BAB I PENDAHULUAN

I.1 *State of Art*

Dalam kajian mengenai efektivitas Security Operations Centres (SOC), studi terbaru oleh Enoch Agyepong, Yulia Cherdantseva, Philipp Reinecke, dan Pete Burnap (2023) memperkenalkan metode SOC Analyst Assessment Method (SOC-AAM), yang memberikan kontribusi signifikan terhadap penilaian kinerja analis SOC. Penelitian ini berfokus pada evaluasi sistematis terhadap kemampuan analis dalam menangani insiden siber, dengan hasil yang menunjukkan bahwa SOC-AAM mampu memberikan kerangka kerja yang terstruktur bagi manajer SOC dan pemangku kepentingan untuk menilai kualitas analisis dan laporan insiden. Metode ini telah diuji dalam dua SOC melalui studi kasus eksperimental, sehingga memberikan data empiris yang relevan tentang efektivitas metode dalam konteks operasional nyata (Agyepong, et al., 2023).

Namun, penelitian ini memiliki kelemahan penting karena fokusnya yang terbatas pada kinerja tugas analis SOC. Penelitian tidak mempertimbangkan dimensi kinerja lain, seperti kinerja adaptif (kemampuan untuk beradaptasi terhadap perubahan) dan kinerja kontekstual (kontribusi non-teknis yang memperkaya lingkungan kerja), yang sama-sama penting dalam meningkatkan efektivitas SOC secara keseluruhan. Dengan mengintegrasikan pendekatan yang lebih holistik, termasuk evaluasi kinerja adaptif dan kontekstual, penelitian lanjutan dapat memperbaiki keterbatasan ini dan menghasilkan model penilaian yang lebih komprehensif.

Lebih lanjut, SOC-AAM cenderung memakan banyak waktu dalam penerapannya, yang menjadi hambatan praktis bagi operasional SOC sehari-hari. Sebagai solusi, metode ini bisa dioptimalkan melalui kolaborasi dengan perancang SOC untuk mengintegrasikan SOC-AAM ke dalam sistem yang sudah ada secara otomatis. Ini memungkinkan evaluasi yang lebih efisien tanpa mengorbankan kualitas hasil penilaian.

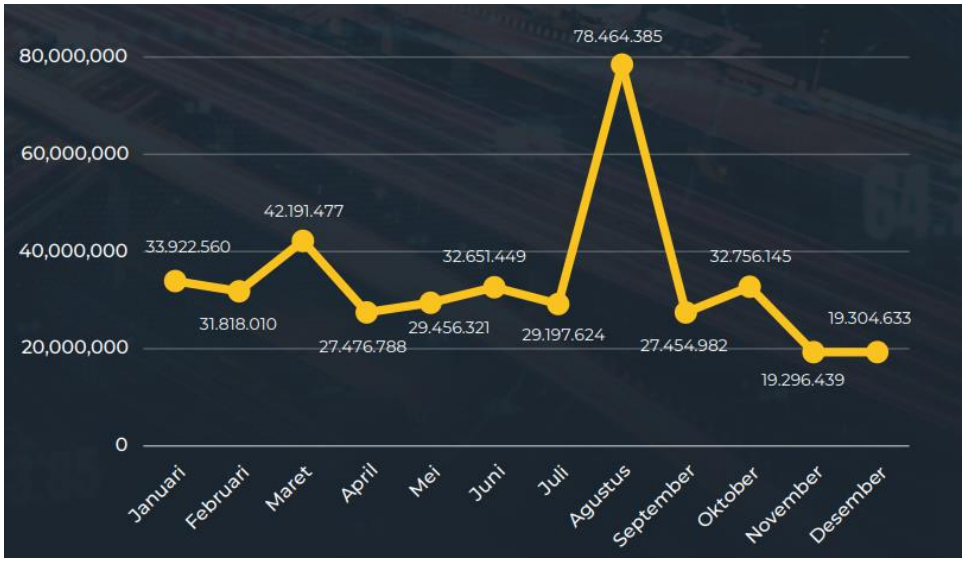
Penelitian ini memberikan fondasi penting untuk memahami SOC dan metodologi penilaiannya, tetapi keterbatasan yang telah disebutkan membuka peluang

penelitian lanjutan yang lebih mendalam. Oleh karena itu, studi ini mencoba mengatasi kekurangan tersebut dengan mengevaluasi keamanan sistem informasi menggunakan framework ISO 27005:2018 dan NIST SP 800-30 pada studi kasus PT NBFC. Framework ini diharapkan mampu menentukan parameter penilaian yang lebih komprehensif dalam konteks keamanan sistem informasi, serta memberikan dasar bagi pengembangan framework baru yang dapat digunakan oleh organisasi lain di masa depan, memperluas cakupan dan relevansi penelitian terhadap pengelolaan risiko keamanan informasi yang lebih luas.

