ISM/ISPS/MLC Information

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

Phone : +82-70-8799-8344
Fax : +82-70-8799-8319
E-mail: kimgh@krs.co.kr
Person in charge : Kim Geun-hyeo

Recipients : Person in charge of ISM

No. : 2019-02 Date : 24 December, 2019

Subject : Information of KR audit application for company and ship's cyber security management

1. In the result of IMO MSC 98. IMO encourages Administrations to ensure the cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021.

2. The company which is holding Marshall Islands Document of Compliance(DOC) shall establish and implement cyber risk management(CRM) procedure and other Flag administrations are encouraged to establish CRM procedure.

3. In particular, it is strongly recommended that the company operating in the some of the major PSC regions should establish CRM procedure in the company's safety management system, since it may be imposed as PSC deficiency due to lack of the CRM after 2021.

4. In this regard, from 01 January 2020 to 31 December 2020 in the Interim, Initial, Annual, Intermediate and Renewal audit of Company and ship under Marshall Islands, the KR auditor shall verify the relevant requirements in accordance with attached checklists. If the CRM procedures have not been established and implemented, it will be identified as observation. In the other, after 01 January 2021, it will be identified as non-conformity.

5. In case of the other Flag administrations, if the CRM procedures have not been established and implemented during company and ship ISM audit after 01 January 2020, KR auditor will make the remark in the audit report concerning the recommendation to establish the CRM procedures. However, if the Flag administration issued the updated requirements, it shall be applied preferentially.

Attachment 1 : DOC Checklist for Cyber Risk Management – 1set
2 : SMC Checklist for Cyber Risk management – 1set (end)

General Manager

Statutory System Certification Team

DOC CHECK LIST for Cyber Risk Management(CRM)

This checklist was developed for reference to efficiently implement the cyber risk management in accordance with Res.MSC.428(98), and it is recommended to use this checklist in conjunction with the Checklist for ISM company audit.

※ Mark methods for the each questionnaire in a square box

☒ or ☑ : Verified as sampling basis

⊟ : Not Applicable

* If a check item is identified as a non-conformity on a sampling verification, it shall be recorded in the non-conformity report

No.	Code	Check items	Result
1	1	**Does the company implement cyber risk assessment for cyber assets and establish Cyber Risk Management (CRM) in the approved safety management systems?** - Check the CRM in accordance with ISM Code 1.2(objectives) and 1.4(functional requirements) - Check the identification of cyber assets (software, hardware, etc.) - Check the existing controls according to data transmission method provided to the vessel	
2	3	**Does the company establish allocation of responsibility and authority for CRM in the SMS?** - Check the identification of responsibility, authority and designated PIC.(D.P, Master, etc.)	
3	6	**Does the company provide any Cyber risk training with shore staff and crews?** - Check the cyber risk awareness training provided to the shore staff and crews - Check the updated information for cyber risk provided to the vessel	
4	6	**Does the company provide appropriate support at the request of the vessel?** - Hardware, Software, update patches, USB/LAN Blocker, information for Cyber risk, etc.	
5	7	**Does the company establish any additional procedure or existing controls in relation to key shipboard operation resulted from cyber risk assessment?** - Check the additional procedure or existing controls such as physical security for visitor, list of personal device(For visitors), password-account locks, statement of oath for security and etc.	
6	8	**Does the company establish emergency plans/procedures for response of cyber incidents?** - Check the emergency plans/recovery procedures, contact details for technical IT support	
7	6 8	**Does the company provide emergency plans/procedures with hard copy for response of cyber incidents?** - Check the hard copy of emergency plans/recovery procedures and familiarization of PIC. - Check the measures to prevent cyber incidents from the attacker	
8	10	**Does the company establish maintenance procedures for cyber security equipment resulted from cyber risk assessment?** - Check the periodical inspection / Maintenance / update / Inventory of spare parts, etc. - Check the designated PIC., records of maintenance	
9	12	**Does the company periodically verify/review/assess for the CRM, effectiveness of existing controls and appropriate implementation through internal audit, master review and company review?** - Check the results of internal audit, master review and company review - Check the qualification of internal auditors	
10	12	**Dose the company periodically verify/review/assess the delegated cyber-related tasks and assets?** - Check the relevant procedure/records of delegated cyber-related tasks and assets	

Company Name : Date :

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

DOC CHECK LIST for Cyber Risk Management(CRM)

