BACA: Jurnal Dokumentasi dan Informasi, Vol. 45, No. 1, 2024
ISSN 0125-9008 (Print); ISSN 2301-8593 (Online)
DOI: 10.55981/j.baca.2024.1237
SK Dirjen Dikti Ristek - Kemdikbudristek No. 105/E/KPT/2022 (Peringkat 2 SINTA)

Analisis keamanan siber sistem informasi perpustakaan di Perpustakaan Universitas Jenderal Soedirman

Arif Nurochman[1]*; Endah Yuni Astuti[2]; Sayekti Widianingtias[3]

[1]Fakultas Perikanan dan Ilmu Kelautan, Universitas Jenderal Soedirman
[2]Fakultas Pertanian, Universitas Jenderal Soedirman
[3]Fakultas Hukum, Universitas Jenderal Soedirman

*Korespondensi: arif_nur38@yahoo.com

Diajukan: 07-09-2023; **Direview:** 20-08-2024; **Diterima:** 26-08-2024; **Direvisi:** 23-08-2024

ABSTRACT

The implementation of web technologies in libraries faces challenges from acts of sabotage and cybersecurity, despite the ease of access to information being its main feature. The purpose of this study is to describe the analysis of information system cybersecurity at the Universitas Jenderal Soedirman (Unsoed) library using the NIST cybersecurity framework for the functions of identifying, protecting, detecting, responding, and recovering. Research informants consist of librarians who interact with information systems. The research method used was qualitative with a case study approach with in-depth interviews and observations. The results describe the function of identifying security processes according to the capabilities of librarians. The protect function identifies the identity management process and system vulnerabilities in the form of bugs and forms infiltrated by hackers. The detect function identifies infiltration from abroad. The respond function is handled by the administrator by restoring the server and is incidental after an event. The restore function plans actions to establish communication with library stakeholders. Technical recovery with default security systems and carrying out evaluation of enhancements developed in the system development life cycle continuously. Cybersecurity analysis using the NIST cybersecurity framework can describe the technical and managerial level of security in the application infrastructure so as to anticipate the possibility of cyber attacks.

ABSTRAK

Penerapan teknologi web di perpustakaan menghadapi tantangan dari tindakan sabotase dan keamanan siber meskipun kemudahan akses informasi menjadi ciri utamanya. Tujuan dari penelitian ini untuk mendeskripsikan analisis keamanan siber sistem informasi di UPT Perpustakaan Universitas Jenderal Soedirman (Unsoed) dengan menggunakan kerangka kerja NIST *Cybersecurity Framework* untuk fungsi mengidentifikasi, melindungi, mendeteksi, merespons dan memulihkan. Informan penelitian terdiri atas pustakawan yang berinteraksi dengan sistem informasi. Metode penelitian yang digunakan kualitatif dengan pendekatan studi kasus dengan wawancara mendalam dan observasi. Hasil penelitian mendeskripsikan fungsi mengidentifikasi proses keamanan sesuai kemampuan pustakawan. Fungsi melindungi mengidentifikasi proses manajemen identitas dan kerentanan sistem berupa *bug* dan *form* yang diinfiltrasi oleh *hacker*. Fungsi mendeteksi mengidentifikasi infiltrasi dari luar negeri. Fungsi merespon ditangani administrator dengan me-*restore server* dan bersifat insidental setelah adanya peristiwa. Fungsi memulihkan merencanakan tindakan menjalin komunikasi *stakeholder* perpustakaan. Pemulihan teknis dengan sistem keamanan *default* serta melaksanakan evaluasi penyempurnaan yang dikembangkan dalam siklus hidup pengembangan sistem secara terus menerus. Analisis keamanan siber menggunakan kerangka kerja NIST *Cybersecurity Framework* dapat mendeskripsikan secara teknis dan manajerial tingkat keamanan pada infrastruktur aplikasi sehingga dapat mengantisipasi kemungkinan terjadinya serangan siber.

Keywords: *Cybersecurity*; *Security*; *NIST Cybersecurity framework*

1. PENDAHULUAN

Milenium ketiga ditandai dengan penggunaan perangkat teknologi informasi secara masif dihampir semua aspek kehidupan, tidak terkecuali perpustakaan yang memiliki kompetensi dalam menciptakan, memproses dan mendistribusikan informasi yang dibutuhkan masyarakat. Ketika otomasi dan integrasi digital dapat diwujudkan, kemudahan dan kepraktisan, hemat waktu dalam menjalankan aktivitas semakin banyak dan beragam (Sudibyo, 2019). Produksi informasi yang terkonfirmasi dan *up-to-date* menjadi tulang punggung bagi berbagai kegiatan serta nilai informasi sebagai komoditi publik yang dipengaruhi oleh sinergi antara perangkat teknologi informasi, teknologi *web* dan sumber informasi global yang tersedia di internet.

Perpaduan antara informasi dengan perangkat teknologi *web* memungkinkan kecepatan dan keakuratan informasi menjadi tujuan utama. Kecepatan merupakan aksi dan reaksi dalam peningkatan kemajuan menuju arah perubahan yang spesifik (Perkin & Abraham, 2021). Perubahan dalam penerapan teknologi bagi perpustakaan merupakan kewajiban yang tidak dapat ditinggalkan. Perpustakaan mempunyai wewenang untuk mengolah informasi dalam berbagai media apapun. Sifat teknologi *web* yang mudah diakses dan mudah digunakan menjadi alasan utama untuk diaplikasikan sehingga memberikan layanan terbaik kepada pemustaka. Penerapan nyata penggunaan teknologi *web* dalam sistem kerumahtanggaan perpustakaan adalah sistem informasi perpustakaan, *repository* perpustakaan, layanan akses informasi dan sebagainya. Otomasi sistem perpustakaan pun tidak lepas dari pengaruh penggunaan teknologi *web* karena kemudahan dan cakupan layanan akses informasi yang lebih luas.

Namun demikian penerapan teknologi *web* di perpustakaan disamping memberikan kemudahan akses yang digunakan kapanpun dan dimanapun sejatinya memiliki kerentanan dari tindakan sabotase karena sifat teknologi *web* yang cenderung terbuka. Beberapa contoh kejadian yang sering dialami berupa sistem informasi yang mengalami kerusakan sehingga mengakibatkan sistem informasi tidak dapat diakses, *repository* perpustakaan yang *down*, masuknya virus, *hacking*, infiltrasi hak akses dan lainnya. *Hacking* adalah kegiatan memasuki suatu sistem melalui sistem operasional lain, dengan cara mengidentifikasi kelemahan dalam sistem komputer atau jaringan untuk mengeksploitasi kelemahannya, dan selanjutnya mendapatkan akses ke dalam sistem tersebut (Nugroho *et al*., 2020). Sistem informasi perpustakaan tidak bisa memproses, menyimpan dan mendistribusikan informasi kepada pemustaka. Keamanan siber menjadi celah sekaligus menjadi perhatian khusus bagi perpustakaan dalam penggunaan aplikasi berbasis teknologi *web.*

Sistem informasi yang handal merupakan komponen utama dengan memperhatikan aspek *confidentiality, availability* dan *integrity. Confidentiality* adalah perlindungan terhadap informasi dari pengaksesan yang tidak berwewenang atau pengaksesan tanpa otoritas. *Availability* adalah menyediakan sistem informasi untuk menunjang proses bisnis. *Integrity* adalah menyajikan informasi yang akurat, benar, dan lengkap (Aminzade, 2018) . Pengelolaan penggunaan sistem informasi dan teknologi informasi perpustakaan secara umum pun tidak akan lepas dari ketiga hal diatas sebagai landasan utama bagaimana sistem informasi yang handal, termasuk juga penanganan masalah berbagai sumber ancaman dan hambatan yang mengganggu keberlangsungan sistem informasi perpustakaan.

