요구사항]

본 UR의 적용 범위에 해당하는 모든 하드웨어 장치에 대해, 선박 자산 목록에는 UR E27의 3.1.1(CBS asset inventory)절에 명시된 정보를 최소한 포함해야 합니다.
또한, 자산 목록에는 해당 CBS(컴퓨터기반시스템)와 관련된 시스템 분류 및 보안 영역(Security Zone)을 명시할 수 있습니다.

[UR E26 4.1.1.3.1 하드웨어]

본 UR의 적용 범위에 해당하는 모든 소프트웨어(예: 응용 프로그램, 운영체제, 펌웨어 등)에 대해, 선박 자산 목록에는 UR E27의 3.1.1절(CBS(컴퓨터기반시스템) asset inventory)에 명시된 정보를 최소한 포함해야 합니다.

[UR E26 4.1.1.3.2 소프트웨어]

운영 단계에서의 일반적인 검사 요구사항에 대해서는 5.3(During the operational life of the ship)절을 참조합니다.

[UR E26 4.1.1.4.4 운영 단계]

선주는 선박 사이버보안 및 회복력 프로그램(Ship cyber security and resilience program) 내에서, 본 UR의 적용 범위에 해당하는 CBS(컴퓨터기반시스템)에 대한 변경관리(MoC: Management of Change) 절차를 설명해야 하며, 다음 요구사항을 최소한 포함해야 합니다:

- 변경관리 (5.3(During the operational life of the ship)절)
- 하드웨어 및 소프트웨어 변경사항 (4.1.1.3(Requirement details)절)

[UR E26 4.1.1.4.4 운영 단계]

또한 선주는 선박 사이버보안 및 회복력 프로그램 내에서 소프트웨어 업데이트 관리에 대해서도 설명해야 하며, 다음 요구사항을 최소한 포함해야 합니다:

- 취약점 및 사이버 리스크 (4.1.1.2(Rationale)절 및 4.1.1.3(Requirement details)절)
- 보안 패치 적용 (4.2.6.3.2(Additional requirements for remote maintenance)절)

통제항목	C.4.1 사이버 복원력 검사	Optimized

[UR E26 4.1.1.4.4 운영 단계]

최초 연차 검사 (First annual survey)
선주는 선박 사이버보안 및 회복력 프로그램이 이행되었음을 입증하는 문서화된 증빙자료 또는 기록을 선급협회에 제출해야 하며, 다음 사항을 포함해야 합니다:

- 승인된 변경관리 절차가 준수되었음
- CBS(컴퓨터기반시스템) 내의 소프트웨어에 대해 알려진 취약점 및 기능적 종속성이 고려되었음
- 선박 자산 목록이 최신 상태로 유지되었음

[UR E26 4.1.1.4.4 운영 단계]

후속 연차 검사 (Subsequent annual surveys)
선주는 요청 시 선급협회에 선박 사이버보안 및 회복력 프로그램의 이행 상태를 입증하여야 하며, 최초 연차 검사에서와 같이 문서화된 증빙자료 또는 기록을 제출하여야 합니다.

[UR E26 4.1.1.4.4 운영 단계]

선주는 선박 사이버보안 및 회복력 프로그램 내에서 보안 구역 경계 장치(예: 방화벽)의 관리를 설명해야 하며, 다음 요구사항을 최소한 포함해야 합니다:

- 최소 기능 원칙 (4.2.2.1(Requirement)절)
- 명시적으로 허용된 트래픽 (4.2.1.1(Requirement)절)
- 서비스 거부(DoS) 공격 방지 (4.2.2.1(Requirement)절)
- 보안 감사 기록의 점검 (4.3.1.3(Requirement details)절)

[UR E26 4.2.1.4.4 운영 단계]

최초 연차 검사 (First annual survey)
선주는 구역 및 경로도가 최신 상태로 유지되었음을 선급협회에 입증하여야 하며, 선박 사이버보안 및 회복력 프로그램이 이행되었음을 입증하는 기록 또는 문서화된 증거를 제시해야 합니다. 즉, 보안 구역 경계가 위 요구사항에 따라 관리되고 있음을 증명해야 합니다.

