# EVALUASI EFEKTIVITAS PEMETAAN KEAMANAN SIBER DALAM PENERAPAN SISTEM KEAMANAN INFORMASI BERBASIS ISO/IEC 27001:2022 PT JASA RAHARJA

**Setiawan, Ire Puspa Wardhani**
Sekolah Tinggi Manajemen Informatika dan Komputer Jakarta STI&K
Jl. Bri Radio Dalam No.17 1, RT.14/RW.3, Gandaria Utara, Kec. Kby. Baru,
Kota Jakarta Selatan, Daerah Khusus Ibukota Jakarta 12140
*setiawan.mti10@gmail.com*

**ABSTRAK**

Transformasi digital dalam penggunaan teknologi informasi dan internet semakin meningkat, termasuk di sektor asuransi sosial seperti PT Jasa Raharja, sebagai perusahaan yang berada di bawah naungan Kementerian BUMN, memiliki peran strategis dalam pengelolaan data sensitif yang berkaitan dengan kecelakaan lalu lintas dan kendaraan bermotor. Penerbitan ISO/IEC 27001:2022 menuntut organisasi yang telah tersertifikasi ISO/IEC 27001:2013 melakukan transisi dengan penyesuaian terhadap struktur kontrol dan pendekatan manajemen risiko. Namun, kajian yang mengevaluasi efektivitas pemetaan keamanan siber dalam mendukung proses transisi pada sektor ini masih terbatas. Penelitian ini bertujuan menganalisis efektivitas pemetaan keamanan siber dalam penerapan dan transisi SMKI ke ISO/IEC 27001:2022, mengidentifikasi kesenjangan kontrol, serta mengevaluasi dampaknya terhadap pengelolaan risiko, reputasi, dan kredibilitas organisasi. Metode kualitatif dengan pendekatan triangulasi digunakan melalui wawancara, tinjauan dokumen, dan observasi lapangan pada PT Jasa Raharja sebagai studi kasus. Hasil penelitian menunjukkan implementasi SMKI secara umum telah berjalan cukup baik, namun memerlukan perbaikan pada manajemen risiko dan implementasi kontrol baru (threat intelligence, ICT readiness for business continuity, configuration management, data masking), serta integrasi framework INDEKS KAMI untuk meningkatkan maturitas keamanan siber. Hal ini menegaskan bahwa pemetaan keamanan siber berperan penting dalam memastikan kesesuaian standar, meningkatkan ketahanan organisasi, dan memperkuat kepercayaan pemangku kepentingan sesuai UU PDP dan regulasi pemerintah.

***Kata Kunci**: Infrastruktur Teknologi Informasi, Serangan Siber, Sistem Manajemen Keamanan Informasi (SMKI), ISO/IEC 27001:2022, Perlindungan Data.*

## 1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat mendorong organisasi untuk mengadopsi transformasi digital dalam berbagai proses bisnis. Meskipun digitalisasi memberikan kemudahan dan efisiensi, ketergantungan yang tinggi terhadap sistem informasi juga meningkatkan risiko ancaman keamanan siber, khususnya bagi organisasi yang mengelola data sensitif dan kritikal. Sektor jasa dan keuangan termasuk sektor yang rentan terhadap serangan siber, seperti malware, phishing, dan kebocoran data. Serangan siber pada tahun 2022 terhadap sektor jasa keuangan termasuk dalam 5 besar industri yang menjadi tujuan serangan siber, terhitung sejak tahun 2021 sampai 2022 jumlah serangan terhadap sektor keuangan berkurang dan menempatkan sektor ini pada urutan kedua setelah manufaktur [1].

Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001 menjadi kerangka kerja yang diakui secara internasional dalam pengelolaan keamanan informasi. Penerbitan ISO/IEC 27001:2022 sebagai pembaruan dari ISO/IEC 27001:2013 membawa perubahan khususnya pada struktur Annex A yang kini terdiri dari 93 kontrol keamanan informasi yang dikelompokkan ke dalam empat domain utama: organizational, people, physical, dan technological controls. Perubahan ini menuntut organisasi yang telah tersertifikasi untuk melakukan transisi dengan menyesuaikan pendekatan manajemen risiko, mekanisme pengendalian keamanan, serta implementasi kontrol baru yang lebih adaptif terhadap ancaman siber kontemporer. Selain itu, tuntutan kepatuhan terhadap regulasi nasional, termasuk Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi [2] dan Surat Edaran OJK Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber, semakin memperkuat urgensi peningkatan kapabilitas keamanan siber organisasi, khususnya di sektor asuransi nonperbankan.