Penelitian terdahulu tentang audit keamanan sistem informasi manajemen akademik dan kemahasiswaan menggunakan SNI ISO/IEC 27001:2013 oleh Wahyudi *et al*. (2020) mengungkapkan identifikasi klausul 5 tentang kebijakan keamanan masih belum sesuai dengan kerangka kerja. Klausul 7 tentang manajemen aset juga masih belum sesuai untuk memelihara dan melindungi aset karena tidak adanya surat kebijakan pengelolaan aset. Klausul 9 tentang akses kontrol agar tidak terjadi penyalahgunaan hak akses serta adanya prosedur pengendalian hak akses yang dilanggar, sedangkan klausul 15 kepatuhan belum disesuaikan dengan peraturan akademik, serta waktu yang telah dijadwalkan pada kalender pendidikan dan aspek legal *software* yang digunakan.

Aritonang *et al*. (2018) melaksanakan penelitian tentang audit sistem keamanan sistem informasi menggunakan *Framework* COBIT 5 (APO 13) dengan tujuan mengidentifikasi dan mengukur tingkat kematangan keamanan sistem informasi yang belum pernah dievaluasi dalam lingkup organisasi. Hasil penelitian mendeskripsikan tingkat keamanan sistem informasi di perusahaan X telah mencapai level 1 *(performed process)* sebesar 50% dengan tingkat *managed process* yang memiliki status P *(partially achieved)*. Hasil tersebut menunjukkan bahwa pengelolaan keamanan sistem informasi belum tercapai dengan baik dikarenakan target yang ingin dicapai 80% sampai 90%. Rekomendasi pada penelitian ini memerlukan evaluasi peningkatan keamanan sistem informasi.

Penelitian tentang audit keamanan sistem informasi akademik menggunakan *Framework NIST SP* 800-26 dilatarbelakangi oleh persaingan antar lembaga pendidikan yang mengutamakan kecepatan layanan dengan pengolahan data, tetapi aspek keamanan komputer cenderung diabaikan (Perdana, 2018). Penelitian ini menghasilkan audit keamanan sistem informasi akademik dikelola dengan baik dengan level 3 yang berarti keamanan data menjadi prosedur yang dijalankan oleh organisasi. Sedangkan penelitian Pertama & Ardiyasa (2019) tentang audit keamanan sistem informasi perpustakaan menggunakan kerangka kerja COBIT membahas sistem informasi perpustakaan yang sering mengalami gangguan keamanan yakni *website* sistem informasi perpustakaan tidak bisa diakses beberapa saat. Penelitian ini merekomendasikan kerangka kerja COBIT yang meliputi domain keamanan (APO 13) dan pelayanan keamanan (DSS05) sudah dilakukan dengan baik. Level tata kelola teknologi informasi dalam audit keamanan adalah 1,84 berada pada level 2 yang berarti bahwa proses sudah dijalankan. (Mahendra & Soewito, 2023) mengkaji penerapan kerangka kerja *NIST Cybersecurity* dan *CIS Control* sebagai manajemen risiko keamanan siber yang menghasilkan penilaian risiko keamanan siber dengan tingkat kematangan risiko tinggi dengan skor 2.77. *NIST Cybersecurity* dapat mengukur tingkat keamanan risiko infrastruktur aplikasi sehingga mengurangi risiko serangan siber.

Tujuan dari penelitian ini untuk mendeskripsikan analisis keamanan siber sistem informasi di UPT Perpustakaan Universitas Jenderal Soedirman (Unsoed) dengan menggunakan kerangka kerja NIST *Cybersecurity Framework* untuk fungsi mengidentifikasi, melindungi, mendeteksi, merespons dan memulihkan. Kelima penelitian terdahulu belum membahas keamanan siber dalam mendeskripsikan proses analisis keamanan dari proses identifikasi, perlindungan, deteksi, merespons dan memulihkan sebagai serangkaian prosedur keamanan siber sesuai dengan tujuan penelitian yang dilaksanakan. Khusus untuk sistem informasi perpustakaan di UPT Perpustakaan Unsoed sebagai sistem informasi terintegrasi memerlukan kegiatan analisis keamanan siber dalam mengantisipasi potensi ancaman yang mengganggu alur informasi perpustakaan. Penelitian ini penting karena UPT Perpustakaan sejak menerapkan sistem informasi perpustakaan terpadu Izylib pada tahun 2013 sampai sekarang, belum pernah dilaksanakan evaluasi implementasi sehingga penelitian ini perlu dilaksanakan untuk mengetahui bagaimana UPT Perpustakaan Unsoed mengantisipasi ancaman siber beserta aset informasi yang dilayankan kepada pemustaka.

2. TINJAUAN PUSTAKA

2.1 Pengertian Keamanan

Definisi keamanan dalam konteks sistem informasi dan penggunaan teknologi informasi secara umum merupakan kegiatan perlindungan terhadap kerahasiaan *(confidentiality),* ketersediaan *(availability)* dan integritas keakuratan *(integrity)* informasi. Aset informasi yang terdapat didalam sistem informasi terjaga kerahasiaannya dari berbagai macam pengaksesan yang tidak berwenang. Ketersediaan informasi yang akurat dalam proses pengambilan keputusan dan keakuratan informasi dalam memberikan data akurat tanpa adanya perubahan dan gangguan merupakan bentuk lain dari keamanan sistem informasi. Keamanan adalah perlindungan. Perlindungan dari musuh yang

dengan sengaja merusak sebagai tujuan akhir dari suatu tindakan (Whitman & Mattord, 2021). Bagi organisasi yang rentan terhadap berbagai sumber ancaman, perlindungan yang bersifat menyeluruh dari berbagai unsur organisasi wajib dilaksanakan sebagai prosedur baku sebagai serangkaian proses yang tidak boleh diabaikan. Perlindungan keamanan harus dilaksanakan secara berjenjang dari elemen tempat, insfrastruktur fisik, orang, fungsi, komunikasi dan informasi. Sukses tidaknya organisasi dapat dilihat dari proses perlindungan semua elemen tersebut dilaksanakan sebagai standar baku yang harus dilaksanakan.

Kim & Solomon (2016) mendefinisikan keamanan dalam konteks keamanan sistem informasi sebagai kumpulan aktivitas yang melindungi sistem informasi dan penyimpanan data didalamnya. Sistem informasi terdiri atas perangkat keras, sistem operasi, aplikasi perangkat lunak yang bekerja secara bersama-sama untuk mengoleksi, memproses, dan menyimpan data yang diperlukan oleh individu ataupun oleh organisasi. Sebagai satu kesatuan organisasi maka sistem informasi bekerja untuk menciptakan aliran informasi yang berguna bagi proses kegiatan yang tidak boleh berhenti ataupun terganggu. Oleh karena itu perlindungan sistem informasi dari berbagai macam gangguan perlu dilaksanakan agar alur informasi bekerja dengan baik. Keamanan menitikberatkan pada tindakan pencegahan, pendeteksian dan perlindungan aset informasi dari tindakan yang tidak memiliki hak untuk mendapat akses informasi yang tidak memiliki hak akses baik dalam sistem komputer dan sistem jaringan. Keamanan sistem informasi bertujuan untuk menjaga sistem informasi dan aset informasi agar tidak disusupi oleh yang tidak berhak yang pada akhirnya akan menimbulkan kerusakan sistem informasi secara keseluruhan. Keamanan data mengacu pada langkah-langkah perlindungan privasi digital yang diterapkan untuk mencegah akses tidak sah ke komputer, *database*, dan situs *web* (Silalahi, 2022). Keamanan data adalah prioritas utama bagi organisasi dalam memberikan perlindungan aset data untuk mencegah masuknya akses yang dapat merusak dan akses yang tidak bertanggung jawab.

