SNESTIK

Seminar Nasional Teknik Elektro, Sistem Informasi, dan Teknik Informatika

https://ejurnal.itats.ac.id/snestik dan https://snestik.itats.ac.id

Informasi Pelaksanaan :
SNESTIK V - Surabaya, 26 April 2025
Fakultas Teknik Elektro dan Teknologi Informasi, Institut Teknologi Adhi Tama Surabaya

Informasi Artikel:
DOI : 10.31284/p.snestik.2025.7395

Prosiding ISSN 2775-5126

Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya
Gedung A-ITATS, Jl. Arief Rachman Hakim 100 Surabaya 60117 Telp. (031) 5945043
Email : snestik@itats.ac.id

Penerapan OCTAVE-S untuk Manajemen Risiko Keamanan Informasi di Perusahaan Kredit

Rendy Aditya Rahman, Adib Pakarbudi, Zuli Maulidati

Institut Teknologi Adhi Tama Surabaya
e-mail: adib@itats.ac.id

ABSTRACT

The development of information technology has made information systems a strategic element in business operations, including at PT. ABC, a company engaged in motor vehicle financing. Although information systems such as SOLO's facilitate customer data and transaction management, they remain vulnerable to various security threats and risks. Currently, PT. ABC has not conducted a comprehensive risk assessment of its information systems, leaving potential vulnerabilities unidentified systematically. This study aims to identify IT assets, evaluate security risks, and formulate mitigation strategies using the Operationally Critical Threat, Asset, and Vulnerability Evaluation for Small Organizations (OCTAVE-S) method. The analysis is conducted in three phases: building an asset-based threat profile, identifying infrastructure vulnerabilities, and developing security mitigation strategies. The evaluation results indicate that collaborative security management, IT security monitoring, security architecture, and incident management require greater attention. Therefore, the recommended mitigation strategies include implementing data encryption, enhancing user authentication, and strengthening security monitoring. This study concludes that the OCTAVE-S approach helps PT. ABC systematically and proactively understand IT security risks. By implementing appropriate controls, the company can enhance the protection of IT assets and minimize the impact of threats on business continuity.

Keywords: *Information security, risk management, OCTAVE-S, information systems, threat mitigation*

ABSTRAK

Perkembangan teknologi informasi telah menjadikan sistem informasi sebagai elemen strategis dalam operasional bisnis, termasuk di PT. ABC, yang bergerak di bidang pengkreditan kendaraan bermotor.

Meskipun sistem informasi seperti SOLO's memberikan kemudahan dalam pengelolaan data pelanggan dan transaksi, sistem ini tetap menghadapi berbagai ancaman dan risiko keamanan. Saat ini, PT. ABC belum melakukan penilaian risiko yang komprehensif terhadap sistem informasi yang digunakan, sehingga potensi kerentanan masih belum teridentifikasi secara sistematis. Penelitian ini bertujuan untuk mengidentifikasi aset TI, mengevaluasi risiko keamanan, serta merumuskan strategi mitigasi menggunakan metode Operationally Critical Threat, Asset, and Vulnerability Evaluation for Small Organizations (OCTAVE-S). Analisis dilakukan dalam tiga fase: membangun profil ancaman berbasis aset, mengidentifikasi kerentanan infrastruktur, serta mengembangkan strategi mitigasi keamanan. Hasil evaluasi menunjukkan bahwa aspek manajemen keamanan kolaboratif, pemantauan keamanan TI, arsitektur keamanan, dan manajemen insiden memerlukan perhatian lebih. Oleh karena itu, rekomendasi strategi mitigasi meliputi penerapan enkripsi data, peningkatan autentikasi pengguna, serta pemantauan keamanan yang lebih ketat. Dari penelitian ini, disimpulkan bahwa pendekatan OCTAVE-S membantu PT. ABC dalam memahami risiko keamanan TI secara lebih sistematis dan proaktif. Dengan implementasi kontrol yang tepat, perusahaan dapat meningkatkan perlindungan terhadap aset TI serta meminimalkan dampak ancaman terhadap kelangsungan bisnis.

Kata kunci: Keamanan informasi, manajemen risiko, OCTAVE-S, sistem informasi, mitigasi ancaman.