Kajian yang secara khusus mengevaluasi efektivitas pemetaan keamanan siber dalam mendukung proses transisi ke ISO/IEC 27001:2022 pada sektor asuransi nonperbankan masih terbatas. PT Jasa Raharja sebagai perusahaan asuransi sosial yang mengelola data sensitif dan telah menerapkan SMKI berbasis ISO/IEC 27001:2013 menghadapi tantangan strategis dalam memastikan efektivitas pemetaan keamanan siber dan kesesuaiannya dengan persyaratan standar terbaru. Permasalahan yang muncul meliputi: belum terukurnya efektivitas pemetaan keamanan siber sebagai instrumen evaluasi kesiapan transisi, potensi kesenjangan (gap) antara kondisi eksisting dengan persyaratan ISO/IEC 27001:2022, khususnya pada kontrol baru yang belum terimplementasi serta perlunya kerangka evaluasi sistematis dalam

mendukung proses identifikasi dan pengendalian risiko keamanan informasi.

Oleh karena itu, penelitian ini bertujuan untuk mengevaluasi efektivitas pemetaan keamanan siber dalam penerapan dan transisi SMKI ke ISO/IEC 27001:2022, menganalisis tingkat kesesuaian dengan persyaratan standar, mengidentifikasi kesenjangan kontrol keamanan, serta merumuskan rekomendasi perbaikan strategis guna meningkatkan efektivitas SMKI dan memperkuat kepercayaan stakeholder melalui penguatan perlindungan data dan pengelolaan risiko keamanan informasi secara komprehensif..

## 2. TINJAUAN PUSTAKA

ISO/IEC 27001 merupakan standar internasional yang digunakan secara luas sebagai acuan dalam penerapan SMKI. Versi terbaru, ISO/IEC 27001:2022, menggantikan ISO/IEC 27001:2013 dan membawa perubahan signifikan, khususnya pada struktur Annex A yang kini terdiri dari 93 kontrol keamanan informasi yang dikelompokkan ke dalam empat domain utama, yaitu organizational, people, physical, dan technological controls.

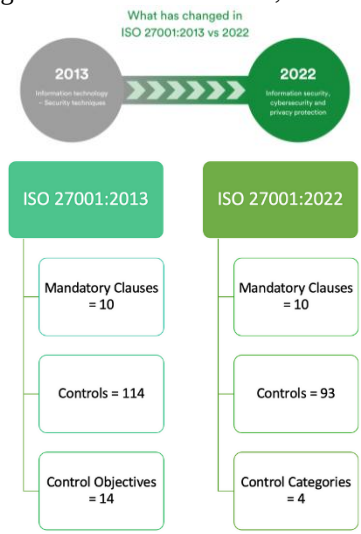

Gambar 1. Manfaat ISO 27001:2022

PT Jasa Raharja sebagai perusahaan asuransi sosial telah menerapkan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001:2013, namun penerbitan ISO/IEC 27001:2022 menuntut penyesuaian signifikan terhadap struktur kontrol dan pendekatan pengelolaan risiko. Hingga saat ini, kajian yang secara khusus mengevaluasi efektivitas pemetaan keamanan siber dalam mendukung proses transisi ke ISO/IEC 27001:2022 pada sektor asuransi nonperbankan masih terbatas. PricewaterhouseCoopers (PwC) tahun 2022, 58% perusahaan fintech global melaporkan adanya ancaman keamanan siber yang mengganggu operasional mereka. Ancaman ini dapat berupa peretasan, pencurian data pribadi, serangan malware, hingga pelanggaran kebijakan privasi yang dapat merugikan pengguna dan merusak reputasi Perusahaan" [3].

Oleh karena itu, penelitian ini menawarkan kontribusi baru dengan mengkaji pemetaan keamanan siber sebagai dasar evaluasi kesiapan transisi SMKI, serta menganalisis dampaknya terhadap pengelolaan risiko, reputasi, dan kredibilitas organisasi, sehingga diharapkan dapat menjadi referensi praktis dan akademik bagi organisasi sejenis.


Gambar 2. CIA Metode

a. Melindungi informasi dalam hal confidentiality, integrity dan availability [5];
b. Memastikan orang-orang, proses, prosedur, dan teknologi yang tepat, tersedia untuk melindungi aset informasi;
c. Membuktikan Komitmen & Tanggung Jawab Top Management terhadap Keamanan informasi organisasi;
d. Membuat suatu Proses Penilaian Rutin yang membantu organisasi untuk terus memantau dan meningkatkan sistem keamanan;




Gambar 3. Transisi Framework ISO 27001

### 2.1. Framework ISO/IEC 27001:2022

Keamanan informasi merupakan upaya sistematis untuk melindungi aset informasi organisasi dari berbagai ancaman guna menjamin kerahasiaan, integritas, dan ketersediaan informasi (confidentiality, integrity, dan availability). Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management System (ISMS) merupakan pendekatan terstruktur berbasis manajemen risiko yang mencakup kebijakan, prosedur, proses, serta kontrol teknis dan nonteknis dalam mengelola keamanan informasi secara berkelanjutan. Pada penelitian ini menggunakan beberapa penilaian, yaitu :

a. Assesmen Mandiri dengan Framework ISO/IEC 27001:2022 sebagai standar global pengelolaan keamanan informasi;
b. Framework Indeks KAMI 4.2 sebagai instrumen nasional evaluasi kesiapan keamanan di institusi publik.