2.2 Kerangka Kerja NIST *Cybersecurity Framework*

NIST *Cybersecurity Framework* merupakan kerangka kerja khusus untuk keamanan siber yang terdiri atas kegiatan prosedur yang dimulai dari fungsi *identify, protect, detect, respond, recover.*

Gambar 1. NIST *Cybersecurity Framework*
Sumber: NIST Cybersecurity Framework (2018)

National Institute of Standart and Technology (NIST) di tahun 2018 menerbitkan rekomendasi versi 1.1 khusus tentang kerangka kerja keamanan siber yang dilatarbelakangi oleh kebutuhan industri di Amerika Serikat, lembaga federal dan masyarakat luas yang memerlukan pedoman dan standar keamanan. Kerangka kerja versi 1.1 merupakan penyempurnaan kerangka kerja versi 1.0 yang dipublikasikan pada tahun 2014. Kerangka kerja NIST sudah mencakup standar, metodologi, prosedur dan pendekatan kebijakan untuk menjaga keamanan siber dalam bisnis dan teknologi untuk mencegah ancaman (Gordon *et al*., 2020). Kerangka kerja *NIST Cybersecurity* digunakan oleh organisasi untuk mengevaluasi sistem dan infrastruktur teknologi informasi yang digunakan untuk menjaga keamanan teknologi dan sistem informasi organisasi dari ancaman siber(Kabanda, 2018; Kwon *et al*., 2020). Kerangka kerja NIST cukup fleksibel untuk dapat digunakan secara sukarela oleh perusahaan besar dan kecil di semua sektor industri serta oleh pemerintah negara bagian dan pemerintah federal (Calder, 2018). NIST *cybersecurity framework* dapat digunakan sebagai alat untuk menganalisis keamanan siber sistem informasi baik yang bersifat teknikal dan manajerial.

Penilaian teknikal merupakan proses penilaian teknis dari mulai proses identifikasi, perlindungan dan deteksi sumber ancaman sistem informasi. Penilaian teknis lebih menitikberatkan pada kemampuan ketaatan pada prosedur kerja yang telah ditetapkan sebagai serangkaian prosedur yang harus dilaksanakan secara berjenjang dan terstruktur dengan berpedoman pada dokumentasi yang telah disepakati. Sedangkan penilaian manajerial merupakan proses bagaimana lingkungan organisasi memandang keamanan sistem informasi memiliki pengaruh terhadap keberlangsungan layanan informasi dan sebagai sarana proses pengambilan keputusan dari organisasi tersebut. Pada proses ini perencanaan, tanggung jawab, analisis komunikasi, mitigasi, pemberdayaan, perencanaan perbaikan dalam lingkup manajemen organisasi apakah dapat dilaksanakan ataupun tidak dilaksanakan menjadi tanggung jawab *top* manajemen untuk melaksanakan kegiatan penilaian analisis keamanan sistem informasi (Pratomo *et al*., 2018).

Kerangka kerja keamanan siber merupakan panduan terstruktur dari tahapan awal hingga akhir yang harus dilaksanakan secara berjenjang sesuai dengan siklus hidup pengembangan sistem informasi. Detail tahapan proses kerangka kerja keamanan siber berdasarkan kerangka kerja keamanan siber NIST *cybersecurity framework* dimulai dari tahapan fungsi, kategori dan sub kategori.

Tabel 1. Fungsi dan Kategori *NIST Cybersecurity Framework*

Fungsi	**Kategori**
Identifikasi (ID)	Manajemen Aset
	Lingkungan Bisnis
	Tata Kelola
	Penilaian Risiko
	Strategi Manajemen Risiko
	Manajemen Risiko Rantai Pasokan
Perlindungan (PR)	Manajemen Identitas, Otentikasi dan Akses
	Pengetahuan dan Pelatihan
	Keamanan Data
	Proses dan Prosedur Perlindungan Informasi
	Pemeliharaan
	Teknologi Perlindungan
Deteksi (DE)	Anomali dan Peristiwa
	Pemantauan Keamanan Berkelanjutan
	Proses Deteksi
Tanggapan (RS)	Perencanaan Tanggapan Respons
	Komunikasi
	Analisis

Fungsi	Kategori
	Peringanan/Mitigasi
	Penyempurnaan
Pemulihan (RC)	Perencanaan Pemulihan
	Penyempurnaan Pemulihan
	Komunikasi Pemulihan

Sumber: *NIST Cybersecurity Framework*, 2018

3. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus. Penelitian ini dilakukan dengan teliti, mendalam dan menyeluruh dengan cara melakukan wawancara mendalam dan pengamatan langsung (observasi) serta mendeskripsikan hal-hal yang berkaitan dengan objek penelitian. Kajian utama yang akan diteliti yakni mendeskripsikan pelaksanaan analisis siber sistem informasi perpustakaan dengan menggunakan kerangka kerja *NIST Cybersecurity Framework*. Apabila dilihat dari tujuan penelitian, jenis penelitian ini adalah studi kasus. Secara umum studi kasus merupakan strategi yang lebih cocok bila pokok pertanyaan suatu penelitian berkenaan dengan *how* dan *why* (Yin, 2018). Penelitian dilaksanakan pada bulan Maret sampai dengan April 2023. Penentuan sumber data pada orang yang diwawancarai dilakukan secara *purposive*, yakni dipilih dengan pertimbangan dan tujuan tertentu. Informan dalam penelitian ini adalah pustakawan yang memiliki pengalaman dan berinteraksi dengan sistem informasi perpustakaan. Informan terdiri atas Kepala UPT Perpustakaan Unsoed, Koordinator Teknologi Informasi dan Sistem Informasi, Operator Layanan Sirkulasi, Sub Koordinator Sistem Informasi, dan Operator Sistem Informasi Perpustakaan. Analisis data dalam penelitian ini bersifat deskriptif analitis. Semua data baik berupa jawaban dari informan atas pertanyaan yang diajukan melalui wawancara, ataupun yang diperoleh dari observasi dihimpun menjadi satu. Setelah terkumpul lengkap, data diolah dan dianalisis secara kualitatif yakni memperhatikan fakta yang betul-betul terjadi dilapangan berdasarkan variabel yang sudah ditentukan sesuai dengan kerangka kerja *NIST*, kemudian dideskripsikan dalam tahap-tahap analisis dari kategori dan subkategori kerangka kerja yang diacu. Selanjutnya, diambil kesimpulan dengan menggunakan metode deduktif yakni berdasarkan teori yang bersifat umum untuk menjelaskan hubungan data dengan data lainnya. Teknik pemeriksaan data pada penelitian ini menggunakan metode triangulasi dengan menggabungkan teknik pengumpulan data dan sumber data yang telah ada.

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil penelitian yang telah dilaksanakan dalam menganalisis keamanan siber sistem informasi perpustakaan dengan menggunakan kerangka kerja NIST *cybersecurity framework*, maka dihasilkan sebagai berikut:

4.1 Mengidentifikasi

Fungsi mengidentifikasi dideskripsikan kategori dan subkategori keamanan siber sistem informasi perpustakaan.

4.1.1 Manajemen Aset

Kategori manajemen aset mengidentifikasi subkategori perangkat fisik dan perangkat sistem informasi perpustakaan, perangkat lunak, komunikasi organisasi, inventarisasi sistem informasi, sumberdaya fisik dan SDM, serta peran dan tanggungjawab dalam implementasi keamanan siber. Perangkat fisik dan perangkat lunak untuk implementasi sistem informasi perpustakaan dicatat sesuai dengan kebutuhan perpustakaan berdasarkan kategori sumberdaya manusia atau operator dalam menjalankan sistem informasi perpustakaan. Perangkat fisik berupa perangkat keras komputer untuk *client, server* dan jaringan. Perangkat lunak yakni *windows 8* dan *windows 10,* sistem aplikasi menggunakan *apache server, mysql, php* dan *virtual server*. Sistem informasi perpustakaan terpadu

IzyLib sebagai sistem informasi perpustakaan terpadu di lingkungan Unsoed. Identifikasi ancaman paling besar tingkat kerentanan pada sistem informasi perpustakaan terpadu IzyLib yang disebabkan oleh tidak dilaksanakannya proses *update* sistem sejak pertama kali sistem informasi perpustakaan diimplementasikan. Pelimpahan wewenang kegiatan yang berkaitan dengan teknologi informasi dan sistem informasi yang berlaku di seluruh lingkungan Unsoed merupakan tanggung jawab Lembaga Pengembangan Teknologi dan Sistem Informasi (LPTSI), termasuk juga keamanan siber yang merupakan tugas dan wewenang dari lembaga tersebut.

