Evaluasi Keamanan Informasi: Studi Kasus PT. Bahtera Bahari Shipyard

Ulfa Amanda [1]*, Antoni Haikal [2]**
* Teknik informatika, Politeknik Negeri Batam
** Rekayasa Keamanan Siber, Politeknik Negeri Batam
ulfa.amanda@students.polibatam.ac.id [1], antoni@polibatam.ac.id [2]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

Information Security; ISO/IEC 27001:2022; Management System; PT. Bahtera Bahari Shipyard.

ABSTRACT

PT. Bahtera Bahari Shipyard is a shipyard company that has implemented ISO 9001; 14001, and 45001 establishes an organized is quality, environment, occupational health and safety. However, as the company relies more on digital operations and must strengthen data protection require the company to establish a more structured information security management approach. Internal audit results indicate that information security remains outside a dedicated system framework. The present research seeks to evaluate organization readiness, identify information security gaps within the existing system, as well as to recommend ISO/IEC 27001:2022 as the Information Security Management System (ISMS). is expected to strengthen the protection of information assets, enhance Standard risk management and control, and integrate information security into the company's existing management systems.

I. PENDAHULUAN

Dalam era digitalisasi industri maritim, keamanan informasi menjadi aspek strategis yang berpengaruh langsung terhadap keberlangsungan operasional dan reputasi perusahaan [1]. PT. Bahtera Bahari Shipyard sebagai salah satu galangan kapal nasional telah menerapkan beberapa sistem manajemen berbasis standar internasional mencakup aspek mutu, lingkungan, serta keselamatan dan kesehatan kerja (ISO 9001:2015; 14001;2015; 45001:2018) [2]-[4], ialah fondasi penting dalam memastikan kualitas layanan, kepatuhan terhadap regulasi lingkungan, serta perlindungan terhadap keselamatan tenaga kerja [5].

Meskipun sistem manajemen tersebut telah berjalan, perkembangan teknologi dan meningkatnya penggunaan sistem informasi dalam kegiatan operasional galangan kapal menghadirkan risiko baru terkait keamanan informasi [6]. Ancaman seperti kebocoran data, serangan siber, penyalahgunaan akses, dan gangguan pada sistem operasional dapat berdampak serius terhadap stabilitas proses bisnis [7]. Hal ini menjadi semakin kritis mengingat perusahaan mengelola data yang bersifat sensitif, antara lain desain kapal, dokumen teknis proyek, informasi pelanggan, dan data operasional lainnya [8].

Untuk menjawab tantangan tersebut, diperlukan suatu kerangka kerja keamanan data yang terstruktur serta terukur. Sistem Manajemen Keamanan Informasi (ISO/IEC 27001:2022) memberikan panduan komprehensif dalam menetapkan kebijakan, mengelola risiko, serta menerapkan kontrol keamanan informasi yang sistematis [6]. Standar ini dirancang dengan struktur Annex SL, sehingga memungkinkan integrasi yang lebih mudah dengan ISO 9001; 14001; 45001 diterapkan oleh perusahaan [6].

Penerapan ISO/IEC 27001:2022 berpotensi memperkuat perlindungan aset informasi PT. Bahtera Bahari Shipyard sekaligus membangun Integrated Management System (IMS) yang mengelola mutu, lingkungan, keselamatan kerja, dan keamanan informasi secara terpadu [9]. Dengan demikian, penelitian ini menjadi penting untuk mengevaluasi kesiapan perusahaan dalam mengelola keamanan informasi serta memberikan rekomendasi penerapan ISO/IEC

27001:2022 guna meningkatkan keandalan operasional dan daya saing di industri galangan kapal modern [10].

II. TINJAUAN LITERATUR

2.1 Keamanan Informasi

Penerapan keamanan informasi agar data terjaga dari gangguan guna menjaga kelangsungan bisnis, meminimalkan risiko, serta memastikan nilai informasi tetap terjaga [12]. Keamanan informasi mencakup kebijakan, prosedur, teknologi, serta aktivitas yang dirancang untuk mencegah penyalahgunaan, kebocoran, dan kerusakan informasi [13].

2.2 CIA Triad

Model CIA Triad adalah konsep fundamental dalam keamanan informasi dan menjadi dasar penyusunan kontrol pada standar internasional seperti ISO/IEC 27001 [12], [14].