PENDAHULUAN

Perkembangan teknologi informasi telah mengubah peran sistem informasi dari sekadar sistem pendukung menjadi sistem strategis yang mendukung tujuan perusahaan dan menciptakan nilai tambah. Di berbagai sektor, sistem informasi tidak hanya meningkatkan efisiensi operasional, tetapi juga mendorong inovasi, mempercepat pengambilan keputusan berbasis data, serta membangun keunggulan kompetitif[1][2][3]. Dalam bisnis, sistem informasi memungkinkan otomatisasi dan analisis data yang lebih cepat, sementara dalam pendidikan dan pemerintahan, digitalisasi melalui sistem informasi meningkatkan akses, transparansi, dan efektivitas layanan [4]. Dengan integrasi yang tepat, sistem informasi menjadi kunci dalam meningkatkan produktivitas dan daya saing di era digital[1]. Salah satu perusahaan yang menerapkan SI/TI dalam operasional bisnisnya adalah PT.ABC.

PT. ABC adalah perusahaan yang bergerak di bidang pengkreditan kendaraan bermotor dan memiliki beberapa cabang. Untuk mendukung operasionalnya, perusahaan menggunakan sistem informasi yang terkomputerisasi dan terintegrasi guna mempermudah pencapaian tujuan bisnis. Namun, meskipun sistem ini memberikan banyak manfaat, ditemukan beberapa kendala dalam implementasinya. Sistem tidak selalu berjalan optimal atau sesuai dengan tujuan perusahaan akibat perubahan kebutuhan manajemen, seperti pembaruan (*update*), peningkatan fitur (*enhancement*), serta adaptasi terhadap situasi tertentu, seperti fluktuasi suku bunga.Selain itu, kerahasiaan dan keamanan data menjadi perhatian utama perusahaan, mengingat PT. ABC bergerak di sektor jasa yang menyimpan data pelanggan. Kepedulian terhadap keamanan data ini sejalan dengan Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Selain untuk memenuhi regulasi, menjaga data perusahaan juga menjadi prioritas guna mencegah kebocoran informasi yang dapat dimanfaatkan oleh kompetitor. Permasalahan ini menunjukkan bahwa pengelolaan sistem informasi dan teknologi informasi (SI/TI) harus dilakukan dengan tepat dan diaudit secara berkala agar selaras dengan tujuan organisasi.

Ketidakpastian dari risiko dalam pengelolaan SI/TI dapat menimbulkan konsekuensi yang merugikan atau membahayakan bagi perusahaan[5][6][7]. Namun, risiko dan ancaman ini dapat dihadapi dengan menerapkan manajemen risiko yang baik, sehingga perusahaan dapat mengambil keputusan secara terstruktur dengan mempertimbangkan berbagai ketidakpastian [8][9][10]. Dengan pendekatan yang tepat, perusahaan dapat mengelola risiko SI/TI secara efektif untuk memastikan keberlanjutan operasional dan keamanan aset bisnisnya. Namun, meskipun terdapat beberapa kendala dan risiko yang mungkin terjadi pada PT.ABC, namun hingga saat ini pihak manajemen belum pernah melakukan penilaian risiko pada sistem informasi yang saat ini digunakan. Salah satu sistem yang menjadi aset penting perusahaan adalah Sistem SOLO's. Sistem ini merupakan sistem transaksi dalam perusahaan yang menyimpan data-data krusial