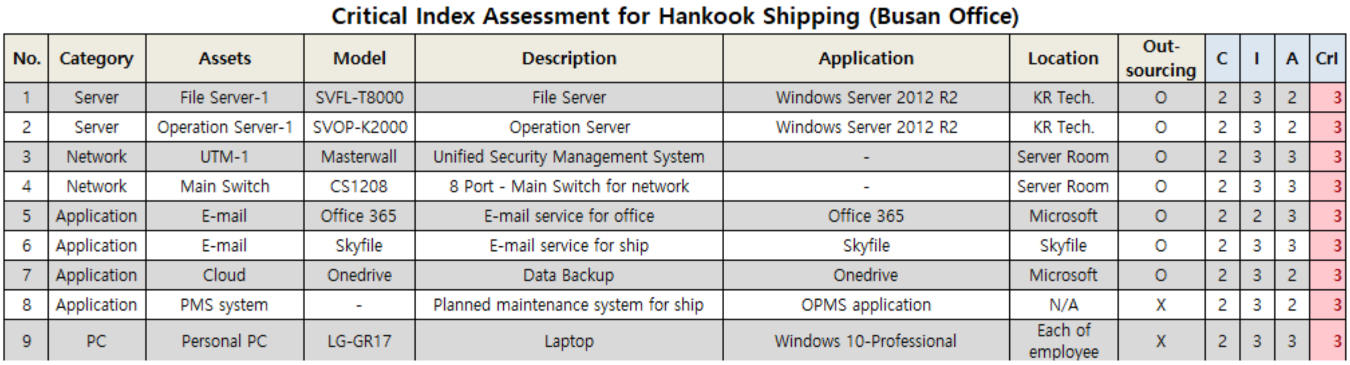
Annex

1. Does the company implement cyber risk assessment for cyber assets and establish Cyber Risk Management (CRM) in the approved safety management systems?

< Reference 1. Examples of cyber assets>

Tangible assets	Intangible assets
Storage server (UNIX, Linux, etc.) Network (Router, Switch, Hub, etc.) Security system (Firewall, IDS, IPS, VPN, etc.) Personal Device (PC, Notebook, Laptop, etc.) Medium (USB Memory, Disc, etc.)	Software (OS, Package software, Vaccine, etc.) Application program Data(company's staff information, Business information, etc.) Document (Drawing, etc.)

< 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

- Including the delegated cyber assets and service
- Considering Confidentiality, Integrity and Availability level with regard to cyber assets
- Identification of Cybersecurity threat and Vulnerability for assets

< Reference 3. General Threats>

* Unauthorized network access (Logical/Physical)