1. Confidentiality (Kerahasiaan), menjamin hanya akses informasi pada pihak yang berhak.
2. Integrity (Integritas), menjaga keaslian, utuh, serta terlindungi dari perubahan tanpa izin.
3. Availability (Ketersediaan), menjamin informasi tersedia saat dibutuhkan oleh pengguna yang berwenang.

CIA Triad menjadi kerangka utama dalam mengidentifikasi risiko dan merancang kontrol keamanan informasi pada perusahaan seperti galangan kapal yang bergantung pada data teknis dan operasional.

2.3 ISO/IEC 27001:2022

Standar internasional menjadi pedoman agar mengembangkan, menjalankan, menjaga, serta menyempurnakan ISMS secara konsisten. Melalui pendekatan manajemen risiko, standar ini membantu organisasi memastikan aset informasi tetap terlindungi dan penerapan kontrol keamanan yang sistematis.

ISO/IEC 27001:2022 menggunakan Annex SL, yang memiliki struktur seragam dengan standar manajemen lainnya (ISO 9001, 14001, 45001). Struktur ini mempermudah integrasi dalam sistem manajemen perusahaan. Kontrol keamanan dalam ISO/IEC 27001:2022 mencakup empat kelompok:

a.	Organizational Controls (37 kontrol)
b.	People Controls (8 kontrol)
c.	Physical Controls (14 kontrol)
d.	Technological Controls (34 kontrol)

Kontrol ini digunakan sebagai referensi untuk audit keamanan informasi PT Bahtera Bahari Shipyard.

2.4 Indeks KAMI Versi 4.0

Instrumen penilaian KAMI dikembangkan Badan Siber dan Sandi Negara (BSSN) menggambarkan tingkat kesiapan organisasi mengelola keamanan informasi serta melihat sejauh mana penerapannya berjalan secara matang.

Indeks KAMI Versi 4.0 digunakan sebagai instrumen menilai sejauh mana penerapan keamanan informasi telah dilakukan oleh organisasi sebelum mengimplementasikan ISO/IEC 27001:2022. Indeks KAMI 4.0 mengevaluasi sejumlah bidang penting ialah:

a.	Tata Kelola Keamanan Informasi
b.	Pengelolaan Risiko Keamanan Informasi
c.	Kerangka Kerja Keamanan Informasi
d.	Manajemen Aset Informasi
e.	Teknologi serta Keamanan Informasi

III. METODE PENELITIAN

Metodologi berperan sebagai acuan dalam pelaksanaan studi agar jalannya proses menjadi teratur, terfokus, dan mampu dipertanggung jawabkan secara ilmiah [18]. Analisis kajian difokuskan pada implementasi sistem manajemen terintegrasi pada PT. Bahtera Bahari Shipyard, serta melakukan evaluasi dan rekomendasi penerapan ISO/IEC 27001:2022 sebagai standar tambahan keamanan informasi berperan mendukung sistem manajemen ISO 9001; 14001, dan 45001.

3.1 Jenis dan Pendekatan Penelitian

Jenis deskriptif kualitatif dengan studi kasus sebagai metode penelitian. Pemilihan pendekatan ini bertujuan menggali secara mendalam kondisi nyata di PT Bahtera Bahari Shipyard, khususnya dalam konteks integrasi standar ISO dan kesiapan implementasi ISO/IEC 27001:2022 [21].

Metode deskriptif kualitatif memungkinkan peneliti menggambarkan kondisi sistem keamanan informasi yang ada, melakukan analisis kesenjangan (gap analysis), serta menggunakan Indeks KAMI 4.0 sebagai

instrumen penilaian keamanan informasi.

3.2 Lokasi dan Waktu Penelitian

PT. Bahtera Bahari Shipyard, kawasan industri galangan kapal di Indonesia dipilih lokasi penelitian. Waktu penelitian dilaksanakan selama 4 bulan (Februari-Mei 2025), meliputi tahapan pengamatan aktual, pengumpulan informasi, penelaahan data, serta perancangan laporan akhir.