4.1.2 Lingkungan bisnis

Kategori lingkungan bisnis lebih menekankan pada aspek komunikasi dan peran dari lembaga dalam implementasi keamanan siber apakah terdapat pembagian peran, fungsi dan tanggung jawab dari lembaga dalam kegiatan tersebut. Komunikasi yang bersifat internal dan eksternal dilaksanakan tidak saja menyangkut tentang adanya gangguan teknis yang dapat menganggu sistem informasi perpustakaan, tetapi komunikasi tersebut dilaksanakan dengan prosedural terhadap aset-aset kritis yang dimiliki oleh UPT Perpustakaan Unsoed. Validitas dari data dan pengolahan informasi menjadi bentuk pertanggungjawaban dalam memberikan layanan prima sesuai dengan visi misi. Dengan demikian dalam menjaga prioritas misi yang dijalankan dan bagaimana peran dari lembaga induk dalam proses implementasi keamanan siber sistem informasi perpustakaan, maka dengan segera dapat ditangani dan berusaha diantisipasi dengan prosedur organisasi sesuai dengan peran dan tanggung jawab dari organisasi dan adanya proses koordinasi komunikasi dengan lembaga di lingkungan Unsoed.

4.1.3 Tata Kelola

Kategori tata kelola keamanan siber memproses subkategori prosedur kerangka kerja keamanan siber tentang kebijakan UPT Perpustakaan Unsoed dalam implementasi sistem keamanan siber, peran dan tanggung jawab dalam mengamankan aset informasi lembaga, landasan hukum dan regulasi yang mengatur implementasi keamanan siber dan proses penerapan manajemen risiko keamanan siber. Kebijakan UPT Perpustakaan Unsoed dalam tata kelola keamanan siber sistem informasi perpustakaan berdasarkan hasil analisis memang tidak ditetapkan secara prosedural dengan kerangka kerja yang baku, tetapi hanya bersifat insidental pada kejadian yang mengancam sistem informasi perpustakaan. Landasan hukum tidak spesifik dibuatkan dan dicatat sebagai pedoman dalam melaksanakan kegiatan yang berkaitan dengan keamanan siber sistem informasi perpustakaan, hanya secara umum masuk dalam rencana induk pengembangan sistem informasi di semua lingkungan universitas.

Proses penerapan manajemen risiko tidak melaksanakan kegiatan penilaian risiko, mitigasi risiko dan evaluasi risiko sesuai dengan prosedur ataupun kerangka kerja manajemen risiko terstandarisasi. UPT Perpustakaan Unsoed melaksanakan kegiatan pengalihan *server* ke LPTSI sebagai langkah antisipasi keamanan. Secara tidak langsung, pengalihan *server* sistem informasi perpustakaan ke LPTSI merupakan tindakan mitigasi dalam proses manajemen risiko dalam upaya untuk meminimalisasi tingkat kerusakan dan tindakan pencegahan berupa kegiatan perawatan yang diserahkan kepada pihak yang memiliki kemampuan dalam bidang teknologi informasi.

4.1.4 Penilaian Risiko

Kategori penilaian risiko pada implementasi keamanan siber sistem informasi perpustakaan merupakan tindakan mengidentifikasi subkategori kerentanan sistem informasi perpustakaan, identifikasi sumber ancaman dari pihak internal dan eksternal, mengidentifikasi dampak ancaman yang ditimbulkan, menganalisis dan mengkalkulasi sumber ancaman dan dampak yang ditimbulkan, melaksanakan tindakan respons dan prioritas risiko yang teridentifikasi serta kemampuan sumber daya manusia dalam menilai berbagai macam sumber ancaman risiko dan dampak yang yang ditimbulkan dari ancaman risiko yang mengancam keamanan siber sistem informasi perpustakaan.

Identifikasi hanya dilaksanakan pada saat ada kejadian, sehingga UPT Perpustakaan tidak memiliki dokumentasi secara prosedural dalam melaksanakan penilaian kerentanan keamanan siber sistem informasi perpustakaan. *Infiltrasi hacker* dari luar negeri menjadi sumber ancaman yang dapat diantisipasi. Proses analisis dampak risiko berdasarkan kerangka kerja penilaian risiko dirasakan oleh operator dan pengguna sistem informasi tersebut, tetapi kembali lagi kepada faktor kemampuan SDM UPT Perpustakaan yang belum memiliki kualifikasi kemampuan teknologi informasi, maka dampak tersebut dirasakan hanya sebagai hal yang biasa sepanjang tidak menghentikan proses layanan informasi perpustakaan.

4.1.5 Strategi Manajemen Risiko

Kategori strategi manajemen risiko keamanan siber sistem informasi perpustakaan di UPT Perpustakaan Unsoed dilaksanakan tetapi tanpa menggunakan kerangka kerja dan prosedur baku serta tidak didokumentasikan secara tertulis. Mitigasi risiko hanya bersifat koordinasi lembaga sebagai tanggung jawab lembaga induk dalam semua komponen sistem informasi di seluruh Universitas. Mitigasi risiko tidak dilaksanakan secara prosedural dengan kerangka kerja terstandar yang berlaku selama ini. Kegiatan strategi manajemen risiko keamanan siber sistem informasi perpustakaan dilaksanakan dengan pola komunikasi semua sumber daya manusia yang terlibat yakni, operator, koordinator sistem informasi dan teknologi informasi dan Kepala UPT Perpustakaan yang berinteraksi dengan sistem informasi perpustakaan. Hasil toleransi dan analisis dampak risiko berusaha diminimalisir dan kegiatan penilaian, mitigasi serta evaluasi manajemen risiko berusaha dikomunikasikan kepada pihak internal dan eksternal.

4.1.6 Manajemen Risiko Rantai Pasokan

Kategori manajemen risiko rantai pasokan mendeskripsikan proses subkategori bagaimana manajemen risiko keamanan siber ditetapkan, dikelola dan disetujui oleh pemangku kepentingan. Bagaimana keterlibatan pihak ketiga dalam proses kegiatan tersebut, bagaimana sistem kontrak dan cara bekerjanya, apakah pihak eksternal diaudit secara periodik dan bagaimana hasil respons serta rencana pemulihan keamanan dari pihak ketiga dalam implementasi keamanan siber sistem informasi perpustakaan. Berdasarkan hasil analisis terdeskripsikan semua kegiatan tersebut dilaksanakan oleh pihak ketiga yakni LPTSI yang bertanggung jawab dalam mengelola sistem informasi di seluruh universitas. UPT Perpustakaan hanya sebagai unit layanan informasi yang menjalankan sistem informasi perpustakaan sesuai dengan hak akses yang diberikan oleh LPTSI Unsoed.

Penelitian terdahulu oleh Mahendra & Soewito (2023) menyebutkan tentang tingkat kematangan manajemen risiko keamanan siber dapat digunakan untuk menilai risiko sistem informasi di UPT Perpustakaan Unsoed, meskipun dengan metode yang berbeda. Tingkat kematangan risiko yang dianalisis menggambarkan skor 2.77 dengan nilai maksimal 3.00. Nilai risiko keamanan siber di UPT Perpustakaan Unsoed tidak dapat dideskripsikan karena tidak ada catatan dan proses penilaian yang dilaksanakan, administrator hanya melaksanakan kegiatan penanganan apabila ada kejadian yang menganggu sistem informasi perpustakaan. Penilaian risiko tidak berdasarkan tingkat kematangan yang ditunjukan dengan menggunakan angka, tetapi hanya dilakukan tindakan penanganan atas adanya kejadian pada saat layanan terganggu. Proses fungsi identifikasi pada kerangka kerja keamanan siber hanya mengantisipasi dampak risiko dengan proses *update software* untuk menutupi celah keamanan siber serta berkoordinasi dengan LPTSI untuk meminimalisasi dampak yang lebih besar tanpa adanya kegiatan penilaian risiko sebagai proses awal analisis keamanan siber secara keseluruhan.

