Jurnal Infosecure Vol.2 No.2, Oktober 2021
p-ISSN: 2087-1023
MTI-UNLA

Tata Kelola Pengamanan Informasi pada Sistem *Hybrid Lending* dengan NIST *Cybersecurity Framework*

(Studi kasus: PT. Amartha Mikro Fintek)

Bonar Panjaitan[1], Mokhamad Hendayun[2], Agus Iim Suryana[3]

Magister Teknik Informatika, Fakultas Teknik, Universitas Langlangbuana[1,2,3]

[1]bonarp@gmail.com

[2]hendayun@unla.ac.id

[3]agus.iim.suryana@unla.ac.id

Abstrak—Dalam dunia Fintek, sistem *hybrid lending* yang mengintegrasikan teknologi digital dalam proses pengamanan membutuhkan pendekatan pengelolaan keamanan informasi yang efektif untuk melindungi data sensitif dan memastikan keberlangsungan operasional bisnis. Penelitian ini menganalisis penerapan Tata Kelola Pengamanan Informasi berlandaskan NIST *Cybersecurity Framework* dalam konteks sistem *hybrid lending*. Kerangka ini melibatkan pengembangan kerangka kerja utama yang terdiri dari *Identify, Protect, Detect, Respond* dan *Recover*. Masing-masing tingkat menggambarkan evolusi organisasi dalam mengidentifikasi, menilai, dan mengelola risiko keamanan informasi. Hasil implementasi menunjukkan bahwa dengan mengikuti NIST *Cybersecurity Framework*, organisasi dapat meningkatkan kesadaran keamanan, konsistensi penerapan kebijakan, serta respon yang lebih cepat terhadap insiden keamanan. Penelitian ini memberikan rekomendasi untuk memperkuat keamanan sistem informasi di sektor *hybrid lending* dengan memanfaatkan teknologi terbaru dan mengintegrasikan pembelajaran berkelanjutan dalam strategi keamanan. Dengan demikian, penelitian ini bertujuan untuk memberikan kontribusi signifikan dalam pengembangan praktik terbaik pengelolaan keamanan informasi di era digital yang terus berkembang**.**

Kata kunci—Fintek, *Hybrid lending*, NIST *Cybersecurity*, Keberlangsungan bisnis

I. PENDAHULUAN

Dalam era digital yang semakin maju, industri teknologi finansial (Fintek) telah mengalami perkembangan pesat, terutama dalam penyediaan layanan keuangan yang lebih cepat dan efisien. Salah satu inovasi Fintek yang signifikan adalah sistem *hybrid lending*, yaitu platform peminjaman yang menggabungkan model pinjaman tradisional dan digital untuk menjangkau lebih banyak pengguna. Dibalik kemudahan ini, Fintek juga menghadapi tantangan besar terkait keamanan informasi, karena data sensitif seperti data keuangan dan pribadi pengguna berada dalam risiko pencurian dan penyalahgunaan.

Menurut data dari Badan Siber dan Sandi Negara (2022), ancaman terhadap keamanan siber di Indonesia terus meningkat setiap tahun. Fintek, sebagai sektor yang memproses dan menyimpan data keuangan dalam jumlah besar, menjadi target utama bagi serangan siber. Kehadiran sistem *hybrid lending*, yang menggabungkan teknologi *cloud*, aplikasi seluler, dan infrastruktur IT tradisional, membuka potensi lebih besar terhadap serangan ini. Penggunaan beragam teknologi juga memperbesar permukaan serangan (*attack surface*) dan mempersulit pengamanan.

Seiring dengan itu, NIST *Cybersecurity Framework* (CSF) telah menjadi standar internasional dalam pengelolaan dan pengamanan informasi. Kerangka kerja ini memberikan panduan sistematis dalam identifikasi, perlindungan, deteksi, respon, dan pemulihan dari ancaman keamanan siber. Dalam konteks sistem *hybrid lending*, implementasi tata kelola keamanan berdasarkan NIST CSF sangat relevan dan penting.

Kerangka kerja ini membantu perusahaan Fintek meningkatkan resiliensi keamanan informasi serta meminimalkan risiko yang dapat mengganggu operasional dan kepercayaan pelanggan. Tata kelola keamanan informasi yang kuat melalui penerapan NIST CSF tidak hanya memastikan kepatuhan terhadap regulasi, tetapi juga mengurangi risiko finansial, reputasi, dan operasional. Sebagai industri yang mengandalkan kepercayaan, gangguan keamanan pada Fintek dapat menyebabkan hilangnya kepercayaan pelanggan, yang berdampak langsung pada keberlanjutan bisnis. Selain itu, dengan meningkatnya tuntutan Otoritas Jasa Keuangan (OJK) terkait keamanan data di sektor keuangan, penerapan kerangka kerja ini menjadi semakin mendesak untuk memastikan perlindungan optimal.

Oleh karena itu, penelitian tentang tata kelola pengamanan informasi pada sistem *hybrid lending* dengan mengacu pada NIST CSF menjadi sangat penting. Penelitian ini tidak hanya bertujuan untuk mengidentifikasi risiko keamanan, tetapi juga memberikan solusi tata kelola yang dapat diimplementasikan oleh perusahaan Fintek dalam menghadapi ancaman keamanan siber yang terus berkembang.

Pengamanan informasi dalam sistem *hybrid lending* merupakan aspek krusial yang tidak dapat diabaikan, mengingat meningkatnya penggunaan teknologi digital dalam sektor keuangan. Menurut ISO/IEC 27001:2013, pengamanan informasi mencakup perlindungan terhadap

data dan informasi yang bersifat sensitif, baik yang disimpan secara elektronik maupun yang berbentuk fisik (ISO/IEC 27001, 2013). *Hybrid lending*, yang menggabungkan elemen pinjaman tradisional dan teknologi finansial, menghadirkan berbagai tantangan baru dalam hal pengelolaan risiko keamanan informasi. Menurut laporan dari *Cybersecurity & Infrastructure Security Agency* (CISA) tahun 2021, sektor keuangan menjadi salah satu target utama serangan siber, dengan lebih dari 30% insiden yang dilaporkan berasal dari serangan *ransomware* (CISA, 2021). Hal ini menunjukkan bahwa perlindungan data dan informasi nasabah harus menjadi prioritas utama bagi lembaga keuangan yang menerapkan sistem *hybrid lending*.