* Infection of Malicious code

< Reference 4. General Vulnerabilities>

* Simple password

* No installation of network firewall

* Outdated or missing antivirus software and protection from malware

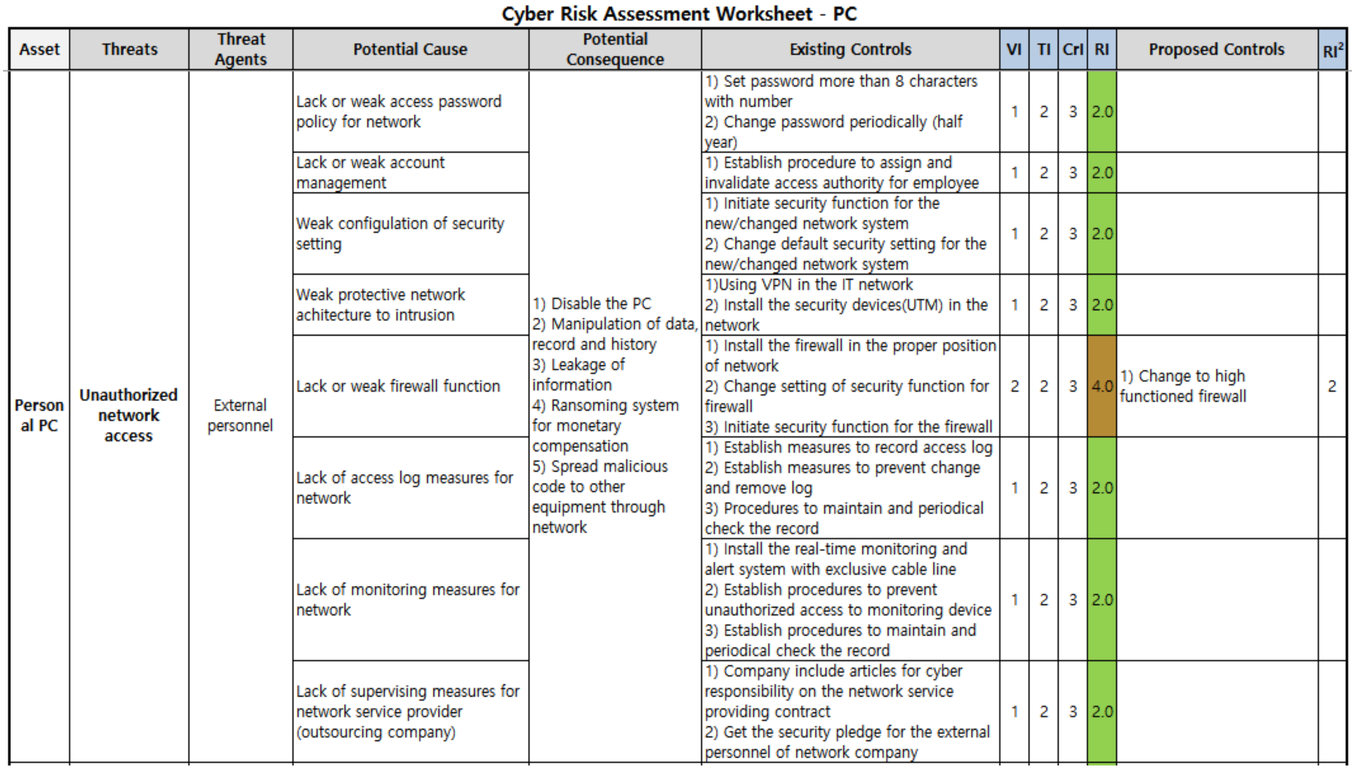
* Inappropriate physical access control

* Inappropriate removable storage medium

* Although physical access is naturally controlled by the ISPS Code for ship, the company needs to prepare separate procedures for controlling access to cyber assets.

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		

- Targeted assets identified as critical cyber assets that need to be assessed for vulnerabilities.

- List the Existing controls for identified threats and vulnerabilities, and assess their risk level(RI).

Provide additional Proposed controls as required and assess the expected residual risk level(RI2.)

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

	Minimum management	**Enhanced management**
Condition	Managing conventional ships with little impact on ship operations by IT - The ship's data is exchanged only by E-mail, and executed by satellite connection for a short time when necessary on the ship.	Managing ships exposed to the internet environment, even if it is not a real time connection
Control	* Management of infection - Management of malware including OS management, vaccine management, and E-mail service provider management of PCs that transmit data to ships.	* Considering "Intrusion" aspect as well as infection - Review risk and action/measures against unauthorized access(intrusion). Also, requires company network configuration to identify vulnerabilities. More stringent service provider verification required. More rigorous access control procedures are required for ships.

- If data is provided to ships through only temporary E-mail access from ships, it can be managed at a basic Malware monitoring & filtering level, but of the ship is provided with an internet environment, the company network needs to take into account the unauthorized access and perform a c complex vulnerability analysis.

DOC CHECK LIST for Cyber Risk Management(CRM)

2. Does the company establish allocation of responsibility and authority for CRM in the SMS?

- Check the identification of responsibility, authority and designated PIC.(D.P, Master, etc.)
- Designation of Cyber-related contact details to the existing emergency contact system
- Add cyber Technical advisor contact details to organization if needed

3. Does the company provide any Cyber risk training with shore staff and crews?

- The training on cyber-related company's policies and procedure(SMS) should be implemented. The training interval(cycle) may be based on the company's policy(risk assessment) ,and the procedures or methods may be applied to the existing training procedures.

- Cyber-related knowledge and basic training to the crews should be implemented after boarding and evaluated. In particular, the officers or engineers who in charge of operation for critical IT/OT related systems on board should be aware of the cyber precautions for their devices

< Reference 7. Recommended basic awareness items>

- Risks related to emails and how to behave in a safe manner. Examples are phishing attacks where the user clicks on a link to a malicious site.
- Risks related to internet usage, including social media(SNS), chat forums and cloud-based file storage where data movement is less controlled and monitored
- Risks related to the use of own devices. These devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment, to which they are connected.
- Risks related to installing and maintaining software on company hardware using infected hardware(removable media) or software (infected package).
- Risks related to poor software and data security practices, where no anti-virus checks or authenticity verifications are Performed.
- Safeguarding user information, passwords and digital certificates

4. Does the company provide appropriate support at the request of the vessel?

- Review and reflect on cyber-related support requested by ships.
- Establish and implement periodic support procedures, including associated hardware/software/updated patches/technical advisor visiting on board the ship.