[UR E26 4.2.1.4.4 운영 단계]

선주는 선박 사이버보안 및 회복력 프로그램(Ship cyber security and resilience program) 내에서 악성 코드 보호 관리에 대해 설명하여야 하며, 다음의 요구사항을 최소한 포함하여야 합니다:

- 유지관리 및 업데이트 (4.2.3.3(Requirement details)절 참조)
- 운영 절차 및 물리적 보호 조치 (4.2.3.3(Requirement details)절 참조)
- 모바일, 휴대용, 이동식 매체의 사용 (4.2.3.4.3(Commissioning phase)절 및 4.2.7.3절 참조)
- 접근 통제 (4.2.4(Access control)절 참조)

[UR E26 4.2.3.4.4 운영 단계]

최초 연차 검사 (First annual survey)
선주는 선박 사이버보안 및 회복력 프로그램이 이행되었음을 입증하는 기록

통제항목	C.4.1 사이버 복원력 검사	Optimized

또는 문서화된 증거를 선급협회에 제출하여야 하며, 다음 사항을 포함하여야 합니다:

- 모든 안티멀웨어 소프트웨어가 유지 및 업데이트되었음
- 휴대용, 모바일 또는 이동식 장치 사용에 관한 절차가 준수되었음
- 접근 통제에 관한 정책 및 절차가 준수되었음
- 물리적 보호 조치가 유지되었음

[UR E26 4.2.3.4.4 운영 단계]

선주는 선박 사이버보안 및 회복력 프로그램 내에서 논리적 및 물리적 접근 관리에 대해 다음 요구사항을 최소한 포함하여 설명해야 합니다:

- 물리적 접근 통제 (4.2.4.3.1(Physical access control)절)
- 방문자에 대한 물리적 접근 통제 (4.2.4.3.2(Physical access control for visitors)절)
- 공유기에 대한 물리적 접근 통제 (4.2.4.3.3(Physical access control of network access points)절)
- 자격 증명 관리 (4.2.4.3.5(Management of credentials)절)
- 최소 권한 원칙 (4.2.4.3.6(Least privilege principle)절)

[UR E26 4.2.4.4.4 운영 단계]

또한 선주는 선박 사이버보안 및 회복력 프로그램 내에서 기밀 정보 관리에 대해 다음 요구사항을 최소한 포함하여 설명해야 합니다:

- 기밀 정보 (4.1.1.3(Requirement details)절)
- 인가된 인원에게 허용된 정보 (4.2.4.3(Requirement details)절)
- 무선 네트워크로 전송된 정보 (4.2.5.3(Requirement details)절)

[UR E26 4.2.4.4.4 운영 단계]

최초 연차 검사 (First annual survey)
선주는 선박 사이버보안 및 회복력 프로그램의 이행을 입증하기 위해 아래 항목을 포함한 기록 또는 기타 문서화된 증빙자료를 기관에 제출해야 합니다:

- 인원은 각자의 책임에 따라 CBS(컴퓨터기반시스템)에 접근할 수 있도록 인가되어야 합니다.
- 인가된 장비만 CBS(컴퓨터기반시스템)에 연결되어야 합니다.
- 방문자는 관련 정책 및 절차에 따라 CBS(컴퓨터기반시스템)에 접근할 수 있도록 해야 합니다.
- 물리적 접근 통제는 유지되고 적용되어야 합니다.
- 자격 증명, 키, 비밀, 인증서, 관련 CBS(컴퓨터기반시스템) 문서 및 기타 민감 정보는 관련 정책 및 절차에 따라 관리되고 기밀로 유지되어야 합니다.

[UR E26 4.2.4.4.4 운영 단계]

선주는 선박 사이버보안 및 회복력 프로그램에서 신뢰되지 않은 네트워크와의 원격 접속 및 통신 관리에 대해 아래 UR에서 요구하는 최소한의 요건들을 포함하여 설명하여야 합니다:

- 사용자 매뉴얼 (섹션 4.2.6.3(Requirement details))

통제항목	C.4.1 사이버 복원력 검사	Optimized

- 역할 및 권한 (섹션 4.2.6.3(Requirement details))
- 패치 및 업데이트 (섹션 4.2.6.3.2(Additional requirements for remote maintenance)
- 원격 소프트웨어 업데이트 수행 전 확인 절차 (섹션 4.2.6.3.2(Additional requirements for remote maintenance))
- 중단, 중지, 롤백 절차 (섹션 4.2.6.3.2)

[UR E26 4.2.6.4.4 운영 단계]

최초 연차 검사 (First annual survey)
선주는 선박 사이버보안 및 회복력 프로그램의 이행을 입증하기 위해 협회에 다음을 포함한 기록 또는 기타 문서화된 증거를 제시하여야 합니다:

- 원격 접속 세션이 기록되었거나 로깅되었으며, 관련 정책 및 사용자 매뉴얼에 따라 수행되었음.
- 보안 패치 및 기타 소프트웨어 업데이트가 변경 관리 절차에 따라, 그리고 공급자와의 협력을 통해 수행되었음.