II. METODE

A. Objek Penelitian

PT. Amartha Mikro Fintek memberikan platform teknologi keuangan mikro terdepan yang memiliki misi mewujudkan kesejahteraan bersama lewat pembangunan infrastruktur keuangan digital bagi ekonomi akar rumput. Berdiri sejak 2010, Amartha hadir sebagai *microfinance* untuk menghubungkan usaha mikro pedesaan yang dijalankan oleh para perempuan tangguh dengan akses permodalan terjangkau. Amartha memberdayakan lebih banyak UMKM perempuan, menciptakan lapangan kerja dan membangun pertumbuhan ekonomi yang lebih inklusif.

B. Metode Penelitian

Dalam penelitian ini, penulis menggunakan pendekatan penelitian kualitatif dan kuantitatif untuk mendapatkan gambaran yang komprehensif mengenai tata kelola pengamanan informasi pada sistem *hybrid lending*. Penelitian kualitatif akan memberikan wawasan mendalam tentang praktik dan tantangan yang dihadapi oleh pelaku usaha dalam menerapkan kerangka kerja NIST CSF.

Sementara itu, pendekatan kuantitatif digunakan untuk mengukur dan menganalisis data yang berkaitan dengan implementasi dan efektivitas kerangka kerja NIST dalam sistem *hybrid lending*. Penelitian kuantitatif dapat memberikan data statistik yang kuat dan valid, yang dapat digunakan untuk menarik kesimpulan yang lebih umum. Menurut Babbie (2020), metode kuantitatif memungkinkan peneliti untuk melakukan generalisasi dari sampel yang diambil, sehingga hasilnya dapat diterapkan pada populasi yang lebih luas.

Kombinasi kedua pendekatan ini diharapkan dapat memberikan gambaran yang lebih holistik mengenai tata kelola pengamanan informasi. Dengan demikian penelitian ini diharapkan dapat memberikan kontribusi yang signifikan dalam pengembangan kebijakan dan praktik keamanan informasi di sektor *hybrid lending*.

C. Tahapan Penelitian

Tahap ini menggambarkan serangkaian tahapan penelitian atau cara memecahkan masalah dalam proses penelitian ini. Metodologi penelitian ini terdiri dari beberapa tahapan, yaitu:

a. Tahap perencanaan: perumusan masalah dan studi literatur
b. Tahap desain penelitian: penelitian kualitatif dan kuantitatif
c. Tahap pengumpulan data: melalui wawancara dan *survey* kuesioner
d. Tahap analisis data: pengolahan data menggunakan framework NIST CSF
e. Integrasi temuan, dan
f. Rekomendasi: penulisan laporan dan penyampaian hasil.

Langkah awal dalam penelitian ini adalah melakukan tahap perencanaan, tahap perencanaan terdiri dari dua yaitu merumuskan masalah dan studi literatur.

Penelitian ini akan difokuskan pada bagaimana NIST CSF dapat digunakan sebagai panduan untuk membangun tata kelola pengamanan informasi yang komprehensif, sehingga mampu mengatasi tantangan keamanan yang ada pada sistem *hybrid lending* di sektor Fintek. Penelitian ini juga akan mengidentifikasi kekuatan dan kelemahan penerapan NIST CSF, serta rekomendasi untuk mengoptimalkan keamanan informasi di dalam konteks *hybrid lending*.

Setelah masalah ditentukan, peneliti merancang desain penelitian dengan melibatkan pengembangan struktur untuk pengumpulan data yang mencakup elemen kualitatif dan kuantitatif. Desain ini juga mencakup pemilihan metode pengumpulan data yang akan digunakan, seperti survei untuk data kuantitatif dan wawancara atau kelompok diskusi untuk data kualitatif.

D. Tahap Analisis

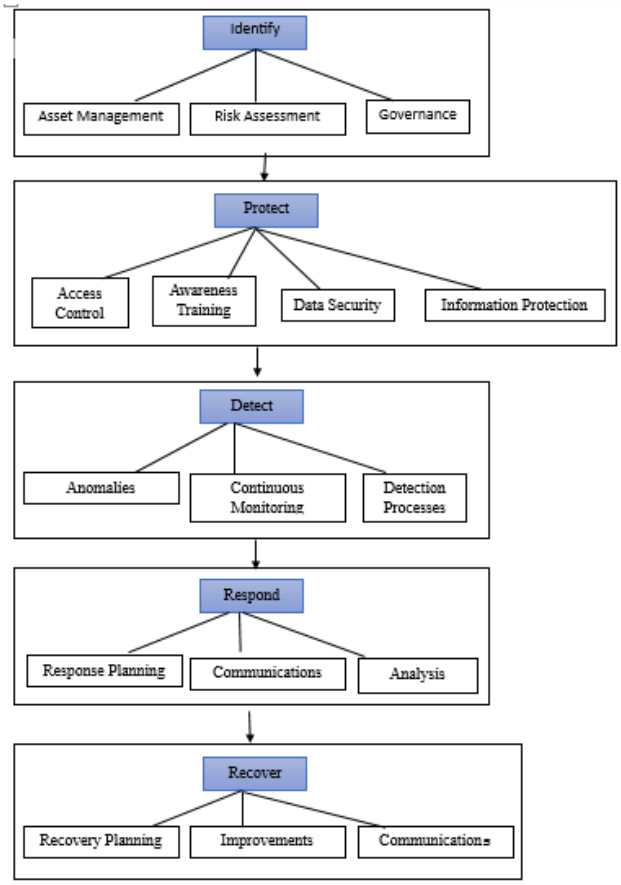
Setelah data terkumpul, peneliti melakukan analisis data berdasarkan jenis data yang telah dikumpulkan:

a. Analisis Kualitatif: Menggunakan teknik analisis seperti analisis tematik atau analisis konten untuk menggali pola, tema, dan wawasan dari data kualitatif yang diperoleh.
b. Analisis Kuantitatif: Menggunakan analisis statistik untuk menginterpretasikan data kuantitatif. Ini bisa meliputi analisis deskriptif, inferensial, dan penggunaan perangkat lunak statistik untuk memudahkan proses.

Tahap analisis dan pengolahan data ini untuk memberikan gambaran yang komprehensif mengenai implementasi tata kelola pengamanan informasi pada sistem *hybrid lending*, menggunakan NIST CSF sebagai acuan. Dengan kombinasi analisis kuantitatif dan kualitatif, penelitian ini akan menghasilkan wawasan mendalam tentang efektivitas NIST CSF dalam mengelola risiko keamanan siber dan memberikan panduan bagi perusahaan Fintek untuk meningkatkan sistem keamanan mereka.