5. Does the company establish any additional procedure or existing controls in relation to key shipboard operation resulted from cyber risk assessment?

- Establish and implement any additional procedure or existing controls in relation to key shipboard operation resulted from cyber risk assessment. Checklist, etc. can be established separately

6. Does the company establish emergency plans/procedures for response of cyber incidents?

- Designation of shore staff and PIC.
- Check the emergency plans/recovery procedures, contact details for technical IT support

7. Does the company provide emergency plans/procedures with hard copy for response of cyber incidents?

- Check the hard copy of emergency plans/recovery procedures and familiarization of PIC.
- Check the emergency plans/recovery procedures, contact details for technical IT support

- It is necessary to consider that the company's IT does not necessarily require immediate response unlike ship's OT.

8. Does the company establish maintenance procedures for cyber security equipment resulted from cyber risk assessment?

- According to the cyber risk assessment, equipment that requires periodic testing/inspection should be registered on PMS, etc.
- Designation of PIC. / Interval of maintenance / Keeping records
- Needs to support of cyber-related spare parts : e.g. Periodic support of latest patches of the OS, vaccine. Provides back-up programs and storage.
- Critical system(items) needs to improve reliability of equipment through installing standby equipment and periodic Test.

9. Does the company periodically verify/review/assess for the CRM, effectiveness of existing controls and appropriate implementation through internal audit, master review and company review?

- Check the existing company procedures for internal audit, master review and company review, and include cyber risk existing controls.
- Internal audit should be conducted by qualified personnel who can verify cyber-related tasks or information(complete a course cyber-related training).

10. Dose the company periodically verify/review/assess the delegated cyber-related tasks and assets?

- The delegated cyber-related tasks and assets such as e-mail service, server handling, etc. should be verified / reviewed / assessed by the company(Code 12.2) [END]

SMC CHECK LIST for Cyber Risk Management(CRM)

This checklist was developed for reference to efficiently implement the cyber risk management in accordance with Res.MSC.428(98), and it is recommended to use this checklist in conjunction with the Checklist for ISM shipboard audit.

※ Mark methods for the each questionnaire in a square box

☒ or ☑ : Verified as sampling basis

⊟ : Not Applicable

* If a check item is identified as a non-conformity on a sampling verification, it shall be recorded in the non-conformity report

No.	Code	Check items	Result
1	1	**Does the company implement cyber risk assessment for cyber assets and establish Cyber Risk Management (CRM) in the approved safety management systems?** - Check the CRM in accordance with ISM Code 1.2(objectives) and 1.4(functional requirements) - Check the identification of cyber assets (software, hardware, etc.) - Check the cyber risk assessment for ECDIS, if fitted	
2	3	**Does the company establish allocation of responsibility and authority for CRM in the SMS?** - Check the identification of responsibility, authority and designated PIC.(D.P, Master, etc.)	
3	6	**Does the company provide any Cyber risk training with crews?** - Check the cyber risk awareness training provided to the crews before/after boarding - Check the updated information for cyber risk provided to the vessel	
4	6	**Does the company provide appropriate support at the request of the vessel?** - Hardware, Software, update patches, USB/LAN Blocker, information for Cyber risk, etc.	
5	7	**Does the company establish any additional procedure or existing controls in relation to key shipboard operation resulted from cyber risk assessment?** - Check the additional procedure or existing controls such as physical security for visitor, list of personal device(For visitors), password-account locks, statement of oath for security and etc.	
6	8	**Does the company establish emergency plans/procedures for response of cyber incidents and implement relevant training to the crews?** - Check the emergency plans/recovery procedure, contact details for technical IT support	
7	6 8	**Does the company provide emergency plans/procedures with hard copy for response of cyber incidents?** - Check the hard copy of emergency plans/recovery procedures and familiarization of PIC.	
8	9	**Does the company establish procedures for reporting non-conformities, accidents and hazardous situations relating to cyber incidents?** - Available for existing procedures relating to non-conformities	
9	10	**Does the company establish maintenance procedures for cyber security equipment resulted from cyber risk assessment?** - Check the periodical inspection / Maintenance / update / Inventory of spare parts, etc. - Check the designated PIC., records of maintenance	
10	12	**Does the company periodically verify/review/assess for the CRM, effectiveness of existing controls and appropriate implementation through internal audit, master review and company review?** - Check the results of internal audit, master review and company review - Check the qualification of internal auditors	