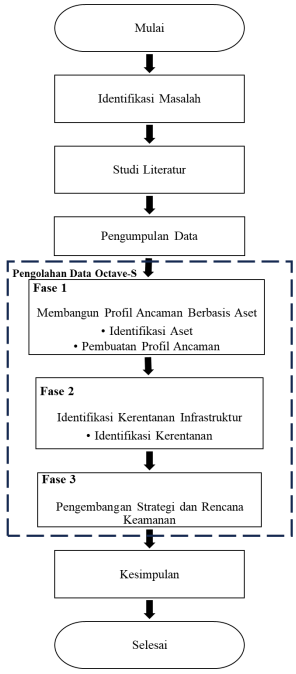
seperti informasi nasabah, riwayat pembayaran, detail kredit kendaraan, serta laporan keuangan. Data-data ini bersifat sensitif dan memiliki peran penting dalam operasional perusahaan, sehingga gangguan atau ancaman terhadap sistem dapat berdampak signifikan pada kelangsungan bisnis dan kepercayaan nasabah. Tetapi pada kenyataanya, aset penting ini tidak terlepas dari gangguan ataupun ancaman. Seperti yang diketahui bahwa gangguan atau ancaman pada suatu sistem akan mempengaruhi keberlangsungan proses bisnis sebuah perusahaan [11][12]. Sedangkan, sebuah institusi atau lembaga yang menggantungkan sebagian besar proses bisnisnya pada sistem informasi akan mengalami kendala yang serius ketika sistem yang diterapkan tidak berjalan dengan semestinya menurut [13][14].

Untuk meminimalkan risiko ancaman pada PT. ABC, perlu dilakukan penilaian terhadap sistem informasi yang digunakan. Dengan demikian, perusahaan dapat mengidentifikasi tingkat kerentanan dan besarnya risiko pada setiap aset kritis. Hasil penilaian ini memungkinkan PT. ABC menerapkan kontrol yang tepat berdasarkan tingkat prioritas dan tingkat ancaman risiko yang paling besar. Berbagai kerangka kerja telah dikembangkan untuk menghadapi risiko TI dalam suatu organisasi. Salah satunya adalah *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE), yang digunakan untuk mengidentifikasi ancaman dan risiko TI[5]. Namun, bagi perusahaan kecil dengan jumlah pegawai kurang dari 80 orang, pendekatan OCTAVE-S lebih sesuai. Implementasi metode ini dapat membantu mengevaluasi risiko pada setiap aset TI serta menghasilkan rekomendasi infrastruktur TI berdasarkan hasil mitigasi risiko. Dalam beberapa tahun terakhir penelitian serupa yang berkaitan dengan penerapan metode Octave-S telah banyak dilakukan di Indonesia. Namun dari penelitian-penelitian tersebut tidak banyak yang berfokus pada satu aplikasi atau aplikasi keuangan, melainkan keamanan informasi secara umum[8][11][15]. Selain itu tidak banyak peneliti yang menjelaskan keunggulan dan keefektifan dari metode OCTAVE-S dan hanya berfokus hasil manajemen risiko pada studi kasus yang digunakan[7][13].

Berdasarkan uraian tersebut, penelitian ini bertujuan untuk membantu PT. ABC dalam mengidentifikasi aset TI dan profil risiko yang dihadapi. Dalam proses manajemen risiko ini, peneliti akan menggunakan pendekatan OCTAVE-S untuk mengevaluasi keamanan aset TI yang dimiliki perusahaan. Pendekatan ini dipilih karena sesuai untuk perusahaan dengan skala kecil hingga menengah dan dapat memberikan gambaran komprehensif mengenai tingkat risiko serta ancaman terhadap sistem informasi. Hasil analisis ini akan digunakan untuk menyusun rekomendasi langkah mitigasi guna meningkatkan keamanan sistem informasi perusahaan, sehingga PT. ABC dapat lebih siap dalam menghadapi potensi ancaman dan memastikan keberlangsungan operasional bisnisnya.

METODE

Penelitian dilakukan menggunakan pendekatan kualitatif untuk proses pengumpulan data. Adapun Teknik yang digunakan adalah observasi dan wawancara dengan mengacu kerangka OCTAVE-S sebagai metode untuk melakukan analisis risiko. Untuk lebih jelasnya metode penelitian ini telah dipaparkan pada gambar 1.



Gambar 1. Metode Penelitian

Gambar 1 merupakan alur penelitian yang dimulai dari identifikasi permasalahan, studi literatur, pengumpulan data, pengolahan data, serta kesimpulan.

