# LAMPIRAN 1

# DAFTAR RIWAYAT HIDUP

## Data Pribadi

| | |
|---|---|
| Nama | : Sahrudin |
| Jenis Kelamin | : Laki-Laki |
| Tempat/Tanggal Lahir | : Jakarta, 27 Agustus 1982 |
| Alamat Rumah | : Jl. Susilo Blok II/105 Kompl. PU |
| Telepon/HP | : 08561216216 |
| Email | : aloel.ku@gmail.com |
| NIM | : 20180801458 |
| Program Studi | : Teknik Informatika |

## Pendidikan Formal

| Periode | Sekolah | Jurusan |
|---|---|---|
| 1997 – 2000 | SMK Tadika Purti | Perhotelan |
| 2004 – 2005 | Wearnes Education Center, Diploma 1 | Informatika & Teknik Komputer |

## Riwayat Pekerjaan

| Tahun | Perusahaan | Jabatan |
|---|---|---|
| Ags 2006 – Apr 2009 | PT Auto Daya Keisindo | IT Support |
| Mei 2009 – Jun 2010 | PT Galiba Daya Mitra Utama | IT Staff |
| Nov 2010 – Feb 2013 | PT Berdikari Cita Sejahtera | IT Staff |
| Mar 2013 – Sekarang | PT Sekawan Intiperkasa | IT Staff |

# LAMPIRAN 2

# SURAT PERMOHONAN PENELITIAN

Universitas Esa Unggul
Fakultas Ilmu Komputer

Jakarta, 28 November 2022

Nomor : 81-116 /SP/KAPRODI-IF/FASILKOM/UEU/EXT/XI/2022
Lampiran : -
Perihal : *Surat Permohonan Izin Untuk Penelitian*

Kepada Yth HR Unit Head PT Indobaruna Bulk Transport
The Prominence Office Tower Lt. 19
Jl. Jalur Sutera Barat Kav. 15 Alam Sutera
Tangerang 15143

Dengan Hormat,

Sehubungan dengan mata kuliah Skripsi/Tugas Akhir yang memerlukan data dan informasi bagi mahasiswa Fakultas Ilmu Komputer Program Studi Teknik Informatika, bersama ini kami sampaikan bahwa mahasiswa kami bermaksud untuk mencari beberapa data / informasi. Adapun nama mahasiswa tersebut adalah :

| NIM | Nama | No HP | Judul |
|---|---|---|---|
| 20180801458 | Sahrudin | 08561216216 | PENERAPAN KEAMANAN SIBER PADA SISTEM TRANSPORTASI LAUT |

Kami berharap Bapak/Ibu memberikan izin pengambilan data untuk Mahasiswa tersebut.

Demikianlah atas perhatian dan kerjasamanya, kami ucapkan terima kasih

Hormat kami,

Universitas Esa Unggul

M.Bahrul Ulum, S.Kom, M.Kom
*Kaprodi Teknik Informatika*

C.c : 1. Arsip

Note : pada saat pengambilan data bisa mengikuti protokol covid (memakai masker, handsanitizer dan pengecekan suhu tubuh, dan sangat disarankan untuk mengambil data secara online).

Jl. Arjuna Utara 9, Tol Tomang, Kebon Jeruk, Jakarta 11510, Indonesia
(021) 567 4223 ext. 206, 207 (021) 567 4248
www.esaunggul.ac.id

# LAMPIRAN 3

# SURAT PENERIMAAN PENELITIAN

**PT INDOBARUNA BULK TRANSPORT**
PERUSAHAAN PELAYARAN

Tangerang, 01 Desember 2022

Nomor : 081/HRGA/IBT/XII/22
Perihal : Jawaban permohonan izin penelitian

Kepada Yth.
Bpk. Bahrul Ulum, S.Kom, M.Kom
Kaprodi Teknik Informatika
Universitas Esa Unggul
di tempat

Dengan hormat,

Berdasarkan surat dengan nomor 81-116 /SP/KAPRODI-IF/FASILKOM/UEU/EXT/XI/2022 mengenai permohonan izin untuk melakukan penelitian di PT Indobaruna Bulk Transport bagi mahasiswa Universitas Esa Unggul atas nama :

| | |
|---|---|
| Nama | : Sahrudin |
| NIM | : 20180801458 |
| Fakultas | : Ilmu Komputer / Jurusan Teknik Informatika |
| Judul Penelitian | : **Penerapan Keamanan Siber pada Sistem Transportasi Laut** |

Bersama ini kami informasikan bahwa Sdr. Sahrudin dapat kami izinkan untuk melakukan penelitian mengenai dengan topik tersebut di atas. Untuk hasil penelitian agar diinformasikan ke PT Indobaruna Bulk Transport.

Demikian disampaikan. Terima kasih

Hormat kami,
PT INDOBARUNA BULK TRANSPORT

Indria Prasetyani
HR Unit Head

**PORT OFFICE :**
Jl. Tongkol No. 5
Tanjung Priok
Jakarta 14310, Indonesia
Phone : +62 - 21 - 4371228
Fax : +62 - 21 - 4371227
E-mail : ibt@indobaruna.com

**TOWN OFFICE :**
The Prominence Office Tower, 19th Floor
Jl. Jalur Sutera Barat Kav. 15, Alam Sutera
Tangerang 15143, Indonesia
Phone : +62 - 21 - 5700240
Fax : +62 - 21 - 5700241
E-mail : ibt@indobaruna.com

# LAMPIRAN 4

# PERATURAN KEAMANAN SIBER

KEMENTERIAN PERHUBUNGAN
DIREKTORAT JENDERAL PERHUBUNGAN LAUT
JL. MEDAN MERDEKA BARAT No. 8 JAKARTA - 10110
TELP :(021) 3813269, 3842440
FAX :(021) 3811786, 3845430
EMAIL : djpl@dephub.go.id
IG :@djplkemenhub151
FB :Ditjen Perhubungan Laut
Twitter : @djplkemenhub151

**SURAT-EDARAN**
Nomor : SE. 35 TAHUN 2020

**TENTANG**

**PENGEMBANGAN PROSEDUR PENERAPAN SISTEM MANAJEMEN KESELAMATAN KAPAL UNTUK PENANGANAN RESIKO PADA SISTEM JARINGAN MAYA (*CYBER RISK MANAGEMENT*)**

1. Memperhatikan:
   a. *International Convention for the Safety of Life at Sea (SOLAS), 1974, chapter IX;*
   b. *International Safety Management (ISM) Code, 2018 Edition;*
   c. *IMO Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems (adopted on 16 June 2017);*
   d. *IMO* MSC-FAL.1/Circ.3 on *Guidelines On Maritime Cyber Risk Management;*
   e. Peraturan Menteri Perhubungan Nomor PM 45 Tahun 2012 tentang Manajemen Keselamatan Kapal;
   f. Peraturan Direktur Jenderal Perhubungan Laut Nomor HK. 103/1/16/DJPL-16 tentang Petunjuk Teknis Pelaksanaan Audit Manajemen Keselamatan Kapal.

2. Dalam rangka melindungi operasional kapal berbendera Indonesia dari kerentanan resiko jaringan maya *(cyber)*, implementasi Sistem Manajemen Keselamatan oleh pemilik dan/atau operator kapal berbendera Indonesia wajib meliputi prosedur kesiapan darurat pencegahan dan penanganan resiko di bidang sistem informasi operasional kapal sesuai *Circullar IMO Number MSC-FAL.1/Circ.3* tanggal 5 Juli 2017.