E. Tahapan Cara Kerja NIST *Cybersecurity Framework*

Berikut adalah diagram sederhana yang menggambarkan tahapan dalam NIST *Cybersecurity Framework*:



Gambar 1 Tahapan Cara Kerja NIST *Cybersecurity Framework*

Berdasarkan NIST (2018), NIST CSF terdiri dari lima fungsi inti yang saling berhubungan: Identify, Protect, Detect, Respond, dan Recover. Setiap fungsi ini dirancang untuk menangani berbagai aspek keamanan siber secara holistik, mencakup pencegahan hingga pemulihan dari ancaman siber. Berikut penjelasan rinci setiap tahapan cara kerja NIST CSF:

1. *Identify* (Identifikasi)

Dalam tahap ini, organisasi melakukan inventarisasi aset dan sumber daya yang perlu dilindungi. Ini meliputi pemetaan data, sistem, perangkat keras, perangkat lunak, dan orang yang memiliki peran penting dalam keamanan informasi. Selain itu, organisasi juga melakukan penilaian risiko untuk mengidentifikasi potensi ancaman dan kerentanan serta mengembangkan kebijakan dan prosedur keamanan yang sesuai. Adapun yang terlibat diantaranya:

a. *Asset Management*: Mengidentifikasi dan mengelola aset IT dan data penting.
b. *Risk Assessment*: Menganalisis risiko dan menetapkan prioritas untuk mitigasi.
c. *Governance*: Mengembangkan kebijakan keamanan untuk memastikan kepatuhan terhadap peraturan.

2. *Protect* (Perlindungan)

Tahap ini bertujuan untuk mengimplementasikan langkah-langkah pengendalian yang diperlukan untuk melindungi aset identifikasi dari risiko yang telah diidentifikasi. Ini mencakup berbagai tindakan yang mencegah atau mengurangi dampak potensi insiden keamanan. Adapun yang terlibat diantaranya:

a. *Access Control*: Mengendalikan akses ke informasi dan sistem.
b. *Awareness Training*: Meningkatkan kesadaran karyawan tentang risiko keamanan siber.
c. *Data Security*: Melindungi integritas dan kerahasiaan data.
d. *Information Protection*: Mengimplementasikan perlindungan tambahan untuk informasi sensitif.

3. *Detect* (Deteksi)

Pada tahap ini, organisasi berfokus pada pengembangan dan penerapan aktivitas untuk mendeteksi insiden keamanan. Deteksi yang tepat waktu dan akurat adalah kunci untuk menanggapi insiden sebelum menyebabkan kerusakan lebih lanjut. Adapun yang terlibat diantaranya:

a. *Anomalies*: Mendeteksi perilaku anomali yang menunjukkan potensi serangan.
b. *Continuous Monitoring*: Memantau jaringan secara terus menerus untuk mendeteksi insiden.
c. *Detection Processes*: Mengembangkan prosedur dan teknologi untuk mendeteksi serangan dengan cepat.

4. *Respond* (Respon)

Setelah insiden terdeteksi, langkah selanjutnya adalah berhasil menanggapi insiden tersebut. Ini mencakup pengembangan rencana respon yang jelas, komunikasi dengan pihak terkait, serta analisis untuk memahami dampak dan penyebab insiden. Adapun yang terlibat diantaranya:

a. Respon *Planning*: Merencanakan respon yang lebih baik untuk insiden masa depan.
b. *Communications*: Mengelola komunikasi internal dan eksternal selama dan setelah insiden.
c. *Analysis*: Menganalisis insiden untuk memahami penyebab dan dampaknya.

5. *Recover* (Pemulihan)

Tahap terakhir ini berfokus pada pemulihan sistem dan data ke keadaan normal setelah insiden keamanan. Organisasi harus mengevaluasi pemulihan, meningkatkan implementasi keamanan, dan memberi tahu pemangku kepentingan terkait. Adapun yang terlibat diantaranya:

a. *Recovery Planning*: Menyusun rencana untuk *pemulihan* cepat dan sistematis.
b. Improvements: Membuat perbaikan berdasarkan pelajaran yang diperoleh setelah insiden.
c. *Communications*: Memastikan komunikasi yang jelas dengan semua pihak terkait pada saat pemulihan.

F. Instrumen Pengumpulan Data

Dalam penelitian ini ada beberapa cara untuk pengumpulan data yang sesuai dengan penggunaan NIST CSF, diantaranya:

1. Kuesioner *Survey* dalam penelitian ini meliputi:

a. Informasi Demografis yang diperlukan untuk mengetahui keadaan penggunaan NIST CSF pada PT. Amartha Mikro Fintek, dengan data yang diperlukan disesuaikan dengan format data yang ada.
b. NIST CSF untuk mendapatkan data tentang penggunaan penerapan NIST CSF

2. Wawancara

Pada tahap ini peneliti akan melakukan wawancara kepada manajemen dan karyawan yang terlibat dalam pengelolaan *Hybrid lending*.

III. HASIL DAN PEMBAHASAN

A. Implementasi Standar kerangka kerja Penerapan NIST *Cybersecurity* pada *Hybrid Lending*

Standar ini disusun dengan tujuan untuk memfasilitasi implementasi Kerangka Kerja NIST CSF di dalam organisasi, memperkuat ketahanan siber, serta meningkatkan kesiapan dalam menghadapi insiden keamanan informasi. Standar ini memberikan panduan tentang cara mengadopsi dan mengadaptasi kerangka kerja NIST, dengan memperhatikan konteks operasional dan risiko yang unik dari setiap organisasi. Standar ini juga bertujuan untuk mendorong praktik terbaik dalam mengelola risiko keamanan siber serta membangun kesadaran dan budaya keamanan yang lebih tinggi di seluruh lapisan organisasi.

Berikut adalah tabel yang menggambarkan kerangka kerja Tata Kelola Pengamanan Informasi pada Sistem *Hybrid lending* berdasarkan NIST CSF. Tabel ini mencakup kategori, sub-kategori, tujuan, serta contoh aktivitas yang dapat dilakukan untuk setiap kategori dalam konteks keamanan informasi.