4.2 Melindungi

4.2.1 Manajemen Identitas, Otentikasi dan Kendali Akses

Proses identifikasi *software* berdasarkan tingkat kerentanan karena sistem informasi perpustakaan yang menggunakan desain *web server* dan penempatan *server* di LPTSI sebagai penanggung jawab seluruh sistem informasi yang digunakan di tingkat Universitas. *Update software* dilaksanakan untuk mengantisipasi ancaman terhadap celah (*bug*) yang teridentifiksi, *update form-form* sistem informasi yang tidak digunakan, dan identifikasi potensi ancaman dari sistem informasi yang digunakan. Akses jarak jauh berhubungan dengan akses *database* dalam *web server* yang dikelola oleh LPTSI dikelola dengan baik dan sesuai dengan peran dan tanggung jawab antara UPT Perpustakaan dan LPTSI. UPT Perpustakaan dapat *meremote* aplikasi sistem informasi perpustakaan dengan menggunakan *password* yang terverifikasi oleh pihak LPTSI, dan LPTSI menyediakan sub domain untuk situs sistem informasi perpustakaan. Hak akses bagi operator disesuaikan dengan pembagian pekerjaan untuk kegiatan pengolahan, pelayanan dan administrator sistem informasi perpustakaan. Otorisasi hak akses dapat digunakan untuk antisipasi kerentanan keamanan siber sistem informasi perpustakaan. Kegiatan antisipasi tersebut oleh UPT Perpustakaan dilakukan kegiatan *reset user* dan *password* secara berkala, dan diusahakan menggunakan satu user untuk satu operator.

4.2.2 Pengetahuan dan Pelatihan

Pada kategori pengetahuan dan pelatihan dideskripsikan subkategori sumber daya manusia dalam hal ini adalah operator sistem informasi perpustakaan diberi pengetahuan dan pelatihan tentang keamanan siber sistem informasi perpustakaan, dan mengetahui perlunya tindakan antisipasi melalui kegiatan pelatihan untuk menjaga aset informasi perpustakaan. Pelatihan dan pengetahuan operator akan kerentanan keamanan siber belum dilaksanakan, tetapi apabila ada berbagai macam ancaman yang berkaitan dengan kelancaran sistem informasi perpustakaan, administrator akan secara khusus melaksanakan kegiatan antisipasi, pencegahan dan kegiatan penanganan secara langsung sesuai dengan kemampuan dan keterampilan dan berkoordinasi dengan LPTSI.

4.2.3 Keamanan Data

Keamanan data terkait dengan subkategori kebijakan UPT Perpustakaan Unsoed memproses dan melindungi data-data sensitif, serta prosedur pengelolaan aset informasi dalam mengantisipasi berbagai acaman yang menghambat proses layanan informasi perpustakaan. Aset informasi berupa data sensitif di UPT Perpustakaan dilindungi secara sistem yang dimitigasi dengan cara memindahkan sistem informasi perpustakaan ke LPTSI sebagai penanggung jawab sistem informasi di tingkat universitas.

Perlindungan data sebagai aset informasi di UPT Perpustakaan dilaksanakan baik dalam prosedur sebagai pengolah informasi dan proses perlindungan secara sistem yang telah diaplikasikan. UPT Perpustakaan melaksanakan kegiatan pengelolaan aset informasi sebagai bagian dari usaha melindungi data-data sensitif dengan kegiatan penghapusan, transfer, disposisi yang dilaksanakan secara prosedur dalam jangka waktu 5-10 tahun. UPT Perpustakaan secara prosedural tetap menjalin komunikasi dan koordinasi dengan LPTSI dalam melindungi, meng-*upgrade* dan melaksanakan kegiatan evaluasi serta uji coba sistem sebagai bagian dari proses perlindungan data secara menyeluruh di sistem informasi perpustakaan. Pusat data dalam hal ini *server* sistem informasi perpustakaan yang dikelola oleh LPTSI sudah sesuai dengan kapasitas dan kebutuhan sistem informasi perpustakaan.

4.2.4 Proses dan Prosedur Perlindungan Informasi

Konfigurasi dasar teknologi informasi dalam implementasi keamanan siber sistem informasi perpustakaan menggunakan konfigurasi standar teknologi informasi pada umumnya. Sistem informasi perpustakaan berbasis *web server* yang dapat diakses oleh banyak *client* dengan menggunakan jaringan (*network*) baik yang bersifat internet dan *intranet*. Jaringan menggunakan TCP/IP untuk

dapat mengakses database melalui teknologi *web server* dan bahasa pemrograman PHP. Sistem informasi perpustakaan dapat juga disebutkan sebagai siklus hidup pengembangan sistem karena sistem informasi perpustakaan selalu dikembangkan sesuai kebutuhan layanan agar maksimal dan sistem secara berkala dilaksanakan kegiatan *updating software* untuk mengantisipasi celah-celah keamanan yang memungkinkan akan mengancam sistem informasi perpustakaan. Apabila terjadi insiden UPT Perpustakaan melaksanakan kegiatan rencana pemulihan sistem sesuai dengan siklus hidup pengembangan sistem dengan melaksanakan kegiatan uji coba setelah adanya insiden yang mengganggu layanan sistem informasi perpustakaan, meskipun dilaksanakan sesuai dengan proses *try and error* karena keterbatasan pengetahuan sumber daya manusia di UPT Perpustakaan yang memiliki keterampilan dan keahlian khusus pada bidang teknologi informasi.

4.2.5 Pemeliharaan

Pemeliharaan sistem informasi dilaksanakan sesuai dengan anggaran UPT Perpustakaan selama satu tahun. Pemeliharaan juga mencakup akses jarak jauh *(remote access)* yang diberikan oleh LPTSI untuk *mengupdate* sistem dan membuka hak akses jaringan yang disediakan oleh LPTSI. Secara umum kegiatan pemeliharaan sistem informasi perpustakaan di UPT Perpustakaan Unsoed dilaksanakan secara periodik dan prosedural termasuk juga untuk keamanan siber sistem informasi meskipun tidak dilaksanakan secara khusus dalam bidang keamanan siber, hanya bersifat secara umum yakni pemeliharaan sistem informasi perpustakaan.

4.2.6 Teknologi Perlindungan

Kategori teknologi perlindungan pada fungsi melindungi, mengidentifikasi subkategori bagaimana catatan *log* keamanan diimplementasikan, apakah tersedia media lain yang lebih aman dan terlindungi, apakah kebijakan keamanan berdasarkan prinsip fungsional dan kemampuan dasar SDM, bagaimana proses komunikasi dalam jaringan yang aman dan terlindungi, serta bagaimana mekanisme insidental keamanan siber ditetapkan. Catatan *log* keamanan menjadi tanggung jawab khusus dari Koordinator Sistem Informasi dan Teknologi Informasi. Catatan keamanan dibutuhkan untuk kepentingan identifikasi hak akses kepada masing-masing operator dan pengawasan dari administrator sistem, maka *log* keamanan di sistem informasi perpustakaan UPT Perpustakaan Unsoed dapat dikontrol dan dicatat sesuai dengan kebutuhan. UPT Perpustakaan mengambil kebijakan apabila sistem informasi perpustakaan mengalami kendala atau insiden dan penanganan respons yang memerlukan waktu, maka media lain yang digunakan dan bersifat aman serta terlindungi adalah menggunakan media intranet berupa jaringan internal kampus. Jaringan hanya dapat diakses di lingkungan kampus tidak bersifat publik.