3. Sistem informasi operasional kapal yang memiliki kerentanan ancaman jaringan maya *(cyber)* minimal meliputi hal-hal sebagai berikut :
   a. sistem di anjungan atau ruang navigasi;
   b. sistem manajemen penanganan muatan;
   c. manajemen tenaga penggerak dan permesinan serta sistem kontrol daya;
   d. sistem kontrol akses;
   e. sistem pelayanan dan penanganan penumpang;
   f. jaringan publik untuk penumpang;
   g. sistem administrasi dan kesejahteraan karyawan; dan
   h. sistem komunikasi.

4. Prosedur pencegahan dan penanganan terhadap resiko pada sistem jaringan maya (*cyber*) minimal terdiri dari hal-hal sebagai berikut :
   a. Identifikasi *(identify)* : penetapan tugas dan tanggung jawab setiap personil perusahaan dan kapal untuk penanganan resiko jaringan maya (*cyber*) dan mengidentifikasi sistem, aset, data, dan kemampuan yang apabila terganggu, dapat menimbulkan resiko untuk operasional kapal;

/b. Perlindungan ...

b. Perlindungan *(protect)* : penerapan proses dan langkah-langkah pengendalian resiko dan rencana antisipasi untuk perlindungan terhadap aktivitas jaringan maya *(cyber)* dan memastikan kesinambungan operasional kapal;

c. Deteksi *(detect)* : mengembangkan dan mengimplementasikan langkah yang diperlukan untuk mendeteksi aktifitas jaringan maya *(cyber)* pada waktu yang tepat.

d. Respon *(respond)* : mengembangkan dan mengimplementasikan kegiatan dan rencana untuk memberikan ketahanan dalam memulihkan sistem yang diperlukan untuk operasional kapal atau layanan yang terganggu karena aktivitas jaringan maya *(cyber)*;

e. Pemulihan *(recover)* : mengidentifikasi langkah-langkah untuk mencadangkan dan memulihkan sistem jaringan maya *(cyber)* yang diperlukan untuk operasional kapal yang dipengaruhi oleh aktivitas jaringan maya *(cyber)*.

5. Pengembangan prosedur pencegahan dan penanganan terhadap resiko sistem jaringan maya (*cyber*) pada Sistem Manajemen Keselamatan akan menjadi obyek audit dalam pelaksanaan eksternal audit untuk penerbitan atau pengukuhan Dokumen Penyesuaian Manajemen Keselamatan (*Document of Compliance/ DOC*) untuk perusahaan mulai tanggal 1 Januari 2021.

6. Demikian surat edaran ini dibuat, agar Para Kepala Kantor Kesyahbandaran Utama, Para Kepala Kantor Kesyahbandaran dan Otoritas Pelabuhan, Kepala Kantor Kesyahbandaran dan Otoritas Pelabuhan Khusus Batam dan Para Kepala Unit Penyelenggara Pelabuhan dapat menyampaikan kepada seluruh *stakeholder* terkait di wilayah kerja masing-masing serta melakukan pengawasan terhadap pemberlakuannya.

Ditetapkan di : JAKARTA
pada tanggal : 27 AGUSTUS 2020

DIREKTUR JENDERAL PERHUBUNGAN LAUT

KEMENTERIAN PERHUBUNGAN DIREKTORAT JENDERAL PERHUBUNGAN LAUT

R. AGUS H. PURNOMO

INTERNATIONAL MARITIME ORGANIZATION

E

4 ALBERT EMBANKMENT
LONDON SE1 7SR
Telephone: +44 (0)20 7735 7611 Fax: +44 (0)20 7587 3210

MSC-FAL.1/Circ.3
5 July 2017

# GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

1 The Facilitation Committee, at its forty-first session (4 to 7 April 2017), and the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), having considered the urgent need to raise awareness on cyber risk threats and vulnerabilities, approved the *Guidelines on maritime cyber risk management*, as set out in the annex.

2 The Guidelines provide high-level recommendations on maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

3 Member Governments are invited to bring the contents of this circular to the attention of all stakeholders concerned.

4 This circular supersedes the interim guidelines contained in MSC.1/Circ.1526.

***

ANNEX

GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

## 1 INTRODUCTION

1.1 These Guidelines provide high-level recommendations for maritime cyber risk management. For the purpose of these Guidelines, *maritime cyber risk* refers to a measure of the extent to which a technology asset is threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures as a consequence of information or systems being corrupted, lost or compromised.

1.2 Stakeholders should take the necessary steps to safeguard shipping from current and emerging threats and vulnerabilities related to digitization, integration and automation of processes and systems in shipping.

1.3 For details and guidance related to the development and implementation of specific risk management processes, users of these Guidelines should refer to specific Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

1.4 Risk management is fundamental to safe and secure shipping operations. Risk management has traditionally been focused on operations in the physical domain, but greater reliance on digitization, integration, automation and network-based systems has created an increasing need for cyber risk management in the shipping industry.

1.5 Predicated on the goal of supporting safe and secure shipping, which is operationally resilient to cyber risks, these Guidelines provide recommendations that can be incorporated into existing risk management processes. In this regard, the Guidelines are complementary to the safety and security management practices established by this Organization.

## 2 GENERAL

### 2.1 Background

2.1.1 Cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. In some cases, these systems are to comply with international standards and Flag Administration requirements. However, the vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed. Vulnerable systems could include, but are not limited to:

.1 Bridge systems;
.2 Cargo handling and management systems;
.3 Propulsion and machinery management and power control systems;
.4 Access control systems;
.5 Passenger servicing and management systems;
.6 Passenger facing public networks;
.7 Administrative and crew welfare systems; and
.8 Communication systems.

2.1.2 The distinction between information technology and operational technology systems should be considered. Information technology systems may be thought of as focusing on the use of data as information. Operational technology systems may be thought of as focusing on the use of data to control or monitor physical processes. Furthermore, the protection of information and data exchange within these systems should also be considered.

2.1.3 While these technologies and systems provide significant efficiency gains for the maritime industry, they also present risks to critical systems and processes linked to the operation of systems integral to shipping. These risks may result from vulnerabilities arising from inadequate operation, integration, maintenance and design of cyber-related systems, and from intentional and unintentional cyberthreats.

2.1.4 Threats are presented by malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions). In general, these actions expose vulnerabilities (e.g. outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology. Effective cyber risk management should consider both kinds of threat.

2.1.5 Vulnerabilities can result from inadequacies in design, integration and/or maintenance of systems, as well as lapses in cyberdiscipline. In general, where vulnerabilities in operational and/or information technology are exposed or exploited, either directly (e.g. weak passwords leading to unauthorized access) or indirectly (e.g. the absence of network segregation), there can be implications for security and the confidentiality, integrity and availability of information. Additionally, when operational and/or information technology vulnerabilities are exposed or exploited, there can be implications for safety, particularly where critical systems (e.g. bridge navigation or main propulsion systems) are compromised.

2.1.6 Effective cyber risk management should also consider safety and security impacts resulting from the exposure or exploitation of vulnerabilities in information technology systems. This could result from inappropriate connection to operational technology systems or from procedural lapses by operational personnel or third parties, which may compromise these systems (e.g. inappropriate use of removable media such as a memory stick).

2.1.7 Further information regarding vulnerabilities and threats can be found in the additional guidance and standards referenced in section 4.