I.2 Latar Belakang

Dalam era digitalisasi yang semakin berkembang, keamanan informasi menjadi isu yang semakin penting. Setiap perusahaan, baik besar maupun kecil, harus dapat melindungi sistem informasi mereka dari serangan luar yang dapat menyebabkan kerugian finansial dan kerusakan reputasi. Perusahaan keuangan non-bank merupakan salah satu jenis perusahaan yang memiliki risiko tinggi terhadap ancaman keamanan informasi, mengingat mereka memperoleh pendanaan dari institusi keuangan lain seperti bank. Oleh karena itu, perusahaan keuangan non-bank harus memiliki strategi keamanan informasi yang efektif untuk melindungi sistem informasi mereka.

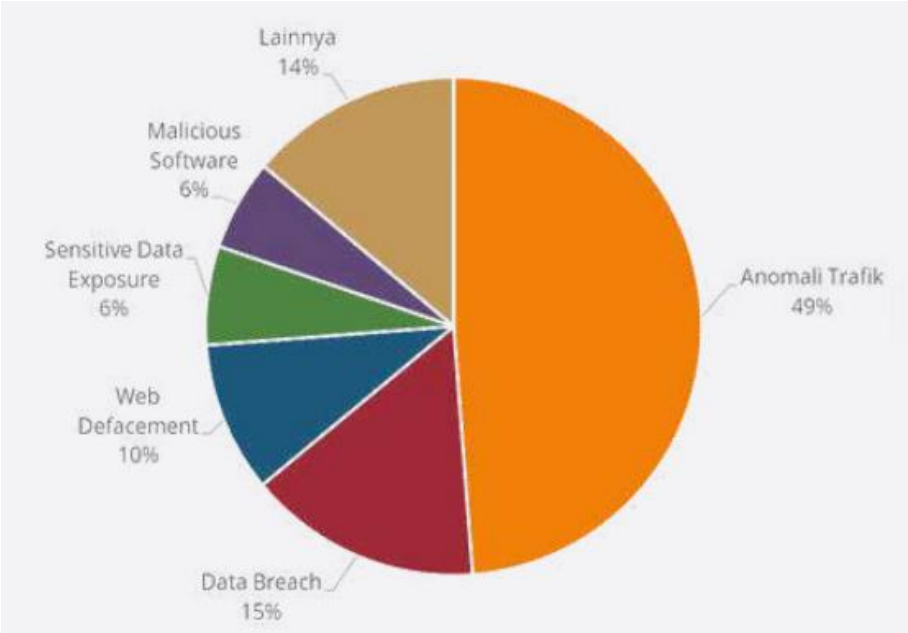
Menurut data yang berasal dari Lanskap Keamanan Siber Indonesia pada Tahun 2023 menyebutkan bahwa serangan yang terjadi pada sistem informasi organisasi berjumlah 403.990.813 anomali. Anomali trafik tertinggi terjadi pada bulan Agustus dengan jumlah 78.464.385 anomali, sedangkan anomali terendah terjadi pada bulan November dengan jumlah 19.296.439 anomali. Aktivitas anomali trafik ini dapat berdampak pada penurunan performa perangkat dan jaringan, pencurian data sensitif, hingga perusakan reputasi dan penurunan kepercayaan terhadap suatu organisasi (Badan Siber dan Sandi Negara, 2023).



Gambar I-1 Trafik Anomali Serangan di Indonesia

Sumber: Badan Siber dan Sandi Negara (Badan Siber dan Sandi Negara, 2023)

Dari serangan tersebut, mengungkapkan bahwa Tim Pusat Kontak Siber BSSN mengirimkan 1.762 Notifikasi, didapatkan hasil Top 5 Klasifikasi Indikasi Insiden yang dinotifikasi oleh BSSN yaitu Anomali Trafik sebanyak 858, Data Breach sebanyak 268, Web Defacement sebanyak 172, Senisitive Data Exposure sebanyak 113, dan Malicious Software sebanyak 104 (Badan Siber dan Sandi Negara, 2023).