Pada penelitian terdahulu tentang kepatuhan dan kendali akses untuk keamanan siber yang dikemukakan oleh Wahyudi *et al*. (2020) dapat menjadi referensi bagaimana kepatuhan terhadap akses terhadap keamanan siber dapat diterapkan. Kendali akses harus digunakan sesuai prosedur untuk mencegah ancaman keamanan siber. Klausul tentang perlindungan aset dan akses kontrol agar tidak terjadi penyalahgunaan hak akses sesuai prosedur dapat dijadikan model yang dapat digunakan meskipun dengan kajian analisis sistem informasi akademik. Pada penelitian tersebut terdapat surat kebijakan pengelolaan aset yang dapat diterapkan bagi perpustakaan dalam mencegah dan melindungi aset informasi dengan peraturan legal antar lembaga terkait. Penelitian tersebut dapat dijadikan rekomendasi proses fungsi melindungi pada kerangka kerja keamanan siber sistem informasi perpustakaan. Proses ini sejalan dengan adanya relasi hubungan sistem antara UPT Perpustakaan Unsoed dengan Lembaga PTSI.

4.3 Mendeteksi

4.3.1 Anomali dan Peristiwa

Perpustakaan melaksanakan kegiatan analisis tentang metode dan cara serangan yang kemudian dilaporkan kepada Kepala UPT Perpustakaan. Deteksi ancaman dari peristiwa atau kejadian yang telah teridentifikasi menjadi data awal tentang kejadian keamanan yang dikumpulkan dan dianalisis untuk ditindaklanjuti, dilaporkan dan dievaluasi untuk pembenahan sistem keamanan yang lebih baik. Analisis dampak peristiwa kejadian serangan juga ditentukan untuk menilai kuantitas serangan peristiwa apakah berdampak besar, sedang dan kecil. Hasil analisis dampak serangan dari peristiwa tersebut juga dikomunikasikan kepada LPTSI selaku penanggung jawab semua sistem informasi yang berlaku di Unsoed. Ambang batas serangan diusahakan diminimalkan dampaknya bahkan harus dihilangkan untuk memberikan layanan maksimal kepada pengguna perpustakaan. Secara kuantitatif tentang ambang batas serangan siber, UPT Perpustakaan tidak menentukan nilai ambang batas sesuai dengan prosedur kerangka kerja. Faktor keterbatasan kemampuan administrator dalam menilai insiden menjadi kendala yang teridentifikasi dalam proses penilaian ambang batas serangan. Administrator sistem hanya berusaha melaksanakan tindakan secepat mungkin dan meminimalkan dampak insiden bahkan berusaha menghilangkan insiden tersebut sesuai dengan kebutuhan UPT Perpustakaan.

4.3.2 Pemantauan Keamanan Berkelanjutan

Proses pemantauan dimulai dari sistem jaringan yang dipantau sistem keamanannya dan bagaimana proses koordinasi dengan lembaga terkait dalam kegiatan sistem informasi perpustakaan. UPT Perpustakaan secara periodik melaksanakan kegiatan pemantauan jaringan dengan berkoordinasi dengan LPTSI baik yang bersifat teknis jaringan dan *update software* sistem informasi perpustakaan. Pemantauan berupa *update software* tentang kerentanan aplikasi yang dapat memungkinkan lubang dapat diinfiltrasi oleh pihak yang tidak bertanggung jawab dan penilaian *traffic* penggunaan jaringan internet pada saat insiden terjadi. Sumberdaya di UPT Perpustakaan secara sistem terbagi menjadi operator dan administrator. Operator sepenuhnya menyerahkan kegiatan pemantauan keamanan siber kepada administrator dalam hal ini koordinator sistem informasi dan teknologi informasi yang dipandang memiliki pengetahuan terkait dengan teknologi informasi dan keamanan sistem informasi perpustakaan. Jika ada kode bahaya yang terdeteksi baik yang bersumber dari pihak internal dan eksternal, maka kegiatan koordinasi antara operator dan administrator yang pertama dilaksanakan dengan menilai dan memproses seberapa besar tingkat kerentanan ancaman tersebut dapat mengganggu sistem informasi perpustakaan. Komunikasi dan koordinasi dengan pihak LPTSI juga dilaksanakan dalam memantau keamanan siber secara berkelanjutan yang dilaksanakan baik secara formal dan informal, secara formal dengan melaksanakan kegiatan koordinasi surat menyurat antara UPT Perpustakaan dan LPTSI, secara informal dengan cara melaksanakan kegiatan komunikasi antara administrator UPT Perpustakaan dengan LPTSI.

4.3.3 Proses Deteksi

Hasil deteksi ancaman yang berhasil diidentifikasi oleh administrator, diinformasikan dan dikomunikasikan ke setiap operator tentang adanya gangguan yang menyebabkan *error*. Komunikasi dengan menggunakan grup Whatshapp tentang adanya masalah pada sistem dan sedang dilaksanakan tindakan perbaikan menjadi prosedur tidak baku yang dilaksanakan di UPT Perpustakaan Unsoed. Proses deteksi pada keamanan siber memerlukan tindakan antisipasi yang berkaitan dengan sistem dan deteksi dini ancaman yang selalu diuji dan dikembangkan. Meskipun secara prosedural dengan mengacu pada kerangka kerja keamanan siber yang bersifat standar belum dilaksanakan oleh UPT Perpustakaan Unsoed, tetapi administrator perpustakaan berusaha melaksanakan tindakan deteksi dan antisipasi terhadap keamanan siber dengan melaksanakan kegiatan semaksimal mungkin untuk antisipasi agar layanan informasi perpustakaan tidak berhenti.

Berdasarkan penelitian sebelumnya yang dilaksanakan oleh Aritonang *et al*. (2018) tentang audit sistem keamanan sistem informasi menggunakan *Framework* COBIT 5 (APO 13) dengan tujuan mengidentifikasi dan mengukur tingkat kematangan keamanan sistem informasi yang belum pernah dievaluasi, menunjukkan bahwa pengelolaan keamanan sistem informasi yang ada secara garis besar belum tercapai dengan baik karena target yang ingin dicapai yakni 80% hingga 90%. Penelitian ini sejalan dengan proses identifikasi fungsi mendeteksi keamanan siber meskipun dengan analisis kerangka kerja yang berbeda. Proses deteksi ancaman keamanan siber dideskripsikan dengan menganalisis nilai kematangan potensi ancaman berdasarkan nilai kuantitatif dari setiap potensi ancaman yang terdeteksi, berbeda dengan hasil analisis dengan fungsi deteksi yang dihasilkan karena memang UPT Perpustakaan tidak memiliki catatan statistik tentang potensi deteksi ancaman keamanan siber. Deteksi hanya dilakukan apabila ada peristiwa yang mengganggu sistem informasi perpustakaan dan itupun harus segera mungkin ditangani jangan sampai menghambat kelancaran sistem informasi perpustakaan. Apabila ada potensi ancaman yang berhasil dideteksi, maka secepat mungkin diantisipasi bahkan dihilangkan.

4.4 Merespons

4.4.1 Perencanaan Respons

UPT Perpustaan Unsoed pada proses perencanaan respons keamanan siber sistem informasi perpustakaan melaksanakan tindakan respons atas adanya insiden setelah adanya kejadian yang berhasil teridentifikasi, bukan pada saat kejadian berlangsung. Perencanaan respons pada keamanan siber sistem informasi perpustakaan dilaksanakan setelah adanya insiden teridentifikasi. Proses identifikasi ancaman berdasarkan laporan dari pihak internal dan eksternal perpustakaan. Proses selanjutnya adalah tindakan respons yang dilaksanakan oleh administrator untuk me-*restore* sistem agar berjalan dengan baik serta melaksanakan kegiatan pelaporan kepada Kepala UPT Perpustakaan tentang proses perencanaan dan tindakan respons dalam menghadapi ancaman insiden keamanan siber sistem informasi perpustakaan.