2.1.8 These rapidly changing technologies and threats make it difficult to address these risks only through technical standards. As such, these Guidelines recommend a risk management approach to cyber risks that is resilient and evolves as a natural extension of existing safety and security management practices.

2.1.9 In considering potential sources of threats and vulnerabilities and associated risk mitigation strategies, a number of potential control options for cyber risk management should also be taken into consideration, including amongst others, management, operational or procedural, and technical controls.

**2.2 Application**

2.2.1 These Guidelines are primarily intended for all organizations in the shipping industry, and are designed to encourage safety and security management practices in the cyberdomain.

2.2.2 Recognizing that no two organizations in the shipping industry are the same, these Guidelines are expressed in broad terms in order to have a widespread application. Ships with limited cyber-related systems may find a simple application of these Guidelines to be sufficient; however, ships with complex cyber-related systems may require a greater level of care and should seek additional resources through reputable industry and Government partners.

2.2.3 These Guidelines are recommendatory.

## 3 ELEMENTS OF CYBER RISK MANAGEMENT

3.1 For the purpose of these Guidelines, *cyber risk management* means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

3.2 The goal of maritime cyber risk management is to support safe and secure shipping, which is operationally resilient to cyber risks.

3.3 Effective cyber risk management should start at the senior management level. Senior management should embed a culture of cyber risk awareness into all levels of an organization and ensure a holistic and flexible cyber risk management regime that is in continuous operation and constantly evaluated through effective feedback mechanisms.

3.4 One accepted approach to achieve the above is to comprehensively assess and compare an organization's current, and desired, cyber risk management postures. Such a comparison may reveal gaps that can be addressed to achieve risk management objectives through a prioritized cyber risk management plan. This risk-based approach will enable an organization to best apply its resources in the most effective manner.

3.5 These Guidelines present the functional elements that support effective cyber risk management. These functional elements are not sequential – all should be concurrent and continuous in practice and should be incorporated appropriately in a risk management framework:

.1 Identify: Define personnel roles and responsibilities for cyber risk management and identify the systems, assets, data and capabilities that, when disrupted, pose risks to ship operations.

.2 Protect: Implement risk control processes and measures, and contingency planning to protect against a cyber-event and ensure continuity of shipping operations.

.3 Detect: Develop and implement activities necessary to detect a cyber-event in a timely manner.

.4 Respond: Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations or services impaired due to a cyber-event.

.5 Recover: Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber-event.

3.6 These functional elements encompass the activities and desired outcomes of effective cyber risk management across critical systems affecting maritime operations and information exchange, and constitute an ongoing process with effective feedback mechanisms.

3.7 Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

## 4 BEST PRACTICES FOR IMPLEMENTATION OF CYBER RISK MANAGEMENT

4.1 The approach to cyber risk management described herein provides a foundation for better understanding and managing cyber risks, thus enabling a risk management approach to address cyberthreats and vulnerabilities. For detailed guidance on cyber risk management, users of these Guidelines should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

4.2 Additional guidance and standards may include, but are not limited to:[1]

.1 The Guidelines on Cyber Security Onboard Ships produced and supported by BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, OCIMF and IUMI.

.2 ISO/IEC 27001 standard on Information technology – Security techniques – Information security management systems – Requirements. Published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

.3 United States National Institute of Standards and Technology's Framework for Improving Critical Infrastructure *Cyber*security (the NIST Framework).

4.3 Reference should be made to the most current version of any guidance or standards utilized.

---

[1] The additional guidance and standards are listed as a non-exhaustive reference to further detailed information for users of these Guidelines. The referenced guidance and standards have not been issued by the Organization and their use remains at the discretion of individual users of these Guidelines.

ANNEX 10

RESOLUTION MSC.428(98)
(adopted on 16 June 2017)

MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS

THE MARITIME SAFETY COMMITTEE,

RECOGNIZING the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks,

RECOGNIZING ALSO that Administrations, classification societies, shipowners and ship operators, ship agents, equipment manufacturers, service providers, ports and port facilities, and all other maritime industry stakeholders should expedite work towards safeguarding shipping from current and emerging cyber threats and vulnerabilities,

BEARING IN MIND MSC-FAL.1/Circ.3 on *Guidelines on maritime cyber risk management* approved by the Facilitation Committee, at its forty-first session (4 to 7 April 2017), and by the Maritime Safety Committee, at its ninety-eighth session (7 to 16 June 2017), which provides high-level recommendations for maritime cyber risk management that can be incorporated into existing risk management processes and are complementary to the safety and security management practices established by this Organization,

RECALLING resolution A.741(18) by which the Assembly adopted the International Management Code for the Safe Operation of Ships and for Pollution Prevention (International Safety Management (ISM) Code) and recognized, inter alia, the need for appropriate organization of management to enable it to respond to the need of those on board ships to achieve and maintain high standards of safety and environmental protection,

NOTING the objectives of the ISM Code which include, inter alia, the provision of safe practices in ship operation and a safe working environment, the assessment of all identified risks to ships, personnel and the environment, the establishment of appropriate safeguards, and the continuous improvement of safety management skills of personnel ashore and aboard ships,

1 AFFIRMS that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code;

2 ENCOURAGES Administrations to ensure that 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;

3 ACKNOWLEDGES the necessary precautions that could be needed to preserve the confidentiality of certain aspects of cyber risk management;

4 REQUESTS Member States to bring this resolution to the attention of all stakeholders.

***

# LAMPIRAN 5

# SURAT TUGAS KUNJUNGAN KAPAL

**PT. INDOBARUNA BULK TRANSPORT**
**PERUSAHAAN PELAYARAN**

## SURAT TUGAS

No. : 1017/IBT/FLT/N/XII/2022

Yang bertanda tangan dibawah ini :

Nama : Michael Inkiarto
Jabatan : Direktur PT. Indobaruna Bulk Transport.

Bersama ini kami memberikan tugas kepada :

Nama : Sdr. Sahrudin (0856 1216216).
Jabatan : -
Tanggal : 20 Desember 2022 – sampai dengan selesai.
Tempat : MV. Oceanic Success.
Keperluan : Analisa Jaringan Keamanan Siber Kapal

Demikian surat tugas ini dibuat untuk dipergunakan sebagaimana mestinya.

Tangerang, 19 Desember 2022.
PT.Indobaruna Bulk Transport

**Melvin Alvin**
Deputy of Fleet

**Note :**
ISM Code dan ISPS Code prosedur bagi Visitor yang akan naik ke kapal, sebagai berikut : (+62 812-9684-316)

1. Menerapkan protocol sesuai arahan email DPA, Re : PT. IBT , Protokol kesiagaan COVID-19
2. Visitor menggunakan Personal Safety Equipments (Safety Shoes, Safety Glove & Safety Helmet), jika yang bersangkutan akan melaksanakan suatu pekerjaan diatas kapal.
3. Registrasi ISPS yaitu tunjukan surat tugas atau sejenisnya, mengisi Visitor Book, tukar ID (KTP/SIM) dengan Visitor Card
4. Sampaikan maksud kunjungannya kepada personel jaga ISPS, jika visitor adalah Teknisi atau orang yang bermaksud melaksanakan suatu pekerjaan diatas kapal, agar bertemu terlebih dahulu dengan Nakhoda.
5. Meminta izin kepada Nakhoda untuk melaksanakan Safety Meeting dengan melibatkan crew terkait, sebelum memulai pekerjaannya, sehingga crew yang ditugaskan untuk mendampingi lebih mengerti dengan lakah-lungkah yang harus dilakukan.
6. Setelah selesai pekerjaannya dan sebelum turun ke kapal, agar menghadap kembali ke Nakhoda.