Tabel 2 Standar Kerangka Kerja NIST *Cybersecurity*

Kategori	Sub-Kategori	Tujuan	Aktivitas
Identification	ID.AM-1: *Asset Manage-ment*	Menginventarisasi semua aset yang digunakan dalam sistem *hybrid lending*	Membuat dan memelihara daftar lengkap perangkat keras, perangkat lunak, dan data sensitif yang digunakan.
	ID.RA-1: *Risk Assesment*	Mengidentifikasi dan menilai risiko terhadap aset dan proses bisnis	Melakukan penilaian risiko secara teratur untuk mengidentifikasi potensi ancaman dan kelemahan.
	ID.GV-1: *Governance*	Menyusun kebijakan keamanan informasi yang komprehensif	Mengembangkan dan mendistribusikan kebijakan pengelolaan keamanan informasi kepada seluruh karyawan.
Protect	PR.AC-1: *Access Control*	Mengelola akses ke aset berdasarkan kebijakan keamanan	Menerapkan kontrol akses berbasis peran (RBAC) untuk membatasi akses ke data sensitif.
	PR.IP-1: *Information Protection*	Menyusun kebijakan operasional untuk pengelolaan data dan keamanan	Menetapkan prosedur operasional baku (SOP) untuk perlindungan data dan pemeliharaan sistem.
	PR.DS-1: *Data Security*	Melindungi data sensitif dari akses yang tidak sah	Menggunakan enkripsi untuk data dalam penyimpanan dan transmisi.
	PR.AT-1: *Awareness Tranning*	Meningkatkan kesadaran karyawan tentang ancaman keamanan	Mengadakan program pelatihan keamanan informasi untuk semua karyawan secara berkala.
Detect	DE.CM-1: *Continuous Monitoring*	Memastikan bahwa sistem dipantau untuk mendeteksi insiden	Mengimplementasikan sistem pemantauan berbasis peristiwa (*event monitoring*) untuk kegiatan mencurigakan.
	DE.AE-1: *Detect Anamalies*	Menganalisis informasi untuk mendeteksi dan merespon insiden	Melakukan analisis dan investigasi forensik setelah terjadi insiden keamanan.
	DE.DP-1: *Detection Proces*	Menyusun prosedur untuk mendeteksi	Mengembangkan dan menerapkan prosedur pelaporan insiden

Kategori	Sub-Kategori	Tujuan	Aktivitas
		insiden keamanan	untuk memastikan respon yang cepat.
Respon	RS.RP-1: *Respon Planning*	Mempersiapkan rencana respon terhadap insiden	Menyusun rencana tanggap insiden yang mencakup komunikasi, tindakan pemulihan, dan pemulihan sistem.
	RS.AN-1: *Analysis*	Memahami penyebab dan dampak dari insiden keamanan	Mengadakan sesi pasca insiden (*post-incident review*) untuk membahas pelajaran yang didapat dan langkah perbaikan.
	RS.CO-1 *Communication*	Mengkomunikasikan dampak-dampak dari insiden	Mengkomunikasikan antar tim rencana pemecahan insiden-insiden yang terjadi
Recover	RC.RP-1: *Recovery Planning*	Menyusun rencana untuk memulihkan sistem setelah insiden	Mengembangkan dan menguji rencana pemulihan bencana untuk memastikan pemulihan sistem yang cepat dan efektif.
	RC.IM-1: Improvement	Melanjutkan perbaikan berdasarkan pembelajaran dari insiden yang telah terjadi	Melakukan peninjauan kebijakan keamanan secara berkala dan memperbarui berdasarkan hasil analisis insiden sebelumnya.
	RC.CO-1 Communication	Mengkomunikasikan penanganan pemulihan	Mengkomunikasikan dengan tim rencana dan teknis pemulihan insiden

B. Kinerja *Core Identify* pada *Hybrid Lending*

Mengidentifikasi sistem, aset, data, dan kemampuan yang penting untuk keberlangsungan organisasi. Ini melibatkan proses penilaian risiko dan pemahaman akan konteks bisnis serta kebutuhan keamanan dan kegiatan utama di sini termasuk membuat inventaris aset (*asset management*) dan memahami risiko (*Risk Management*) yang sesuai, untuk penjelasan lebih lanjut bisa dilihat dalam keterangan di bawah ini.

1. Indentifikasi *Asset Management*

Hasil penilaian pada aset manajemen untuk membahas mengenai Tata Kelola Pengamanan Informasi pada Sistem *Hybrid lending* dengan NIST CSF, menyediakan informasi tentang aset yang dikelola, klasifikasinya, nilai kerentanan yang teridentifikasi, serta kategori risiko yang terkait sebagaimana tertera dalam tabel di bawah ini.

Tabel 3 Tabel Hasil *Assesment* untuk *Asset Management*

Nama Aset	Klasifi-kasi	Nilai Aset	Kerentanan yang Teridentifikasi	Kategori Risiko
Basis Data Pelanggan	Data Sensitif	Tinggi	Enkripsi tidak kuat, akses tanpa otorisasi	Kebocoran Data
Aplikasi Pinjaman Online	Aplikasi	Tinggi	Kerentanan aplikasi, risiko serangan DDoS	Serangan Siber
Server *Cloud*	Infrastruktur TI	Sangat Tinggi	Pemeliharaan yang tidak memadai	*Down time*, Kehilangan Data
Sistem Manajemen Identitas	Infrastruktur TI	Tinggi	Sistem otentikasi yang rentan	Penyalahgunaan Akses
Jaringan Internal	Infrastruktur Jaringan	Tinggi	*Firewall* yang tidak terkonfigurasi	Akses Tidak Sah
Sistem Pembayaran	Data Transaksi	Sangat Tinggi	Proses transaksi yang tidak aman, XSS	Penipuan Finansial
Email Internal	Data Komunikasi	Sedang	*Phishing* dan *malware*	Kebocoran Data
Laporan Keuangan	Data Sensitif	Tinggi	Akses tidak terbatas	Kebocoran Data, Penipuan
API Pinjaman	Aplikasi	Tinggi	Kerentanan API, kurangnya otentikasi	Serangan Siber

Sistem *Backup*	Infrastruktur TI	Tinggi	*Backup* tidak terenkripsi	Kehilangan Data

Tabel hasil penilaian ini memberikan gambaran yang jelas tentang aset yang dikelola oleh organisasi dalam sistem *hybrid lending*. Identifikasi kerentanan dan penilaian risiko yang terkait dengan setiap aset memungkinkan organisasi untuk mengembangkan strategi pelindung yang lebih baik guna meningkatkan keamanan informasi. Dengan mengikuti NIST CSF, organisasi dapat memprioritaskan langkah-langkah mitigasi yang diperlukan untuk melindungi aset yang paling penting dan berisiko.