### 2.2. PDCA (Plan Do Check Act)

Dengan siklus kegiatan ini, terdapat fase aktivitas-aktivitas utama yang terdapat pada masing-masing fase pada siklus PDCA.

Pendekatan yang dilakukan dalam penerapan SMKI berdasarkan ISO 27001:2022 ini serupa dengan pendekatan proses pada sistem manajemen kualitas berdasarkan ISO 9001 yaitu dengan menggunakan konsep Plan-Do-Check-Act (PDCA). Pendekatan PDCA ini akan memudahkan pengendalian efektifitas dan efisiensi dan mengarah pada upaya penciptaan suatu struktur yang berdasarkan proses sehingga memungkinkan sekali diintegrasikan dengan sistem-sistem lainnya. Resiko yang terjadi akibat rendahnya tingkat keamanan adalah terjadinya pencurian data, kerugian finansial, pencurian identitas, kehilangan kepercayaan dari client, dan lain-lain [7].


Gambar 4. Plan Do Check Act (PDCA)

Tabel 1. Plan Do Check Act (PDCA)

| Fase PDCA | Tujuan Utama | Klausul ISO 27001 | Aktivitas | Output / Deliverables |
|---|---|---|---|---|
| **PLAN** | Menetapkan dan merencanakan ISMS sesuai konteks organisasi | Klausul 4 – Context of the OrganizationKlausul 5 – LeadershipKlausul 6 – PlanningKlausul 7 – Support | Menentukan konteks organisasi dan stakeholder<br>Menetapkan ruang lingkup ISMS<br>Menetapkan kebijakan keamanan informasi<br>Risk assessment (identifikasi, analisis, evaluasi risiko)<br>Risk treatment dan pemilihan kontrol<br>Menetapkan sasaran keamanan informasi<br>Perencanaan sumber daya dan kompetensi | Dokumen konteks organisasi<br>Scope ISMS<br>Kebijakan keamanan informasi<br>Risk Assessment Report<br>Risk Treatment Plan<br>Statement of Applicability (SoA)<br>Sasaran keamanan informasi |
| **DO** | Mengimplementasikan dan mengoperasikan ISMS | Klausul 7 – SupportKlausul 8 – Operation | Penyediaan SDM, infrastruktur, dan tools<br>Pelatihan dan awareness keamanan informasi<br>Implementasi kontrol Annex A sesuai SoA<br>Pengelolaan aset informasi<br>Pengendalian akses, enkripsi, keamanan jaringan<br>Penanganan insiden keamanan informasi<br>Business Continuity & Disaster Recovery | Dokumen prosedur & SOP ISMS<br>Bukti pelatihan & awareness<br>Kontrol keamanan terimplementasi<br>Incident response record<br>BCP / DRP<br>Log sistem dan catatan operasional |
| **CHECK** | Memantau, mengukur, dan mengevaluasi efektivitas ISMS | Klausul 9 – Performance Evaluation | Monitoring KPI keamanan informasi<br>Evaluasi pencapaian sasaran ISMS<br>Internal audit ISMS<br>Management review<br>Review kepatuhan terhadap regulasi<br>Vulnerability assessment & penetration testing<br>Analisis tren insiden | KPI / dashboard keamanan informasi<br>Laporan internal audit<br>Notulen management review<br>Laporan kepatuhan<br>Hasil VA / PT<br>Laporan analisis insiden |
| **ACT** | Melakukan perbaikan dan peningkatan berkelanjutan ISMS | Klausul 10 – Improvement | Penanganan non-conformity (NC)<br>Root cause analysis<br>Corrective & preventive action<br>Perbaikan proses dan kontrol keamanan<br>Update risk assessment & risk treatment<br>Revisi kebijakan, prosedur, dan SoA | NCR (Non-Conformity Report)<br>Corrective Action Plan / Report<br>Bukti tindakan perbaikan<br>Risk assessment update<br>SoA versi terbaru<br>Improvement action plan |

## 3. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan triangulasi digunakan melalui wawancara, tinjauan dokumen, dan observasi lapangan untuk mengevaluasi kesiapan organisasi dalam mengimplementasikan dan melakukan transisi Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001:2022.