**Port Office :**
Jl. Tongkol No.5
Tanjung Priok, Jakarta 14310, Indonesia
15143 Phone : +62-21 4371228 ; Fax : +62-21 4371227
29779677
Email : ibt@indobaruna.com

**Town Office :**
The Prominence Office Tower 19th Floor
Jl. Jalur Sutera Barat Kav.15, Tangerang
Phone : +62-21 29779688 ; Fax : +62-
Email : ibt@indobaruna.com

# LAMPIRAN 6

# KEBIJAKAN KEAMANAN SIBER IBT

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

**KEAMANAN JARINGAN KAPAL CYBER SECURITY**

**A. PENGENALAN**

Semakin berkembangnya teknologi, membuat *information technology* (IT) dan *operational technology* (OT) harus saling bekerjasama dalam melindungi informasi data dari serangan *cyber crime*. Serta merancang keamanan atas tindakan kriminialitas akibat *cyber attack*.

Sesuai dengan definisinya, *cyber security* adalah aktifitas pencegahan dan pengamanan terhadap sumber daya telematika agar tidak terjadinya kriminalitas di dunia *cyber* (*cyber crime*). *Cyber security* juga dapat diartikan upaya untuk menahan dari penyerangan-penyerangan di dunia *cyber*.

*Cyber security* adalah upaya untuk melindungi informasi dari adanya *cyber attack*. *Cyber attack* dalam operasi informasi adalah semua jenis tindakan yang sengaja dilakukan untuk mengganggu kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersedian (*availability*) informasi.

**B. KEBIJAKAN KEAMANAN DAN PELINDUNGAN**

Demi menjaga sebuah keamanan dan melindungi data dari segala tindakan yang merugikan. Maka dibutuhkan sebuah kebijakan keamanan dan pelindungan. Adapun kebijakan keamanan dan pelindungan yang diterapkan pada operasional kapal untuk hal keamanan sebagai berikut :

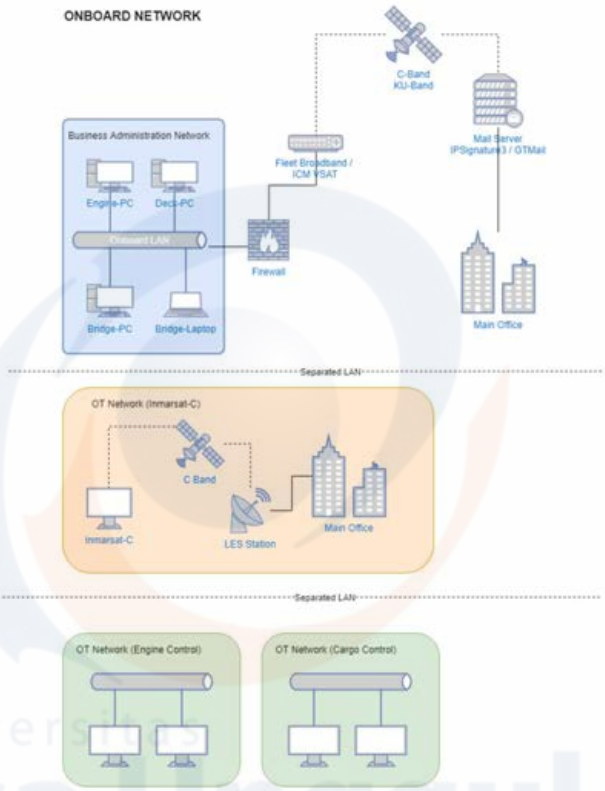
1. Pembatasan akses *internet*, bekerjasama dengan pihak *satellite* dalam hal ini.
2. Harus adanya persetujuan dari IT Dept jika ingin dibukakan akses *internet* ini.
3. Komunikasi terbatas dengan menggunakan *email*, semua komunikasi dari pihak luar ke kapal hanya melalui *email* yang dibatasin dengan menggunakan metode *white list email*.
4. Pemberian hak terbatas atas penggunaan *usb drive* di operasional kapal.
5. Melakukan *scan usb drive* dengan menggunakan *antivirus*.
6. Penggunaan *hotspot* harus menginformasikan ke IT Dept.
7. Kapal wajib melaporkan jika terjadi sesuatu yang mencurigakan pada komputer kerja.

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

## C. INFRASTRUKTUR INFORMASI

Infrastruktur informasi sangat dibutuhkan sebagai dasar dalam menganalisa dan mendeteksi *backdoor* yang dapat menjadi pintu masuk dari sebuah serangan *cyber crime*.

### 1. Infrastruktur Jaringan Kapal



Adapun struktur jaringan pada kapal memiliki *segment IP Address* yang berbeda-beda berdasarkan masing-masing fungsi jaringan operasional. Sehingga keamanan atas sebuah jaringan lebih terjaga dengan adanya perpisahan *segment* ini.

a. **Jaringan Operasional Kerja (*Business Administration Network*)**
   - Jaringan ini berfungsi sebagai jaringan operasional kerja dalam membuat laporan kerja kapal.
   - Sebagai jaringan komunikasi untuk proses pengiriman informasi data dengan menggunakan *interface email*.
   - Dalam proses pengiriman data dan informasi, kapal menggunakan jalur *satellite* yang terdiri dari *Fleet Broadband* atau *VSAT*.
   - Dengan dilengkapi *hardware firewall*, untuk menutup akses *port-port* yang tidak digunakan dan sebagai keamanan proses pengiriman dan juga serangan dunia *cyber*.
   - Memiliki *segment IP Address* sendiri dan tidak terkoneksi dengan jaringan operasional kapal (*operation technology network*).

b. **Jaringan Operasional Kapal *(Operation Technology Network)***
   - Jaringan ini merupakan *main control* atas operasional kerja sebuah kapal, meliputi operasional Engine dan Cargo.
   - Jaringan ini tidak terhubung ke *satellite* atau *internet*.
   - *Segment* untuk *IP Address* ini terpisah dari jaringan operasional kerja (*Business Administration Network*).

2. **Infrastruktur *Email Server***

Adapun aplikasi yang digunakan di kapal untuk proses pengiriman data dan informasi menggunakan salah satu dari dua provider yaitu *IP Signature* dan *GTMailPlus*, sebagai sebuah *mail server local*.


Adapun fitur-fitur pada aplikasi pihak ketiga meliputi :

a. Setiap *mail server* dilengkapi dengan *firewall* dan proses filtering *spam* & *Anti-virus*.
b. Melalui proses *data compression* dalam pengiriman informasi data *email*.
c. Adanya keamanan dalam *white list email*, sehingga *email* yang terdaftar saja yang dapat melakukan pengiriman ke kapal.

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

**D. KOMPONEN PERTAHANAN PADA JARINGAN KAPAL**

Adapun komponen pertahanan pada jaringan dan teknologi yang ada di kapal.

1. Perbedaan *segment IP Address* pada tiap-tiap *network* dan terpisah dari jaringan operasional kerja (*business administration network)* dan jaringan operasional kapal (*operational technology network*) .
2. *Hardware Firewall,* untuk menutup *port-port* yang tidak digunakan dan membuka *port-port* yang dibutuhkan saja.
3. Adanya *firewall* dalam proses pengiriman *email* oleh pihak ketiga (*IP Signature* dan *GTMailPlus*).
4. Pembatasan *email* pengiriman ke kapal dengan *white list email.*
5. Mematikan akses ke *satellite* maupun *internet*, jika terdapat gejala *cyber attack.*
6. Mematikan *switch hub* yang terhubung pada jaringan komputer kapal.