2. Identifikasi *Risk Assessment*

Hasil kuesioner ini menunjukkan bahwa, meskipun terdapat proses penilaian risiko yang formal serta pengenalan pentingnya manajemen risiko dalam organisasi, masih ada banyak area yang perlu diperbaiki, terutama dalam hal efektivitas identifikasi risiko dan pemahaman kesadaran risiko di kalangan karyawan. Adapun rekomendasi untuk identifikasi *risk assessment* tertera terdapat dalam tabel dibawah.

Tabel 4 Hasil *Assesment* dan Rekomendasi *Risk Assessment*

Risiko	Level Risiko	Rekomendasi Mitigasi	Referensi
Kebocoran Data Pelanggan	Tinggi	Implementasi enkripsi data, kontrol akses ketat, dan pelatihan karyawan.	ID.RA.01
Serangan Siber Aplikasi Pinjaman	Tinggi	Penyediaan sistem mitigasi DDoS dan *monitoring real-time*.	ID.RA.02
Down time, Kehilangan data	Sangat Tinggi	Penggunaan otentikasi multi-faktor (MFA) dan *logging* aktivitas akses.	ID.RA.05
Penyalahgunaan Akses	Tinggi	Prosedur yang jelas, pelatihan, dan penggunaan *checklist* dalam transaksi.	ID.RA.06
Akses tidak sah	Tinggi	Pengawasan akses dan pelatihan etika serta keamanan bagi pegawai.	ID.RA.05
Penipuan Transaksi melalui API	Sangat Tinggi	Penerapan otentikasi yang kuat dan pemantauan aktivitas API.	ID.RA.03
Malware dan *Phishing* melalui Email	Sedang	Pelatihan kesadaran keamanan, dan penggunaan alat filter spam.	ID.RA.03
Kehilangan data dan penipuan	Tinggi	Audit reguler dan penilaian kepatuhan terhadap kebijakan dan regulasi.	ID.RA.04
Kerentanan dalam Aplikasi Pinjaman	Tinggi	Pemindaian kerentanan dan perbaikan sistem secara berkala.	ID.RA.05
Kehilangan Data akibat kegagalan *backup*	Tinggi	Rutinitas pengujian pemulihan data dan memastikan *backup* terenkripsi.	ID.RA.05

Tingkat kemungkinan terjadinya risiko, pada tabel hasil *Risk Assessment* ini memberikan gambaran tentang potensi risiko yang dihadapi oleh organisasi dalam sistem *hybrid lending*. Dengan mengidentifikasi risiko dan memberikan level risiko secara sistematis, organisasi dapat lebih fokus dalam menerapkan langkah-langkah mitigasi yang tepat. Pendekatan berbasis NIST CSF memungkinkan organisasi untuk mengelola dan mengurangi risiko, serta memastikan keberlanjutan operasional dan perlindungan data yang lebih baik.

C. Kinerja *Core Detect* pada *Hybrid Lending*

Proses *Detect* memiliki kemampuan untuk mendeteksi kejadian-kejadian keamanan yang telah terjadi. Ini membantu organisasi untuk mengenali anomali atau insiden lebih awal. Oleh karena itu, ini mencakup pemantauan terus-menerus, pengujian dan evaluasi sistem, serta pengelolaan log. Hasil kuesioner ini menunjukkan bahwa organisasi umumnya memiliki kebijakan dan praktik pemantauan berkelanjutan yang baik. Namun, ada beberapa area yang perlu perbaikan, terutama dalam hal pembaruan kebijakan, peningkatan efektivitas pemantauan, dan peningkatan pelatihan serta kesadaran di kalangan karyawan.

Data ini dapat digunakan oleh manajemen untuk mengevaluasi dan memperkuat inisiatif pemantauan berkelanjutan, membantu organisasi dalam mendeteksi dan mengatasi ancaman keamanan lebih cepat dan lebih efektif. Dari hasil analisis dan temuan di atas maka dapat direkomendasikan sesuai dengan tabel 5 di bawah ini.

Tabel 5 Hasil *Assesment* dan Rekomendasi *Detect Continuous Monitoring*

Elemen Pemantauan	Deskripsi	Metode Implementasi	Status Saat Ini	Rekomendasi	Referensi
Pengumpulan Data Keamanan	Mengumpulkan data dari berbagai sumber keamanan	Alat *Monitoring* Keamanan, SIEM,	Implementasi - Baik	Pastikan data dari semua sistem dan perangkat diintegrasikan.	DE. AE-3

Elemen Pemantauan	Deskripsi	Metode Implementasi	Status Saat Ini	Rekomendasi	Referensi
		log server			
Analisis Risiko Secara *Real-Time*	Menganalisis risiko secara terus-menerus	Risk *Assessment tools* yang terintegrasi	Implementasi - Cukup	Kembangkan algoritma untuk analisis risiko otomatis.	DE.CM-3
Pemantauan Kebijakan dan Kepatuhan	Memantau kepatuhan terhadap kebijakan keamanan	Audit berkala dan penggunaan *checklist*	Implementasi - Rutin	Tinjau dan pertahankan *checklist* kepatuhan dengan standar terkini.	DE.DP-1
Visibilitas Keamanan	Menyediakan visibilitas menyeluruh terhadap status keamanan	*Dashboard* keamanan yang terpusat	Implementasi - Baik	Tingkatkan tampilan visualisasi pada *dashboard* untuk kejelasan.	DE.DP-5
Deteksi Anomali	Mengidentifikasi perilaku mencurigakan dalam sistem	Penggunaan alat deteksi anomali	Implementasi - Cukup	Implementasikan *machine learning* untuk meningkatkan deteksi anomali.	DE.DP-5
Pelaporan Keamanan	Membuat laporan berkala tentang kegiatan pemantauan	Laporan bulanan dari alat *monitoring*	Implementasi - Baik	Tambahkan analisis tren dan kondisi untuk laporan.	DE.CM-6
Tanggapan terhadap Insiden	Prosedur untuk merespon insiden keamanan	Tim respon insiden dan simulasi	Implementasi - Terdokumentasi	Uji dan revisi prosedur tanggap insiden secara berkala.	DE.AE-4
Integrasi Sistem *Monitoring*	Membangun integrasi antar alat pemantauan keamanan	API dan sistem terpusat	Implementasi - Terbatas	Evaluasi dan perbarui jalan pengintegrasian untuk melacak dan memantau ancaman lebih efisien.	DE.CM-1
Pelatihan Staf tentang *Continuous Monitoring*	Menerapkan program pelatihan reguler untuk karyawan	*Workshop* dan pelatihan	Implementasi - Terdapat sesi	Kembangkan materi pelatihan agar lebih aplikatif dengan studi kasus nyata.	DE.AE-1
Uji Keefektifan Proses *Monitoring*	Menguji secara berkala efektivitas sistem dan proses *monitoring*	Simulasi dan audit jadi pemangku kepentingan	Implementasi - Rutin	Rencanakan secara teratur untuk melakukan evaluasi menyeluruh.	DE.CM-6