Pengumpulan Data

Proses pengumpulan data dalam studi kasus penerapan OCTAVE-S untuk manajemen risiko keamanan informasi di PT ABC dilakukan melalui wawancara, kuesioner, dan observasi. Wawancara dilakukan dengan menggunakan pedoman metode OCTAVE-S kepada pihak-pihak terkait dalam manajemen risiko dan keamanan informasi di perusahaan, seperti tim IT dan manajemen operasional. Kuesioner digunakan untuk mengidentifikasi praktik keamanan yang telah diterapkan serta kesadaran karyawan terhadap risiko keamanan informasi. Selain itu, observasi dilakukan untuk memahami proses bisnis yang berjalan, mengidentifikasi aset-aset penting yang mendukung layanan perusahaan, serta mengamati potensi risiko yang dapat terjadi. Untuk memastikan keakuratan data, proses verifikasi dilakukan agar informasi yang diperoleh benar-benar valid dan dapat dipertanggungjawabkan.

Pengolahan Data OCTAVE-S

Pengolahan data dalam penerapan OCTAVE-S untuk manajemen risiko keamanan informasi di PT ABC dilakukan berdasarkan tiga fase utama. Sebelum dilakukan pengolahan data, validasi data dilakukan menggunakan teknik *member checking*, yaitu dengan mengonfirmasi hasil identifikasi aset, ancaman, dan kerentanan kepada informan untuk memastikan bahwa interpretasi data sesuai dengan pengalaman mereka.. Fase pertama, Membangun Profil Ancaman Berbasis Aset, mencakup dua proses, yaitu identifikasi aset yang bertujuan untuk mengidentifikasi aset-aset kritis yang mendukung operasional perusahaan, serta pembuatan profil ancaman guna mengevaluasi potensi ancaman yang dapat mempengaruhi aset tersebut. Fase kedua, Identifikasi Kerentanan Infrastruktur yang berfokus pada analisis kelemahan sistem yang dapat dieksploitasi oleh ancaman. Fase ketiga, Pengembangan Strategi dan Rencana Keamanan, melibatkan identifikasi dan analisis risiko guna menentukan tingkat

risiko yang dihadapi perusahaan, serta pengembangan strategi perlindungan dan mitigasi sebagai langkah untuk meminimalkan dampak dari ancaman yang telah diidentifikasi. Dengan mengikuti pedoman OCTAVE-S ini, PT ABC dapat menyusun strategi keamanan informasi yang lebih terstruktur dan efektif dalam melindungi aset pentingnya.

HASIL DAN PEMBAHASAN

Berdasarkan hasil wawancara dan observasi yang telah dilakukan, berikut ini merupakan analisis dan pembahasan yang disusun berdasarkan data yang diperoleh dengan mengacu pada metode OCTAVE-S sebagai kerangka evaluasi.

Profil Ancaman Berbasis Aset

Dalam penelitian ini Penentuan Profil Ancaman Berbasis aset merupakan langkah Pada fase pertama dalam proses pengolahan data. Pada tahap ini dilakukan evaluasi aspek organisasi yang meliputi penetapan kriteria evaluasi dampak dan identifikasi aset penting organisasi serta mengevaluasi praktik keamanan yang saat ini diterapkan dalam organisasi. Proses penetapan kriteria evaluasi dampak berfungsi sebagai pedoman dalam proses identifikasi dampak risiko pada tahap evaluasi kerentanan. Dari hasil wawancara di dapatkanlah hasil seperti yang tertera pada tabel 1.

Tabel 1. Kriteria Evaluasi Dampak

No	Kategori Dampak	Kriteria Dampak
1	Privasi	Sedang
2	Ketersediaan dan Keamanan Sistem	Sedang
3	Finansial	Tinggi
4	Reputasi & Kepercayaan Pelanggan	Rendah
5	Produktivitas	Rendah

Penetapan kriteria evaluasi dampak tersebut diambil melalui proses wawancara serta Menggunakan data dari insiden atau kejadian sebelumnya. Proses ini Setelah mengetahui berbagai data insiden yang telah terjadi selanjutnya adalah mengidentifikasi Aset apa saja yang terdampak dari insiden tersebut. Adapun daftar aset yang telah teridentifikasi dapat dilihat pada tabel 2. Dengan menetapkan kriteria evaluasi dampak Untuk mengetahui hasil Tabel 2.

