BAB I PENDAHULUAN

I.1 Latar Belakang

Digitalisasi yang berkembang dengan pesat membuat perusahaan menjadi ketergantungan pada sistem informasi dalam pengelolaan operasional data pelanggan. Saat ini ancaman siber, seperti malware, ransomware, dan serangan phishing, menjadi semakin umum dan canggih, sehingga perusahaan perlu menyiapkan strategi mitigasi yang efektif (Whitman & Mattord, 2019). Penelitian menunjukkan bahwa kerugian yang diakibatkan oleh insiden keamanan informasi berdampak pada finansial yang serius, serta dapat merusak reputasi dan kepercayaan *stakeholder* (Ripa Sitompul & Muhammad Nasution, 2023). Menurut laporan dari Badan Siber dan Sandi Negara tercatat bahwa pada tahun 2023, ditemukan 279,84 juta serangan siber dan dalam paruh kedua 2023, tercatat 43 serangan siber per detik di berbagai sektor, termasuk pemerintahan dan perusahaan (BSSN, 2023). Selain itu, banyaknya trafik anomali yang terdeteksi, seperti aktivitas *backdoor communication* dan *command-and-control* menunjukkan bahwa implementasi infrastruktur digital di Indonesia masih rentan sehingga BSSN dan organisasi terkait mengambil langkah sistematis untuk meningkatkan kesadaran serta perlindungan yang lebih baik. Namun, dikarenakan tren serangan bervariasi dan semakin canggih menunjukkan bahwa masih ada kesenjangan dalam mitigasi risiko (BSSN, 2023). Manajemen risiko keamanan sistem informasi diperlukan untuk mengidentifikasi kebutuhan perusahaan terkait persyaratan keamanan informasi dan untuk menciptakan Sistem Manajemen Keamanan Informasi (SMKI) yang efektif (ISO 27005, 2018).

Perusahaan seperti PT. Super Pembayaran Indonesia, yang beroperasi di bidang *fintech* (*financial technology)* memiliki tantangan besar dalam memastikan perlindungan data sensitif pelanggan, termasuk data keuangan perusahaan agar tetap aman. Hal ini didukung dengan peningkatan serangan siber yang membuat PT. SPI sebagai perusahaan *fintech* menjadi target utama karena nilai strategis data yang dikelola. Mengacu pada Peraturan Otoritas Jasa Keuangan (POJK) No. 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank mewajibkan perusahaan yang berada dalam sektor

jasa keuangan atau bermitra dengan bank melakukan manajemen risiko IT yang komprehensif, utamanya dalam penilaian risiko yang mencakup ancaman terhadap data, sistem IT dan operasional, serta memastikan perusahaan memiliki langkah mitigasi yang terdokumentasi dengan baik. Selain itu, Peraturan Bank Indonesia (PBI) No. 9/15/2007 tentang Sistem Manajemen Keamanan Informasi bagi Penyedia Jasa Sistem Pembayaran, bahwa penyelenggara jasa pembayaran harus melindungan keamanan data transaksi dan menyusun kebijakan serta prosedur terkait keamanan informasi. Terdapat pula Peraturan Pemerintah (PP) No. 71 Tahun 2019 tentang Penyelenggaran Sistem dan Transaksi Elektronik (PSTE) mewajibkan penyelenggaran sistem elektronik untuk menjaga kerahasiaan, keutuhan dan ketersediaan data.

Implementasi standar internasional seperti ISO/IEC 27005:2022 memberikan kesempatan bagi PT. SPI yang belum menerapkan SMKI memiliki landasan yang lebih kuat untuk mengelola risiko keamanan informasi khususnya pada aset IT perusahaan. ISO 27005:2022 memberikan panduan yang komprehensif untuk manajemen risiko keamanan informasi, dengan fokus pada proses identifikai, analisis, dan pengelolaan risiko yang berkaitan dengan aset IT. Kerangka kerja ini dirancang untuk membantu perusahaan mengintegrasikan manajemen risiko ke dalam praktik bisnis sehari-hari (ISO 27005, 2018). Penerapan ISO/IEC 27005:2022 tidak hanya akan meningkatkan keamanan informasi di perusahaan, tetapi juga memungkinkan perusahaan untuk memenuhi standar internasional yang diakui, yang penting dalam membangun kepercayaan dengan klien dan mitra bisnis. Selain itu, ISO 27005:2022 fleksibel dalam diterapkan di berbagai perusahaan, baik bagi yang telah menerapkan sebelumnya bahkan yang belum menerapakan standar manajemen risiko di perusahaannya.