Tabel hasil *Assessment Continuous Monitoring* ini memberikan gambaran rinci mengenai elemen-elemen penting dalam pemantauan berkelanjutan yang diperlukan untuk pengelolaan keamanan informasi dalam sistem *hybrid lending*. Dengan mendokumentasikan setiap elemen, status saat ini, dan rekomendasi perbaikan, organisasi dapat mengidentifikasi area yang memerlukan perhatian untuk meningkatkan kemampuan deteksi dan respon terhadap ancaman keamanan. Penerapan prinsip-prinsip dari NIST CSF dalam konteks pemantauan berkelanjutan akan membantu organisasi dalam memperkuat ketahanan sistem terhadap risiko yang mungkin muncul.

D. Kinerja *Core Protect* pada *Hybrid Lending*

Menerapkan kontrol keamanan untuk melindungi aset organisasi dari ancaman. Ini mencakup strategi dan teknologi yang bertujuan untuk mengurangi risiko. Kegiatan ini termasuk pengendalian akses (*access control*), pelatihan dan kesadaran pengguna (*awareness training*), dan penerapan perlindungan data (*data security*) dan proteksi informasi (*information protection*).

Hasil kuesioner menunjukkan bahwa meskipun sebagian besar organisasi memiliki kebijakan keamanan dan prosedur untuk melindungi data, masih ada beberapa area yang perlu ditingkatkan, terutama dalam hal pembaruan kebijakan, penggunaan autentikasi yang lebih kuat, serta frekuensi audit dan *monitoring*. Data ini dapat digunakan oleh manajemen untuk mengevaluasi dan memperkuat strategi keamanan data, meminimalisir risiko, dan meningkatkan perlindungan terhadap data sensitif dalam organisasi. Dari data analisis dan temuan maka dapat direkomendasikan sebagaimana tertera dalam tabel di bawah ini

Tabel 6 Hasil *Assesment* dan Rekomendasi *Protect, Data Security*

Elemen Keamanan Data	Deskripsi	Metode Implementasi	Status Saat Ini	Rekomendasi	Referensi
Enkripsi Data	Mengamankan data sensitif dengan enkripsi	AES, RSA, enkripsi data di penyimpanan dan transit	Implementasi – Baik	Tinjau dan perbarui algoritma enkripsi secara berkala.	PR.DS-1
Perlindungan Data Pribadi	Melindungi data pribadi sesuai regulasi	Kebijakan kepatuhan GDPR, CCPA, dan lainnya	Implementasi - Memadai	Uji kepatuhan secara berkala terhadap peraturan yang berlaku.	PR.DS-2
Pengendalian Akses Data	Pembatasan akses ke data sensitif	Kontrol akses berbasis peran (RBAC)	Implementasi - Cukup	Audit hak akses dan penerapan prinsip *least privilege*.	PR.AC-4
Backup dan Pemulihan Data	Proses cadangan dan pemulihan data	Sistem *backup* harian dan pemulihan bencana	Implementasi – Baik	Uji pemulihan data secara berkala untuk memastikan efektivitas.	PR.DS-4
Pemantauan dan *Logging* Data	Mencatat aktivitas akses data	SIEM dan sistem *logging*	Implementasi – Baik	Integrasi analisis perilaku untuk mendeteksi aktivitas mencurigakan.	PR.DS-5
Data Masking	Menyembunyikan data sensitif saat diolah	Tokenisasi dan *masking* data	Implementasi - Terbatas	Tingkatkan penggunaan data *masking* selama pengujian produk.	PR.DS-2
Kebijakan Retensi Data	Kebijakan pengelolaan siklus hidup data	Prosedur penghapusan data yang sudah tidak diperlukan	Implementasi - Memadai	Tinjau dan perbarui kebijakan retensi secara berkala.	PR.IP-5
Pelatihan Karyawan	Kesadaran karyawan tentang	Sesi pelatihan dan sumber	Implementasi - Terda	Kembangkan modul pelatihan yang lebih	PR.AT-2
tentang Keamanan Data	pengelolaan data	belajar daring	pat sesi	interaktif dan praktis.	
Penggunaan Alat Keamanan Data	Alat untuk melindungi dan mengelola data	*Antivirus*, *firewall*, dan alat DLP	Implementasi – Baik	Tinjau efektivitas alat dan perbarui sesuai perkembangan teknologi.	PR.DS-5
Audit dan Penilaian Keamanan Data	Proses evaluasi keamanan data	Audit keamanan tahunan	Implementasi – Rutin	Tingkatkan frekuensi audit dan penggunaan laporan untuk tindakan perbaikan.	PR.DS-6

Tabel hasil *Assessment Data Security* ini memberikan gambaran komprehensif tentang berbagai elemen yang penting dalam keamanan data dalam konteks sistem *hybrid lending*. Dengan mendokumentasikan setiap elemen, status saat ini, dan rekomendasi perbaikan, organisasi dapat mengidentifikasi area yang memerlukan perhatian untuk meningkatkan kebijakan dan praktik pengelolaan data. Penerapan NIST CSF dalam konteks keamanan data akan membantu organisasi dalam melindungi informasi sensitif dan memastikan kepatuhan terhadap regulasi yang berlaku, serta meningkatkan ketahanan terhadap ancaman siber.

E. Kinerja *Core Respond* pada *Hybrid Lending*

Mengembangkan rencana respon insiden yang efektif meliputi penanganan kejadian keamanan yang terdeteksi, untuk mengurangi dampak dan memperbaiki situasi. Kegiatan di sini mencakup pengembangan rencana respon, penanganan dan mitigasi insiden, serta pelatihan dan simulasi. Hasil kuesioner menunjukkan bahwa organisasi umumnya memiliki kebijakan dan tim yang baik dalam perencanaan respon insiden. Namun, terdapat beberapa area yang perlu diperbaiki, terutama dalam hal pembaruan kebijakan, pengujian prosedur respon, dan pelatihan yang lebih teratur. Data ini dapat digunakan oleh manajemen untuk mengevaluasi dan memperbaiki proses perencanaan respon, meningkatkan kesiapsiagaan organisasi dalam menangani insiden yang tidak terduga serta mengurangi dampak yang mungkin terjadi. Dari hasil analisis dan temuan maka dapat direkomendasikan sebagaimana tertera dalam tabel dibawah ini.