Vessel Name : Date :

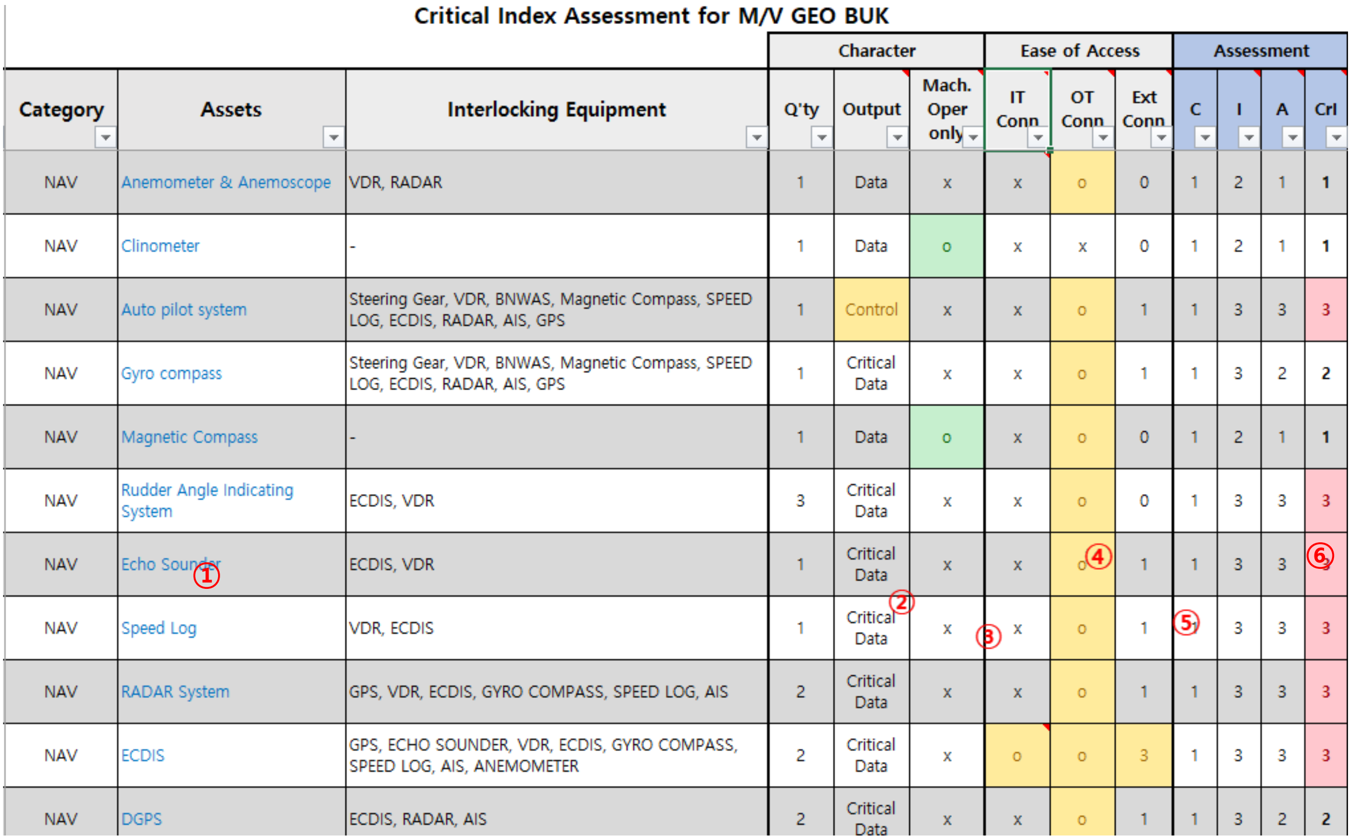
Captain (with Signature) :______________________ Auditor (with Signature) :_____________________

SMC CHECK LIST for Cyber Risk Management(CRM)

Annex

1. Does the company implement cyber risk assessment for cyber assets and establish Cyber Risk Management (CRM) in the approved safety management systems?