Gambar I-2 Rekapitulasi Notifikasi Berdasarkan Klasifikasi Indikasi Insiden

Sumber: Badan Siber dan Sandi Negara (Badan Siber dan Sandi Negara, 2023)

Salah satu solusi yang banyak digunakan oleh perusahaan untuk mengatasi ancaman keamanan informasi terhadap serangan siber adalah dengan membangun *Security Operation Center* (SOC). SOC adalah pusat pengendalian keamanan yang berfokus pada pengawasan atau monitoring, pendeteksian, analisis, serta respon cepat terhadap ancaman keamanan siber. SOC juga bertujuan untuk melindungi organisasi dari serangan siber yang dapat merugikan aset, reputasi, dan bisnis (Noosc Security Global, 2024). SOC yang dirancang dengan baik dapat membantu organisasi mempertahankan postur keamanannya, mengurangi risiko, dan merespons insiden keamanan dengan cepat (Mughal, 2022). SOC bertanggung jawab atas manajemen insiden keamanan siber, deteksi serangan siber, pemantauan keamanan yang berkelanjutan dan protektif, manajemen log dan peristiwa, koordinasi dan investigasi (Onwubiko & Ouazzane, 2019).

Dengan adanya SOC memberikan manfaat untuk keamanan siber di perusahaan (Nabil & Yazid, 2023). Dari segi *people*, pembentukan SOC dinilai dapat menyelesaikan tantangan untuk ketersediaan tenaga ahli keamanan siber yang masih sedikit dengan perekrutan, pelatihan, dan penjagaan tenaga ahli tersebut sehingga keahlian dan pengalaman mereka dapat menyamai perusahaan induk (Nabil & Yazid, 2023). Dari segi proses, SOC dinilai dapat membentuk kerangka kerja yang efisien dan efektif, baik secara tenaga maupun finansial (Nabil & Yazid, 2023). Secara teknologi, SOC dapat menyeimbangkan ketersediaan infrastruktur teknologi yang ada di lingkup grup perusahaan sehingga dapat menyesuaikan sesuai kebutuhan dari keamanan siber suatu perusahaan (Nabil & Yazid, 2023). Meskipun SOC telah menjadi bagian yang penting dalam strategi keamanan informasi perusahaan, belum banyak penelitian yang mengevaluasi efektivitas SOC dalam mengatasi ancaman keamanan informasi.

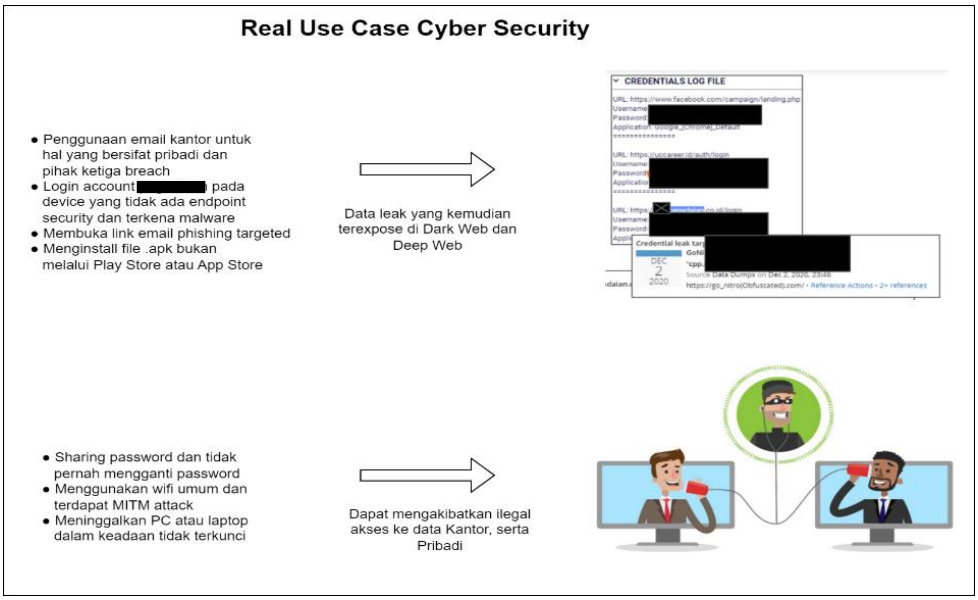
Penelitian sebelumnya mengenai SOC telah dilakukan di beberapa negara, namun belum banyak yang dilakukan di Indonesia, terutama pada perusahaan keuangan non-bank. Indonesia merupakan negara yang memiliki perkembangan teknologi informasi yang sangat pesat, sehingga risiko terhadap ancaman keamanan informasi semakin besar. Oleh karena itu, penelitian ini perlu dilakukan untuk mengevaluasi efektivitas SOC dalam mengatasi ancaman keamanan informasi pada perusahaan

keuangan non-bank di Indonesia. Perusahaan yang digunakan sebagai objek penelitian yaitu PT NBFC (*Non-Bank Financial Company)*, PT NBFC merupakan sebuah badan yang kegiatannya menghimpun dana dari masyarakat dengan mengeluarkan surat-surat berharga, lalu menyalurkan untuk pembiayaan investasi perusahaan yang membutuhkan pinjaman (Koke, 2023).