3.3 Teknik Pengumpulan Data

1. Observasi (Field Observation) — mengamati aktual aktivitas operasional, sistem manajemen, dan infrastruktur keamanan informasi yang diterapkan di perusahaan.
2. Wawancara Terstruktur (Structured Interview) — dilakukan dengan manajer sistem manajemen mutu, kepala departemen IT, serta staf keamanan informasi untuk memperoleh informasi mendalam terkait penerapan ISO dan kebijakan keamanan data.
3. Studi Dokumentasi (Documentation Study) — mengkaji dokumen perusahaan seperti Standard Operating Procedures (SOP), kebijakan mutu, laporan audit internal, serta dokumen sistem manajemen ISO yang telah diterapkan.
4. Checklist Keamanan Informasi dengan Indeks KAMI 4.0 — mengumpulkan informasi menggunakan berbagai teknik pengumpulan data di antaranya wawancara dan pengamatan.

3.4 Instrumen Penelitian

Peneliti berperan sebagai instrumen kunci dengan dukungan alat bantu penelitian:

1. Pedoman wawancara
2. Checklist Indeks KAMI 4.0
3. Formulir observasi lapangan

3.5 Teknik Analisis Data

Analisa interaktif dari Miles dan Huberman (2014) digunakan dalam pengolahan data melalui tiga tahap pokok.

1. Pemilahan Data (Data Reduction) — memilah serta merangkum data penting observasi, interview, serta dokumen.
2. Pemaparan Data (Data Display) — mengorganisasi melalui tabel, grafik, serta narasi.
3. Penyimpulan Data (Conclusion Drawing) — menginterpretasikan temuan penelitian untuk menghasilkan rekomendasi penerapan ISO/IEC 27001:2022.

3.6 Daftar Responden Penelitian

Pemilihan 20 responden dilakukan secara *purposive* sesuai kebutuhan penelitian, yaitu pemilihan responden berdasarkan jabatan, pengalaman kerja, dan keterlibatan langsung dalam pengelolaan sistem manajemen perusahaan. Responden berasal dari berbagai departemen, seperti manajemen, teknologi informasi, engineering, produksi, quality assurance, HSE, keuangan, sumber daya manusia, proyek, dan gudang. Pemilihan responden dari berbagai fungsi organisasi bertujuan agar data yang diperoleh melalui instrumen Indeks KAMI 4.0 dapat menggambarkan kondisi keamanan informasi perusahaan secara menyeluruh dan sesuai dengan ISO/IEC 27001:2022 (SMKI).

No	Kode Responden	Jabatan	Departemen	Masa Kerja	Keterlibatan dalam SMKI
1	R1	General Manager	Manajemen	15 Tahun	Penanggung jawab kebijakan perusahaan
2	R2	Management Representative (MR)	IMS	10 Tahun	Koordinator sistem manajemen ISO
3	R3	QA/QC Manager	Quality Assurance	9 Tahun	Pengendalian mutu dan audit internal
4	R4	HSE Manager	HSE	8 Tahun	Pengelolaan ISO 14001 dan ISO 45001
5	R5	IT Manager	Information Technology	8 Tahun	Pengelolaan sistem informasi
6	R6	IT Supervisor	Information Technology	6 Tahun	Administrasi jaringan dan server
7	R7	System Administrator	Information Technology	5 Tahun	Pengelolaan server dan hak akses
8	R8	Network Administrator	Information Technology	5 Tahun	Keamanan jaringan komputer
9	R9	Engineering Manager	Engineering	12 Tahun	Pengelolaan desain kapal
10	R10	Engineering Supervisor	Engineering	8 Tahun	Pengendalian dokumen desain
11	R11	Production Manager	Produksi	10 Tahun	Pengawasan proses produksi
12	R12	Production Supervisor	Produksi	7 Tahun	Pengendalian proses operasional
13	R13	Procurement Manager	Purchasing	8 Tahun	Pengelolaan dokumen pengadaan
14	R14	Finance Manager	Finance	9 Tahun	Pengelolaan data keuangan
15	R15	HRGA Manager	Human Resources	9 Tahun	Pengelolaan data karyawan
16	R16	Document Control Officer	Document Control	6 Tahun	Pengelolaan dokumen perusahaan
17	R17	Internal Auditor ISO	IMS	7 Tahun	Audit sistem manajemen
18	R18	Project Manager	Project	8 Tahun	Pengelolaan dokumen proyek kapal
19	R19	Warehouse Supervisor	Gudang	6 Tahun	Pengelolaan aset perusahaan
20	R20	Staff Information Technology	Information Technology	4 Tahun	Operasional dan pemeliharaan sistem TI