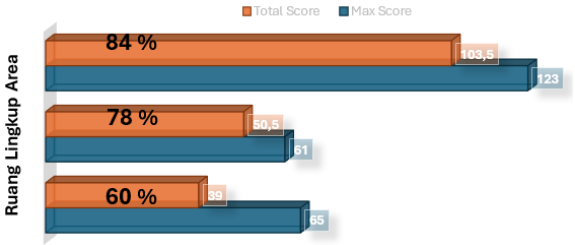
Pendekatan ini dipilih untuk memperoleh pemahaman yang mendalam terhadap kondisi aktual pengelolaan keamanan informasi, perkembangan ancaman siber, kebutuhan akan kepatuhan regulasi, serta pentingnya keamanan informasi sebagai keunggulan kompetitif [4], termasuk kebijakan, proses, kontrol, serta tingkat kesadaran pemangku kepentingan di dalam organisasi;

a. Wawancara (Interview) : Memahami pengeloaan manajemen keamanan informasi dan kesiapan organisasi terhadap transisi ISO/IEC 27001:2022;
b. Tinjauan Dokumen (Document Review) : Mengevaluasi kelengkapan dan kesesuaian dokumen dengan persyaratan ISO/IEC 27001:2022;
c. Observasi Lapangan (Field Observation) : Memverifikasi penerapan kontrol keamanan secara langsung.

## 4. HASIL DAN PEMBAHASAN

Tabel 2. Hasil Pembahasan dengan Framework ISO 27001:2022

| Clause / Annex A | Max Score | Score | Percentage | Max Score | Score | Percentage | Max Score | Score | Percentage |
|---|---|---|---|---|---|---|---|---|---|
| 1. Konteks Organisasi | 2 | 1 | 50% | 2 | 1 | 50% | 4 | 4 | 100% |
| 2. Kepemimpinan | - | - | - | - | - | - | 3 | 3 | 100% |
| 3. Perencanaan | 3 | 0 | 0% | 3 | 2 | 67% | 5 | 3,5 | 70% |
| 4. Dukungan | 5 | 2,5 | 50% | 5 | 4,5 | 90% | 7 | 5,5 | 79% |
| 5. Operasi | 2 | 1 | 50% | 2 | 1,5 | 75% | 3 | 3 | 100% |
| 6. Evaluasi Kinerja | - | - | - | - | - | - | 6 | 6 | 100% |
| 7. Peningkatan | 2 | 2 | 100% | 2 | 2 | 100% | 2 | 2 | 100% |
| 8. Kontrol Organisasi | 23 | 13,5 | 59% | 23 | 19 | 83% | 37 | 30 | 81% |
| 9. Kontrol Orang | 3 | 1,5 | 50% | 3 | 3 | 100% | 8 | 7 | 88% |
| 10.Kontrol Fisik | 14 | 9,5 | 68% | 14 | 11,5 | 82% | 14 | 12,5 | 89% |
| 11.Kontrol Teknologi | 11 | 8 | 73% | 11 | 6 | 55% | 34 | 27 | 79% |
| | **Kantor Wilayah DKI** | **Max Score** | **65** | **Kantor Wilayah Jawa Timur** | **Max Score** | **65** | **Kantor Pusat** | **Max Score** | **123** |
| | | **Total Score** | **39** | | **Total Score** | **50,5** | | **Total Score** | **103,5** |
| | | **Avg %** | **60%** | | **Avg %** | **78%** | | **Avg %** | **84%** |




Gambar 4. Penilaian Hasil dengan Framework ISO 27001:2022

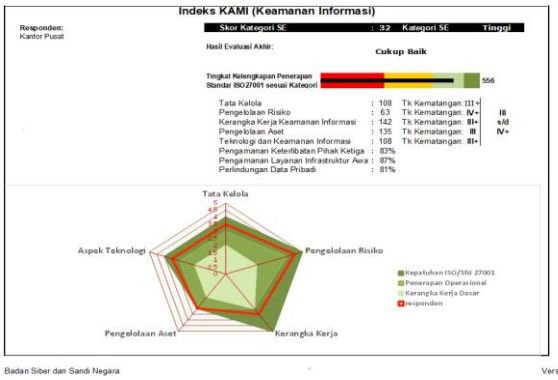
Tabel tersebut menampilkan skor evaluasi kesiapan implementasi ISO 27001:2022 yang terstruktur berdasarkan klausul dan Annex A, kondisi implementasi SMKI di Kantor Pusat dan Kantor Wilayah Jawa Timur untuk implementasi ISO 27001:2022 cukup baik, namun masih ada beberapa area yang perlu diperbaiki untuk memastikan kesesuaian (conformity) terhadap persyaratan ISO 27001:2022.

a. Klausul/Annex A dengan skor terendah menunjukkan prioritas perbaikan, organisasi perlu mengembangkan sistem pemantauan ancaman siber;
b. Proses manajemen risiko, yaitu dengan menambahkan risiko lain yang belum diidentifikasi dan pemetaannya terhadap kontrol Annex A.
c. Finalisasi terhadap dokumen sistem manajemen perlu segera dilakukan diantaranya dokumen kebijakan dan SPO yang terkait.