PT. SPI merupakan perusahaan yang bergerak di bidang solusi pembayaran digital yang menyediakan layanan pembayaran, pulsa, paket data, tagihan PLN (Perusahaan Listrik Negara), dan PPOB (*Payment Point Online Bank*). Sebagai perusahaan yang telah beroperasi selama 15 tahun, PT. SPI memiliki lebih dari 50.000 mitra di seluruh Indonesia. Hal ini menuntut perusahaan untuk terus melakukan pengembangan manajemen risiko IT, khususnya pada aset IT yang sangat bergantung pada infrastruktur yang stabil dan aman. Namun, dalam

operasionalnya, PT. SPI pernah menghadapi permasalahan praktis terkait keamanan sistem informasi, seperti kebakaran perangkat keras yang disebabkan oleh tegangan arus pendek dan ledakan yang mengakibatkan kerusakan signifikan pada perangkat penting. Insiden ini menyebabkan kerusakan pada beberapa PC dan komputer yang digunakan untuk operasional perusahaan, serta hilangnya dokumen-dokumen penting, termasuk data karyawan yang tidak terduga. Data karyawan yang hilang mencakup informasi pribadi yang sensitif dan catatan riwayat kerja yang menjadi bagian penting dalam pengelolaan sumber daya manusia perusahaan.

Konsekuensi dari insiden ini sangat signifikan. Selain kerugian material berupa perangkat keras yang rusak, kehilangan data yang vital dapat mengganggu operasional perusahaan dalam jangka panjang. Hilangnya data karyawan dapat menimbulkan masalah terkait pemrosesan penggajian, pengelolaan absensi, dan manajemen sumber daya manusia lainnya. Selain itu, kerusakan perangkat keras juga dapat menghambat produktivitas tim, memperlambat proses pembayaran dan layanan lainnya yang bergantung pada sistem digital yang ada. Insiden ini juga menimbulkan risiko terhadap reputasi perusahaan, karena kebocoran atau kehilangan data pribadi karyawan berpotensi menimbulkan masalah hukum atau tuntutan dari pihak terkait, seperti karyawan atau badan pengatur yang bertanggung jawab atas perlindungan data pribadi.

Menanggapi permasalahan tersebut, PT. SPI menyadari pentingnya penerapan manajemen risiko yang lebih matang. Penerapan ISO 27005 memiliki pendekatan terstruktur yang tidak hanya meningkatkan postur keamanan organisasi secara keseluruhan, tetapi juga selaras dengan standar ISO/IEC 27001 yang lebih luas, yang berfokus pada pembentukan Sistem Manajemen Keamanan Informasi (SMKI) untuk memastikan perlindungan yang lebih baik terhadap aset IT Perusahaan (Alheadary, 2023). Dengan mengintegrasikan ISO 27005 ke dalam operasi mereka, PT. SPI dapat memastikan bahwa strategi manajemen risiko mereka disesuaikan dengan konteks dan kerentanan spesifik mereka, sehingga meningkatkan ketahanan mereka terhadap ancaman siber dan risiko keamanan lainnya (Hamit et al., 2020).

Manfaat lain dari penerapan ISO 27005 adalah peningkatan kepercayaan pemangku kepentingan melalui komitmen yang lebih kuat untuk melindungi informasi sensitif, yang secara signifikan dapat meningkatkan kepercayaan di antara klien, mitra, dan badan pengatur (Alheadary, 2023). Selain itu, penetapan kerangka kerja yang jelas untuk manajemen risiko memungkinkan PT. SPI untuk mengoptimalkan sumber daya yang dimiliki, meminimalkan dampak finansial dari insiden keamanan, fokus pada risiko kritis, serta meningkatkan kinerja operasional perusahaan melalui integrasi ISO/IEC 27005 dengan sistem manajemen lainnya (Junior Abinel & Arima Carlos, 2023). Dengan langkah-langkah ini, PT. SPI diharapkan dapat lebih siap dalam menghadapi risiko yang dapat mengancam keamanan informasi dan operasional perusahaan di masa depan.

Penelitian ini bertujuan untuk menganalisis dan menerapkan ISO 27005:2022 sebagai metode untuk mengidentifikasi, menganalisis, mengevaluasi dan mengelola risiko keamanan informasi khususnya pada aset IT di PT. SPI. Fokus utama dari penelitian ini meliputi proses manajemen risiko yang dilakukan pada klausul *context establishment, risk assessment,* dan *risk treatment*. Melalui pendekatan ini, diharapkan penelitian ini dapat memberikan wawasan yang lebih baik bagi manajemen dalam mengambil keputusan yang informasional dan strategis. Penelitian ini diharapkan dapat memberikan kontribusi signifikan terhadap praktik keamanan informasi di sektor *fintech*, dengan fokus khusus pada perlindungan aset IT. Dengan menerapkan ISO 27005:2022, PT. SPI dapat meningkatkan ketahanan sistem informasi mereka, mengurangi risiko yang dihadapi, dan membangun budaya keamanan informasi yang berkelanjutan. Hasil dari penelitian ini tidak hanya akan bermanfaat bagi PT. SPI, tetapi juga dapat menjadi panduan bagi perusahaan lain dalam industri serupa untuk memperkuat sistem keamanan informasi mereka di dunia digital yang terus berubah.