**E. TINDAKAN PERBAIKAN AKIBAT *CYBER CRIME***

Jika terjadi sebuah kriminalitas akibat *cyber crime*, adapun tindakan perbaikan yang dilakukan sebagai berikut :

1. Pengecekan jaringan yang terkena dampak serangan *cyber attack.*
2. Analisa *system* komputer dan perangkat yang terhubung pada jaringan yang terserang.
3. Melakukan *recovery* pada system komputer dan perangkat pada jaringan.
4. Menutup celah (*backdoor*) sumber dari *cyber attack* tersebut.

# LAMPIRAN 7

# RISK ASSESSMENT REPORT



PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

## RISK ASSESSMENT CYBERSECURITY REPORT

PROJECT: MV OCEANIC SUCCESS
DATE : 23 DESEMBER 2022

FINAL SCORE : 42
LEVEL IMPACT : MEDIUM

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

## IDENTIFY[23]

| Roles and responsibilities[24] | |
|---|---|
| **Action** | **Remarks** |
| ISM Code: 3.2<br>This publication: 1.1<br>Update the safety and environment protection policy to include reference to the risk posed by unmitigated cyber risks. | An updated safety and environment protection policy should demonstrate:<br>■ a commitment to manage cyber risks as part of the overall approach to safety management (including safety culture) and protection of the environment<br>■ an understanding that CRM has both safety and security aspects, but the emphasis is on managing the safety risks introduced by OT, IT and networks<br>■ an understanding that without appropriate technical and procedural risk protection and control measures, OT is vulnerable to disruption affecting the safe operation of a ship and protection of the environment.<br>Nothing in the updated policy should suggest that CRM is given any more or less attention than any other risks identified by the company. |
| ISM Code: 3.3<br>This publication: 1.1<br>Update the responsibility and authority information provided in the SMS to include appropriate allocation of responsibility and authority for cyber risk management (CRM). | In general, IT personnel should understand potential vulnerabilities in computer-based systems and know the appropriate technical and procedural protection measures to help ensure the availability and integrity of systems and data. Operational and technical personnel should generally understand the safety and environmental impacts of disruption to critical systems[25] onboard ships and are responsible for the SMS.<br>Allocation of responsibility and authority may need to be updated to enable CRM. This should include:<br>■ allocation of responsibilities and authorities which encourage cooperation between IT personnel (which may be provided by a third party) and the company's operational and technical personnel<br>■ incorporating compliance with cyber risk management policies and procedures into the existing responsibility and authority of the Master. |
| ISM Code: 6.5<br>This publication: 7.3<br>Using existing company procedures, identify any training which may be required to support the incorporation of cyber risk management into the SMS. | Cyber awareness training is not a mandatory requirement. Notwithstanding this, training is a protection and control measure that forms the basis of CRM. It helps to ensure that personnel understand how their actions will influence the effectiveness of the company's approach to CRM. Existing company procedures for identifying training requirements should be used to assess the benefits and need for:<br>■ all company personnel to receive basic cyber awareness training in support of the company's CRM policies and procedures<br>■ company personnel, who have been assigned CRM duties, to receive a type and level of cyber training appropriate to their responsibility and authority. |

## PROTECT

| Implement risk control measures | |
|---|---|
| **Action** | **Remarks** |
| ISM Code: **1.2.2.2**<br>This publication: 2, 3, 4, 5 and Annex 1<br>Assess all identified risks to ships, personnel and the environment and establish appropriate safeguards. | The full scope of risk control measures implemented by the company should be determined by a risk assessment, taking into account the information provided in these guidelines.<br>As a baseline, the following measures should be considered before a risk assessment is undertaken. The baseline consists of the technical and procedural measures, which should be implemented in all companies to the extent appropriate. These measures are:<br>■ **Hardware inventory.** Develop and maintain a register of all critical system hardware on board, including authorized and unauthorized devices on company controlled networks. The SMS should include procedures for maintaining this inventory throughout the operational life of the ship.<br>■ **Software inventory.** Develop and maintain a register of all authorized and unauthorized software running on company-controlled hardware onboard, including version and update status. The SMS should be updated to include procedures for:<br>• maintaining this inventory when hardware controlled by the company is replaced<br>• maintaining this inventory when software controlled by the company is updated or changed<br>• authorizing the installation of new or upgraded software on hardware controlled by the company<br>• prevention of installation of unauthorized software, and deletion of such software if identified<br>• software maintenance.<br>■ **Map data flows.** Map data flows between critical systems and other equipment/technical systems on board and ashore, including those provided by third parties. Vulnerabilities identified during this process should be recorded and securely retained by the company. The SMS should be updated to include procedures for:<br>• maintaining the map of data flows to reflect changes in hardware, software and/or connectivity<br>• identifying and responding to vulnerabilities introduced when new data flows are created following the installation of new hardware<br>• reviewing the need for connectivity between critical systems and other OT and IT systems. Such a review should be based on the principle that systems should only be connected where there is a need for the safe and efficient operation of the ship, or to enable planned maintenance<br>• controlling the use of removable media, access points and the creation of ad-hoc or uncontrolled data flows. This may be achieved by restrictions on the use of removable media and disabling USB and similar ports on critical systems.<br>■ **Implement secure configurations for all hardware controlled by the company.** This should include documenting and maintaining commonly accepted security configuration standards for all authorized hardware and software. The SMS should include policies on the allocation and use of administrative privileges by ship and shore-based personnel, and third parties. However, it is not recommended that the details of secure configurations are included in the SMS. This information should be retained separately and securely by the company.<br>■ **Audit logs.** Security logs should be maintained and periodically reviewed. Security logging should be enabled on all critical systems with this capability. The SMS should be updated to include procedures for:<br>• policies and procedures for the maintenance of security logs and periodic review by competent personnel as part of the operational maintenance routine<br>• procedures for the collation and retention of security logs by the company, if appropriate.<br>■ **Awareness and training.** Maintain situational awareness of current cyber threats. See line 3 above.<br>■ **Physical security.** The physical security of the ship is enhanced by compliance with the security measures addressed in the ship security plan (SSP) required by the ISPS Code. Measures should be taken to restrict access and prevent unauthorized access to critical system network infrastructure onboard. |

| Develop contingency plans | |
|---|---|
| **Action** | **Remarks** |
| ISM Code: 7<br>This publication: 1.5 and 9<br>Update procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment which rely on OT. | An approved SMS should already address procedures, plans and instructions for key shipboard operations concerning the safety of the personnel, ship and protection of the environment. In general, these plans should be unaffected by the incorporation of CRM into the SMS. This is because the effect of the loss of availability of OT, or loss of integrity of the data used or provided by such systems, is the same as if the OT was unavailable or unreliable for some other reason.<br>Notwithstanding this, consideration should be given to developing instructions on the actions to be taken if disruption to critical systems is suspected. This could include procedures for reverting to back-up or alternative arrangements as a precaution whilst any suspected disruption is investigated.<br>Procedures for periodically checking the integrity of information provided by OT to operators should be considered for inclusion in operational maintenance routines. |
| ISM Code: 8.1<br>This publication: 9<br>Update emergency plans to include responses to cyber incidents. | An approved SMS should already address emergency plans for the disruption of critical systems required for the safe operation of ships and protection of the environment. In general, these plans should be unaffected by the incorporation of cyber risk management into SMS. This is because the effect of common shipboard emergencies should be independent of the root cause. For example, a fire may be caused by equipment malfunctioning because of a software failure or inappropriate maintenance or operation of the equipment.<br>Notwithstanding the above, consideration should be given to the development of a cyber incident module in the integrated system of shipboard emergency plans for significant disruption to the availability of OT or the data used by them. The purpose of the module could be to provide information on the actions to be taken in the event of a simultaneous disruption to multiple OT systems required for the safe operation of the ship and protection of the environment. In this more complex situation, additional information on appropriate immediate actions to be taken in response may be necessary. |