<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	Crl
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	1	1	3	3	3
NAV	Speed Log	VDR, ECDIS	1	Critical Data	x	x	o	1	1	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

①List all possible vessel equipment for the first assessment.

②Identify the role or output of the equipment in ship operation and its importance.

③Devices with little data connection and low cyber threats are identified separately to exclude from cyber equipment.

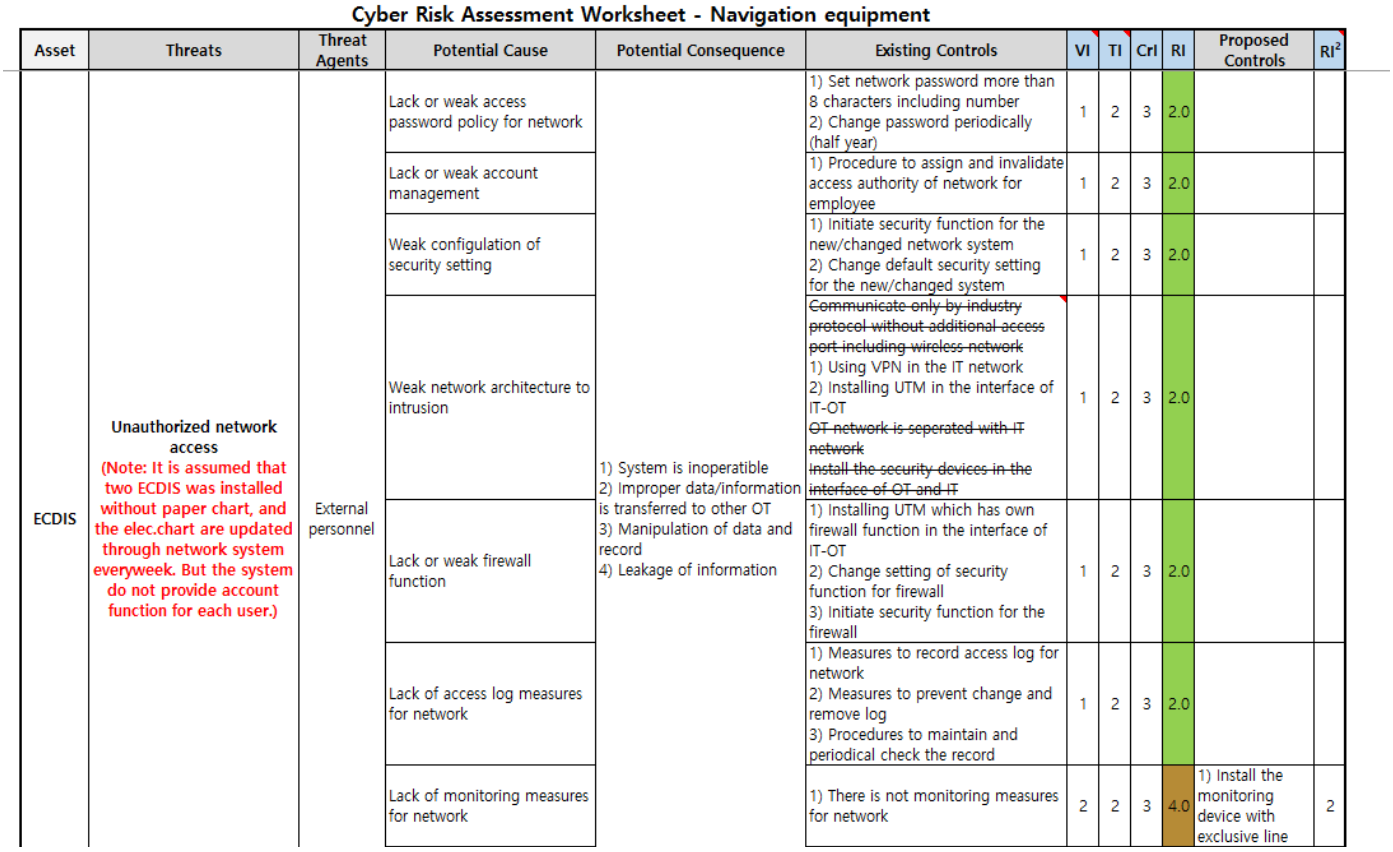
④Need to identify connection status to identify network vulnerabilities.(Interlocking, IT Connection)

⑤Check external connections to identify possible cyber incident through a USB port, even if it is not connected to a network.