Tabel 2. Identifikasi Aset Kritis

No	Kategori Aset	Aset Penting
1	Aset Informasi, Sistem, dan Aplikasi	Aplikasi SOLO's
2	Aset Manusia	Staff IT
		Staff Accounting
		Staff Sales and Marketing
		Staff Purchasing

Setelah mengidentifikasi aset kritis maka selanjutnya mengidentifikasi apa saja praktik keamanan yang telah dilakukan oleh PT. ABC dalam memproteksi aset-aset yang dimiliki. Berdasarkan hasil evaluasi praktik keamanan di PT ABC, ditemukan bahwa beberapa aspek telah dikelola dengan baik, sementara lainnya masih memerlukan perbaikan. Tiga praktik dengan status *green* menunjukkan bahwa pengendalian akses fisik, sistem dan manajemen jaringan, serta

autentikasi dan otorisasi telah diterapkan dengan efektif. Namun, sembilan praktik berada pada status *yellow* yang mengindikasikan perlunya peningkatan dalam kebijakan, pengelolaan kerentanan, serta enkripsi data. Selain itu, tiga praktik masuk dalam kategori *red* yang menunjukkan adanya risiko tinggi akibat lemahnya koordinasi, pemantauan, serta desain sistem keamanan. Oleh karena itu area yang memiliki status *stoplight* kuning dan merah akan dilakukan upaya mitigasi. Adapun hasil dari evaluasi tersebut ditampilkan pada tabel 3.

Tabel 3. Evaluasi Praktik Keamanan

No	Praktik Keamanan	*Stoplight*
1.	Kesadaran dan Pelatihan Keamanan	*Yellow*
2.	Strategi Keamanan	*Yellow*
3.	Manajemen Keamanan	*Yellow*
4.	Peraturan dan Kebijakan Keamanan	*Yellow*
5.	Manajemen Keamanan Kolaboratif	*Red*
6.	Perencanaan Contingency/ Pemulihan Bencana	*Yellow*
7.	Pengendalian Akses Fisik	*Green*
8.	Pemantauan dan Audit Keamanan Fisik	*Yellow*
9.	Sistem dan Manajemen Jaringan	*Green*
10.	Pemantauan dan Audit Keamanan TI	*Red*
11.	Auntentikasi dan Otoritasi	*Green*
12.	Manajemen Kerentanan	*Yellow*
13.	Enkripsi	*Yellow*
14.	Perencangan dan Arsitektur Keamanan	*Red*
15.	Manajemen Insiden	*Yellow*

Berdasarkan hasil evaluasi praktik keamanan tersebut maka menunjukkan bahwa keamanan informasi pada PT. ABC memiliki berbagai ancaman. Hasil identifikasi ancaman terhadap aset yang dimiliki PT. ABC telah disusun menjadi profil ancaman seperti yang ditampilkan pada tabel 4.

Tabel 4. Profil Ancaman

No	**Aset Penting**	**Ancaman**	**Sumber Ancaman**
1	Aplikasi SOLO's	Serangan siber (hacking, malware, ransomware)	Peretas eksternal
		Kebocoran data pelanggan	Insider threat (karyawan yang tidak bertanggung jawab)
2	Staff IT	Insider threat	Karyawan yang tidak beretika
		Social engineering (phishing, manipulasi psikologis)	Pihak eksternal yang ingin mengeksploitasi kelemahan SDM
3	Staff Accounting	Pencurian atau penyalahgunaan data keuangan	Karyawan internal
			Pihak eksternal yang berhasil mendapatkan akses

4	Staff Sales and Marketing	Kebocoran data pelanggan	Serangan phishing
		Akses tidak sah ke sistem CRM	Pihak eksternal yang menyusup ke sistem
5	Staff Purchasing	Penyalahgunaan data pemasok	Karyawan internal yang menyalahgunakan akses
		Manipulasi transaksi	Pihak eksternal dengan akses tidak sah

Kerentanan Infrastruktur

Berdasarkan hasil evaluasi praktik keamanan, keamanan informasi di PT ABC tidak hanya menghadapi berbagai ancaman, tetapi juga menunjukkan tingkat kerentanan yang tinggi terhadap risiko keamanan. Kategori *yellow* dalam evaluasi mengindikasikan bahwa beberapa aspek keamanan meningkatkan kemungkinan terjadinya pelanggaran keamanan. Sementara itu, kategori *red* menunjukkan adanya kelemahan yang dapat memperbesar dampak risiko apabila terjadi serangan atau kegagalan sistem. Tabel 5 menunjukkan kerentanan yang telah teridentifikasi.