## DETECT

| Develop and implement activities necessary to detect a cyber-event in a timely manner | |
|---|---|
| **Action** | **Remarks** |
| ISM Code: 9.1<br>This publication: 1.5<br>Update procedures for reporting non-conformities, accidents and hazardous situations to include reports relating to cyber incidents. | An approved SMS should already address procedures relating to non-conformities. When incorporating CRM into the SMS, company reporting requirements for non-conformities may need to be updated to include cyber related non-conformities. Consider sharing the facts of a cyber related non-conformity with information sharing organisations.<br>Examples of such non-conformities and cyber incidents:<br>■ unauthorised access to network infrastructure<br>■ unauthorized or inappropriate use of administrator privileges<br>■ suspicious network activity<br>■ unauthorised access to critical systems<br>■ unauthorised use of removable media<br>■ unauthorised connection of personal device<br>■ failure to comply with software maintenance procedures<br>■ failure to apply malware and network protection updates<br>■ loss or disruption to the availability of critical systems<br>■ loss or disruption to the availability of data required by critical systems. |

## RESPOND

| Develop and implement activities and plans to provide resilience and to restore systems necessary for shipping operations and/or services impaired due to a cyber-event | |
|---|---|
| **Action** | **Remarks** |
| ISM Code: 3.3<br>This publication: 10.1<br>Ensure that adequate resources and shore-based support are available to support the DPA in responding to the loss of critical systems. | An approved SMS should already be supported by adequate resources to support the DPA. However, the incorporation of CRM into the SMS should require that this resourcing includes appropriate IT expertise. This resource could come from within the company but may also be provided by a third party. In providing the adequate resources, the following should be considered:<br>■ company or third-party technical support should be familiar with onboard IT and OT infrastructure and systems<br>■ any internal response team or external cyber emergency response team (CERT) should be available to provide timely support to the DPA.<br>■ provision of an alternative means of communication between the ship and the DPA, which should be able to function independently of all other shipboard systems, if and when the need arises<br>■ internal audits should confirm that adequate resources, including third parties when appropriate, are available to provide support in a timely manner to support the DPA. |
| ISM Code: 9.2<br>This publication: 10<br>Update procedures for implementing corrective actions to include cyber incidents and measures to prevent recurrence. | An approved SMS should already include procedures for responding to non-conformities. In general, these should not be affected by the incorporation of CRM in SMS. However, the procedures should help ensure that consideration of non-conformities and corrective actions involves the personnel with responsibility and authority for CRM. This should help ensure that corrective actions, including measures to prevent recurrence, are appropriate and effective. |
| ISM Code: 10.3<br>This publication: 7.2<br>Update the specific measures aimed at promoting the reliability of OT. | An approved SMS should already include procedures for operational maintenance routines to promote the reliability of equipment on board. A SMS, which incorporates CRM, should outline procedures for:<br>■ software maintenance as a part of operational maintenance routines. Such procedures should ensure that application of software updates, including security patches, are applied and tested in a timely manner, by a competent person<br>■ authorizing remote access, if necessary and appropriate, to critical systems for software or other maintenance tasks. This should include authorizing access in general (including verification that service providers have taken appropriate protective measures themselves) and for each specific remote access session<br>■ preventing the application of software updates by service providers using uncontrolled or infected removable media<br>■ periodic inspection of the information provided by critical systems to operators and confirmation of the accuracy of this information when critical systems are in a known state<br>■ controlled use of administrator privileges to limit software maintenance tasks to competent personnel. |

## RECOVERY

| Identify measures to back-up and restore cyber systems necessary for shipping operations impacted by a cyber incident | |
|---|---|
| **Action** | **Remarks** |
| ISM Code: 10.4<br>This publication: 10.3<br>Include creation and maintenance of back-ups into the ship's operational maintenance routine. | An approved SMS should already include procedures for maintaining and testing back-up arrangements for shipboard equipment. Notwithstanding this, it may not address procedures for maintaining and storing offline back-ups for data and systems required for the safe operation of the ship and protection of the environment.<br>A SMS, which incorporates CRM, should include procedures for:<br>■ checking back-up arrangements for critical systems, if not covered by existing procedures<br>■ checking alternative modes of operation for critical systems, if not covered by existing procedures<br>■ creating or obtaining back-ups, including clean images for OT to enable recovery from a cyber incident<br>■ maintaining back-ups of data required for critical systems to operate safely<br>■ offline storage of back-ups and clean images, if appropriate<br>■ periodic testing of back-ups and back-up procedures. |

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

INITIAL RISK TARGET SYSTEM

| Category | Sub Category |
|---|---|
| Communication systems | - Integrated communication systems |
| | - Satellite communication equipment |
| | - Voice Over Internet Protocols (VOIP) equipment |
| | - Wireless networks (WLANs) |
| | - Public address and general alarm systems |
| | - Systems used for reporting mandatory information to public authorities |
| Bridge systems | - Integrated navigation system |
| | - Positioning systems (GPS, etc) |
| | - Electronic Chart Display Information System (ECDIS) |
| | - Dynamic Positioning (DP) systems |
| | - Systems that interface with electronic navigation systems and propulsion/manoeuvring systems |
| | - Automatic Identification System (AIS) |
| | - Global Maritime Distress and Safety System (GMDSS) |
| | - Radar equipment |
| | - Voyage Data Recorders (VDRs) |
| | - Bridge Navigational Watch Alarm System (BNWAS) |
| | - Shipboard Security Alarm Systems (SSAS) |
| Propulsion, machinery management and power control systems | - Engine governor |
| | - Power management |
| | - Integrated control system |
| | - Alarm system |
| | - Bilge water control system |
| | - Water treatment system |
| | - Emissions monitoring |
| | - Heating, ventilation and air-conditioning monitoring |
| | - Damage control systems |
| | - Other monitoring and data collection systems eg fire alarms. |
| Access control systems | - Surveillance systems such as CCTV network |
| | - Electronic "personnel-on-board" systems. |
| Cargo management systems | - Cargo Control Room (CCR) and its equipment |
| | - Onboard loading computers and computers used for exchange of loading information and load plan updates with the marine terminal and stevedoring company |
| | - Remote cargo and container tracking and sensing systems |
| | - Level indication system |
| | - Valve remote control system |
| | - Ballast water systems |
| | - Reefer monitoring systems |
| | - Water ingress alarm system. |

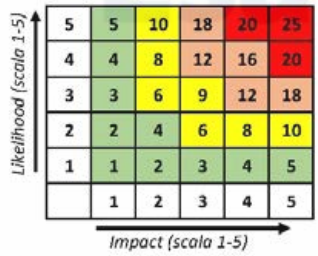
PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