Pada PT NBFC telah menerapkan SOC untuk keamanan sistem informasinya. Akan tetapi, pada PT NBFC masih memiliki permasalahan yaitu belum memiliki proses analisis dampak terhadap *Financial* dan *Regulatory Requirement* serta perhitungan biaya dan usaha yang diperlukan untuk pemulihan (*recovery*) pada *event*/insiden yang terdeteksi, belum ada *Key Performance Indicators* (KPI) dan *Key Risk Indicators* (KRI) yang ditetapkan oleh manajemen untuk memantau efektivitas kontrol akses fisik dan kesesuaian dengan standar yang berlaku, belum memiliki program resmi terkait insider threat (ancaman dari dalam organisasi), belum memiliki proses watchlist dan monitoring tambahan terhadap karyawan yang mengundurkan diri, terutama yang berpotensi menjadi insider threat, ada proses *security* and *compliance review* yang dilakukan kepada pihak ketiga, baik secara *onsite* maupun *offsite,* belum terdapat integrasi antara *File Integrity Monitoring* (FIM) dengan solusi SIEM (*Security Information and Event Management*) untuk mendeteksi perubahan yang tidak sah pada *audit log,* saat ini PT NBFC sudah menggunakan solusi untuk menganalisis tren insiden, namun belum memiliki kemampuan analitik untuk mengolah data insiden, analisis dampak dari laporan insiden yang terjadi di PT NBFC belum mempertimbangkan aspek finansial dan regulatory, belum melakukan analisis data insiden secara berkala untuk mengidentifikasi tren, pola ancaman, serangan, serta area utama yang perlu mendapatkan perhatian khusus, terakhir belum ada kalender pengujian *Business Continuity Plan* (BCP) yang mencakup simulasi kebakaran, gempa bumi, dan bencana lainnya untuk setiap proses dan sistem kritikal yang tercantum dalam *Business Impact Analysis* (BIA).

Dari permasalahan tersebut, *real use case cyber security* yang terjadi di PT NBFC dapat dilihat pada Gambar I-3. Dari Gambar I-3 menjelaskan bahwa terjadinya serangan atau ketidakamanan dalam sistem ketika pengguna melakukan

penggunaan *email* kantor untuk hal yang bersifat probadi dan pihak ketika *breach,* kemudian melakukan *login account* pegadaian pada *device* yang tidak ada *endpoint security* dan beresiko terkena *malware,* membuka *link email phishing targeted,* menginstall file .apk bukan pada *play store,* sehingga data tersebut terexpose di *Dark Web* dan *Deep Web.* Permasalahan selanjutnya yaitu pengguna melakukan *sharing password* dan tidak pernah mengganti *password,* menggunakan *wifi* umum dan terdapat MTM *Attack,* meningggalkan PC atau laptop tidak dalam kondisi terkunci, hal-hal tersebut dapat mengakibatkan ilegal akses ke data kantor serta pribadi.



Gambar I-3 *Real Use Case Cyber Security* Pada PT NBFC

Sumber: Hasil Assessment PT NBFC

Berdasarkan uraian di atas, penelitian ini bertujuan untuk melakukan penilaian terhadap keamanan sistem informasi PT NBFC dengan fokus pada SOC berdasarkan standar ISO 27005:2018 dan NIST SP 800-30. Dengan memahami latar belakang dan *problem statement* yang dihadapi PT NBFC, penelitian ini diharapkan dapat memberikan kontribusi dalam meningkatkan keamanan informasi perusahaan keuangan non-bank dengan memberikan rekomendasi standar SOC usulan yang dapat diterapkan oleh perusahaan yang ingin menerapkan sistem informasi SOC.

I.3 Rumusan Masalah

SOC merupakan komponen penting dari strategi keamanan siber organisasi. SOC bertanggung jawab untuk memantau, mendeteksi, dan merespons insiden keamanan, ancaman, dan kerentanan infrastruktur organisasi (Mughal, 2022). SOC harus memiliki proses dan prosedur yang jelas untuk mengelola insiden keamanan, dan kinerjanya harus diukur menggunakan metrik dan KPI yang telah ditetapkan (Mughal, 2022). Berdasarkan laporan terbaru, jumlah rata-rata pelanggaran keamanan yang dilaporkan oleh organisasi telah meningkat sebesar 11% dari 130 pada tahun 2017 menjadi 145 insiden pada tahun 2018 (Vielberth, et al., 2020).

