36 Myeongji ocean city 9-ro,
Gangseo-gu, Busan, 618-814
Republic of Korea

Phone : +82-70-8799-8342
Fax : +82-70-8799-8319
E-mail: parkjh@krs.co.kr
Person in charge: PARK Jihyun

ISM/ISPS/MLC 동향

수신(Recipients): ISM 담당자

번호(No.) : 2021-04 날짜(Date) : 2021년 9월 30일

제 목(subject) : 사이버 리스크 관리 절차 강제적용 기국 추가 안내

지난 2017년 MSC 98차 회의 결과(Res.MSC.428(98))에 따라 IMO에서는 2021년 1월 1일 이후 도래하는 첫번째 사업장 연차심사까지, 회사의 안전관리시스템(SMS)상 사이버 리스크 관리(CRM) 절차가 수립될 수 있도록 각 기국에 요청하였습니다.

마샬 아일랜드, 싱가폴, 미국 등 일부 기국은 Res.MSC.428(98)를 강제 적용하여 CRM 절차의 수립/시행을 요구하는 자국 지침(Circular)를 발행하였고, 우리 선급에서도 지난 2019년 동향지(2019-02)를 통해 상세 지침을 안내한 바 있습니다.

상기의 기국을 포함하여, 최근 CRM 절차의 수립/시행을 강제 적용하고 있는 기국(총 22개국)을 아래와 같이 안내하오니, 해당 국적의 선박을 운항하는 사업장에서는 첨부의 '**CRM 점검표 및 점검항목 해설 지침**'을 참고하시어 회사의 안전관리시스템(SMS)에 CRM 절차를 수립하시고, 사업장 및 선박에서 시행하여 주시기 바랍니다.

Antigua and Barbuda	Australia	Bahamas	Barbados	Cyprus
Faroe Islands	Georgia	Germany	Greece	India
Isle of Man	Liberia	Malaysia	Marshall Islands	Myanmar
Palau	Singapore	St. Kitts and Nevis	St. Vincent and The Grenadines	Togo
Vanuatu	U.S.A and all ships calling at U.S.A ports			

첨부 - CRM 점검표 및 점검항목 해설 지침 – DOC/SMC 각 1부 (끝)

협약심사팀장

DOC CHECK LIST for Cyber Risk Management(CRM)

이 점검표는 Res.MSC.428(98)에 따른 해상 사이버 리스크에 대한 안전관리체제의 효과적인 이행의 검증을 위해 참고용으로 제공되는 것으로, 사업장심사 점검표와 더불어 사용하여 주시기 바랍니다.

※ 점검표의 해당 항목 점검결과에 대한 표시방법

☒ or ☑ : 표본검증 하였음 (Verified as sampling basis)

☐ : 해당되지 않음 (Not Applicable)

* 표본검증 시, 부적합사항이 식별되는 점검항목은 그 내용을 부적합보고서에 기재한다.

No.	Code	점검 항목	결과
1	1	**사업장은 사이버 자산(cyber assets)에 대하여 사이버 리스크 평가를 시행하였고, 사이버 리스크 관리(CRM) 절차를 SMS 에 반영하였는가?** - ISM Code 1.2(목표) 및 1.4(기능적요건)를 반영한 CRM 절차 보유 확인 - 사이버 자산 식별 확인 (소프트웨어, 하드웨어, 외부위탁 포함) - 선박에 제공하는 데이터 전송 방식에 따른 리스크 관리항목 확인	
2	3	**사이버 관련 사업장의 지휘 및 의사결정 체계가 수립되어 있는가?** - 책임과 권한의 식별. 담당자 지정 확인 (DP 포함)	
3	6	**육상직원 및 선원에 대한 사이버 리스크 관련 교육이 제공되고 있는가?** - 사업장의 CRM 에 대한 일반적인 내용이 교육되는지 확인 - 사이버 사항이 선원에게 교육되도록 절차 및 자료가 마련되어 있는지 확인 - 사이버 관련 최신 정보가 선박에 제공되고 있는지 확인	
4	6	**선박에서 요청된 지원은 적절히 제공되고 있는가?** - 하드웨어 / 소프트웨어 / 업데이트 패치 / 사이버 관련 정보 등	
5	7	**사이버 리스크 평가 결과로 요구되는 선박의 필수적인 운항업무(Key Shipboard Operation) 관련하여 별도 조치(절차)에 대해 적절히 반영 되었는가?** - 관리항목(Existing Controls)에 특별한 조치(절차)가 필요하다고 식별된 내용 확인 - 방문자의 물리적 보안 및 USB 등 이동식 미디어 관리, 정보보호 서약서 등	
6	8	**선박의 사이버 침해에 대비한 사업장의 비상대응 절차가 마련되어 있는가?** - 선박에 기술적 지침을 줄 수 있는 사이버 기술 인력의 연락처 확인	
7	6 8	**사업장의 사이버 침해에 대비한 비상대응 절차가 출력물(hard copy)로서 마련되어 있는가?** - 비상대응 및 복구절차 수립 및 담당자의 숙지도 확인 - 사이버 침해가 선박에 영향을 끼치지 않기 위한 조치 확인	
8	10	**사이버 리스크 평가 결과로 관리가 요구되는 사이버 장비는 유지보수 절차가 수립되고 이행되고 있는가?** - 주기적인 점검 / 보수 / 업데이트 / 예비품 관리 - 담당자 지정 / 관리기록 유지	
9	12	**사이버 관련 절차(시스템) 및 관리항목(Existing Controls)의 효과성 및 적절한 이행이 내부심사, 선장검토 및 경영검토 시 포함되어 검증/검토/평가되었는가?** - 내부심사자의 자격 확인 - 내부심사 점검표 또는 결과 보고서 확인 (검증 범위 및 검증 항목) - 선장검토 및 경영검토 대상에 CRM 항목을 포함하고 있는지 확인	
10	12	**외부 위탁되는 사이버 업무 및 위탁 관리되는 사이버 자산은 주기적으로 검증/검토/평가 되는가?** - 위탁되는 시스템 및 자산에 대한 검증/검토/평가 절차 및 이행기록 확인	