[UR E26 4.2.6.4.4 운영 단계]

운영 단계의 일반 요구사항은 섹션 5.3(During the operational life of the ship)을 참조하시기 바랍니다.
선주는 선박 사이버보안 및 회복력 프로그램(Ship cyber security and resilience program) 내에서 모바일 및 휴대용 장치의 관리에 대해 다음의 요구사항을 최소한으로 포함하여 기술하여야 합니다:

- 정책 및 절차 (섹션 4.2.4.3.4(Removable media controls))
- 인터페이스 포트의 물리적 차단 (섹션 4.2.7.1(Requirement))
- 권한이 있는 인원의 사용 (섹션 4.2.7.3(Requirement details))
- 허가된 장치만 연결 (섹션 4.2.7.3(Requirement details))
- 악성코드 도입 리스크 고려 (섹션 4.2.7.3(Requirement details))

[UR E26 4.2.7.4.4 운영 단계]

최초 연차 검사 (First annual survey)
선주는 협회(Society)에 다음을 입증하는 기록 또는 기타 문서화된 증거를 제시하여 선박 사이버보안 및 회복력 프로그램이 구현되었음을 보여주어야 합니다. 즉:

- 모바일, 휴대용 또는 이동식 매체의 사용은 권한이 있는 인원으로 제한되며 관련 정책 및 절차를 따릅니다.
- CBS(컴퓨터기반시스템)에는 허가된 장치만 연결됩니다.
- 물리적 인터페이스 포트 사용을 제한하는 수단은 승인된 설계 문서에 따라 구현되어야 합니다.

[UR E26 4.2.7.4.4 운영 단계]

선박 소유자는 선박 사이버보안 및 복원력 프로그램(Ship cyber security andresilience program) 내에서 CBS(컴퓨터기반시스템) 및 네트워크의 이상 징후를 탐지하기 위한 관리 활동을 설명하여야 하며, 본 UR에서 최소한

통제항목	C.4.1 사이버 복원력 검사	Optimized

다음 요구사항을 충족하여야 합니다:
- 이상 징후 탐지 및 인지 (섹션 4.3(Detect))
- 보안 감사 기록의 점검 (섹션 4.3.1.3(Requirement details))
- 사고를 탐지하기 위한 지침 또는 절차 (섹션 4.4.1.1(Requirement))

위 활동들은 섹션 4.4.1(Incident response plan)의 사고 대응 절차와 함께 다루어질 수 있습니다.

[UR E26 4.3.1.4.4 운영 단계]

최초 연차 검사 (First annual survey)
선박 소유자는 선박 사이버보안 및 복원력 프로그램의 이행을 입증하는 기록 또는 기타 문서화된 증거를 협회에 제출하여야 하며, 다음 사항을 포함하여야 합니다:
CBS(컴퓨터기반시스템)는 정기적으로 이상 징후에 대해 모니터링되며, 보안 감사 기록의 점검 및 CBS(컴퓨터기반시스템) 내 경고(alert)에 대한 조사 등을 통해 이를 수행합니다.

[UR E26 4.3.1.4.4 운영 단계]

선주는 선박 사이버보안 및 복원력 프로그램(Ship cyber security and resilience program)에 다음 UR의 요구사항을 최소한으로 반영하여, CBS(컴퓨터기반시스템) 및 네트워크의 보안 기능이 올바르게 동작하는지를 검증하기 위한 관리 활동을 기술해야 합니다:
- 시험 및 유지보수 주기(섹션 4.3.2.3(Requirement details))
- 주기적 유지보수(섹션 5.3.3(Special survey))

[UR E26 4.3.2.4.4 운영 단계]

최초 연차 검사 (First annual survey)
선주는 선박 사이버보안 및 복원력 프로그램이 이행되고 있음을 입증하는 기록 또는 기타 문서화된 증거를 선급협회에 제시해야 합니다. 즉,
- CBS(컴퓨터기반시스템)의 보안 기능이 주기적으로 시험되거나 검증되고 있음을 제시해야 합니다.

[UR E26 4.3.2.4.4 운영 단계]

선박 소유자는 선박 사이버보안 및 회복력 프로그램(Ship cyber security and resilience program) 내에 사고 대응 계획을 기술하여야 합니다. 해당 계획은 본 UR의 적용 범위에 포함되는 CBS(컴퓨터기반시스템)(컴퓨터기반시스템)를 다루며, 다음의 최소 요구사항들을 포함하여야 합니다:
- 섹션 4.4.1(Incident response plan)의 요구사항에 따라 사이버 사고에 대해 누가, 언제, 어떻게 대응할지에 대한 설명
- 섹션 4.4.2(Local, independent and/or manual operation)의 요구사항에 따라 로컬/수동 제어에 대한 절차 또는 지침
- 섹션 4.4.3(Network isolation)의 요구사항에 따라 보안 구역(Security zones) 분리 절차 또는 지침
- 섹션 4.4.4(Fallback to a minimal risk condition)의 요구사항에 따라

통제항목	C.4.1 사이버 복원력 검사	Optimized

사이버 사고 발생 시 CBS(컴퓨터기반시스템)의 예상 동작에 대한 설명

[UR E26 4.4.1.4.4 운영 단계]