Dalam lima tahun terakhir, jumlah pelanggaran keamanan terus meningkat sebesar 65%. Akan tetapi, laporan tersebut hanya mencakup insiden yang terdeteksi dan dilaporkan terkait serangan siber. Serangan siber meningkat dan banyak yang tidak terdeteksi dalam jangka waktu yang lama (Vielberth, et al., 2020). Oleh karena itu, tujuan penelitian ini yaitu melakukan analisis penilaian terhadap keamanan sistem informasi PT NBFC dengan fokus pada SOC berdasarkan standar ISO 27005:2018 dan NIST SP 800-30, sehingga didapatkan hasil standar terbaik sebagai rekomendasi untuk menerapkan SOC pada suatu perusahaan.

I.4 Tujuan Penelitian

Berdasarkan informasi yang dijelaskan pada Latar Belakang, maka tujuan penelitian ini adalah:

1. Mengevaluasi *framework* ISO 27005:2018, NIST SP 800-30 dan *framework* usulan pada keamanan sistem informasi di PT NBFC menggunakan *maturity level*.
2. Merancang *framework* usulan sebagai rekomendasi organisasi lain dalam melakukan penilaian keamanan sistem informasi.
3. Mengaplikasikan *framework* usulan penilaian keamanan sistem informasi dengan membuat *guidance assessment* SOC.

I.5 Pertanyaan Penelitian

Dari tujuan penelitian, maka dalam penelitian ini terdapat pertanyaan penelitian yaitu:

1. Bagaimana efektivitas framework ISO 27005:2018 dan NIST SP 800-30 dalam mengevaluasi keamanan sistem informasi di PT NBFC, serta bagaimana perbandingannya dengan framework baru yang dikembangkan?
2. Apa saja parameter kunci yang perlu dikembangkan dalam framework usulan untuk meningkatkan kualitas penilaian keamanan sistem informasi, sehingga dapat diadopsi oleh organisasi lain?
3. Bagaimana strategi implementasi framework usulan dalam bentuk panduan penilaian SOC yang dapat meningkatkan efektivitas penilaian keamanan sistem informasi di organisasi?

I.6 Lingkup Penelitian

Penelitian ini mencakup analisis penilaian sistem keamanan informasi SOC di PT NBFC dengan menggunakan dua framework utama, yaitu ISO 27005:2018 dan NIST SP 800-30, untuk mengevaluasi efektivitas penerapan SOC. Fokus utama adalah menilai standar yang paling sesuai untuk SOC di PT NBFC dan mengembangkan framework usulan yang lebih efektif berdasarkan evaluasi dari kedua standar tersebut. Kebaruan dari penelitian ini terletak pada pengembangan rekomendasi standar SOC yang dapat diterapkan oleh perusahaan lain yang ingin mengimplementasikan SOC dengan lebih baik.

Berdasarkan ruang lingkup yang dijelaskan, penelitian ini memiliki beberapa batasan, yaitu:

1. Lokasi dan Waktu Penelitian
    a. Penelitian dilakukan di Universitas Telkom, Bandung, dan PT NBFC, sebagai lokasi utama pengumpulan data dan studi kasus.
    b. Waktu penelitian berlangsung dari bulan Januari 2023 hingga Juli 2024.

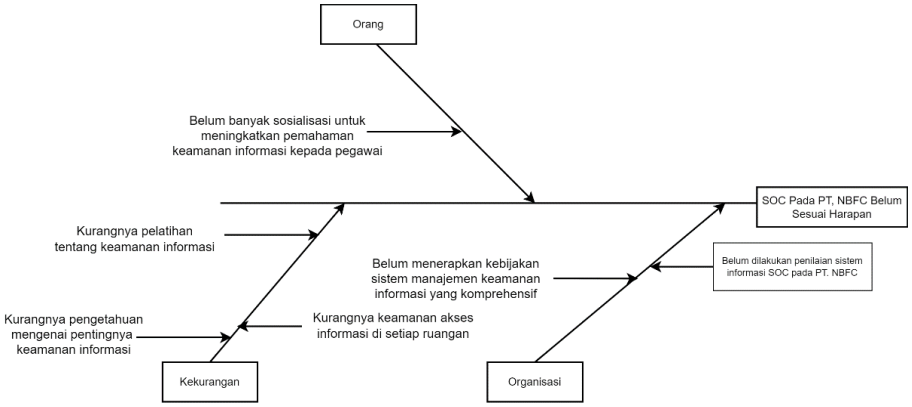
c. Objek penelitian adalah PT NBFC, perusahaan keuangan non-bank. Penelitian tidak melibatkan perusahaan lain, sehingga hasil penelitian difokuskan pada studi kasus PT NBFC.