Company Name : Date :

Company Representative (with Signature) : Auditor (with Signature) :

DOC CHECK LIST for Cyber Risk Management(CRM)

별첨. 점검항목 해설

1. 사업장은 사이버 자산(cyber assets)에 대하여 사이버 리스크 평가를 시행하였고, 사이버 리스크 관리(CRM) 절차를 SMS 에 반영하였는가?

< Reference 1. 자산 유형 예시>

유형자산	무형자산
스토리지 서버(UNIX, Linux 등) 네트워크(라우터, 스위치, 허브 등) 보안시스템(방화벽, IDS, IPS, VPN 등) 단말기(PC, 노트북, 랩탑) 매체(USB 메모리, 디스크, 테이프 등)	소프트웨어(OS, 패키지 소프트웨어, 백신 등) 응용프로그램 데이터(임직원 정보, 회사 영업 정보 등) 문서(도면 등)

< Reference 2. Recommended Cyber Asset Identification List - Company>

Critical Index Assessment for Hankook Shipping (Busan Office)

No.	Category	Assets	Model	Description	Application	Location	Out-sourcing	C	I	A	CrI
1	Server	File Server-1	SVFL-T8000	File Server	Windows Server 2012 R2	KR Tech.	O	2	3	2	3
2	Server	Operation Server-1	SVOP-K2000	Operation Server	Windows Server 2012 R2	KR Tech.	O	2	3	2	3
3	Network	UTM-1	Masterwall	Unified Security Management System	-	Server Room	O	2	3	3	3
4	Network	Main Switch	CS1208	8 Port - Main Switch for network	-	Server Room	O	2	3	3	3
5	Application	E-mail	Office 365	E-mail service for office	Office 365	Microsoft	O	2	2	3	3
6	Application	E-mail	Skyfile	E-mail service for ship	Skyfile	Skyfile	O	2	3	3	3
7	Application	Cloud	Onedrive	Data Backup	Onedrive	Microsoft	O	2	3	2	3
8	Application	PMS system	-	Planned maintenance system for ship	OPMS application	N/A	X	2	3	2	3
9	PC	Personal PC	LG-GR17	Laptop	Windows 10-Professional	Each of employee	X	2	3	3	3

- 외부에 위탁하여 운영하는 자산 및 서비스도 포함
- 선박 운항과 관련하여 해당 시스템의 완전성-데이터는 얼마나 정확해야 하는지 (Integrity) 및 가용성-항시 가용 가능해야 하는지 또는 잠시 작동 안해도 되는지 (Availability) level 식별
- 사이버 자산에 위해를 끼칠 수 있는 위협(Threat)과, 그 위협에 대한 자산의 취약점(Vulnerability)을 식별

< Reference 3. General Threats>

* 승인되지 않은 접근 (논리적/물리적)
* 악의적인 (Malicious) code에의 감염

< Reference 4. General Vulnerabilities>

* 패스워드가 없거나, 간단하거나, 노출되어 있음
* 네트워크에 방화벽이 설치되어 있지 않음
* 운영 시스템이 업데이트 되지 않음
* Malware 방지 백신 프로그램이 설치되지 않음
* 물리적 접근 제어가 적절하지 않음
* 이동식 저장 매체 관리가 적절하지 않음

* 참고 : 선박의 경우, ISPS Code로 인해 자연적으로 물리적 접근이 통제되고 있으나, 사업장의 경우 사이버 자산으로의 별도의 접근 통제 절차를 마련 할 필요가 있음.