⑥Considering Confidentiality, Integrity and Availability level with regard to cyber assets

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

- Identification of Cybersecurity threat and Vulnerability for assets

< Reference 3. General Threats>

* Unauthorized network access (Logical/Physical)

* Infection of Malicious code

< Reference 4. General Vulnerabilities>

* Simple password

* No installation of network firewall

* Outdated or missing antivirus software and protection from malware

* Inappropriate physical access control

* Inappropriate removable storage medium

- Targeted assets identified as critical cyber assets that need to be assessed for vulnerabilities.
- List the Existing controls for identified threats and vulnerabilities, and assess their risk level(RI). Provide additional Proposed controls as required and assess the expected residual risk level(RI2).
- Critical system(items) needs to improve reliability of equipment through installing standby equipment and periodic test.

SMC CHECK LIST for Cyber Risk Management(CRM)

2. Does the company establish allocation of responsibility and authority for CRM in the SMS?

- Check the identification of responsibility, authority and designated PIC.(D.P, Master, etc.)
- Designation of Cyber-related contact details to the existing emergency contact system
- Add cyber Technical advisor contact details to organization if needed

3. Does the company provide any Cyber risk training with crews?

- The training on cyber-related company's policies and procedure(SMS) should be implemented. The training interval(cycle) may be based on the company's policy(risk assessment) ,and the procedures or methods may be applied to the existing training procedures.

- Cyber-related knowledge and basic training to the crews should be implemented after boarding and evaluated. In particular, the officers or engineers who in charge of operation for critical IT/OT related systems on board should be aware of the cyber precautions for their devices

<Reference 5. Recommended basic awareness items>

- Risks related to emails and how to behave in a safe manner. Examples are phishing attacks where the user clicks on a link to a malicious site.
- Risks related to internet usage, including social media(SNS), chat forums and cloud-based file storage where data movement is less controlled and monitored.
- Risks related to the use of own devices. These devices may be missing security patches and controls, such as anti-virus, and may transfer the risk to the environment, to which they are connected.
- Risks related to installing and maintaining software on company hardware using infected hardware(removable media) or software (infected package).
- Risks related to poor software and data security practices, where no anti-virus checks or authenticity verifications are Performed.
- Safeguarding user information, passwords and digital certificates

4. Does the company provide appropriate support at the request of the vessel?

- Review and reflect on cyber-related support to the ships.
- Establish and implement periodic support procedures, including associated hardware/software/updated patches/technical advisor visiting on board the ship.

5. Does the company establish any additional procedure or existing controls in relation to key shipboard operation resulted from cyber risk assessment?

- Establish and implement any additional procedure or existing controls in relation to key shipboard operation resulted from cyber risk assessment. Checklist, list of personal device(For visitors), password-account locks, data backup, statement of oath for security etc. can be established separately..

6. Does the company establish emergency plans/procedures for response of cyber incidents and implement relevant training to the crews?

- Designation of shore staff and PIC.
- Check the emergency plans/recovery procedures, contact details for technical IT support

SMC CHECK LIST for Cyber Risk Management(CRM)

7. Does the company provide emergency plans/procedures with hard copy for response of cyber incidents?

- Check the hard copy of emergency plans/recovery procedures and familiarization of PIC.
- Check the emergency plans/recovery procedures, contact details for technical IT support
- It is necessary to consider that the company's IT does not necessarily require immediate response unlike ship's OT.

8. Does the company establish procedures for reporting non-conformities, accidents and hazardous situations relating to cyber incidents?

- It is applicable to the existing company procedures for Reports and Analysis of Non-conformities, Accidents and related forms.

9. Does the company establish maintenance procedures for cyber security equipment resulted from cyber risk assessment?

- According to the cyber risk assessment, equipment that requires periodic testing/inspection should be registered on PMS, etc.
- Designation of PIC. / Interval of maintenance / Keeping records
- Needs to support of cyber-related spare parts : e.g. Periodic support of latest patches of the OS, vaccine. Provides back-up programs and storage.
- Critical system(items) needs to improve reliability of equipment through installing standby equipment and periodic Test.

10. Does the company periodically verify/review/assess for the CRM, effectiveness of existing controls and appropriate implementation through internal audit, master review and company review?

- Check the existing company procedures for internal audit, master review and company review, and include cyber risk existing controls.
- Internal audit should be conducted by qualified personnel who can verify cyber-related tasks or information(complete a course cyber-related training). [END]