2. Fokus Penelitian
    a. Fokus penelitian ini adalah pada penilaian Security Operation Center (SOC) di PT NBFC menggunakan framework ISO 27005:2018 dan NIST SP 800-30.
    b. Sumber data primer berasal dari PT NBFC, sementara data sekunder diperoleh dari tinjauan literatur yang terkait dengan framework ISO 27005:2018 dan NIST SP 800-30.
    c. Penelitian ini hanya berfokus pada evaluasi SOC saat ini dan usulan perbaikan, tidak mencakup implementasi perubahan atau solusi baru di PT NBFC.
    d. Evaluasi dilakukan menggunakan perhitungan maturity level untuk mengukur tingkat efektivitas penerapan keamanan informasi.

3. Output Penelitian
    a. Penelitian ini akan menghasilkan rekomendasi framework usulan dalam bentuk guidance untuk penilaian keamanan sistem informasi.
    b. Penelitian juga akan menghasilkan penilaian maturity level dari framework ISO 27005:2018, NIST SP 800-30, serta framework usulan sebagai perbandingan efektivitasnya.

I.7 Kesenjangan Penelitian

Kesenjangan penelitian dibuat dengan *gap analysis* menggunakan kerangka *fishbone diagram* yang didalamnya terdapat komponen organisasi, *technology* dan proses. *Fishbone diagram gap analysis* dapat dilihat pada Gambar I-4 (Mahardika, et al., 2020).



Gambar I-4 *Fishbone Diagram Gap Analysis*

Pada Gambar I-4 mengenai *fishbone gap analysis* terdapat 3 komponen yaitu Orang, Kekurangan dan Organisasi. Pada komponen Orang masih terdapat masalah yaitu belum banyak sosialisasi untuk meningkatkan pemahaman keamanan informasi kepada pegawai. Pada komponen Kekurangan menyebutkan bahwa saat ini terdapat kurangnya pelatihan tentang keamanan informasi dan pengetahuan menegenai pentingnya keamanan informasi dalam suatu perusahaan/organisasi, masih terdapat kekurangan terkait keamanan akses informasi di setiap ruangan. Pada komponen organisasi masih belum menerapkan kebijakan sistem manajemen keamanan informasi yang komprehensif dan belum dilakukan penilaian sistem informasi SOC pada PT. NBFC. Maka dari itu, SOC pada PT. NBFC belum sesuai harapan dan menjadi fokus dalam penelitian ini yaitu melakukan analisis penilaian keamanan sistem informasi SOC pada PT. NBFC.

I.8 Rasionalisme Penelitian

Penelitian ini dilatarbelakangi oleh tingginya jumlah anomali trafik dan insiden keamanan yang tercatat di Indonesia pada tahun 2023, dengan total 403.990.813 anomali dan 1.762 notifikasi insiden, yang mencakup kategori seperti anomali trafik, data breach, dan malicious software. Laporan dari BSSN mengungkapkan bahwa lima klasifikasi insiden teratas adalah anomali trafik, data breach, web defacement, sensitive data exposure, dan malicious software. Selain itu, data dari Laporan Ancaman Digital AwanPintar.id menunjukkan bahwa total serangan digital pada tahun 2023 mencapai 347.172.666, dengan puncaknya pada bulan Mei (Suryo, 2023).

Dalam melindungi sistem informasi dari serangan siber dilakukan dengan *security operation centre* (SOC), SOC telah diterapkan pada PT *Non-Bank Financial Company* (NBFC) untuk keamanan sistem informasinya. Akan tetapi, pada PT NBFC masih memiliki permasalahan yaitu belum memiliki proses analisis dampak terhadap *Financial* dan *Regulatory Requirement* serta perhitungan biaya dan usaha yang diperlukan untuk pemulihan (*recovery*) pada *event*/insiden yang terdeteksi, belum ada *Key Performance Indicators* (KPI) dan *Key Risk Indicators* (KRI) yang ditetapkan oleh manajemen untuk memantau efektivitas kontrol akses fisik dan kesesuaian dengan standar yang berlaku, belum memiliki program resmi terkait insider threat (ancaman dari dalam organisasi). Maka dari itu, dalam konteks ini penilaian keamanan sistem informasi pada *Security Operation Centre* (SOC) di PT NBFC menjadi krusial untuk melindungi data sensitif dan mencegah risiko. Penelitian ini bertujuan untuk mengevaluasi parameter penilaian keamanan sistem informasi menggunakan *framework* ISO 27005:2018 dan NIST SP 800-30 melalui penilaian *maturity level*. Hasil evaluasi akan mengidentifikasi parameter yang diterapkan dan memberikan rekomendasi perbaikan, serta mengusulkan *framework* baru yang dapat digunakan oleh berbagai perusahaan atau organisasi, baik yang termasuk dalam sektor bank maupun non-bank. Penelitian ini penting untuk memastikan bahwa SOC dapat efektif dalam mengidentifikasi, mengelola, dan merespons ancaman keamanan dengan lebih baik.