DOC CHECK LIST for Cyber Risk Management(CRM)

< Reference 5. Recommended Cyber Risk Assessment List - Company>

Cyber Risk Assessment Worksheet - PC

Asset	Threats	Threat Agents	Potential Cause	Potential Consequence	Existing Controls	VI	TI	CrI	RI	Proposed Controls	RI^2
Personal PC	Unauthorized network access	External personnel	Lack or weak access password policy for network	1) Disable the PC 2) Manipulation of data, record and history 3) Leakage of information 4) Ransoming system for monetary compensation 5) Spread malicious code to other equipment through network	1) Set password more than 8 characters with number 2) Change password periodically (half year)	1	2	3	2.0		
			Lack or weak account management		1) Establish procedure to assign and invalidate access authority for employee	1	2	3	2.0		
			Weak configulation of security setting		1) Initiate security function for the new/changed network system 2) Change default security setting for the new/changed network system	1	2	3	2.0		
			Weak protective network achitecture to intrusion		1)Using VPN in the IT network 2) Install the security devices(UTM) in the network	1	2	3	2.0		
			Lack or weak firewall function		1) Install the firewall in the proper position of network 2) Change setting of security function for firewall 3) Initiate security function for the firewall	2	2	3	4.0	1) Change to high functioned firewall	2
			Lack of access log measures for network		1) Establish measures to record access log 2) Establish measures to prevent change and remove log 3) Procedures to maintain and periodical check the record	1	2	3	2.0		
			Lack of monitoring measures for network		1) Install the real-time monitoring and alert system with exclusive cable line 2) Establish procedures to prevent unauthorized access to monitoring device 3) Establish procedures to maintain and periodical check the record	1	2	3	2.0		
			Lack of supervising measures for network service provider (outsourcing company)		1) Company include articles for cyber responsibility on the network service providing contract 2) Get the security pledge for the external personnel of network company	1	2	3	2.0		

- 중요한 사이버 자산으로 식별되어 취약성을 평가할 필요가 있는 자산을 대상으로 함
- 식별된 위협과 취약성에 대하여 현재 취하고 있는 조치들(Existing Controls)을 나열하고, 그에 따른 리스크 수준(RI)을 평가. 필요 시 추가 조치 제시하며, 예상(기대)되는 잔여 리스크 수준을 평가함(RI^2)

< Reference 6. Guide on Office Cyber Risk Management Level>

	기본적인 범위만 관리	강화된 관리
조건	- 선박의 IT가 선박 운항(OT)에 영향을 끼치지 않는 선박들만을 관리 - 선박과 데이터는 e-mail을 통해서만 교환하며, 일시적인 위성 연결을 통해 시행	인터넷 환경에 노출되어 있는 선박을 관리함
관리	* 감염 측면 관리. - 데이터를 선박으로 전송하는 PC의 OS를 포함한 Application들의 최신화 관리 - 백신 프로그램 설치 및 최신화 관리 - E-mail 서비스 업체 관리	* 감염에 추가하여 침투 측면 관리 - 데이터 흐름 지도(topology) 등을 통한 네트워크 망의 취약성 추가 검토 필요 - 보다 엄격한 사이버 통제절차 수립 필요 (e.g. 개인 단말기 관리, Account 관리 및 권한 설정 등)

- 선박에서의 일시적인 E-mail 접속만을 통해 선박에 데이터가 제공되는 경우, 기본적인 Malware monitoring & filtering 수준으로 관리될 수 있겠지만, 선박에 인터넷 환경이 제공되는 경우에는, unauthorized access측면까지 고려하여 회사 네트워크가 복합적인 취약성 분석이 시행 될 필요가 있음

DOC CHECK LIST for Cyber Risk Management(CRM)

2. 사이버 관련 사업장의 지휘 및 의사결정 체계가 수립되어 있는가?

- 책임과 권한의 식별. 담당자 지정 확인 (DP포함)
- 상황 발생 시 연락처 및 연락 방법이 정의되어 있어야 하며, 직원이 인지하고 있어야 함.
- 기존의 조직도 및 의사결정 체계 준용 가능하지만 사이버 관련 문구 삽입하여 명확화 필요 있음
- 필요 시 사이버 관련 기술적 지원(Technical Advisor)이 가능한 연락처가 명기 될 필요 있음

3. 육상직원 및 선원에 대한 사이버 리스크 관련 교육이 제공되고 있는가?