Tabel 5. Identifikasi Kerentanan

Aset Penting	Evaluasi Keamanan	Kerentanan	Dampak Potensial
Aplikasi SOLO's	Manajemen Keamanan Kolaboratif (*Red*)	Kurangnya enkripsi data	Kebocoran data
	Pemantauan & Audit Keamanan TI (*Red*)	Kurangnya pemantauan dan audit keamanan	Ketidaktersediaan sistem akibat kegagalan infrastruktur yang tak terdeteksi
	Enkripsi (*Yellow*)	Potensi serangan siber (hacking, malware)	Serangan siber (hacking, malware)
Staff IT	Kesadaran & Pelatihan Keamanan (*Yellow*)	Kesadaran keamanan rendah	Penyalahgunaan akses
	Strategi Keamanan (*Yellow*)	Kurangnya strategi keamanan	Serangan social engineering
	Perencanaan Pemulihan Bencana (*Yellow*)	Tidak ada rencana kontinjensi yang kuat	Downtime layanan
Staff Accounting	Manajemen Keamanan (*Yellow*)	Manajemen keamanan yang lemah	Manipulasi transaksi
	Autentikasi & Otorisasi (*Green*)	Kurangnya autentikasi ganda	Penyalahgunaan data keuangan
Staff Sales and Marketing	Pengendalian Akses Fisik (*Green*)	Kurangnya pengendalian akses	Akses tidak sah ke CRM
	Pemantauan & Audit Keamanan Fisik (*Yellow*)	Kurangnya pemantauan data pelanggan	Kebocoran data pelanggan
Staff Purchasing	Peraturan & Kebijakan Keamanan (*Yellow*)	Kurangnya kebijakan keamanan terkait transaksi	Penipuan atau manipulasi keuangan
	Manajemen Insiden (*Yellow*)	Tidak ada prosedur mitigasi insiden keuangan	Kerugian finansial

Strategi dan Rencana Keamanan

Berdasarkan profil ancaman dan kerentanan mencerminkan ketidaksempurnaan dalam penerapan kontrol keamanan. Sehingga dapat dikatakan bahwa PT ABC masih rentan terhadap risiko kebocoran data, akses tidak sah, serta gangguan operasional yang dapat merugikan bisnis.

Oleh karena itu, peningkatan strategi keamanan dan mitigasi risiko menjadi langkah penting untuk memperkuat ketahanan sistem informasi perusahaan. Adapun rencana mitigasi yang telah disusun ditampilkan pada tabel 6.

Tabel 6. Rencana Mitigasi

No	Aset Penting	Risiko yang Dihadapi	Strategi Perlindungan	Rencana Mitigasi
1	Aplikasi SOLO's	Kebocoran data	Implementasi enkripsi data	Konfigurasi enkripsi AES-256
		ketidaktersediaan sistem akibat kegagalan infrastruktur yang tak terdeteksi	Penerapan pemantauan dan audit berkala	Penerapan SIEM untuk monitoring
		Serangan siber (hacking, malware)	Firewall dan IDS/IPS	Backup data secara berkala
2	Staff IT	Penyalahgunaan akses	Pelatihan kesadaran keamanan rutin	Workshop keamanan 2x setahun
		Serangan social engineering	Penerapan kebijakan akses berbasis peran (RBAC)	Multi-factor authentication (MFA)
		Downtime layanan	Penerapan Kebijakan Disaster Recovery Plan (DRP)	Penyusunan dan pengujian Disaster Recovery Plan (DRP)
3	Staff Accounting	Manipulasi transaksi	Audit internal keuangan rutin	Implementasi sistem logging
		Penyalahgunaan data keuangan	Penerapan autentikasi ganda	Integrasi MFA dengan aplikasi keuangan
4	Staff Sales and Marketing	Akses tidak sah ke CRM	Pemantauan aktivitas user di CRM	Logging & alerting terhadap akses mencurigakan
		Kebocoran data pelanggan	Pengendalian akses berbasis kebutuhan (least privilege)	Implementasi Data Loss Prevention (DLP)
5	Staff Purchasing	Penipuan atau manipulasi keuangan	Penerapan kebijakan persetujuan multi-level	Implementasi digital signature
		Kerugian finansial	Audit transaksi berkala	Penerapan fraud detection system