Gambar 1. Table Daftar responden

departemen	jumlah
manajemen	2
informasi teknologi	5
quality/ IMS	3
engineering	2
produksi	2
HSE	1
finance	1
HRGA	1
purchasing	1
project	1
warehouse	1
total	20 orang

Table 1. Karakteristik responden berdasarkan departemen

IV. HASIL DAN PEMBAHASAN

4.1 Penilaian Menggunakan Indeks KAMI 4.0

Penilaian dilakukan sesuai kondisi skor.

skor	keterangan
1	sangat tidak setuju
2	tidak setuju
3	cukup setuju
4	setuju
5	sangat setuju

tabel 2. Penilaian skor

4.1.1 Hasil dari Responden Menggunakan Indeks KAMI 4.0

Pertanyaan	Mean
Perusahaan memiliki kebijakan keamanan informasi yang terdokumentasi..	3,6
Manajemen memberikan dukungan terhadap penerapan keamanan informasi.	3,5
Tanggung jawab keamanan informasi telah ditetapkan dengan jelas.	3,4
Kebijakan keamanan informasi ditinjau secara berkala.	3,3
Karyawan memahami kebijakan keamanan informasi perusahaan	3,3
Rata-rata Area Tata Kelola	3,42

Tabel 3. Table Kelola kemanan informasi

Pertanyaan	Mean
Risiko keamanan informasi telah diidentifikasi.	2,9
Perusahaan memiliki metode penilaian risiko keamanan informasi.	2,7
Evaluasi risiko dilakukan secara berkala.	2,8
Terdapat tindakan mitigasi terhadap risiko keamanan informasi.	2,9
Hasil penilaian risiko digunakan sebagai dasar pengambilan keputusan.	2,85
Rata-rata Area Risiko	2,83

Tabel 4. Pengelolaan risiko keamanan informasi

Pertanyaan	Mean
Perusahaan memiliki prosedur keamanan informasi yang terdokumentasi.	4,0
SOP keamanan informasi diterapkan dalam operasional.	3,9
Dokumen keamanan informasi diperbarui secara berkala.	4,0
Audit internal keamanan informasi telah dilakukan.	3,95
Terdapat proses evaluasi penerapan keamanan informasi.	3,95
Rata-rata Area Kerangka Kerja	3,96

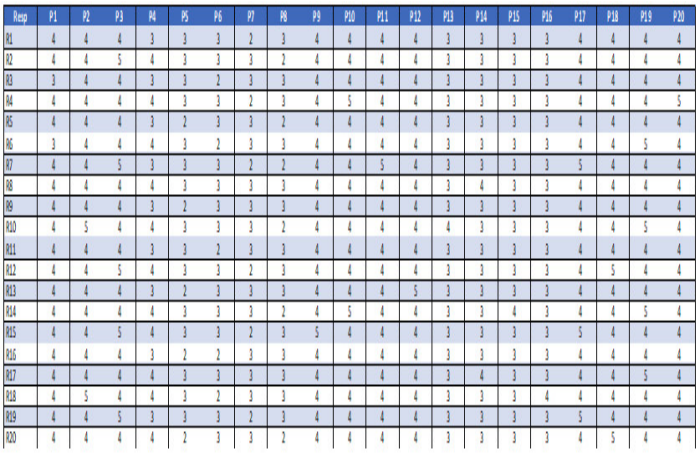
Tabel 5. Kerangka kerja keamanan informasi

Pertanyaan	Mean
Seluruh aset informasi telah diinventarisasi.	3,1
Dokumen penting memiliki klasifikasi keamanan.	3,0
Hak akses diberikan sesuai kewenangan.	3,2
Data proyek kapal disimpan secara aman.	3,1
Aset informasi dievaluasi secara berkala.	3,0
Rata-rata Area Aset Informasi	3,08

Tabel 6. Pengelola asset informasi

Pertanyaan	Mean
Komputer perusahaan menggunakan antivirus yang diperbarui.	3,8
Sistem menggunakan autentikasi pengguna.	3,7
Data perusahaan dicadangkan secara berkala.	3,6
Jaringan perusahaan dilindungi firewall.	3,8
Aktivitas pengguna dicatat dalam log sistem.	3,45
Rata-rata Area Teknologi	3,67