I.9 Ekspektasi Penelitian

Berdasarkan paparan sebelumnya, berikut adalah beberapa manfaat yang dapat dihasilkan dan merupakan pemetaan dari ekspektasi pada penelitian ini, yaitu:

1. Pengembangan Framework Usulan: Framework yang dihasilkan dari penelitian ini diharapkan mampu mengintegrasikan elemen-elemen terbaik dari ISO 27005:2018 dan NIST SP 800-30, memberikan alat evaluasi yang lebih efektif dalam penilaian keamanan sistem informasi pada SOC. Framework ini diharapkan memiliki fleksibilitas yang memadai untuk diterapkan di berbagai jenis organisasi.

2. Peningkatan Keamanan Sistem Informasi: Dengan diterapkannya framework usulan, organisasi diharapkan dapat memperbaiki proses penilaian dan manajemen risiko sistem informasi mereka secara lebih terstruktur, terukur, dan efektif, terutama dalam konteks operasional SOC.

3. Panduan Implementasi Praktis: Framework usulan akan dilengkapi dengan panduan implementasi praktis yang diharapkan dapat memudahkan tim SOC dalam mengidentifikasi, menganalisis, dan merespons ancaman keamanan dengan lebih cepat dan tepat.

4. Peningkatan Maturity Level Organisasi: Implementasi framework ini diharapkan dapat membantu organisasi meningkatkan maturity level dalam hal manajemen risiko dan keamanan informasi secara keseluruhan, sehingga lebih siap menghadapi ancaman-ancaman siber yang berkembang.

5. Inovasi dan Pengembangan: Mengusulkan *framework* baru dan *guidance assessment* SOC dapat memicu inovasi dalam praktik keamanan informasi, membantu organisasi dalam menyusun strategi yang lebih efektif untuk melindungi sistem informasi mereka dan memperbaiki proses penilaian keamanan yang ada.

I.10 Signifikansi Penelitian

Penelitian ini memiliki beberapa signifikansi penting, baik dari segi pengetahuan, manfaat praktis, maupun relevansi sosial dan ekonomi:

1. Kontribusi terhadap Pengetahuan: Penelitian ini memberikan kontribusi signifikan terhadap literatur keamanan informasi dengan menawarkan analisis baru tentang cara ISO 27005:2018 dan NIST SP 800-30 dapat dievaluasi dan diintegrasikan dalam framework yang lebih efektif. Hal ini memperluas pemahaman mengenai efektivitas framework yang digunakan dalam SOC, serta memberikan wawasan baru tentang metode penilaian yang lebih terukur.

2. Manfaat Praktis bagi Organisasi: Framework usulan ini menawarkan pendekatan praktis dan terintegrasi untuk penilaian keamanan sistem informasi, yang dapat diadopsi oleh organisasi lain di luar PT NBFC. Dengan penerapan framework ini, organisasi dapat meningkatkan keamanan sistem mereka secara lebih efektif, dengan pedoman yang sistematis dan didukung oleh data penilaian yang jelas.

3. Relevansi Sosial dan Ekonomi: Dengan meningkatkan efektivitas penilaian dan respons terhadap ancaman keamanan informasi, framework ini berkontribusi secara langsung dalam melindungi data sensitif organisasi. Hal ini tidak hanya menjaga kerahasiaan informasi tetapi juga meningkatkan stabilitas ekonomi dengan mencegah potensi kerugian akibat pelanggaran data dan serangan siber.

4. Inovasi dalam Praktik Keamanan Informasi: Framework dan panduan yang dihasilkan dari penelitian ini berpotensi memicu inovasi dalam praktik keamanan informasi, yang dapat membantu organisasi menyusun strategi pertahanan yang lebih proaktif dan terukur terhadap ancaman siber yang terus berkembang.

I.11 Pertimbangan Penelitian

Pertimbangan penelitian yang dilakukan dalam penelitian terkait analisis penilaian sistem informasi SOC pada PT NBFC adanya beberapa pertimbangan. Pertimbangan penelitian ini sebagai berikut:

1. Memastikan standar ISO 27005:2018, NIST SP 800-30 yang digunakan dapat berguna untuk penilaian sistem informasi SOC.
2. Pemahaman terhadap standar SOC yang digunakan untuk penilaian sistem informasi SOC.
3. Pemilihan metodologi penelitian yang sesuai agar mendapatkan hasil penelitian yang valid.