Improvement perlu dilakukan secara terus menerus terhadap implementasi SMKI, diantaranya dengan mereview kembali ruang lingkup implementasi SMKI. Beberapa hal yang dapat menjadi pertimbangan dalam menentukan ruang lingkup :

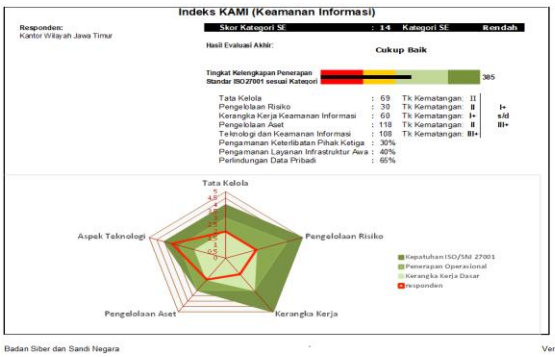
a. Perluasan ruang lingkup mencakup seluruh modul yang ada di dalam aplikasi;
b. Perluasan ruang lingkup mencakup tambahan lokasi kantor wilayah selain dari yang sudah termasuk di dalam cakupan ruang lingkup sebelumnya.

Penilaian dengan menggunanakan Indeks KAMI kemudian mengintegrasikan Indeks KAMI ke dalam program peningkatan SMKI berbasis ISO/IEC 27001:2022 memberikan pendekatan komprehensif yang menggabungkan standar internasional dengan konteks regulasi nasional, sehingga organisasi tidak hanya mencapai compliance tetapi juga membangun kapabilitas keamanan informasi yang matang dan berkelanjutan



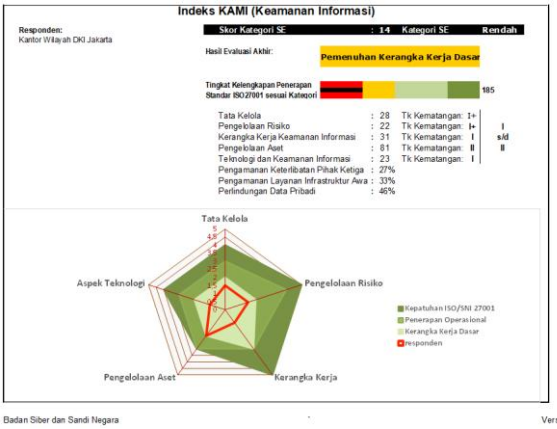

Gambar 5. Penilaian Hasil dengan Indeks KAMI 4.2 Kantor Pusat

- Skor Kategori Sistem Elektronik 32 dengan Kategori Tinggi
- Hasil evaluasi skhir cukup baik




Gambar 6. Penilaian Hasil dengan Indeks KAMI 4.2 Kantor Wilayah Jawa Timur

- Skor Kategori Sistem Elektronik 14 dengan Kategori Rendah
- Hasil evaluasi akhir cukup baik




Gambar 7. Hasil Penilaian dengan Indeks KAMI 4.2 Kantor Wilayah DKI Jakarta

- Skor Kategori Sistem Elektronik 14 dengan Kategori Rendah
- Hasil evaluasi Akhir pemenuhan kerangka kerja dasar

Berdasarkan kegiatan penilaian kesiapan yang telah dilakukan, ditemukan beberapa poin kesenjangan yang dapat ditingkatkan untuk memastikan pemenuhan (compliance) terhadap standard ISO 27001:2022.

Tabel 3. Hasil Analisis

| KLAUSUL / ANNEX A | KESENJANGAN |
|---|---|
| 6.1.2. Asesmen risiko keamanan informasi<br>6.1.3. Penanganan risiko keamanan informasi | Risiko yang ada di dalam risk register tidak dipetakan terhadap kontrol Annex A di SoA |
| A.5.1. Kebijakan keamanan informasi | Dokumen kebijakan masih dalam bentuk draft |
| A.5.12. Klasifikasi informasi | Klasifikasi informasi ditentukan hanya berdasar aspek kerahasiaan saja |
| A.5.16. Manajemen identitas | Review hak akses belum dilakukan secara berkala |
| A.5.21. Memanajemeni keamanan informasi dalam rantai pasokan TIK | Belum ada poin keberlangsungan pasokan dari suplier dengan cara yang ditetapkan oleh organisasi |
| A.5.22. Pemonitoran, reviu, dan manajemen perubahan layanan pemasok | Formulir evaluasi suplier belum ada poin yang menyatakan terkait evaluasi keamanan informasi |
| A.5.29. Keamanan informasi selama disrupsi | Di dalam pedoman BCM belum mencantumkan kriteria keamanan informasi di lokasi alternatif |
| A.5.31. Persyaratan legal, statutori, regulatori, dan kontraktual | Belum ada identifikasi pendekatan yang harus dilakukan untuk pemenuhan persyaratan Undang-Undang |