4.4.2 Komunikasi

Kategori komunikasi merupakan serangkaian prosedur bagaimana subkategori sumberdaya manusia mengetahui peran dan tanggungjawabnya dalam merespons insiden keamanan siber, bagaimana pelaporan kriteria insiden ditetapkan, bagaimana sistem koordinasi dengan pemangku kepentingan dan bagaimana proses komunikasi dengan pihak eksternal tentang adanya respons terhadap insiden yang mengancam keamanan siber sistem informasi perpustakaan. Proses komunikasi respons yang telah ditetapkan terhadap suatu insiden juga dilaporkan dalam bentuk informasi dan tindakan koordinasi yang dilaksanakan secara berjenjang baik yang bersifat internal maupun yang bersifat eksternal dengan pihak LPTSI. Koordinasi eksternal antara LPTSI dilaksanakan melalui komunikasi antara administrator sistem informasi perpustakaan dan juga melibatkan Kepala UPT Perpustakaan karena menyangkut koordinasi semua sistem informasi yang berlaku di lingkungan Unsoed.

4.4.3 Analisis

Proses analisis ancaman setelah adanya kejadian dan hanya mengandalkan kemampuan dari administrator. Berkaitan dengan dampak ancaman dari insiden yang dianalisis, UPT Perpustakaan juga telah memahami dampak dari ancaman yang dianalisis. Konsekuensi dari dampak insiden yang dapat diterima oleh UPT Perpustakaan adalah dengan beralihnya layanan informasi *online* ke *offline*. Analisis forensik dilaksanakan dengan melihat sumber infiltrasi dari internal atau eksternal organisasi, analisis jaringan yang digunakan, besar kecilnya *traffic* yang digunakan dan media atau metode serangan yang digunakan. Penanggung jawab sistem informasi perpustakaan yang menganalisis dan mencatat analisis forensik tersebut dengan bekerja sama dengan LPTSI Unsoed. Dampak dari proses analisis insiden yang berhasil diidentifikasi dicatat dan dikategorikan menjadi

nilai kategori insiden yang berfungsi sebagai informasi tentang hasil analisis dampak dari suatu insiden untuk digunakan sebagai langkah respons yang harus diambil.

Nilai kategori tersebut terdiri atas nilai kecil, sedang dan besar. Apabila mengacu pada nilai kategori sesuai dengan kerangka kerja keamanan siber tersebut, maka pengkategorian nilai dampak tersebut dapat digunakan untuk pengambilan respons yang paling relevan untuk diambil. Proses analisis dan respons keamanan siber sistem informasi perpustakaan secara sistem memang menjadi tanggung jawab dari lembaga terkait, tetapi bagi UPT Perpustakaan kegiatan analisis dan respons tersebut minimal diungkapkan dan dikomunikasikan ke semua anggota organisasi baik operator dan administrator. Proses pengembangan dan evaluasi juga perlu dilaksanakan untuk kegiatan tersebut sehingga dampak yang ditimbulkan tidak sampai menghentikan layanan sistem informasi perpustakaan.

4.4.4 Mitigasi

Langkah pertama mitigasi oleh UPT Perpustakaan adalah melaksanakan proses isolasi terhadap insiden dengan melaksanakan kegiatan identifikasi sumber ancaman, pencatatan, komunikasi dan koordinasi dengan operator dan Kepala UPT Perpustakaan, serta melakukan kegiatan tindakan perbaikan oleh administrator sistem informasi perpustakaan. Mitigasi keamanan siber setelah proses isolasi juga dilaksanakan dengan melaksanakan kegiatan pemantauan terhadap sistem informasi perpustakaan berjalan dengan baik ataupun masih terjadi gangguan. Tindakan identifikasi, mitigasi dan dokumentasi kerentanan siber sistem informasi perpustakaan pada dasarnya telah dilaksanakan oleh UPT Perpustakaan meskipun tidak menggunakan kerangka kerja dan prosedur yang terstandarisasi, hanya merupakan kegiatan insidental terhadap adanya insiden yang harus diantisipasi dan berusaha dihilangkan dampaknya. Pada keamanan siber sistem informasi perpustakaan di UPT Perpustakaan Unsoed, proses mitigasi ini dengan cara memindahkan atau mentransfer *server* sistem informasi perpustakaan yang ditempatkan di LPTSI. Secara kelembagaan sesuai dengan prosedur keamanan siber sistem informasi karena semua sistem informasi yang berjalan di lingkungan Unsoed menjadi tanggung jawab LPTSI Unsoed.

4.4.5 Penyempurnaan

Kategori penyempurnaan mendeskripsikan subkategori rencana respons dengan menggabungkan pelajaran yang dipetik dari insiden sebelumnya dan bagaimana strategi respons diperbaharui. Proses perencanaan respons yang telah berjalan di UPT Perpustakaan Unsoed memberikan pemahaman dan pelajaran bagi sumber daya manusia dalam proses implementasi keamanan siber sistem informasi perpustakaan. Respons tindakan atas terjadinya insiden yang berhasil teridentifikasi dan pengambilan tindakan mitigasi yang tepat saat ini sesuai dengan kebutuhan UPT Perpustakaan. Evaluasi penyempurnaan tindakan respons dilaksanakan yang berhubungan dengan komunikasi dan kecepatan dalam tindakan respons untuk memberikan layanan maksimal kepada pengguna perpustakaan. Strategi penyempurnaan dengan perlu adanya *upgrage* kemampuan operator UPT Perpustakaan agar mampu menilai, mendeteksi dan melaksanakan tindakan respons tentang keamanan siber sistem informasi perpustakaan agar layanan informasi perpustakaan menjadi lebih maksimal.

Penelitian oleh Pertama & Ardiyasa (2019) tentang audit keamanan sistem informasi perpustakaan menggunakan kerangka kerja COBIT merekomendasikan kerangka kerja COBIT yang meliputi domain keamanan (APO 13) dan pelayanan keamanan (DSS05) sejalan dengan hasil penelitian ini pada fungsi merespons. Fungsi respons telah dilaksanakan dengan baik yakni melaksanakan tindakan mitigasi risiko serta menjalin komunikasi dengan berbagai *stakeholder* perpustakaan. Meskipun tindakan mitigasi risiko tidak dilaksanakan sesuai dengan kerangka kerja terstandarisasi, tetapi UPT Perpustakaan melaksanakan tindakan peringanan risiko keamanan siber dengan cara memindahkan/mentransfer aset data sistem informasi perpustakaan ke lembaga yang lebih berwewenang. Tindakan lain pun telah dilaksanakan dengan baik oleh UPT Perpustakaan dalam subkategori fungsi merespons.

4.5 Memulihkan

4.5.1 Perencanaan Pemulihan

Proses perencanaan pemulihan keamanan siber UPT Perpustakaan Unsoed tidak dilaksanakan berdasarkan kerangka kerja sebagai prosedur baku. Penelitian ini mengungkap peran administrator sistem informasi dan teknologi informasi yang hanya mencatat dan melaksanakan perbaikan tindakan segera meskipun dengan kemampuan dan keterampilan yang terbatas. Perencanaan pemulihan insiden hanya terbatas pada proses pencatatan insiden tidak sesuai dengan kerangka kerja keamanan siber.

4.5.2 Penyempurnaan

Proses kategori penyempurnaan pemulihan memberikan gambaran dan deskripsi bagaimana UPT Perpustakaan Unsoed melaksanakan kegiatan subkategori evaluasi terhadap tindakan pemulihan insiden keamanan siber sistem informasi perpustakaan yang telah dilaksanakan. Pengembangan sistem sesuai dengan siklus hidup pengembangan sistem informasi perpustakaan pun menjadi proses yang berkelanjutan untuk penyempurnaan pemulihan keamanan siber yang lebih baik. Proses penyempurnaan pemulihan memang memerlukan tindakan dan kerja sama dari semua pihak yang berinteraksi dengan sistem informasi perpustakaan. Semua komponen harus bersama-sama merumuskan prosedur, pencatatan dan evaluasi kegiatan untuk menciptakan sistem layanan informasi handal sesuai dengan kebutuhan UPT Perpustakaan. Meskipun dengan berbagai macam kendala yang menyertai, tetapi proses penyempurnaan dalam pemulihan keamanan siber sistem informasi perpustakaan di UPT Perpustakaan tetap dilaksanakan sesuai dengan kebutuhan organisasi dan berdasarkan siklus hidup pengembangan sistem informasi yang diimplementasikan.