**INITIAL RISK TARGET SYSTEM**

| Category | Sub Category |
|---|---|
| Passenger or visitor servicing and management systems | - Property Management System (PMS) |
| | - Shipmanagement systems (often including electronic health records) |
| | - Financial related systems |
| | - Ship passenger/visitor/seafarer boarding access systems |
| | - Infrastructure support systems like domain naming system (DNS) and user authentication/authorisation systems |
| | - Incident management systems. |
| Passenger-facing networks | - Passenger Wi-Fi or Local Area Network (LAN) internet access, for example where onboard personnel can connect their own devices |
| | - Guest entertainment systems. |
| Core infrastructure systems | - Security gateways |
| | - Routers |
| | - Switches |
| | - Firewalls |
| | - Virtual Private Network(s) (VPN) |
| | - Virtual LAN(s) (VLAN) |
| | - Intrusion prevention systems |
| | - Security event logging systems. |
| Administrative and crew welfare systems | - Administrative systems |
| | - Crew Wi-Fi or LAN internet access, for example where onboard personnel can connect their own devices |

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

**RISK SCORE MATRIX (SCALE 1-25)**




| Likelihood | | Impact | |
|---|---|---|---|
| 1 | *Improbable* | 1 | *Insignificant* |
| 2 | *Unlikely* | 2 | *Minor* |
| 3 | *Reasonable Possible* | 3 | *Moderate* |
| 4 | *Likely* | 4 | *Major* |
| 5 | *Expected* | 5 | *Catastrophic* |

| Initial Risk Assessment - Unweighted & Averaged - Scoring Range (1 to 25) | | | |
|---|---|---|---|
| Low (1-5) | Medium (6-10) | High (11-19) | Extreme (20-25) |

| Final Risk Assessment - Unweighted & Averaged - Scoring Range (1 to 125) | | | |
|---|---|---|---|
| Low (1-27) | Medium (28-59) | High (60-99) | Extreme (100-125) |

| Lv | Impact | Description |
|---|---|---|
| 1 | *Insignificant* (Sangat Rendah) | Aksi dari sumber ancaman terhadap kerentanan sistem telah terjadi sehingga mengakibatkan sangat sedikit kerugian pada organisasi. dampak akibat kejadian dalam waktu relatif singkat |
| 2 | *Minor* (Rendah) | Aksi dari sumber ancaman terhadap kerentanan sistem telah terjadi sehingga mengakibatkan sedikit kerugian pada organisasi. dampak akibat kejadian dalam waktu relatif singkat |
| 3 | *Moderate* (Sedang) | Aksi dari sumber ancaman terhadap kerentanan sistem telah terjadi sehingga mengakibatkan kerugian tidak terlalu besar pada organisasi. |
| 4 | *Major* (Tinggi) | Aksi dari sumber ancaman terhadap kerentanan sistem telah terjadi sehingga mengakibatkan kerugian besar pada organisasi, tidak melumpukan sistem |
| 5 | *Catastrophic* (Sangat Tinggi) | Aksi dari sumber ancaman terhadap kerentanan sistem telah terjadi sehingga mengakibatkan kerugian sangat besar pada organisasi, dapat melumpukan sistem. |

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

**RISK SCORE MATRIX (SCALE 1-25)**

| Lv | Likelihood | Description |
|---|---|---|
| 1 | *Improbable* (Mustahil) | Sumber ancaman belum pernah terjadi, atau belum ada |
| 2 | *Unlikely* (Tidak Berdampak) | Sumber ancaman hampir tidak ada atau tidak terjadi dan tidak termotivasi dan kontrol menanganinya sudah ada |
| 3 | *Reasonable Possible* (Kemungkinan Berdampak) | Sumber ancaman mungkin terjadi dan termotivasi dan kontrol untuk menanganinya sudah ada |
| 4 | *Likely* (Sangat Berdampak) | Sumber ancaman sangat mungkin terjadi, biasanya dalam konteks peralatan yang rusak atau karena kesalahan oleh orang-orang terlibat (jenis kesalahan yang cenderung terjadi di kapal dari waktu ke waktu) dan kontrol untuk menanganinya tidak efektif atau belum ada |
| 5 | *Expected* (Berdampak) | Sumber ancaman sangat terjadi dan berdampak signifikan |

| Lv Risk | Description |
|---|---|
| Extreme | Kebutuhan perbaikan sangat dibutuhkan untuk dilakukan. Sistem tetap berjalan, tetapi perbaikan harus segera dilakukan secepatnya |
| High | Perbaikan sistem dibutuhkan dan harus segera dibuat perencanaan dari proses perbaikan |
| Medium | Perbaikan sistem bisa dilakukan atau resiko bisa diterima |
| Low | Mempersiapkan langkah-langkah perbaikan sistem yang praktis |

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

**INITIAL RISK ACCEPTANCE SYSTEM**

| Index | Category | System | Impact | Likelihood | Initial Risk | Mitigation | Residul Risk |
|---|---|---|---|---|---|---|---|
| 1 | Communication systems | VSAT | Score 4 due to risk of major events like grounding and collision | Score 4 due to password default, IP public, no firewall, connection to business network for access internet | Risk = 4 x 4 = 16 | Password protect and using IP Private | Risk = 4 x 3 = 12 |
| | | | | | | Add Firewall | Risk = 4 x 2 = 8 |
| | | | | | | Limit access internet | Risk = 4 x 1 = 4 |
| 2 | | FBB | Score 4 due to risk of major events like grounding and collision | Score 4 due to password default, IP public, no firewall, connection to business network for access internet | Risk = 4 x 4 = 16 | Password protect and using IP Private | Risk = 4 x 3 = 12 |
| | | | | | | Add Firewall | Risk = 4 x 2 = 8 |
| | | | | | | Limit access internet | Risk = 4 x 1 = 4 |
| 3 | | INM-C | Score 4 due to risk of major events like grounding and collision | Score 2 due to connection to business network for access internet | Risk = 4 x 2 = 8 | Disconnect from business network | Risk = 4 x 1 = 4 |
| 4 | | EMAIL | Score 4 due to risk of major events like spamming/phising Email | Score 2 due to Security Email | Risk = 4 x 2 = 8 | Have Security Email | Risk = 4 x 1 = 4 |
| 5 | Bridge systems | ECDIS | Score 5 due to risk of catastrophic events like grounding and collision | Score 4 due to active USB ports, computer used for other purposes, connection to admin network for access to shared printer, connection to automatic chart updates via satellite via trusted vendor | Risk = 5 x 4 = 20 | Password protect and restrict PC use to ECDIS only | Risk = 5 x 3 = 15 |
| | | | | | | Disconnect from admin network | Risk = 5 x 2 = 10 |
| | | | | | | Blind off USB ports | Risk = 5 x 1 = 5 |
| 6 | | Radar and Radio Communication | Score 3 due to risk of moderate events like data and spoofing | Score 4 due to GPS spoofing, Autonomus vessel, Insufficient data protection | Risk = 3 x 4 = 12 | GPS spoofing | Risk = 3 x 3 = 9 |
| | | | | | | No Autonomus vessel | Risk = 3 x 2 = 6 |
| | | | | | | Data protection | Risk = 3 x 1 = 6 |
| 7 | | AIS | Score 2 due to risk of minor events like open system and encryption | Score 3 due to open system, lack of encryption algorithms | Risk = 2 x 3 = 6 | System Close | Risk = 2 x 2 = 4 |
| | | | | | | New encryption algorithms | Risk = 2 x 1 = 4 |