| KLAUSUL / ANNEX A | KESENJANGAN |
|---|---|
| A.6.1. Skrining | Screening untuk pegawai existing belum dilakukan |
| A.6.2. Syarat dan ketentuan ketenagakerjaan | Di dalam kontrak kerja pegawai belum terdapat tanggung jawab perusahaan untuk menjaga data pegawai |
| A.7.8. Penempatan dan proteksi peralatan | Makan dan minum di meja kerja masih diperbolehkan |
| A.8.1. Perangkat titik akhir pengguna | Sudah ada peraturan dalam pedoman, namun masih belum ada implementasi dan identifikasi risiko terkait penggunaan perangkat pribadi. |
| A.8.4. Akses ke kode sumber | Kebijakan mengenai pengendalian terhadap source code sudah terdapat di kebijakan pedoman keamanan informasi, namun masih belum spesifik |
| A.8.7. Proteksi terhadap perangkat perusak | Pada device yang menggunakan OS mac belum ada peraturan perlindungan tekait dengan virus/malware |
| A.8.9. Manajemen konfigurasi | Belum terdapat pedoman yang mengatur konfigurasi standard perangkat |
| A.8.11. Penyamaran (masking) data | • Peraturan data masking terkait dengan PII masih dalam on progres<br>• Pedoman data masking secara umum belum ada |
| A.8.12. Pencegahan kebocoran data | Pernah menggunakan tools DLP untuk di email |
| A.8.13. Pencadangan informasi | • Belum terdapat rencana backup di organisasi<br>• Uji restore belum ada laporannya |
| A.8.15. Membuat log | Log Activity masih belum ada |
| A.8.26. Persyaratan keamanan aplikasi | Dalam aktivitas pegembangan aplikasi, security requirement definition masih belum ada |
| A.8.27. Prinsip-prinsip arsitektur dan rekayasa sistem yang aman | Prinsip pengembangan yang aman belum dicantumkan dalam pedoman |

Dengan pertimbangan dalam melakukukan pengembangan rekomendasi bahwa meningkatkan kualitas implementasi kontrol SMKI untuk aplikasi kritikal lebih baik diutamakan dibandingkan dengan memperluas cakupan lokasi implementasi namun dengan kualitas kontrol yang minimum.

Tabel 4. Pengembangan Rekomendasi

| KLAUSUL / ANNEX A | REKOMENDASI |
|---|---|
| 6.1.2. Asesmen risiko keamanan informasi<br>6.1.3. Penanganan risiko keamanan informasi | • Melakukan identifikasi ulang untuk seluruh risiko dan dipetakan terhadap kontrol Annex A.<br>• Memastikan bahwa seluruh kontrol Annex A yang applicable di SoA telah dipetakan terhadap risiko yang ada di Risk Register |
| A.5.1. Kebijakan keamanan informasi | Pastikan sebelum audit internal/eksternal dokumen sudah disahkan |
| A.5.12. Klasifikasi informasi | Klasifikasi informasi sebaiknya mengacu pada aspek CIA, bukan hanya berdasarkan aspek kerahasiaan saja |
| A.5.16. Manajemen identitas | • Pastikan hak akses di review secara berkala dan didokumentasikan<br>• Berdasarkan hasil review jika diperlukan lakukan update terhadap hak akses<br>• Pastikan setiap individu mendapatkan hak akses yang unik sesuai dengan kewenangannya |
| A.5.21. Memanajemeni keamanan informasi dalam rantai pasokan TIK | Organisasi harus memastikan pasokan dari suplier di antaranya:<br>• mengindentifikasi apakah suplier memiliki sub suplier<br>• ditambahkan risiko kegagalan suplier pada risk register |
| A.5.22. Pemonitoran, reviu, dan manajemen perubahan layanan pemasok | Memasukan poin keamanan informasi pada formulir evaluasi suplier di kolom checklist evaluasi. |
| A.5.29. Keamanan informasi selama disrupsi | Pastikan Business Continuity Plan mencantumkan persyaratan kontrol keamanan informasi |
| A.5.31. Persyaratan legal, statutori, regulatori, dan kontraktual | Identifikasi pendekatan yang dilakukan untuk pemenuhan persyaratan perundang undangan |
| A.6.1. Skrining | Pastikan screening social media analytic dilakukan baik untuk pegawai existing dan juga untuk non pegawai |
| A.6.2. Syarat dan ketentuan ketenagakerjaan | Kontrak kerja pegawai harus mencantumkan bahwa perusahaan bertanggung jawab menjaga data pegawai |
| A.7.8. Penempatan dan proteksi peralatan | Sebaiknya meja kerja dan perangkat kerja dijauhkan dari sumber potensi risiko seperti makanan dan minuman |
| A.8.1. Perangkat titik akhir pengguna | • Pastikan dalam risk register dimasukkan terkait dengan perangkat user dan juga perangkat pribadi<br>• Menambahkan bab khusus terkait dengan penggunaan perangkat pribadi dan kontrol mengenai perangkat pribadi |