최초 연차 검사 (First annual survey)
선박 소유자는 선박 사이버보안 및 회복력 프로그램의 구현을 입증하는 문서 또는 기타 증거 자료를 선급(Society)에 제출하여야 합니다. 해당 문서는 다음 사항들을 포함해야 합니다:

- 사고 대응 계획이 책임 있는 승무원에게 제공되어 있음
- 로컬/수동 제어에 대한 절차 또는 지침이 책임 있는 승무원에게 제공되어 있음
- 보안 구역 분리/차단에 대한 절차 또는 지침이 책임 있는 승무원에게 제공되어 있음
- 사이버 사고가 사고 대응 계획에 따라 대응되었음

[UR E26 4.4.1.4.4 운영 단계]

후속 연차 검사 (Subsequent annual surveys)
선박 소유자는 선급의 요청이 있을 경우, 선박 사이버보안 및 회복력 프로그램의 이행을 입증하기 위하여, 최초 연간 점검 시와 동일한 기준에 따른 문서 또는 기타 증거를 제출하여야 합니다.

[UR E26 4.4.1.4.4 운영 단계]

선주는 선박 사이버보안 및 회복력 프로그램(Ship cyber security and resilience program)에 사이버 사고 복구 계획을 포함하여야 합니다. 해당 계획은 이 UR이 적용되는 CBS(컴퓨터기반시스템)를 포함하여야 하며, 최소한 다음 요구사항을 다루어야 합니다:

- 사이버 사고로부터 누구(Who)가, 언제(When), 어떻게(How) 복구 및 복원하는지에 대한 설명 (섹션 4.5.1(Recovery plan) 요구사항 준수)
- 백업 정책: 백업 주기, 유지관리, 테스트에 대한 방침으로, 허용 가능한 다운타임, 대체 제어 수단의 가용성, 공급업체 지원 체계, 그리고 CBS(컴퓨터기반시스템)의 중요도를 고려하여야 함 (섹션 4.5.2(Backup and restore capability) 요구사항 준수)
- 백업, 셧다운, 리셋, 복원 및 재시작에 대한 사용자 매뉴얼 또는 절차 참조, 섹션 4.5.2(Backup and restore capability) 및 4.5.3(Controlled shutdown, reset, restore and restart) 요구사항 준수

[UR E26 4.5.1.4.4 운영 단계]

최초 연차 검사 (First annual survey)
선주는 선급협회(Society)에 다음 내용을 포함하는 기록 또는 기타 문서화된 증거를 제시하여, 선박 사이버보안 및 회복력 프로그램의 구현을 입증하여야 합니다:

- 사고 복구에 대한 지침 및/또는 절차가 탑승한 책임자에게 제공되고 있는지
- 필요한 장비, 도구, 문서, 소프트웨어 및 데이터가 책임자에게 제공되고 있는지

통제항목	C.4.1 사이버 복원력 검사	Optimized
		• CBS(컴퓨터기반시스템)의 백업이 정책 및 절차에 따라 수행되었는지 • 셧다운, 리셋, 복원, 재시작에 대한 매뉴얼 및 절차가 책임자에게 제공되고 있는지 **[UR E26 4.5.1.4.4 운영 단계]** 후속 연차 검사 (Subsequent annual surveys) 선주는 선급협회의 요청이 있을 경우, 최초 연차 검사에서의 조건과 동일한 방식으로 기록 또는 문서화된 증거를 제시하여 사이버보안 및 회복력 프로그램의 구현을 입증하여야 합니다. **[UR E26 4.5.1.4.4 운영 단계]** 정책, 절차, 계획 및 기타 정보가 포함되어야 합니다. **[UR E26 5.3.1 최초 연차 검사]** 선급협회 선박 사이버보안 및 복원력 프로그램을 승인한 후, 선주는 최초 연차 검사 시 승인된 선박 사이버보안 및 복원력 프로그램에 명시된 절차의 이행을 기록 또는 기타 문서화된 증거를 통해 입증하여야 합니다. **[UR E26 5.3.1 최초 연차 검사]** 선박 관리 회사의 변경이 있을 경우, 선박 사이버보안 및 복원력 프로그램에 대한 새로운 검증이 요구됩니다. **[UR E26 5.3.1 최초 연차 검사]** 선박의 후속 연차 검사에서, 선주는 요청이 있을 경우 선급협회에 선박 사이버보안 및 복원력 프로그램의 이행을 입증하여야 합니다. **[UR E26 5.3.2 후속 연차 검사]** 선박의 선급(Classification) 인증 갱신 시, 선주는 선급협회가 승인한 선박 사이버 복원력 시험 절차에 따라 선급협회의 입회 하에 시험을 수행하여야 합니다. 특정 사이버보안 조치는 최초 특별 검사에서 입증되어야 하며, 다른 특별 검사는 CBS(컴퓨터기반시스템)의 변경 사항이 발생한 경우 선급협회의 요청에 따라 수행되어야 하며, 본 UR의 제4절 "운영 단계(Operation phase)"에 명시된 조건에 따릅니다. **[UR E26 5.3.3 특별 검사]**
비고		