Berdasarkan pemaparan di atas, peningkatan ancaman siber yang semakin canggih dan kompleks membuat perusahaan seperti PT. Super Pembayaran Indonesia (SPI) menghadapi tantangan besar dalam melindungi data sensitif dan memastikan keamanan sistem informasi mereka. Penerapan ISO 27005:2022 sebagai kerangka kerja manajemen risiko keamanan informasi memberikan

landasan yang kuat untuk mengidentifikasi, menganalisis, dan mengelola risiko terkait aset IT perusahaan secara sistematis. Selain meningkatkan ketahanan terhadap ancaman, penerapan standar ini juga mendukung kepatuhan terhadap regulasi nasional, seperti POJK, PBI, dan PP PSTE, sekaligus memperkuat kepercayaan pemangku kepentingan melalui komitmen terhadap perlindungan informasi. Penelitian ini bertujuan memberikan wawasan strategis bagi PT. SPI dalam meningkatkan postur keamanan informasi mereka, yang tidak hanya relevan untuk perusahaan tetapi juga dapat menjadi referensi berharga bagi industri *fintech* lainnya dalam menghadapi dinamika keamanan di era digital.

I.2 Perumusan Masalah

Berdasarkan pemaparan latar belakang di atas, maka dapat dirumuskan beberapa masalah yang mendasari penelitian ini, di antaranya :

1. Bagaimana kondisi pengelolaan risiko keamanan sistem informasi pada aset IT PT. SPI berdasarkan ISO 27005:2022 ?
2. Bagaimana rekomendasi pengelolaan risiko keamanan sistem informasi pada aset IT PT. SPI berdasarkan ISO 27005:2022 ?

I.3 Tujuan Penelitian

Mengacu pada rumusan malasah, maka tujuan dari penelitian ini melakukan implementasi dan penilaian menggunakan metode *risk assessment* berdasarkan ISO 27005:2022 terhadap aset IT dengan tahapan sebagai berikut :

1. Melakukan analisis pengelolan risiko keamanan sistem informasi pada aset IT PT. SPI berdasarkan ISO 27005:2022.
2. Merancang rekomendasi pengelolaan risiko keamanan sistem informasi pada aset IT PT. SPI berdasarkan ISO 27005:2022 yang mampu mengurangi peluang terjadinya ancaman.

I.4 Batasan Penelitian

Keluaran dari penelitian ini terbatas pada perancangan dan rekomendasi strategis mengenai penanganan risiko pada aset IT PT. SPI, yang mencakup aset utama dan aset pendukung, termasuk perangkat keras dan perangkat lunak. Oleh karena itu, penelitian ini tidak mencakup tahap implementasi teknis dari kontrol yang

diusulkan, maupun evaluasi efektivitas pasca-implementasi. Selain itu, analisis risiko hanya difokuskan pada aset-aset teknologi informasi yang berada di bawah pengelolaan langsung Divisi IT PT. SPI. Dengan demikian, temuan yang diperoleh akan didasarkan pada data dan kondisi internal perusahaan yang relevan dengan lingkup penelitian yang telah ditentukan.

I.5 Manfaat Penelitian

Manfaat yang diperoleh dari penelitian ini sebagai berikut :

1. Bagi PT. SPI, penelitian ini bermanfaat sebagai masukan dalam meningkatkan pengelolaan manajemen risiko keamanan sistem informasi khususnya pada aset IT dari berbagai macam ancaman eksternal maupun internal melalui rekomendasi yang diberikan.
2. Bagi penulis, penelitian ini bermanfaat untuk mengasah kompetensi dan pemahaman terkait manajemen risiko keamanan sistem informasi melalui pengalaman dalam menganalisa dan merancangan rekomendasi manajemen risiko keamanan sistem informasi secara langsung pada perusahaan.
3. Bagi peneliti berikutnya, penelitian bermanfaat untuk menjadi acuan dalam mengembangkan efektivitas manajemen risiko SMKI khususnya pada aset IT perusahaan yang bergerak di bidang *fintech* dan sejenisnya.