Tabel 7 Hasil *Assesment* dan Rekomendasi *Respond*, Respon *Planning*

Elemen Perencanaan Respon	Deskripsi	Metode Implementasi	Status Saat Ini	Rekomendasi	Referensi
Kebijakan tanggap Insiden	Menyusun kebijakan yang jelas untuk menanggapi insiden keamanan	Dokumen kebijakan yang disetujui	Implementasi - Terdokumentasi	Tinjau dan perbarui kebijakan secara berkala.	RSRP-1
Tim Respon Insiden	Pembentukan tim khusus untuk menangani insiden keamanan	Pembentukan tim dengan peran yang jelas	Implementasi - Baik	Lakukan pelatihan teratur untuk anggota tim.	RS.CO-1
Rencana Tanggap Insiden	Penyusunan rencana terperinci untuk menangani berbagai jenis insiden	Rencana respon tertulis berdasarkan jenis insiden	Implementasi - Cukup	Uji rencana dengan simulasi insiden sesekali.	RSRP-1
Prosedur Komunikasi Tanggap Insiden	Menyusun prosedur untuk komunikasi selama insiden	Rencana komunikasi yang jelas dan terorganisir	Implementasi - Terdokumentasi	Pastikan semua *stakeholder* diberi tahu sesuai kebutuhan.	RS.CO-4
Pemulihan Pasca Insiden	Penetapan prosedur untuk pemulihan data dan sistem setelah insiden	Prosedur pemulihan dan cadangan data	Implementasi - Baik	Uji dan tinjau prosedur pemulihan secara berkala.	RS.MI-2
Analisis Pasca Insiden	Evaluasi dan analisis insiden setelah kejadian untuk perbaikan	Proses *review* insiden dan pembelajaran	Implementasi - Cukup	Dokumentasikan hasil analisis dan tindakan perbaikan.	RS.AN-2
Pelatihan dan Uji Praktik	Penyediaan pelatihan untuk karyawan tentang prosedur tanggap insiden	Sesi pelatihan dan simulasi kasus nyata.	Implementasi - Terdapat sesi	Tingkatkan pelatihan dengan studi	RS.AN-5
Rencana Kontinjensi	Penyusunan rencana alternatif untuk situasi yang tidak terduga	Prosedur kontingensi yang terstruktur	Implementasi - Cukup	Tinjau dan uji rencana setiap tahun.	RS.IM-1
Evaluasi dan Pembaruan	Proses untuk mengevaluasi dan memperbarui rencana respon secara reguler	Peninjauan berkala terhadap kebijakan dan prosedur	Implementasi - Rutin	Tetapkan jadwal tinjauan periodik untuk evaluasi.	RS.IM-2
Dokumentasi Insiden	Mencatat dan mendokumentasikan setiap insiden dan responnya	Sistem pencatatan insiden	Implementasi - Baik	Pastikan dokumentasi dapat diakses dan ditelusuri dengan mudah.	RS.AN-5

Tabel hasil *Assessment* Respon *Planning* ini memberikan gambaran mendalam mengenai elemen-elemen penting dalam perencanaan respon terhadap insiden yang diperlukan untuk pengelolaan keamanan informasi dalam sistem *hybrid lending*. Dengan mendokumentasikan setiap elemen, status saat ini, dan rekomendasi perbaikan, organisasi akan memiliki pemahaman yang lebih baik tentang kesiapan mereka dalam menghadapi insiden keamanan. Penerapan prinsip-prinsip dari NIST CSF dalam konteks perencanaan respon akan membantu organisasi dalam mitigasi risiko, mempercepat pemulihan pasca insiden, dan memastikan keamanan data yang lebih baik.

F. Kinerja *Core Recover* pada *Hybrid Lending*

Mengembangkan dan menerapkan rencana pemulihan untuk memperbaiki dan memulihkan fungsi operasional setelah serangan siber. Ini mencakup perencanaan pemulihan, pemulihan sistem yang terdampak, dan pembelajaran dari insiden untuk perbaikan yang berkelanjutan. Hasil kuesioner menunjukkan bahwa organisasi memiliki kebijakan dan praktik yang baik dalam mengimplementasikan tindakan perbaikan setelah pemulihan dari insiden. Namun, ada beberapa area yang dapat ditingkatkan, seperti kecepatan implementasi, pembaruan kebijakan, dan penyediaan pelatihan untuk karyawan. Data ini dapat digunakan oleh manajemen untuk mengevaluasi dan memperbaiki proses tindakan perbaikan,

yang sangat penting untuk meningkatkan ketahanan organisasi dan kecepatan respon terhadap insiden di masa mendatang. Dari hasil analisis dan temuan maka dapat direkomendasikan sebagaimana tertera dalam tabel dibawah ini.