D. 사이버 사고 대응

D.1 사이버보안 모니터링

통제항목	D.1.2 네트워크 운영 모니터링	Optimized
레퍼런스 상세	IACS UR E26	본 통합요건서(UR)의 적용 범위에 포함된 네트워크는 지속적으로 모니터링되어야 하며, 장애 또는 용량 저하/감소가 발생할 경우 경보가 생성되어야 합니다. **[UR E26 4.3.1.1 요구사항]** 사이버 공격은 점점 더 정교해지고 있으며, 건조 당시에는 알려지지 않았던 취약점을 표적으로 하는 공격은 선박이 이러한 위협에 대해 제대로 준비되지 못한 상황에서 사고를 야기할 수 있습니다. 이러한 유형의 알려지지 않은 취약점을 노린 공격에 신속히 대응하기 위해서는, 이상 징후를 탐지할 수 있는 기술이 필요합니다. 네트워크 상의 이상 현상을 탐지할 수 있고, 사이버 사고 발생 이후 사후 분석(post-incident analysis)에 사용할 수 있는 모니터링 시스템은 적절한 대응 및 회복을 가능하게 해줍니다. **[UR E26 4.3.1.2 근거]** 본 UR의 적용 범위에 있는 네트워크를 모니터링하기 위한 조치는 다음과 같은 기능을 갖추어야 합니다: • 과도한 트래픽에 대한 모니터링 및 보호 • 네트워크 연결 상태 모니터링 • 장치 관리 활동의 모니터링 및 기록 • 비인가 장치의 연결에 대한 보호 • 네트워크 대역폭의 사용률이 공급자가 정의한 비정상 기준치를 초과할 경우 경보 생성(참고: UR E22, 섹션 7.2.1(General requirements for category II and III systems) 참조) **[UR E26 4.3.1.3 세부 요구사항]**
비고		

D.3 사이버 복구 계획

통제항목	D.3.1 사이버 백업 관리		Optimized
레퍼런스 상세	IMO	정기적인 시스템 백업, 소프트웨어 업데이트, 사고 대응 계획을 유지합니다. **[IMO 3.5.3.7 보호(protect)]**	
	IACS UR E26	일반적으로, 백업 및 복원 전략의 목적은 데이터 손실로부터 보호하고, 손실 이후 데이터베이스를 복원할 수 있도록 하는 데 있습니다. 통상적으로 백업 관리 작업에는 다음이 포함됩니다. 다양한 장애 유형에 대한 대응 계획 및 테스트 백업 및 복구용 데이터베이스 환경 구성 백업 일정 수립 백업 및 복구 환경의 모니터링 장기 보관을 위한 데이터베이스 복사본 생성 한 데이터베이스 또는 호스트에서 다른 곳으로의 데이터 이동 등 **[UR E26 4.5.2.2 근거]** 이 UR의 적용 범위 내에 있는 CBS(컴퓨터기반시스템)는 백업 및 복원 기능을 갖추어야 하며, 이를 통해 선박이 사이버 사고 이후 항해 및 운영 상태를 안전하게 회복할 수 있어야 합니다. **[UR E26 4.5.2.3.1 복원 기능]** 데이터는 보안된 복사본 또는 이미지로부터 복원 가능하여야 합니다. **[UR E26 4.5.2.3.1 복원 기능]** 사이버 사고로부터 복구하기에 충분한 정보 및 백업 수단이 제공되어야 합니다. **[UR E26 4.5.2.3.1 복원 기능]** 이 UR의 적용 범위 내에 있는 CBS(컴퓨터기반시스템) 및 네트워크는 데이터 백업 기능을 제공하여야 합니다. 또한, 오프라인 백업의 사용도 고려하여, 온라인 백업 장비에 영향을 미치는 랜섬웨어 및 웜에 대한 내성을 향상시켜야 합니다. **[UR E26 4.5.2.3.2 백업]** 백업 계획은 다음 항목을 포함하여 수립되어야 합니다. 범위, 방식, 주기, 저장 매체, 보존 기간 **[UR E26 4.5.2.3.2 백업]**	
	OCIMF SIRE 2.0	사이버 사고 이후 복구를 지원하기 위해 백업 설비가 마련되어야 하고 사용되어야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]** 항해 및 추진에 중요한 OT 시스템은 사이버 사고 발생 후 신속하고 안전하게 복구할 수 있도록 백업 시스템을 갖추어야 합니다. **[OCIMF SIRE 2.0 7.5 사이버보안]**	
	BIMCO	사이버보안 담당자와 사이버 사고 지원 업무를 담당하는 담당자는 선상 및 육상에서 인쇄본 형태의 복구 계획을 이용할 수 있어야 합니다. 이 계획은 조직의 전반적인 사업 연속성 계획의 일부가 되어야 하며, 목적은 IT 및 OT를 정상 작동 상태로 복구하는 데 필요한 시스템 및 데이터의 복구를 지원하는 것입니다. 또한 선상 인력의	