- 사이버 리스크 평가에 따른 조치(Existing Controls)에서 '교육'으로 식별한 사항이 실제로 시행되었는지 기록 확인
- 주기적인 교육계획에 사이버 리스크 교육 반영 및 시행 기록 확인. 특히 비상상황에 대한 대비 및 대응 내용이 교육 (주기 및 필요성은 회사의 판단에 따름)

< Reference 8. Recommended basic awareness items>

* 일반적인 사이버 리스크의 종류 및 기법
* 패스워드 사용, 주기적인 운영시스템(OS)의 업데이트, 백신 설치 등의 보호 조치
* 이메일 및 인터넷 사용 주의사항
* 개인적인 사이버 자산 사용과 업무용 사이버 자산 사용의 철저한 분리 (이동식 저장매체 포함)
* 주기적인 데이터 백업의 중요성

- 선원 교육을 위한 절차 및 교육자료가 마련되어 있는지 확인

4. 선박에서 요청된 지원은 적절히 제공되고 있는가?

- 사이버 자산의 운영, 유지보수 등에 필요한 하드웨어/소프트웨어/업데이트 패치 등이 적절히 요청되어 공급됨을 확인

5. 사이버 리스크 평가 결과로 요구되는 선박의 필수적인 운항업무(Key Shipboard Operation) 관련하여 별도 조치(절차)에 대해 적절히 반영 되었는가?

- Existing Controls에 특별한 조치(절차)가 필요하다고 식별된 내용이 있다면 (e.g. 개인 PC의 화면보호기 정책, 전출/퇴직자 Account 관리, 외부인 접근통제 절차 등) 그러한 내용이 적절히 절차나 점검표에 반영되어 이행되고 있는지 확인.

6. 선박의 사이버 침해에 대비한 사업장의 비상대응 절차가 마련되어 있는가?

- 육상의 책임자 및 담당자 지정. 담당자의 비상대응 숙지도 확인.
- 대응 및 회복에 대한 기술적 지원을 받을 수 있는 연락처를 확보 하였는지 확인

7. 사업장의 사이버 침해에 대비한 비상대응 절차가 출력물(hard copy)로써 마련되어 있는가?

- 사이버 침해 시 전자문서는 가용 가능하지 않을 수 있기 때문에 비상대응 매뉴얼은 출력물로 담당 사관이 인지 할 수 있는 곳에 비치되어 있어야 함
- 육상의 책임자 및 담당자 지정. 담당자의 비상대응 숙지도 확인
- 복구에 대한 기술적 지원을 받을 수 있는 연락처 확보 하였는지 확인
- 선원관리팀, 선박관리팀과 같은 부서는 선박과 잦은 데이터 교환 또는 메일 송수신이 이루어지므로 사이버 자산에 침해가 발생하는 경우 선박에 전파되지 않도록 하는 조치 마련 필요함

DOC CHECK LIST for Cyber Risk Management(CRM)

- 사업장의 IT는 선박의 OT와는 달리 즉각적인 대응이 반드시 필요하지는 않음을 고려할 필요 있음.

8. 사이버 리스크 평가 결과로 관리가 요구되는 사이버 장비는 유지보수 절차가 수립되어 적절히 이행되고 있는가?

- 사이버 리스크 평가 결과로 특정 관리가 필요한 사이버 자산은 주기적인 정비 또는 점검 등의 관리 절차 수립 확인
- 장비별로 담당자 / 점검 및 보수 주기 / 예비품 개수 및 관리방안 등 설정
- 점검 / 테스트 / 보수 기록 확인

9. 사이버 관련된 절차(시스템) 및 관리항목(Existing Controls)의 효과성 및 적절한 이행이 내부심사, 선장검토 및 경영검토 시 평가되는가

- 내부심사 점검표 또는 보고서에 CRM 내용을 포함하고 있는지 확인.
- 내부심사자는 적절히 검증 할 수 있는 자격이 있는지 확인 (사이버 관련 교육 이수 등)
- 점검표/보고서/결과서 등에 일반적인 문구로만 되어있고 CRM 내용이 없다 할지라도 사이버 내용을 포함하여 다루고 있는 것으로 간주 할 수 있음(검토 하였으나 특이사항이 없음). 이런 경우 인터뷰 등을 통해 실제로 검증하고 있는지 확인 필요
- 선장검토 및 경영검토 대상에 사이버 리스크 관리 항목을 포함하고 있는지 확인.

10. 외부 위탁되는 사이버 업무 및 위탁 관리되는 사이버 자산은 주기적으로 검증/검토/평가되는가?