4.5.3 Komunikasi

Kategori faktor komunikasi berhubungan dengan bagaimana subkategori penyampaian informasi tentang adanya insiden yang mengganggu layanan sistem informasi perpustakan kepada pihak internal dan ekternal perpustakaan. Proses komunikasi yang baik akan menimbulkan tingkat kepercayaan kepada UPT Perpustakaan sebagai lembaga yang memiliki kompetensi dalam pelayanan dan pemrosesan informasi secara umum kepada pihak ekternal. Khusus untuk pihak internal, perpustakaan memberikan tingkat reputasi yang lebih tinggi sebagai lembaga yang memiliki keterampilan dan pengetahuan akan kegiatan pemrosesan informasi dengan implementasi teknologi informasi sesuai dengan prosedur dan terstandarisasi. Komunikasi proses pemulihan keamanan siber sistem informasi perpustakaan pada intinya telah dilaksanakan oleh UPT Perpustakaan kepada semua pihak yang terlibat dalam sistem layanan informasi. Secara birokrasi dan komunikasi non-formal pun dilaksanakan untuk memberikan layanan prima kepada pemustaka perpustakaan secara umum.

Fungsi memulihkan merupakan representasi dari penelitian Perdana (2018). Penelitian ini menghasilkan audit keamanan sistem informasi akademik dikelola dengan baik dengan level 3 yang berarti keamanan data menjadi prosedur yang dijalankan oleh organisasi, meskipun dengan hasil yang berbeda. Sebagai serangkaian prosedur yang harus dijalankan oleh organisasi, maka fungsi memulihkan pada keamanan siber ini harus diterapkan secara prosedural. Hasil penelitian ini berbeda dengan penelitian sebelumnya tentang sistem keamanan akademik yang dikelola dengan baik, hasil pada penelitian dengan kerangka kerja *NIST Cybersecurity* menunjukkan sebaliknya secara kualitatif belum dijalankan dengan baik oleh UPT Perpustakaan. Perpustakaan hanya berusaha memulihkan kejadian yang bersifat insidental, secara prosedural sesuai kerangka kerja keamanan siber belum dilaksanakan.

5. KESIMPULAN

Berdasarkan hasil penelitian dapat disimpulkan bahwa fungsi kerangka kerja keamanan siber menggunakan kerangka kerja *NIST Cybersecurity* belum diaplikasikan oleh UPT Perpustakaan Unsoed secara prosedural. Proses identifikasi kerentanan menggantungkan pada lembaga universitas bukan oleh pustakawan yang bertanggung jawab dalam mengelola sistem informasi. Teknologi deteksi perlindungan dari ancaman hanya bergantung pada *default* sistem dan pengalaman administrator. Mitigasi risiko keamanan siber dilaksanakan oleh UPT Perpustakaan dengan cara mentransfer sistem informasi perpustakaan ke LPTSI. Proses pemulihan, evaluasi dan penyempurnaan dilaksanakan secara terus-menerus sebagai siklus hidup pengembangan sistem informasi di UPT Perpustakaan Unsoed. Hasil penelitian memberikan rekomendasi agar perpustakaan memiliki catatan dan prosedur keamanan siber yang harus diterapkan karena besarnya aset informasi yang dilayankan oleh perpustakaan dan evaluasi infrastruktur teknologi informasi perlu dilaksanakan dengan kemampuan pustakawan terhadap teknologi keamanan siber yang harus ditingkatkan dengan melaksanakan pelatihan khusus. Penelitian lanjutan perlu dilaksanakan dengan kajian teknis kuantitatif untuk menganalisis tingkat keamanan siber.

6. UCAPAN TERIMA KASIH

Terima kasih penulis ucapkan kepada LPPM Unsoed yang telah memberikan kesempatan dan dana hibah penelitian untuk tenaga fungsional non-dosen.

DAFTAR PUSTAKA

Aminzade, M. (2018). Confidentiality, integrity and availability – finding a balanced IT framework. *Network Security*, 2018(5), 9–11. https://doi.org/10.1016/s1353-4858(18)30043-6

Aritonang, I., Udayanti, E., & Iksan, N. (2018). Audit keamanan sistem informasi menggunakan framework Cobit 5 (APO13). *ITEJ (Information Technology Engineering Journals), 3*(2), 6-10. https://doi.org/10.24235/itej.v3i2.27

Calder, A. (2018). NIST cybersecurity framework: A pocket guide. IT Governance Publishing Ltd.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2020). Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model. *Journal of Cybersecurity, 6*(1). https://doi.org/10.1093/cybsec/tyaa005

Kabanda, G. (2018). A cybersecurity culture framework and its impact on Zimbabwean organizations. *Asian Journal of Management, Engineering & Computer Science, 3*(4), 17–34. https://crsdindia.com/AJMECS/vol.3(4)oct.2018/1.Gabriel%20Kabanda.1-16.pdf

Kim, D., & Solomon, M. G. (2016). Fundamentals of information systems security: Print bundle. Jones & Bartlett Learning.

Kwon, R., Ashley, T., Castleberry, J., Mckenzie, P., & Gourisetti, S. N. G. (2020). Cyber threat dictionary using MITRE ATT&CK matrix and NIST cybersecurity framework mapping. *IEEE Xplore*, 106–112. https://doi.org/10.1109/RWS50334.2020.9241271

Mahendra, V., & Soewito, B. (2023). Penerapan kerangka kerja NIST cybersecurity dan CIS controls sebagai manajemen risiko keamanan siber. *Techno.Com, 22*(3), 527–538. https://doi.org/10.33633/tc.v22i3.8491

Nugroho, C., Sos, S., & Kom, M. I. (2020). Cyber society: Teknologi, media baru, dan disrupsi informasi. Prenada Media.

Perdana, R. S. (2018). Audit keamanan sistem informasi akademik menggunakan framework NIST SP 800-26 (Studi kasus: Universitas Sangga Buana YPKP Bandung). *Infotronik: Jurnal Teknologi Informasi dan Elektronika*, *3*(1), 9–14. https://doi.org/10.32897/infotronik.2018.3.1.83

Perkin, N., & Abraham, P. (2021). Building the agile business through digital transformation. Kogan Page Publishers.

Pertama, P. P. G. P., & Ardiyasa, I. W. (2019). Audit keamanan sistem informasi perpustakaan STMIK STIKOM Bali menggunakan kerangka kerja COBIT. *Jurnal Sistem dan Informatika (JSI), 13*(2), 77-86. https://jsi.stikom-bali.ac.id/index.php/jsi/article/view/215.

Pratomo, B. A., Marwan, A., Wibowo, S., Kariadi, M. T. (2018). Kerangka kerja untuk meningkatkan keamanan siber infrastruktur kritis. https://nist.gov/system/files/documents/2021/11/29/NIST%20Cybersecurity_Indonesian_Updated.pdf

Silalahi, F. D. (2022). Keamanan cyber (cyber security). Penerbit Yayasan Prima Agus Teknik, 1–285.

Sudibyo, A. (2019). Jagat digital: Pembebasan dan penguasaan. Kepustakaan populer gramedia.

Wahyudi, H., Zulianto, A., & Maulana, A. (2020). Audit keamanan sistem informasi manajemen akademik dan kemahasiswaan menggunakan SNI ISO/IEC 27001:2013 : Studi kasus STMIK Mardira Indonesia. *Jurnal Computech & Bisnis (e-Journal), 14*(1), 40–46. https://jurnal.stmik-mi.ac.id/index.php/jcb/article/view/88

Whitman, M. E., & Mattord, H. J. (2021). Principles of information security. Cengage learning.

Yin, R. K. (2018). Case study research and applications. Sage Thousand Oaks, CA.