통제항목	D.3.1 사이버 백업 관리	Optimized
		안전을 보장하기 위해 선박의 운항 및 항해를 계획의 최우선순위에 두어야 합니다. 복구 계획의 세부 사항과 복잡성은 선박의 종류와 선상에 설치된 IT, OT 및 기타 시스템에 따라 달라집니다. 사고 대응팀은 복구 작업(예: 드라이브 삭제)이 사고 원인에 대한 귀중한 정보를 제공할 수 있는 증거를 파괴할 수 있으므로, 복구 작업의 결과를 신중하게 고려해야 합니다. 적절한 경우, 운영 역량을 복구하는 동시에 증거를 보존하기 위해 전문적인 사이버 사고 대응 지원을 받아야 합니다. 또한, 7.2(Technical protection measures)절에서 설명한 대로 데이터 복구 기능은 귀중한 기술적 보호 조치입니다. 데이터 복구 기능은 일반적으로 IT 데이터의 소프트웨어 백업 형태로 제공됩니다. 선상 또는 해상에 소프트웨어 백업이 있으면 사이버 사고 발생 후 IT 시스템을 운영 상태로 복구할 수 있습니다. 단, 랜섬웨어와 웜은 역사적으로 백업 어플라이언스에도 확산되어 왔으므로 오프라인 백업 활용도 반드시 고려해야 합니다. 특히 백업 시스템이 없는 경우, OT 복구는 더욱 복잡해질 수 있으며 해안에서의 지원이 필요할 수 있습니다. 따라서 복구 계획에는 이러한 지원을 받을 수 있는 장소와 지원자에 대한 세부 정보가 포함되어야 합니다. 예를 들어, 항구로 이동하여 서비스 엔지니어의 지원을 받는 것이 바람직합니다. 자격을 갖춘 인력이 선박에 탑승할 수 있는 경우, 더욱 광범위한 진단 및 복구 조치를 수행할 수 있지만, 그렇지 않은 경우 복구 계획은 신속한 기술 지원 확보에 국한될 수 있습니다. 따라서 사고 대응 계획, 비상 계획, 그리고 사업 연속성 계획은 모두 상호 보완적이어야 하며, 회사 전체의 역할과 책임을 포함해야 합니다. 또한 기업은 사이버 사고 대응을 위한 복구 절차와 선박-해상 간 협력 전체 과정을 자주 테스트하는 것이 중요합니다. **[BIMCO 10.3 복구 계획]** 데이터 복구 기능은 시스템 및/또는 데이터를 안전한 복사본 또는 이미지로부터 복원함으로써, 깨끗한 시스템을 복원할 수 있도록 하는 능력을 의미합니다. 사이버 사고 이후 복구를 보장하기 위해 필수 정보와 소프트웨어에 적합한 백업 설비가 제공되어야 합니다. **[BIMCO 10.4 데이터 복구 기능]** 보존 기간 및 복구 시나리오는 어떤 중요 시스템이 빠른 복구 기능을 필요로 하는지를 우선순위로 정하고, 그 영향을 줄이기 위해 수립되어야 합니다. 높은 데이터 가용성을 요구하는 시스템은 복원력이 있도록 설계되어야 합니다. 선박의 안전한 항해 및 운항에 필수적인 OT 시스템은, 사이버 사고 이후 선박이 항해 및 운항 능력을 빠르고 안전하게 회복할 수 있도록 백업 시스템을 갖추고 있어야 합니다. **[BIMCO 10.4 데이터 복구 기능]**
	DCSA	핵심 자산 손실의 리스크가 있는 경우, 선상에서 접근 가능한 백업을 마련해야 합니다. 시스템 수준 정보에는 시스템 상태 정보, 운영 체제, 애플리케이션 소프트웨어, 라이선스 등이 포함되며, 사용자 수준 정보는 시스템 수준 외의 모든 정보를 의미합니다. 정보 백업 무결성 보호를 위한 메커니즘으로는 디지털 서명, 암호 해시 등이 있습니다. 전송 중인 백업 보호는 이 통제 범위에 포함되지 않으며, 정보 시스템 백업은 비상계획