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

**INITIAL RISK ACCEPTANCE SYSTEM**

| Index | Category | System | Impact | Likelihood | Initial Risk | Mitigation | Residul Risk |
|---|---|---|---|---|---|---|---|
| 8 | Core infrastructure systems | Business Network | Score 5 due to risk of major events like cyber attack | Score 4 due to no firewall, access internet, network segment, connection to OT network | Risk = 5 x 5 = 25 | Add Firewall | Risk = 5 x 4 = 20 |
| | | | | | | Disconnect from admin network | Risk = 5 x 3 = 15 |
| | | | | | | Limit access internet | Risk = 5 x 2 = 10 |
| | | | | | | Different network | Risk = 5 x 1 = 5 |
| 9 | | OT Network | Score 5 due to risk of catastrophic events like cyber attack | Score 5 due to access internet, no firewall, network segment, connection to admin network | Risk = 5 x 5 = 25 | Add Firewall | Risk = 5 x 4 = 20 |
| | | | | | | Disconnect from admin network | Risk = 5 x 3 = 15 |
| | | | | | | No access internet | Risk = 5 x 2 = 10 |
| | | | | | | Different network | Risk = 5 x 1 = 5 |
| 10 | Passenger-facing networks | Passenger/Public | Score 4 due to risk of major events like cyber attack | Score 4 due to open access internet, no firewall, same segment IP with business network for shared folder or printer share | Risk = 4 x 4 = 16 | Add Firewall | Risk = 4 x 3 = 12 |
| | | | | | | Limit access internet | Risk = 4 x 2 = 8 |
| | | | | | | Different network | Risk = 4 x 1 = 4 |
| 11 | Administrative and crew welfare systems | Crew | Score 4 due to risk of major events like cyber attack | Score 4 due to active USB ports, no firewall, connection to business network for access internet via satellite | Risk = 4 x 4 = 16 | Add Firewall | Risk = 4 x 3 = 8 |
| | | | | | | Limit access internet | Risk = 4 x 2 = 8 |
| | | | | | | Blind off USB ports | Risk = 4 x 1 = 4 |

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

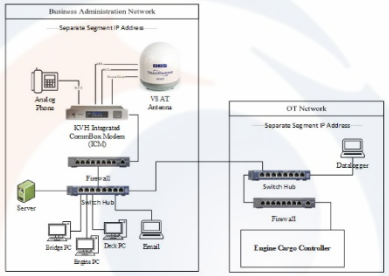
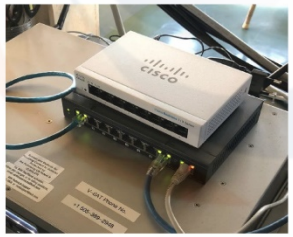
**RISK ASSESSMENT CYBERSECURITY** **PROJECT: MV OCEANIC SUCCESS**

| No | Category | System | Inspect Activity | Result | Score | | Lv | Recommendation Control | Action By |
|---|---|---|---|---|---|---|---|---|---|
| | | | | | Impact | Likelihood | | | |
| 1 | Communication systems | VSAT | 1 Infrastruktur VSAT | 1 Have Own Network Segment | 4 | 1 | L | Keep monitoring traffic data from outside or Portal VSAT | IT |
| | | | 2 Firewall VSAT | 2 Firewall Integrated at ICM KVH | | | | | |
| | | | 3 Password Default | 3 Password Access by Vendor | | | | | |
| | | | 4 IP VSAT | 4 Using IP Private VSAT | | | | | |
| | | | 5 Access Internet | 5 Limited Access Internet | | | | | |
| 2 | | Email | 1 Infrastruktur Email | 1 Have Application email | 4 | 1 | L | Keep monitoring unkown traffic Email | IT |
| | | | 2 Security Email | 2 Integrated Security Email | | | | | |
| 3 | Core infrastructure systems | Business Network | 1 Infrastruktur Network | 1 Different Network Segment | 5 | 1 | L | Change different segment for VDR | IT |
| | | | 2 Firewall | 2 Firewall for Block Access Internet | | | | | |
| | | | 3 Internet Access | 3 Limited Access Internet, Email Only | | | | | |
| 4 | | OT Network | 1 Infrastruktur Network | 1 Different Network Segment | 5 | 1 | L | Keep limit for access internet | IT |
| | | | 2 Firewall | 2 Firewall for Block Another Network | | | | | |
| | | | 3 Internet Access | 3 No Access Internet | | | | | |
| 5 | Administrative and crew welfare systems | Server Business | 1 Access Internet | 1 Limited Access Internet, Email Only | 4 | 2 | M | USB usage monitoring | IT |
| | | | 2 Firewall device | 2 Software and Hardware Firewall | | | | | |
| | | | 3 USB Port | 3 USB Port Active | | | | | |
| 6 | | Laptop Email | 1 Access Internet | 1 Limited Access Internet, Email Only | 4 | 2 | M | USB usage monitoring | IT |
| | | | 2 Firewall device | 2 Software and Hardware Firewall | | | | | |
| | | | 3 USB Port | 3 USB Port Active | | | | | |
| 7 | | OT Dataloger | 1 Access Internet | 1 No Access Internet | 4 | 2 | M | USB usage monitoring | IT |
| | | | 2 Firewall device | 2 Software and Hardware Firewall | | | | | |
| | | | 3 USB Port | 3 USB Port Active | | | | | |

| FINAL SCORE | LEVEL RISK |
|---|---|
| 42 | MEDIUM |

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

**RISK ASSESSMENT TEHNICAL REPORT**

| No | Task | Assessment Result | Summary |
|---|---|---|---|
| 1 | Network Diagram |  | There is 2 segment network onboard, business network and OT network, have separated firewall both of network |
| 2 | Business Firewall |  | Interface business firewall, configuration setup only open some port for application |

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

**RISK ASSESSMENT TEHNICAL REPORT**

| No | Task | Assessment Result | Summary |
|---|---|---|---|
| 3 | OT Firewall |  | Interface OT firewall, configuration block from another network |
| 4 | ICM KVH |  | Integrated Firewall, monitoring, and control by KVH |
| 5 | Datalogger OT |  | Datalogger connection via own firewall |

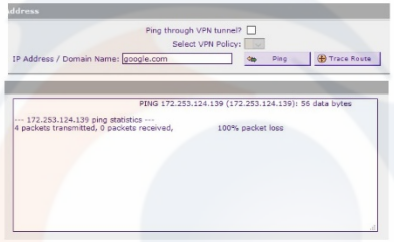
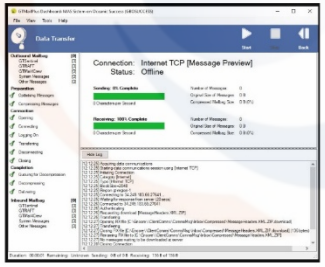
PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

**RISK ASSESSMENT TEHNICAL REPORT**

| No | Task | Assessment Result | Summary |
|---|---|---|---|
| 6 | Network Mapping |  | Using application nmap for network mapping onboard result<br>2 network segment between business and OT<br>At business there's 9 interface connect to network, at OT there's 4 interface connect to network |

PT INDOBARUNA BULK TRANSPORT
PERUSAHAAN PELAYARAN

**RISK ASSESSMENT TEHNICAL REPORT**

| No | Task | Assessment Result | Summary |
|---|---|---|---|
| 7 | Internet Access |  | test result ping to internet using VSAT connection, result can't connect |
| 8 | Email Sending Check |  | Sending email using VSAT connection, result good using thrid party application |