Tabel 8 Hasil *Assessment* dan Rekomendasi *Recover Improvements*

Elemen Perbaikan	Deskripsi	Metode Implementasi	Status Saat Ini	Rekomendasi	Referensi
Audit dan Penilaian Kebijakan	Melakukan audit kebijakan keamanan informasi secara berkala	Audit internal dan *review* kebijakan	Implementasi - Rutin	Lakukan audit tambahan setelah insiden besar.	RC.RP-1
Peningkatan Pendidikan dan Pelatihan	Meningkatkan kesadaran dan pengetahuan keamanan siber di kalangan karyawan	Program pelatihan berkelanjutan	Implementasi - Cukup	Kembangkan modul pelatihan baru berdasarkan tren terbaru.	RC.IM-1
Penguatan Teknologi Keamanan	Mengimplementasikan teknologi keamanan yang lebih canggih	Pemanfaatan alat dan perangkat lunak modern	Implementasi - Baik	Tinjau dan optimasi-kan peng-gunaan alat yang sudah ada.	RC.IM-2
Peningkatan Prosedur Respon Insiden	Memperbarui dan memperbaiki prosedur respon insiden berdasarkan pelajaran yang didapat	*Review* dan pengujian prosedur	Implementasi - Cukup	Lakukan simulasi untuk menguji prosedur baru.	RC.CO-2
Pengembangan Rencana Pemulihan	Penyusunan dan pengujian ulang rencana pemulihan bencana yang lebih rinci	*Worksh op* dan latihan pemulihan	Implementasi - Terdokumentasi	Evaluasi kinerja rencana selama insiden nyata atau latihan.	RC.CO-3
Pengumpulan dan Analisis Data	Mengumpulkan data insiden untuk analisis mendalam dan perbaikan berkelanjutan	*Centralisasi* data insiden dan analisis tren	Implementasi - Cukup	Kembangkan alat analisis untuk memperm udah pengolahan data.	RC.RP-1
Memperkuat Komunikasi Internal	Meningkatkan komunikasi di antara tim keamanan dan pemangku kepentingan lainnya	Pertemuan dan laporan rutin	Implementasi - Baik	Tetapkan jadwal komunikasi teratur dan laporan status.	RC.IM-1
Peninjauan Berkelanjutan	Melakukan tinjauan dan evaluasi berkala terhadap semua kebijakan dan prosedur	Monitor dan *review* berkala	Implementasi - Rutin	Tampung umpan balik dari seluruh *stakeholder* untuk perbaikan.	RC.CO-3
Inovasi dalam Proses dan Teknologi	Menerapkan teknologi baru dan inovatif untuk meminimalkan risiko keamanan	Riset dan adopsi solusi teknologi baru	Implementasi - Cukup	Lakukan *pilot project* untuk menguji teknologi baru sebelum implementasi penuh.	RC.CO-3
Pengawasan dan Pelaporan yang Lebih Baik	Meningkatkan sistem pelaporan dan *monitoring* untuk deteksi dini ancaman	Penggunaan *dashboard* analitik	Implementasi – Baik	Evaluasi dan sesuaikan parameter dan metrik yang digunakan.	RC.CO-3

Tabel hasil *Assessment Improvements* ini memberikan gambaran yang komprehensif mengenai elemen-elemen yang dapat diperbaiki dalam pengelolaan keamanan informasi pada sistem *hybrid lending*. Dengan mendokumentasikan setiap elemen, status saat ini, dan rekomendasi perbaikan, organisasi dapat secara sistematis mengevaluasi dan meningkatkan keamanan informasi mereka. Penerapan prinsip-prinsip dari NIST CSF dalam konteks perbaikan ini akan membantu organisasi dalam berevolusi dan beradaptasi dengan tantangan keamanan yang terus berkembang.

IV. SIMPULAN

A. Kesimpulan

1. Peneliti menganalisis penerapan NIST CSF dalam konteks sistem *hybrid lending* dengan melakukan membagikan kuesioner kepada karyawan yang terlibat di PT. Amartha Mikro Fintek dengan menghasilkan *outcome* sebagai berikut:

a. Implementasi NIST CSF dalam sistem *hybrid lending* dapat menunjukkan permasalahan yang terjadi sehingga Perusahaan bisa mitigasi pengamanan informasi. Dengan menerapkan kelima komponen NIST CSF (*Identify, Protect, Detect, Respond,*

*Recov*er), organisasi dapat lebih memahami aset informasi perusahaan, mengelola akses, serta merespon insiden keamanan dengan lebih efektif.

b. Penelitian ini menghasilkan rekomendasi untuk pengembangan kebijakan keamanan informasi yang lebih komprehensif. Kebijakan ini tidak hanya mengatur aspek teknis, tetapi juga mengedepankan aspek manusia dan prosedural, yang menjadi kunci dalam mengurangi potensi risiko keamanan, dokumen rekomendasi kebijakan terlampir.
c. Salah satu hasil dari penelitian ini adalah peningkatan kesadaran akan pentingnya keamanan siber di kalangan karyawan. Program pelatihan dan sosialisasi yang diusulkan mampu membangun budaya keamanan yang lebih baik, di mana setiap individu berperan aktif dalam melindungi informasi sensitif, rekomendasi program pelatihan dan kurikulum terlampir.
d. Penelitian ini mengevaluasi risiko yang dihadapi oleh sistem *hybrid lending* melalui alat ukur yang dirancang berdasarkan NIST CSF. Hasil evaluasi menunjukkan adanya area yang membutuhkan perhatian dalam pengamanan informasi dan memberikan dasar yang kuat untuk pengambilan keputusan strategis oleh manajemen.

2. Peneliti membuat rekapitulasi hasil kuesioner, melakukan analisis dan temuan serta memberikan rekomendasi pada setiap kinerja terhadap manajemen PT. Amartha Mikro Fintek terkait pengamanan informasi dan risiko pada penerapan sistem *hybrid lending*

B. Saran

1. Hasil penelitian ini sebagai referensi untuk manajemen PT. Amartha Mikro Fintek dalam penerapan pengamanan informasi dan risiko pada penerapan sistem *hybrid lending* dengan masukan sebagai berikut:
   a. Perusahaan harus menerapkan semua komponen dari NIST CSF (*Identify, Protect, Detect, Respond, Recover*) sebagai kerangka kerja yang menjadi pedoman dalam pengelolaan keamanan siber. Proses ini mencakup pengidentifikasian aset, penilaian risiko, serta pengembangan kebijakan untuk melindungi data pelanggan dan memperkuat ketahanan terhadap serangan.
   b. Perusahaan perlu menyusun dan memperbarui kebijakan keamanan informasi secara berkala. Kebijakan tersebut harus mengatur prosedur akses, pengelolaan data, dan pelaporan insiden serta diintegrasikan dengan praktik terbaik industri. Melibatkan semua pihak terkait dalam penyusunan kebijakan ini akan memastikan adanya pemahaman dan penerimaan yang lebih baik di seluruh organisasi.

2. Penelitian ini bisa dikembangkan lagi dengan kasus yang lebih luas yang berkaitan dengan pengaman Informasi dalam bidang Fintek

3. Penelitian ini bisa dijadikan sumber referensi bagi peneliti-peneliti yang lain, khusus nya penelitian di bidang pengamanan informasi.

REFERENSI

Badan Siber dan Sandi Negara. (2022). Laporan Tahunan *Monitoring* Keamanan Siber Tahun 2021

Cybersecurity & Infrastructure Security Agency of United States of America (CISA). (2021). Understanding Denial-of-Service Attacks. https://www.cisa.gov/newsevents/news/understanding-denial-service-attacks

Babbie, E R. (2020). The Practice of Social Research, Cengage Learning

ISO/IEC 27001. (2013). Information technology — Security techniques — Information Security management systems — Requirements. Retrieved from ISO, https://www.iso.org/isoiec-27001-Information-Security.html

National Institute of Standards and Technology (NIST), "NIST *Cybersecurity* Framework," Version 1.1, 2018.