통제항목	D.3.1 사이버 백업 관리	Optimized
	(Contingency Plans)과 조직적 요구사항을 반영해야 합니다. **[DCSA 2.4.3 구현]** 데이터 복구 기능은 일반적으로 IT 데이터에 대한 소프트웨어 백업의 형태로 제공됩니다. 소프트웨어 백업이 선박 내 또는 육상에 존재할 경우, 사이버 사고 이후 IT를 운영 가능한 상태로 복구할 수 있어야 합니다. OT의 복구는 백업 시스템이 없는 경우 특히 더 복잡할 수 있으며, 육상으로부터의 지원이 필요할 수 있습니다. 이러한 지원이 어디에서, 누구에 의해 제공되는지에 대한 세부 사항은 복구 계획의 일부가 되어야 합니다. 예를 들어 서비스 엔지니어의 지원을 받기 위해 항구로 이동하는 방식이 있을 수 있습니다. 만약 자격을 갖춘 인력이 선박 내에 있다면, 보다 광범위한 진단 및 복구 조치를 수행할 수 있습니다. 그렇지 않은 경우, 복구 계획은 기술 지원에 신속하게 접근하는 수준으로 제한될 것입니다. **[DCSA 5.1.2 설명]** 데이터 복구 능력(Data recovery capability)이란 시스템 및/또는 데이터를 안전한 복사본이나 이미지로부터 복원하여 깨끗한 시스템을 되돌릴 수 있는 능력을 말합니다. 이를 통해 사이버 사고 이후 복구가 가능하도록 필수적인 정보와 소프트웨어 백업 설비가 제공되어야 합니다. 또한 보존 기간(retention period)과 복원 시나리오를 수립하여, 어떤 중요한 시스템이 영향을 줄이기 위해 신속한 복원 기능을 필요로 하는지를 우선순위로 정해야 합니다. 데이터 가용성 요구가 높은 시스템은 복원력이 갖추어져야 합니다. 선박의 안전한 항해와 운항에 필수적인 OT 시스템은 사이버 사고 이후 선박이 신속하고 안전하게 항해 및 운항 능력을 회복할 수 있도록 백업 시스템을 갖추어야 합니다. **[DCSA 5.1.2 설명]** 승인된 SMS(안전관리시스템)에는 다음 사항을 포함한 선박 장비의 백업 유지 및 테스트 절차가 이미 포함되어 있어야 합니다. 단, SMS(안전관리시스템)는 선박 안전 운항과 환경 보호를 위한 오프라인 백업 유지 및 보관 절차는 포함하지 않을 수 있습니다. 다음의 절차가 마련되어야 합니다: (a) 기존 절차에 포함되어 있지 않은 경우, 중요 시스템의 백업 계획 확인 (b) 기존 절차에 포함되어 있지 않은 경우, 중요 시스템의 대체 운영 모드 점검 (c) 사이버 사고로부터의 복구를 위한 OT 시스템 백업 이미지 포함 백업 데이터 확보 (d) 중요 시스템의 필수 데이터 백업 유지 및 필요 시 정리(clean-up) 수행 (e) 오프라인 백업 보관 및 정리 수행 (f) 백업 및 복구 절차의 주기적 테스트 수행 **[DCSA 5.1.3 구현]**	
비고		

통제항목	D.3.3 사이버 보험		Optimized
레퍼런스 상세	BIMCO	사이버 사고는 경제적 손실이나 손상된 데이터를 복구하는 비용을 초래할 수 있습니다. 이러한 손실은 일반적으로 보험의 대상이 아니지만, 독립형 랜섬웨어 보험 상품은 현재 해상 및 비해상 보험 시장 모두에서 제공되어 이러한 리스크에 대비할 수 있습니다. 그러나 손실의 빈도, 심각도 또는 물리적 피해의 가능성에 대한 데이터가 제한적이며, 시스템 전반에 영향을 미치는 리스크는 보험사에게 주요한 언더라이팅 과제로 작용합니다. **[BIMCO 10.6 사이버 사고로 인한 손실]** 성공적인 사이버 공격은 다음과 같은 보험 관련 영향을 초래할 수 있습니다: • 인명 피해, • 오염, • 화물 손실/손상, • 화물 장비 또는 재산 손해, • 영업 중단, • 책임, • 생산 손실, • 데이터 손실, • 평판 손실, • 기타 결과적 손해. **[BIMCO 10.6 사이버 사고로 인한 손실]** 2017년 로이드(Lloyd's of London)의 연구에 따르면, 사이버 사고는 시스템 전체에 영향을 줄 수 있는 체계적 리스크(systemic risk)으로 발전할 수 있으며, 이에 따라 단일한 모니터링 및 정량화 접근법은 적합하지 않을 수 있습니다. 사이버 사고 노출은 신속하게 진화하고 있으며, 적절한 통제 조치 하에서 언더라이팅되고 총노출 및 한도 역시 적절하게 모니터링되어야 합니다. **[BIMCO 10.6 사이버 사고로 인한 손실]** 자산 손해에 대한 보장 사이버 사고로 인한 손해를 보장하는 보험 솔루션은 회사별로 다르게 마련될 수 있으며, 현재 상태는 다음과 같이 요약됩니다: • 일부 지역 보험 시장은 여전히 사이버 관련 손해를 보장 제외 대상으로 권고합니다. 가장 널리 사용되는 제외 조항은 CL380 (Institute Cyber Attack Exclusion Clause)이며, 화물, 에너지, 초과 손해, 선체, 책임, 특수부문 등 해운 업종 전반에 사용됩니다. 또 다른 널리 사용되는 제외 조항은 American Institute Cyber Exclusion Clause (2015년 1월 6일)입니다. • 일부 보험 상품은 사이버 리스크를 모든 리스크 포괄(all-risk) 보장에서 명시적으로 제외하며, 명시적으로 언급되지 않은 경우 "침묵 보장(silent cover)"으로 간주될 수 있습니다. 하지만 보험 시장에서는 이러한 침묵 보장도 점차 재검토되고 있다는 점에 유의해야 합니다. • 마지막으로 "재포함(Buy-back)" 솔루션이 있습니다. 이는 계약상 제외된 리스크를 추가 보험료를 조건으로 다시 포함시킬 수 있는 선택지를 제공하는 방식입니다. 단, 이 역시 사전에 정의된 조건 및 추가 비용이 요구됩니다.	