- 외부 업체를 통해 관리되고 있는 사이버 자산 및 외부 사이버 서비스에 대한 주기적인 검증/검토 필요하며 이에 대한 기록 확인. 이 역시 선박에 인터넷 환경에 제공되는 경우 보다 강화하여 적용할 필요 있음.

  e.g.1) 서버 및 네트워크 관리 업체에 대한 주기적인 2자(자체) 검증

  e.g.2) 시장에서 신뢰할 만 하다고 인정되는 e-mail 서비스 업체 사용 (e.g. Microsoft)

  e.g.3) 사이버 관련 3자 검증 및 증서 요구 (e.g. ISO27001, 한국선급 사이버 보안 인증) [끝]

SMC CHECK LIST for Cyber Risk Management(CRM)

이 점검표는 Res.MSC.428(98)에 따른 해상 사이버 리스크에 대한 안전관리체제의 효과적인 이행의 검증을 위해 참고용으로 제공되는 것으로, 선박심사 점검표와 더불어 사용하여 주시기 바랍니다.

※ 점검표의 해당 항목 점검결과에 대한 표시방법

☒ or ☑ : 표본검증 하였음 (Verified as sampling basis)

☐ : 해당되지 않음 (Not Applicable)

* 표본검증 시, 부적합사항이 식별되는 점검항목은 그 내용을 부적합보고서에 기재한다.

No.	Code	점검 항목	결과
1	1	**사업장은 사이버 자산(cyber assets)에 대하여 사이버 리스크 평가를 시행하였고, 사이버 리스크 관리(CRM) 절차를 SMS 에 반영하였는가?** - ISM Code 1.2(목표) 및 1.4(기능적요건)를 반영한 CRM 절차 보유 확인 - 사이버 리스크 평가서의 사이버 자산 목록 확인 - ECDIS 가 설치된 선박은 ECDIS 평가 내용, 그렇지 않은 선박은 이외 장비 확인	
2	3	**사이버 관련 사업장의 지휘 및 의사결정 체계가 수립되어 있는가?** - 책임과 권한의 식별. 담당자 지정 확인 - 선장 및/또는 선박 사이버 관리 책임자의 책임과 역할 확인	
3	6	**선원에 대한 사이버 리스크 관련 교육이 시행 되었는가?** - 항해/기관사관의 담당기기의 사이버 관련 육상 또는 신규승선 교육 기록 확인 - 주기적인 교육계획에 사이버 리스크 교육 계획 반영 및 시행 기록 확인	
4	6	**선박으로의 지원은 적절히 제공되고 있는가?** - 하드웨어 / 소프트웨어 / 업데이트 패치 / 사이버 관련 정보 등	
5	7	**사이버 리스크 평가 결과로 요구되는 선박의 필수적인 운항업무(Key Shipboard Operation) 관련하여 별도 조치(절차)에 대해 적절히 반영 되었는가?** - 관리항목(Existing Controls)에 특별한 조치(절차)가 필요하다고 식별된 내용 확인 - 방문자의 물리적 보안 및 USB 등 이동식 미디어 관리, 정보보호 서약서 등	
6	8	**사이버 침해에 대비한 비상대응 절차는 적절히 수립되어 선원에게 교육 되었는가?** - ECDIS 등 기타 하나 이상의 장비에 대한 비상 대응 숙지도 확인 - 사이버 회복 또는 복구 수단 확인	
7	6 8	**선박의 사이버 침해에 대비한 비상대응 절차가 출력물(hard copy)로서 마련되어 있는가?** - ECDIS 및 기타 하나 이상의 주요 사이버 장비에 대한 비상 대응 매뉴얼 확인 - 사이버 관련 비상연락처 확인(게시 및 숙지 여부)	
8	9	**선박의 사이버 침해에 대한 부적합 사항, 사고 및 위험 상황에 대한 보고 및 분석 절차가 수립되고 이행되고 있는가?** - 사업장의 기존 사고 및 부적합사항 보고 절차 및 양식 준용 가능	
9	10	**사이버 리스크 평가 결과로 관리가 요구되는 사이버 장비는 유지보수 절차가 수립되고 이행되고 있는가?** - 주기적인 점검 / 보수 / 업데이트 / 예비품 관리 - 담당자 지정 / 관리기록 유지	
10	12	**사이버 관련 절차(시스템) 및 관리항목(Existing Controls)의 효과성 및 적절한 이행이 내부심사, 선장검토 및 경영검토 시 포함되어 검증/검토/평가되었는가?** - 내부심사자의 자격 확인 - 내부심사 점검표 또는 결과 보고서 확인 (검증 범위 및 검증 항목) - 선장검토 및 경영검토 대상에 CRM 항목을 포함하고 있는지 확인	

Vessel Name : Date :

Captain (with Signature) :_____ Auditor (with Signature) :_____

SMC CHECK LIST for Cyber Risk Management(CRM)

별첨. 점검항목 해설

1. 사업장은 사이버 자산(cyber assets)에 대하여 사이버 리스크 평가를 시행하였고, 사이버 리스크 관리(CRM) 절차를 SMS 에 반영하였는가?