| KLAUSUL / ANNEX A | REKOMENDASI |
|---|---|
| | • Memastikan implementasi pengamanan perangkat mobile milik pribadi dan mengidentifikasi kontrol tambahan perangkat pribadi |
| A.8.4. Akses ke kode sumber | • Perlu ditambahkan aturan spesifik terkait dengan pengendalian dan akses terhadap source code di dalam pedoman pengelolaan keamanan informasi |
| A.8.7. Proteksi terhadap perangkat perusak | Dibuatkan aturan terkait antivirus untuk perangkat yang menggunakan OS Mac |
| A.8.9. Manajemen konfigurasi | Membuat pedoman mengenai standar untuk konfigurasi keamanan, perangkat keras, jaringan, perangkat lunak, dan layanan |
| A.8.11. Penyamaran (masking) data | Membuat aturan mengenai data masking untuk seluruh data yang sifatnya sensitif tidak hanya data pribadi |
| A.8.12. Pencegahan kebocoran data | Pertimbangkan untuk penggunaan tools DLP sebaiknya digunakan kembali |
| A.8.13. Pencadangan informasi | Menyusun backup plan dan melakukan uji restore |
| A.8.15. Membuat log | Memastikan event log pada aplikasi diterapkan dan direview secara berkala |
| A.8.26. Persyaratan keamanan aplikasi | Membuat security requirement definition |
| A.8.27. Prinsip-prinsip arsitektur dan rekayasa sistem yang aman | Menambahkan prinsip pengembangan yang aman mengacu ke standard best practice yang ada |

## 5. KESIMPULAN DAN SARAN

Berdasarkan hasil penilaian kesiapan implementasi ISO/IEC 27001:2022 yang telah dilakukan, dapat disimpulkan bahwa kondisi implementasi SMKI di Kantor Pusat PT Jasa Raharja berada pada kategori cukup baik, namun masih terdapat beberapa area yang memerlukan perbaikan untuk memastikan kesesuaian (conformity) terhadap persyaratan ISO/IEC 27001:2022 [6]. Perbaikan prioritas yang perlu dilakukan mencakup penyempurnaan proses manajemen risiko dengan menambahkan identifikasi risiko lain yang belum teridentifikasi sebelumnya serta melakukan pemetaan ulang terhadap kontrol Annex A yang relevan.

Untuk memperkuat evaluasi kematangan keamanan siber secara komprehensif, organisasi perlu mengintegrasikan framework penilaian maturitas keamanan siber menggunakan Indeks KAMI [8] ke dalam program peningkatan berkelanjutan (continuous improvement) SMKI. Integrasi ini akan memberikan baseline assessment yang terukur dan membantu organisasi dalam mengidentifikasi kesenjangan (gap) secara lebih objektif. Selain itu, terdapat beberapa kontrol baru yang diperkenalkan dalam standar ISO/IEC 27001:2022 yang masih memerlukan implementasi dan perbaikan, di antaranya threat intelligence untuk deteksi dini ancaman siber, ICT readiness for business continuity guna memastikan kesinambungan layanan teknologi informasi, configuration management untuk pengelolaan konfigurasi sistem yang aman, dan data masking sebagai mekanisme perlindungan data sensitif.

Langkah perbaikan strategis lainnya adalah melakukan peninjauan ulang (review) terhadap ruang lingkup implementasi SMKI dengan mempertimbangkan berbagai aspek yang diatur dalam Surat Edaran Otoritas Jasa Keuangan Nomor 29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber. Aspek-aspek tersebut mencakup penilaian risiko terkait keamanan siber, penerapan manajemen risiko keamanan siber, implementasi proses ketahanan siber (cyber resilience), penilaian tingkat maturitas keamanan siber, pelaksanaan pengujian keamanan siber secara berkala, serta mekanisme pelaporan insiden siber yang responsif dan terstruktur. Dengan implementasi rekomendasi perbaikan ini secara sistematis, diharapkan organisasi dapat meningkatkan efektivitas SMKI, memperkuat postur keamanan informasi, serta memenuhi persyaratan regulasi nasional dan standar internasional secara berkelanjutan.