Table 7.Teknologi dan kemaman informasi



Gambar 2. Table Hasil jawaban 20 responden

Perhitungan:

Rata-rata = (3,42 + 2,83 + 3,96 + 3,08 + 3,67) / 5 = 3,39

Nilai maturitas Indeks KAMI 4.0 = 3,39

Kategori: Level III (Terdefinisi)

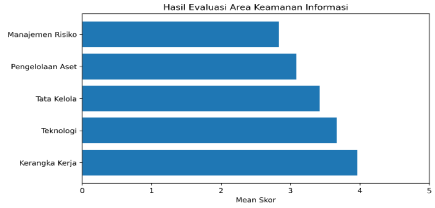
Evaluasi keamanan informasi pada PT. Bahtera Bahari Shipyard dilakukan menggunakan instrumen Indeks KAMI 4.0. Lima aspek utama keamanan informasi menjadi fokus penilaian dengan merujuk pada prinsip ISO/IEC 27001:2022 (SMKI).

area evaluasi	total skor	mean skor
tata kelola kemanan informasi	82	3,42
pengelolaan risiko kemanan informasi	68	2,83
kerangka kerja kemanan informasi	95	3,96
pengelolaan aset informasi	74	3,08
teknologi dan kemananan informasi	88	3,67

Tael 8. Mean skor

Berdasarkan hasil evaluasi, aspek Kerangka Kerja Keamanan Informasi menunjukkan capaian tertinggi dengan mean skor sebesar 3,96, yang menunjukkan bahwa perusahaan telah memiliki prosedur dan dokumentasi yang cukup baik sebagai dampak dari penerapan ISO 9001; 14001, dan 45001 yang mendorong pengendalian proses dan dokumentasi organisasi secara konsisten.

Sementara itu, area Pengelolaan Risiko Keamanan Informasi memperoleh nilai terendah dengan mean skor 2,83. Hal ini menunjukkan bahwa tahapan pengenalan risiko, penialain dampak, serta meminimalkan ancaman masih perlu ditingkatkan agar sesuai dengan persyaratan ISO/IEC 27001:2022.



Gambar 3. Grafik nilai setiap area evaluasi

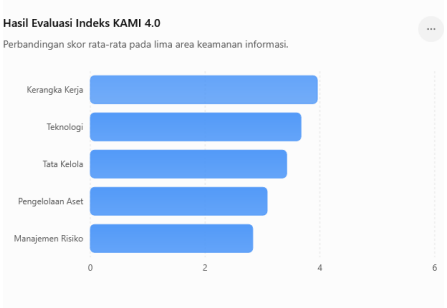
4.2 Total Rata-Rata Area Evaluasi

keterangan	nilai
total skor keseluruhan	407
jumlah area evaluasi	5
rata rata skor	3.39
katagori	cukup baik

Table 9. Skor rata-rata perusahaan

Hasil perhitungan menunjukkan bahwa PT. Bahtera Bahari Shipyard memperoleh rata-rata skor 3,39 di tingkatan Cukup Baik. Perusahaan sudah memiliki pijakan awal baik dalam pengelolaan keamanan informasi, tetapi masih diperlukan perbaikan pada beberapa area, utamanya pengelolaan risiko dan pengelolaan aset informasi agar tingkat kematangan organisasi dapat meningkat secara berkelanjutan.

4.3 Grafik Rata-Rata Skor Perusahaan

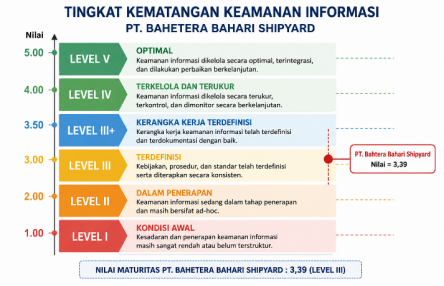


Gambar 4. Hasil Indeks KAMI 4.0

Diagram radar menunjukkan bahwa area Kerja Keamanan Informasi serta Teknologi Keamanan Informasi bernilai tinggi. Sebaliknya, cakupan Pengelolaan Risiko Keamanan Informasi bernilai rendah sehingga menjadi prioritas utama dalam program peningkatan keamanan informasi perusahaan.

Diagram radar juga menunjukkan bahwa tingkat kematangan antar area belum merata, sehingga diperlukan perbaikan yang terintegrasi agar seluruh area dapat mencapai tingkat kematangan yang seimbang.