<Reference 1. Recommended Cyber Asset Identification List - Ship>

Critical Index Assessment for M/V GEO BUK

			Character			Ease of Access			Assessment			
Category	Assets	Interlocking Equipment	Q'ty	Output	Mach. Oper only	IT Conn	OT Conn	Ext Conn	C	I	A	CrI
NAV	Anemometer & Anemoscope	VDR, RADAR	1	Data	x	x	o	0	1	2	1	1
NAV	Clinometer	-	1	Data	o	x	x	0	1	2	1	1
NAV	Auto pilot system	Steering Gear, VDR, BNWAS, Magnetic Compass, SPEED LOG, ECDIS, RADAR, AIS, GPS	1	Control	x	x	o	1	1	3	3	3
NAV	Gyro compass	Steering Gear, VDR, BNWAS, Magnetic Compass, SPEED LOG, ECDIS, RADAR, AIS, GPS	1	Critical Data	x	x	o	1	1	3	2	2
NAV	Magnetic Compass	-	1	Data	o	x	o	0	1	2	1	1
NAV	Rudder Angle Indicating System	ECDIS, VDR	3	Critical Data	x	x	o	0	1	3	3	3
NAV	Echo Sounder	ECDIS, VDR	1	Critical Data	x	x	o ④	1	1	3	3	3 ⑥
NAV	Speed Log ①	VDR, ECDIS	1	Critical Data ②	x	x ③	o	1	1 ⑤	3	3	3
NAV	RADAR System	GPS, VDR, ECDIS, GYRO COMPASS, SPEED LOG, AIS	2	Critical Data	x	x	o	1	1	3	3	3
NAV	ECDIS	GPS, ECHO SOUNDER, VDR, ECDIS, GYRO COMPASS, SPEED LOG, AIS, ANEMOMETER	2	Critical Data	x	o	o	3	1	3	3	3
NAV	DGPS	ECDIS, RADAR, AIS	2	Critical Data	x	x	o	1	1	3	2	2

① 가능한 모든 선박 장비를 1차 평가 대상으로 나열하여, 누락되는 자산이 없도록 함.

② 선박 운항에 있어서의 장비의 역할(Output)이 무엇인지를 식별하여, 중요도를 식별할 수 있음.

③ Data Connection이 거의 없고, 기계적으로만 작동하는 사이버 위협의 발생이 낮은 기기들은 사이버 장비에서 제외하기 위해 별도로 식별해 둠

④ 네트워크 취약성을 식별하기 위하여 연결 상태 식별 필요. (Interlocking, IT Connection 여부)

⑤ 네트워크에 연결되어 있지 않다 하더라도, USB Port와 같은 연결을 통한 사이버 침해 가능성을 식별하기 위해 외부 연결(빈도) 확인.

⑥ 선박 운항과 관련하여 해당 시스템의 완전성-데이터는 얼마나 정확해야 하는지 (Integrity) 및 가용성-항시 가용 가능해야 하는지 또는 잠시 작동 안해도 되는지 (Availability) level 식별

SMC CHECK LIST for Cyber Risk Management(CRM)

< Reference 2. Recommended Cyber Risk Assessment List>

Cyber Risk Assessment Worksheet - Navigation equipment

Asset	Threats	Threat Agents	Potential Cause	Potential Consequence	Existing Controls	VI	TI	CrI	RI	Proposed Controls	RI^2
ECDIS	Unauthorized network access (Note: It is assumed that two ECDIS was installed without paper chart, and the elec.chart are updated through network system everyweek. But the system do not provide account function for each user.)	External personnel	Lack or weak access password policy for network	1) System is inoperatible 2) Improper data/information is transferred to other OT 3) Manipulation of data and record 4) Leakage of information	1) Set network password more than 8 characters including number 2) Change password periodically (half year)	1	2	3	2.0		
			Lack or weak account management		1) Procedure to assign and invalidate access authority of network for employee	1	2	3	2.0		
			Weak configulation of security setting		1) Initiate security function for the new/changed network system 2) Change default security setting for the new/changed system	1	2	3	2.0		
			Weak network architecture to intrusion		~~Communicate only by industry protocol without additional access port including wireless network~~ 1) Using VPN in the IT network 2) Installing UTM in the interface of IT-OT ~~OT network is seperated with IT network~~ ~~Install the security devices in the interface of OT and IT~~	1	2	3	2.0		
			Lack or weak firewall function		1) Installing UTM which has own firewall function in the interface of IT-OT 2) Change setting of security function for firewall 3) Initiate security function for the firewall	1	2	3	2.0		
			Lack of access log measures for network		1) Measures to record access log for network 2) Measures to prevent change and remove log 3) Procedures to maintain and periodical check the record	1	2	3	2.0		
			Lack of monitoring measures for network		1) There is not monitoring measures for network	2	2	3	4.0	1) Install the monitoring device with exclusive line	2