Beberapa aspek seperti penilaian risiko terkait keamanan siber, penerapan menajemen risiko terkait keamanan siber, penerapan proses ketahanan siber, penilaian tingkat maturitas keamanan siber, pengujian keamanan siber dan laporan insiden siber dapat di atur sesuai dengan Surat Edaran Otoritas Jasa Keuangan Nomor 29/SEOJK.03/2022 tentang ketahanan dan keamanan siber [9].

Terdapat beberapa rekomendasi strategis untuk meningkatkan efektivitas implementasi SMKI berbasis ISO/IEC 27001:2022. PT Jasa Raharja perlu melakukan pemutakhiran pemetaan keamanan siber secara berkala agar selaras dengan perkembangan ancaman dan kebutuhan organisasi, serta memperkuat proses manajemen risiko melalui identifikasi risiko baru dan pemetaan kontrol Annex A yang lebih komprehensif. Peningkatan kesadaran dan kompetensi SDM menjadi prioritas yang harus didukung melalui program pelatihan dan sosialisasi berkelanjutan untuk membangun budaya keamanan informasi di seluruh level organisasi. Dokumentasi dan mekanisme pengendalian keamanan informasi perlu diperbaiki dan distandarisasi, termasuk penyusunan kebijakan, prosedur operasional standar, dan work instruction yang jelas.

Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Management System (ISMS) terbukti mampu meningkatkan kepercayaan pelanggan dan mitra bisnis melalui penguatan perlindungan data dan pengelolaan risiko keamanan informasi secara sistematis [10] dan memperluas objek penelitian pada

sektor asuransi nonperbankan lainnya atau industri jasa keuangan berbeda untuk memperoleh hasil yang lebih komprehensif [11].

## DAFTAR PUSTAKA


[1] IBM Security, *X-Force Threat Intelligence Index 2023*, IBM, 2023. [Online]. Available: https://www.ibm.com/downloads/cas/WGL03140.

[2] Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi, 2022. [Online]. Available: https://jdih.setkab.go.id/PUUdoc/176837/Salinan_UU_Nomor_27_Tahun_2022.pdf

[3] M. Lestari, M. E. Puspita, A. F. Wijaya, and Vicky, "Model tata kelola TI terintegrasi untuk keamanan informasi di sektor fintech," *Jurnal Teknologi dan Manajemen Industri Terapan (JTMIT)*, vol. 4, no. 3, pp. 766–776, Sep. 2025.

[4] Frangky and R. Sinaga, "Penerapan ISO/IEC 27001:2022 dalam tata kelola keamanan sistem informasi: Evaluasi proses dan kendala," *Nuansa Informatika*, vol. 18, no. 2, pp. 46–54, Jul. 2024.

[5] N. F. Harahap and M. I. P. Nasution, "Evaluasi keamanan sistem informasi manajemen perusahaan asuransi," *Jurnal Ilmiah Research Student*, vol. 1, no. 3, pp. 200–206, Jan. 2024, doi: 10.61722/jirs.v1i3.564

[6] A. Nurani and F. Arsyad, "Evaluasi Implementasi ISO/IEC 27001:2013 untuk Meningkatkan Keamanan Informasi dan Kepercayaan Stakeholder," *Jurnal Teknologi Informasi & Keamanan Digital*, vol. 5, no. 2, pp. 115–124, 2023.

[7] International Organization for Standardization, ISO/IEC 27001:2022 Information Security, *Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements*, 2022. [Online]. Available: https://www.iso.org/standard/27001

[8] Badan Siber dan Sandi Negara, *Indeks KAMI*. [Online]. Available: https://www.bssn.go.id/indeks-kami/.

[9] Otoritas Jasa Keuangan Republik Indonesia, *Surat Edaran OJK Nomor 29/POJK.03/2022 tentang Ketahanan dan Keamanan Siber Bagi Bank Umum*, 2022. [Online]. Available: https://ojk.go.id/id/regulasi/Pages/Ketahanan-danKeamanan-Siber-Bagi-Bank-Umum.aspx

[10] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements https://www.iso.org/standard/27001

[11] Komisioner, D., & Jasa, O. 2022b. Salinan Surat Edaran Otoritas Jasa Keuangan Republik Indonesia Nomor 29 /POJK.03/2022 Tentang Ketahanan dan Keamanan Siber Bagi Bank Umum. Surat Edaran Otoritas Jasa Keuangan, 111. https://ojk.go.id/id/regulasi/Pages/Ketahanan-danKeamanan-Siber-Bagi-Bank-Umum.aspx