KESIMPULAN

Penerapan metode OCTAVE-S untuk manajemen risiko keamanan informasi di PT ABC dilakukan melalui tiga fase utama. Pada fase pertama, perusahaan mengidentifikasi aset penting dan mengevaluasi praktik keamanannya, menemukan beberapa area seperti manajemen keamanan kolaboratif dan manajemen insiden yang masih perlu diperbaiki. Pada fase kedua, analisis infrastruktur mengungkapkan kerentanan pada aplikasi SOLO's dan data keuangan terhadap serangan siber, kebocoran data, serta penyalahgunaan akses. Untuk itu, pada fase ketiga, PT ABC mengembangkan strategi mitigasi berupa enkripsi data, multi-factor authentication (MFA), audit berkala, dan pelatihan keamanan. Penerapan OCTAVE-S ini membantu PT ABC mengelola risiko keamanan secara lebih terstruktur dan meningkatkan perlindungan aset informasi serta manusia. Dari penerapan metode ini, dapat disimpulkan bahwa kerangka kerja OCTAVE-S memberikan pendekatan yang sistematis dalam manajemen risiko keamanan informasi, dimulai dari identifikasi aset dan ancaman, analisis kerentanan, hingga pengembangan strategi perlindungan yang sesuai dengan kondisi organisasi. Dengan berfokus pada aspek teknologi, proses bisnis, dan manusia, OCTAVE-S memungkinkan organisasi untuk mengelola

risiko keamanan secara proaktif dan meningkatkan ketahanan sistem informasi mereka terhadap berbagai ancaman yang berkembang. Namun Evaluasi berkala tetap diperlukan untuk memastikan efektivitas strategi menghadapi ancaman baru. Oleh karena itu, penelitian selanjutnya disarankan untuk menguji keberhasilan dan efektivitas strategi mitigasi tersebut, khususnya dalam konteks penerapan sistem informasi keuangan di perusahaan kredit.

DAFTAR PUSTAKA

[1] A. Pakarbudi, E. Enjelina, A. P. P. Yoga, and H. A. Bayu, "ANALISIS KESIAPAN PT. ABC DALAM PENERAPAN E- MANUFACTURING MELALUI PENGUKURAN STRATEGIC ALIGNMENT MATURITY MODEL," *INDEXIA Inform. Comput. Intell. J.*, vol. 05, no. 1, pp. 59–71, May 2023, doi: 10.30587/indexia.v5i01.5465.

[2] A. Pakarbudi, W. Lumadi, A. Aisyah P.K., and R. Antika Dewi P., "Analisis Strategi Sistem Informasi dan Teknologi Informasi Pada RS ABC Surabaya di Masa Pandemi COVID-19 Menggunakan Model Ward and Peppard," *JATISI J. Tek. Inform. Dan Sist. Inf.*, vol. 9, no. 3, pp. 2626–2640, Sep. 2022, doi: 10.35957/jatisi.v9i3.2955.

[3] S. N. Rachman and A. Pakarbudi, "Analisa Pengukuran Keselarasan Strategi Bisnis dan TI Menggunakan Metode SAMM LUFTMAN," in *SNESTIK IV*, Surabaya Indonesia: Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya, Apr. 2024, pp. 137–146. [Online]. Available: https://ejurnal.itats.ac.id/snestik/article/view/5836

[4] Adib Pakarbudi, Anugrah Yoga Adipratama, Dicky Eko Ardianto, and Zendi Asriel Adrian Jaya, "PENINGKATAN EFEKTFITAS USER INTERFACE (UI) DAN USER EXPERIENCE (UX) MELALUI PENDEKATAN USER CENTERED DESIGN PADA WEBSITE E – LIBRARY BPSDMP KOMINFO SURABAYA," *ZONAsi J. Sist. Inf.*, vol. 4, no. 2, pp. 76–87, Sep. 2022, doi: 10.31849/zn.v4i2.10974.