- 사이버 자산 식별 단계에서 주요 자산으로 식별되어 취약성을 평가할 필요가 있는 자산을 대상으로 함
- 사이버 자산에 위해(threat)를 끼칠 수 있는 위협(Threat)의 종류와, 그 위협에 대한 사이버 자산의 취약점(Vulnerability)을 식별

< Reference 3. General Threats>

* 승인되지 않은 접근 (논리적/물리적)
* 악의적인 (Malicious) code에의 감염

< Reference 4. General Vulnerabilities>

* 패스워드가 없거나, 간단하거나, 노출되어 있음
* 네트워크에 방화벽이 설치되어 있지 않음
* 운영 시스템이 업데이트 되지 않음
* Malware 방지 백신 프로그램이 설치되지 않음
* 물리적 접근 제어가 적절하지 않음
* 이동식 저장 매체 관리가 적절하지 않음

- 취약성에 대하여 현재 시행하고 있는 조치들(Existing Controls)을 나열하고, 그에 따른 리스크 수준(RI)을 평가. 필요 시 추가 조치를 제시하며, 예상(기대)되는 잔여 리스크 수준을 평가함(RI2)
- 현재 취하고 있는 조치들(Existing Controls) 및 추가 조치의 적절한 시행 여부(기록)를 확인함.
- Existing Controls에 특별한 조치(절차)가 필요하다고 식별된 내용이 있다면 (e.g. ECDIS 차트 업데이트 시 이동식 디스크의 사전 scanning) 그러한 내용이 적절히 절차에 반영되어 있고 실제로 이행되고 있는지 확인.
- Existing Controls에 기기의 주기적인 정비/테스트가 포함된다면, 정비/테스트 절차 및 기록은 Code 10.2에 따라 시행되어야 함. 만약 그것이 본선 자체적으로 시행이 불가능하여 육상의 지원이 필요하다면 육상정비절차에 따라 시행 되어야 하며, 본선에서 자체적으로 하기 위한 kit 및 spare가 필요한 경우 보급 및 보관 절차에 따라 시행되어야 함. 이 모든 것은 사이버 만을 위한 별도의 절차는 반드시 필요하지는 않으며, 회사의 기존의 절차를 준용할 수 있음.
- 작동의 불능이 선박의 위험한 상황을 초래하는 사이버 자산은 이중화, 백업 또는 주기적 점검등의 방법으로 신뢰도를 향상시킬 필요 있음

2. 사이버 관련 지휘 및 의사결정 체계가 수립되어 있는가?

- 선박 사이버 리스크 책임자, 회사의 사이버 책임자 등이 ISM Code에 따라 적절하게 지정되어 있어야 함.
- 선박 사이버 리스크 관리 책임자는 선장이 될 수 있으나, 그렇지 않은 경우 선장과의 사이버 관련 책임과 권한이 명확하게 구분되어 있어야 함.
- 상황 발생 시 연락처 및 연락 방법이 정의되어 있어야 하며, 선원이 인지하고 있어야 함.
- 기존의 조직도 및 의사결정 체계 준용 가능하지만 사이버 관련 문구 삽입하여 명확화 할 필요 있음
- 비상대응 관련, 사이버 관련 기술적 지원(Technical Advisor)이 가능한 연락처가 명기 될 필요 있음

3. 선원에 대한 사이버 리스크 관련 교육이 시행 되었는가?

- 사이버 리스크 평가에 따른 조치(Existing Controls)에서 '교육'으로 식별한 사항이 실제로 시행되었는지 기록 확인
- 선장은 선박의 최고 책임자로서, 사이버 관련한 회사의 절차를 숙지 할 필요 있음.
- 항해/기관사관의 육상 또는 신규승선 교육 기록 확인. 주요 사이버 장비를 바로 다루게 될 책임사관으로서, 해당 장비의 사이버 관련 주의 사항, 특히 관리 절차 및 비상 대응 방법 등을 숙지 할 필요 있음
- 주기적인 교육계획에 사이버 리스크 교육 반영 및 시행 기록 확인. 특히 비상상황대응 내용이 교육될 필요 있음. 주기 및 교육범위는 회사의 판단에 따름

<Sample 5. Recommended basic awareness items>

* 일반적인 사이버 리스크의 종류 및 기법
* 패스워드 사용, 주기적인 운영시스템(OS)의 업데이트, 백신 설치 등의 보호 조치
* 이메일 및 인터넷 사용 주의사항
* 개인적인 사이버 자산 사용과 업무용 사이버 자산 사용의 철저한 분리 (이동식 저장매체 포함)
* 주기적인 데이터 백업의 중요성

SMC CHECK LIST for Cyber Risk Management(CRM)

4. 선박으로의 지원은 적절히 제공되고 있는가?