4.4 Hasil Status Kesiapan Keamanan Informasi Berdasarkan Indeks KAMI 4.0



Gambar 5. Hasil evaluasi Indeks KAMI 4.0

Berdasarkan hasil evaluasi menggunakan Indeks KAMI 4.0, PT. Bahtera Bahari Shipyard memperoleh nilai maturitas sebesar 3,39 yang menempatkan perusahaan pada Level III (Terdefinisi). Tingkat kematangan ini menunjukkan bahwa perusahaan mempunyai ketentuan, prosedur, serta standar terkait perlindungan informasi yang terdokumentasi serta telah diterapkan dalam proses operasional sehari-hari.

Posisi perusahaan yang berada pada Level III menunjukkan bahwa pengelolaan keamanan informasi telah berjalan secara formal dan terstruktur. Hal ini

didukung oleh implementasi sistem manajemen yang telah diterapkan sebelumnya, yaitu ISO 9001:2015; 14001:2015, dan 45001:2018. Seluruh standar tersebut membantu perusahaan dalam membangun budaya dokumentasi, pengendalian proses, dan perbaikan berkelanjutan yang berperan penting dalam implementasi SMKI.

Namun demikian, hasil evaluasi menunjukkan bahwa perusahaan masih berada di bawah Level III+ (Kerangka Kerja Terdefinisi) yang mensyaratkan adanya kerangka kerja keamanan informasi yang lebih komprehensif, terdokumentasi secara menyeluruh, dan diterapkan secara konsisten pada seluruh unit organisasi. Oleh karena itu, diperlukan peningkatan pada aspek pengendalian risiko, manajemen aset informasi, serta pengendalian pengamanan teknologi agar perusahaan dapat mencapai tingkat kematangan yang lebih tinggi.

Dalam perspektif ISO/IEC 27001:2022, pencapaian Level III ini menunjukkan bahwa sebagian besar persyaratan dasar telah tersedia, namun masih diperlukan penyempurnaan pada beberapa klausul utama. Klausul yang telah didukung dengan baik antara lain:

1. Klausul 4 – Context of the Organization, terkait pemahaman konteks organisasi dan ruang lingkup Sistem Manajemen Keamanan Informasi (SMKI).
2. Klausul 5 – Leadership, terkait komitmen manajemen, ketentuan, serta pembagian peran dan kewajiban.
3. Klausul 7 – Support, khususnya dokumentasi dan pengendalian informasi terdokumentasi.
4. Klausul 9 – Performance Evaluation, yang mencakup audit internal dan tinjauan manajemen yang telah diterapkan melalui sistem ISO yang ada.

Sementara itu, klausul yang masih memerlukan peningkatan meliputi:

1. Klausul 6.1 – Risks and Opportunities Management Actions, khususnya proses penilaian dan perlakuan risiko keamanan informasi.
2. Klausul 8.2 dan 8.3 – Information Security Risk Assessment dan Risk Treatment, yang mengharuskan organisasi memiliki metodologi risiko yang terdokumentasi dan diterapkan secara konsisten.
3. Annex A.5 (Organizational Controls), terutama terkait klasifikasi informasi dan kepemilikan aset.
4. Annex A.8 (Technological Controls), khususnya pada penerapan monitoring keamanan, pencatatan log, autentikasi multifaktor (MFA), dan perlindungan data melalui enkripsi.

Dengan nilai maturitas 3,39 (Level III), PT. Bahtera Bahari Shipyard dapat dikatakan memiliki tingkat kesiapan yang cukup baik untuk mengimplementasikan ISO/IEC 27001:2022, namun masih memerlukan peningkatan berkelanjutan agar dapat mencapai Level IV (Terkelola dan Terukur), di mana seluruh proses keamanan informasi telah terukur, dimonitor, dan dievaluasi secara berkala untuk mendukung keberlangsungan bisnis entitas.

V. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Pengamanan informasi PT Bahtera Bahari Shipyard sudah didukung dasar pengelolaan yang cukup kuat. Kondisi ini didukung oleh implementasi standar ISO 9001:2015; 14001:2015, serta 45001:2018 yang diterapkan sebelumnya. Namun demikian, perusahaan masih memerlukan penguatan pada beberapa aspek keamanan informasi agar dapat mencapai tingkat kematangan yang lebih tinggi.