[5] A. Pakarbudi, D. T. Piay, D. Nurmadewi, and A. Rachman, "Analisa Efektivitas Metode Octave Allegro dan Fmea Dalam Penilaian Risiko Aset Informasi Pada Institusi Pendidikan Tinggi," *JURIKOM J. Ris. Komput.*, vol. 10, no. 2, p. 488, Apr. 2023, doi: 10.30865/jurikom.v10i2.5950.

[6] A. Zuhriyah and A. Pakarbudi, "Penilaian Risiko Keamanan Informasi Menggunakan Standar NIST SP 800-30 pada PT.XYZ," in *SNESTIK IV*, Surabaya Indonesia: Fakultas Teknik Elektro dan Teknologi Informasi-Institut Teknologi Adhi Tama Surabaya, Apr. 2024, pp. 377–389. [Online]. Available: https://ejurnal.itats.ac.id/snestik/article/view/5835

[7] A. Gui, S. Gondodiyoto, and I. Timotius, "PENGUKURAN RESIKO Teknologi Informasi (TI) DENGAN METODE OCTAVE-S," *CommIT Commun. Inf. Technol. J.*, vol. 2, no. 1, p. 33, May 2008, doi: 10.21512/commit.v2i1.489.

[8] N. Budarsa, G. Indrawan, and A. Gunadi, "ANALISIS RISIKO KEAMANAN INFORMASI MENGGUNAKAN METODE OCTAVE ALLEGRO DAN ANALYTICAL HIRARCHY PROCESS PADA DATA CENTER PEMERINTAH KABUPATEN BULELENG," *J. Ilmu Komput. Indones. JIK*, vol. 7, no. 1, pp. 11–20, 2022, doi: 10.23887/jik.v7i1.3769.

[9] B. S. Deva and R. Jayadi, "Analisis Risiko dan Keamanan Informasi pada Sebuah Perusahaan System Integrator Menggunakan Metode Octave Allegro," *J. Teknol. Dan Inf.*, vol. 12, no. 2, pp. 106–117, Sep. 2022, doi: 10.34010/jati.v12i2.6829.

[10] S. Stephanus, "Implementation Octave-S and Iso 27001controls in Risk Management Information Systems," *ComTech Comput. Math. Eng. Appl.*, vol. 5, no. 2, p. 685, Dec. 2014, doi: 10.21512/comtech.v5i2.2225.

[11] F. R. B. Butar, E. Saputra, A. Marsal, and M. L. Hamzah, "Analisis Manajemen Risiko Keamanan Sistem Pengolahan Data Accurate Menggunakan Metode OCTAVE-S," *J. Sains Komput. Inform. J-SAKTI*, vol. 7, no. 2, pp. 675–685, Sep. 2023, doi: 10.30645/j-sakti.v7i2.676.

[12] A. N. Kurniawan and B. T. Hanggara, "Penerapan Manajemen Risiko Teknologi Informasi menggunakan Metode OCTAVE-S pada UPT Pusat Komputer Politeknik Negeri Malang," *J. Pengemb. Teknol. Inf. Dan Ilmu Komput.*, vol. 4, no. 6, pp. 1802–1808, Jun. 2020.

[13] F. Nisa, M. Megawati, M. L. Hamzah, and I. Maita, "Analisis Manajemen Risiko Keamanan Sistem BMKGSoft Menggunakan Metode OCTAVE-S," *J. Ilm. Rekayasa Dan Manaj. Sist. Inf.*, vol. 8, no. 1, p. 62, Feb. 2022, doi: 10.24014/rmsi.v8i1.14334.

[14] S. P. Saragih, "Implementasi Octave-S Dalam Evaluasi Manajemen Resiko Sistem Informasi Pada Balai Pelatihan Kesehatan Batam," *J. Ilm. Inform. JIF*, vol. 06, no. 01, pp. 17–22, 2018, doi: 10.33884/jif.v6i01.413.

[15] L. Rahmawati and K. D. Hartomo, "Information Technology Security Risk Management using the OCTAVE-S Method," *SISTEMASI*, vol. 12, no. 3, p. 851, Sep. 2023, doi: 10.32520/stmsi.v12i3.3122.