Selanjutnya, dalam penelitian ini terdapat pertimbangan etika dengan tujuan untuk memastikan bahwa penelitian dilakukan dengan integritas dan memperhatikan

kepentingan semua pihak terkait. Pertimbangan etika yang digunakan sebagai berikut:

1. Hasil penelitian dijelaskan secara keseluruhan dan transparan, tanpa adanya bias atau manipulasi yang dapat mempengaruhi keabsahan dan kepercayaan hasil penelitian.
2. Peneliti harus mematuhi semua peraturan, panduan, dan kode etik yang berlaku. Ini meliputi peraturan dan panduan yang dikeluarkan oleh universitas, peraturan privasi data, dan peraturan hukum yang berlaku.

I.12 Peran Peneliti

Peran peneliti dalam penelitian ini berperan penting. Peran peneliti digambarkan menggunakan RACI *Chart*, RACI *Chart* merupakan elemen penting dalam tata kelola struktur organisasi yang menekankan pada tingkat tanggung jawab, keterlibatan, dan akuntabilitas. Matriks ini menggambarkan peran individu dan struktur organisasi, tidak hanya dalam konteks bisnis tetapi juga dalam bidang Teknologi Informasi (TI) (Yuda, et al., 2024). RACI *Chart* yang digunakan dapat dilihat pada Tabel I-1.

Tabel I-1 *RACI Chart* Untuk Peran Peneliti

Kegiatan	Penulis	Security Analys SOC	Security Engineering SOC	Team Leader SOC	Manager SOC	Pembimbing Penelitian
Identifikasi Masalah	R	C	I	C	I	A
Pengumpulan Data	R	A	C	I	I	C
Analisis literatur	R	C	I	I	I	A
Analisis Kondisi Saat ini	R	A	C	C	I	C
Evaluasi framework	R	C	A	C	I	C
Pembentukan framework baru	R	I	A	C	I	C
Kesimpulan dan saran	R	C	I	C	R	C

Keterangan:

1. R (*Responsible*): Pihak yang melakukan pekerjaan.
2. A (*Accountable*): Pihak yang bertanggung jawab akhir untuk hasil kegiatan.
3. C (*Consulted*): Pihak yang dikonsultasikan untuk memberikan masukan atau pendapat.
4. I (*Informed*): Pihak yang diberitahukan tentang hasil atau kemajuan tetapi tidak terlibat langsung.

I.13 Sistematika Penulisan

Sistematika penulisan pada penelitian ini terdiri dari enam bab, yang tersusun sebagai berikut:

BAB I PENDAHULUAN

Bab ini berisi uraian mengenai Latar Belakang, Perumusan Masalah, Tujuan Penelitian, Batasan Masalah, Manfaat Penelitian, dan Sistematika Penulisan.

BAB II LANDASAN TEORI

Bab ini berisi uraian mengenai literatur yang relevan dengan permasalahan yang dihadapi, penelitian terdahulu yang berkaitan dengan lingkup penelitian yang sedang dilakukan, dan teori-teori yang digunakan dalam penelitian ini seperti *Security Operation Center (*SOC*), Cyber Threats, Information Systems Assessment* dan teori dari standar yang digunakan.

BAB III METODOLOGI PENELITIAN

Bab ini berisi penjelasan mengenai metode penelitian yang digunakan serta penjelasan langkah-langkah penelitian secara rinci meliputi tahap identifikasi, tahap analisis, tahap desain, tahap simulasi, dan tahap akhir dari penelitian ini.

BAB IV PENGUMPULAN DATA

Bab ini berisi penjelasan data-data yang digunakan dalam penelitian untuk analisis parameter penilaian keamanan sistem informasi, gambaran umum dari objek penelitian dan hasil validasi dari *framework* ISO 27005:2018 dan NIST SP 800-30.

BAB V ANALISA DATA

Bab ini berisi penjelasan analisis uji instumen data, pengembangan model data dari SOC modern, solusi yang dihasilkan terhadap parameter yang digunakan dalam penilaian keamanan sistem informasi pada perusahaan non-bank berdasarkan *framework* ISO 27005:2018 dan NIST SP 800-30.

BAB VI KESIMPULAN DAN SARAN

Bab ini berisi penjelasan kesimpulan dari penelitian yang dilakukan serta saran untuk penelitian selanjutnya tentang topik yang sama.