Berdasarkan hasil penelitian, penerapan ISO/IEC 27001:2022 direkomendasikan sebagai langkah strategis untuk meningkatkan efektivitas pengelolaan keamanan informasi, mengurangi risiko keamanan siber, serta mendukung integrasi sistem manajemen.

5.2 Saran

Sehubungan dengan hasil kajian, berikut saran yang bisa dipertimbangan bagi PT. Bahtera Bahari Shipyard adalah sebagai berikut:

1. Perusahaan perlu mengimplementasikan ISO/IEC 27001:2022 sebagai standar SMKI demi meningkatkan perlindungan terhadap aset dan informasi perusahaan.
2. Manajemen perlu menyusun dan memperbarui kebijakan keamanan informasi secara berkala agar mencakup seluruh proses bisnis, aset informasi,

serta penggunaan teknologi informasi, termasuk pemutakhiran infrastruktur teknologi informasi.

3. Perusahaan perlu meningkatkan manajemen risiko keamanan informasi melalui pengenalan risiko, analisa risiko, evaluasi risiko, serta penetapan tindakan pencegahan yang terdokumentasi.
4. Pengelolaan aset informasi perlu diperkuat dengan melakukan inventarisasi aset secara menyeluruh, klasifikasi informasi berdasarkan tingkat kerahasiaan, serta pengendalian akses terhadap aset kritis perusahaan.
5. Integrasi ISO/IEC 27001:2022 dengan ISO 9001:2015; 14001:2015, dan 45001:2018 perlu dilakukan secara Integrated Management System (IMS) agar manajemen mutu, lingkungan, keselamatan kerja, serta keamanan informasi dapat berjalan secara terpadu dan lebih efektif.

DAFTAR PUSTAKA

[1] M. E. Whitman and H. J. Mattord, Principles of Information Security, 7th ed. Boston, MA, USA: Cengage Learning, 2021.

[2] Badan Standardisasi Nasional, SNI ISO 9001:2015 Sistem Manajemen Mutu – Persyaratan. Jakarta, Indonesia: BSN, 2015.

[3] Badan Standardisasi Nasional, SNI ISO 14001:2015 Sistem Manajemen Lingkungan – Persyaratan dan Panduan Penggunaan. Jakarta, Indonesia: BSN, 2015.

[4] Badan Standardisasi Nasional, SNI ISO 45001:2018 Sistem Manajemen Keselamatan dan Kesehatan Kerja – Persyaratan dan Panduan Penggunaan. Jakarta, Indonesia: BSN, 2018.

[5] D. Hoyle, ISO 9000 Quality Systems Handbook, 7th ed. London, U.K.: Routledge, 2017.

[6] International Organization for Standardization, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva, Switzerland: ISO, 2022.

[7] R. von Solms and J. van Niekerk, "From Information Security to Cyber Security," Computers & Security, vol. 38, pp. 97-102, 2013.

[8] A. Calder and S. Watkins, IT Governance: An International Guide to Data Security and ISO 27001/ISO 27002, 7th ed. London, U.K.: Kogan Page, 2023.

[9] S. Karapetrovic and M. Casadesús, "Implementing Environmental with Other Standardized Management Systems: Scope, Sequence, Time and Integration," Journal of Cleaner Production, vol. 17, no. 5, pp. 533-540, 2009.

[10] Badan Siber dan Sandi Negara, Panduan Indeks KAMI 4.0. Jakarta, Indonesia: BSSN, 2024.

[11] M. E. Whitman and H. J. Mattord, Principles of Information Security, 7th ed. Boston, MA, USA: Cengage Learning, 2021.

[12] W. Stallings, Effective Cybersecurity: A Guide to Using Best Practices and Standards. Boston, MA, USA: Addison-Wesley, 2018.

[13] R. von Solms and J. van Niekerk, "From Information Security to Cyber Security," Computers & Security, vol. 38, pp. 97-102, 2013.

[14] Sugiyono, Metode Penelitian Kuantitatif, Kualitatif, dan R&D. Bandung: Alfabeta, 2022.

[15] J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 5th ed. Thousand Oaks, CA: SAGE Publications, 2018.

[16] International Organization for Standardization, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements. Geneva, Switzerland: ISO, 2022