- 사이버 자산의 운영, 유지보수 등에 필요한 하드웨어/소프트웨어/업데이트 패치 등이 적절히 요청되어 공급됨을 확인

5. 사이버 리스크 평가 결과로 요구되는 선박의 필수적인 운항업무(Key Shipboard Operation) 관련하여 별도 조치(절차)에 대해 적절히 반영 되었는가?

- 사이버 리스크 평가 결과로 Existing Controls에 특별한 조치(절차)가 필요하다고 식별된 내용이 있다면 (e.g. ECDIS 차트 업데이트 시 이동식 디스크의 사전 scanning, 주기적인 Data Backup, 방문자의 물리적 보안 및 USB 등 이동식 미디어 관리, 정보보호 서약서 등) 그러한 내용이 적절히 절차나 점검표에 반영되어 이행되고 있는지 확인.

6. 사이버 침해에 대비한 비상대응 절차는 적절히 수립되어 선원에게 교육 되었는가?

- ECDIS 및 기타 하나 이상의 사이버 시스템의 담당자의 사이버 사고(incident) 발생 시 대응 확인
- 별도의 시나리오 구성이나 주기적인 훈련은 반드시 필요하지는 않음

7. 선박의 사이버 침해에 대비한 비상대응 절차가 출력물(hard copy)로써 마련되어 있는가?

- 사이버 침해 시 전자문서는 가용 가능하지 않을 수 있기 때문에 비상대응 매뉴얼은 출력물로 담당 사관이 인지 할 수 있는 곳에 비치되어 있어야 함. 보안 문서로써 인가되지 않은 폭로로부터는 보호될 필요 있음.
- 장비의 사이버 회복 및 복구는 일반적으로 육상 지원으로 이루어 질 수 있으나, 선박의 운항에 필수적인 기기는 필요에 따라 선상에서의 회복 및 복구가 요구될 수 있음
- ECDIS의 경우, 선박에 종이 해도 없이 2대의 ECDIS가 설치되어 있다면 사이버 관점에서는 사실상 장비의 이중화가 없는 것이나 마찬가지이기 때문에 사이버 비상대응은 매우 어려우며, 가능한 조치는 사실상 백업 및 복원 밖에 없음. 하지만 ECDIS가 백업 기능을 지원하지 않는 경우도 있기 때문에 이러한 경우 사이버 침해의 발생 가능성이 매우 낮도록 관리 조치(Existing Controls) 수준을 매우 높일 필요가 있음. 극단적인 경우 종이 해도 비치 및 관리 필요.
- 대응 및 회복에 대한 기술적 지원을 받을 수 있는 연락처 목록 필요.
- 기존의 비상 연락망 준용 가능하지만 사이버 관련 문구 삽입하여 명확화 할 필요 있음

8. 선박의 사이버 침해에 대한 부적합 사항, 사고 및 위험 상황에 대한 보고 및 분석 절차가 수립되고 이행되고 있는가?

- 사업장의 기존 사고 및 부적합 사항 보고 절차 및 양식을 준용하여 사용 가능함
- 사이버 침해에 대해 별도의 보고 절차가 있다면 적용 가능함

9. 사이버 리스크 평가 결과로 관리가 요구되는 사이버 장비는 유지보수 절차가 수립되고 이행되고 있는가?

- 사이버 리스크 평가 결과로 특정 관리가 필요한 장비, 특히 작동의 불능이 선박의 위험한 상황을 초래하는 사이버 자산은 주기적인 정비 또는 점검 등의 관리 절차 수립이 필요함.
- 장비별로 담당자 / 점검 및 보수 주기 / 예비품 개수 및 관리방안 등 설정되어 있는지 확인
- 점검 / 테스트 / 보수 등의 기록 유지

SMC CHECK LIST for Cyber Risk Management(CRM)

10. 사이버 관련된 절차(시스템) 및 관리항목(Existing Controls)의 효과성 및 적절한 이행이 내부심사, 선장검토 및 경영검토 시 평가되는가?

- 내부심사자는 적절히 검증 할 수 있는 자격이 있는지 확인 (사이버 관련 교육 이수 등)
- 점검표/보고서/결과서 등에 일반적인 문구로만 되어있고 사이버 내용이 없다 할지라도 사이버 내용을 포함하여 다루고 있는 것으로 간주 할 수 있음(사업장에서 검토 하였으나 특이사항이 없었을 수 있음). 이러한 경우 인터뷰 등을 통해 실제로 검증하고 있는지 확인 필요. 선장검토도 마찬가지로 적용 [끝]