통제항목	D.3.3 사이버 보험	Optimized
		회사들은 사이버 사고 및 그로 인한 피해를 보장하는 보험 증권이 실제로 해당 리스크를 보장하는지 사전에 보험사/브로커와 확인할 것이 권장됩니다. 보험 시장의 가이드라인에 따르면, 보험사는 보장 심사 시 회사의 사이버 리스크 인식 수준과 비기술적 절차에 대해 질문할 수 있으며, 이에 대비한 정보 제공이 필요합니다. **[BIMCO 10.6 사이버 사고로 인한 손실]** 책임 보장 P&I 클럽(P&I Club)에 연락하여, 선박 소유자 및 용선자가 선박 운영과 관련하여 제3자에 대한 책임(및 관련 비용)에 대해 어떤 보장이 제공되는지를 자세히 확인하는 것이 권장됩니다. [BIMCO 10.6 사이버 사고로 인한 손실] 예를 들어, 선박의 항해 또는 기계 시스템의 오작동이 범죄 행위나 우발적인 사이버 사고로 인해 발생한 경우, 그 자체만으로 일반적인 P&I 보장에서 제외되는 사유가 되지는 않습니다. 사이버 사고와 관련된 청구가 제기될 경우, 청구자는 사이버 대비 수준이 불충분하다는 이유로 청구의 정당성을 주장할 수 있습니다. 따라서 회사가 합리적인 주의 의무를 다하고 사이버 리스크를 적절히 관리하고 있음을 입증할 수 있어야 한다는 점이 더욱 중요해집니다. **[BIMCO 10.6 사이버 사고로 인한 손실]** 사이버 사고로 인해 발생할 수 있는 많은 손실은 선박의 운영 과정에서 생기는 제3자에 대한 법적 책임의 성격이 아니기 때문에 P&I 보험의 보장 대상이 아닐 수 있습니다. 예를 들어, 랜섬웨어로 인한 금전적 손실이나 암호화되어 손상된 데이터를 복구하는 비용 등은 보장 항목에 포함되지 않을 수 있습니다. **[BIMCO 10.6 사이버 사고로 인한 손실]** 그러나 일반적인 P&I(개인보험) 담보에는 전쟁 위험 제외 조항이 적용되며, 전쟁 또는 테러 위험과 관련된 사이버 사고는 일반적으로 보장되지 않습니다. 많은 사이버 공격이 다양한 국가 위협 행위자와 연관되어 있기 때문에, 보험사가 국가 위협 행위자에 의한 이러한 공격을 전쟁 행위로 간주할 가능성이 있는지를 파악하는 것이 중요합니다. **[BIMCO 10.6 사이버 사고로 인한 손실]** 전세 계약자를 위한 사이버보안 조항 해운업계 단체들은 표준 사이버보안 조항을 개발했으며, 이를 용선계약서에 포함하는 것을 고려할 수 있습니다. 사이버 사고 관련 정보를 공유하고, 이를 통해 상대방이 사이버 사고의 영향을 완화하거나 예방할 수 있도록 지원하는 것의 중요성이 강조됩니다. **[BIMCO 10.6 사이버 사고로 인한 손실]**
비고		

해운사 보안 요구사항
대응 가이드