Jurnal Ilmu Informasi Perpustakaan dan Kearsipan
Volume 14 No. 02 Tahun 2025 *ISSN:2302-3511*
http://ejournal.unp.ac.id/index.php/iipk/index

Information Security in Digital Archive Storage at PT Putraduta Buanasentosa (Indoarsip)
Keamanan Informasi pada Penyimpanan Arsip Digital di PT Putraduta Buanasentosa (Indoarsip)

Syalwa Nur Laily[1]; Andi Kasman[1]; Zhahirah Indrawati Zainuddin[1]

[1]Program Studi Kearsipan Digital, Universitas Padjadjaran, Indonesia

*Corresponding author. Email: syalwa22002@mail.unpad.ac.id

ABSTRACT

Information security is a highly important aspect of digital records management because electronic data carries risks of misuse, damage, and operational disruption. These conditions require organizations that provide digital records storage services, including PT Putraduta Buanasentosa, to ensure that every operational process is protected with adequate security mechanisms. This study aims to examine how the company implements information security based on the NIST Cybersecurity Framework (CSF). The research employs a descriptive qualitative method through interviews with technical staff and a review of operational procedure documents related to data protection. The findings indicate that the company has implemented the core functions of the NIST Cybersecurity Framework (CSF) through access control, system monitoring, incident handling, and data recovery, all of which support service continuity. The study also highlights the need for improvements in structured risk assessment, regularly conducted security training, and more complete and consistent incident documentation. In addition, the research identifies that strengthened coordination between internal units and more refined incident response procedures can help the company better anticipate evolving digital threats. Overall, the study concludes that the implementation of information security within the company is moving in the right direction but still requires continuous enhancement to keep pace with the dynamics of digital threats and maintain the reliability of digital records storage services for all users in daily operations.

Keywords : *information security; digital archives; NIST Cybersecurity Framework (CSF)*

ABSTRAK

Keamanan informasi menjadi aspek yang sangat penting dalam pengelolaan arsip digital karena data elektronik memiliki risiko terhadap penyalahgunaan, kerusakan, maupun gangguan operasional. Kondisi ini menuntut organisasi penyedia layanan penyimpanan arsip digital, termasuk PT Putraduta Buanasentosa, untuk memastikan bahwa setiap proses operasional dilindungi dengan mekanisme keamanan yang memadai. Penelitian ini bertujuan untuk menelaah bagaimana perusahaan menerapkan keamanan informasi berdasarkan kerangka NIST Cybersecurity Framework (CSF). Penelitian menggunakan metode deskriptif kualitatif melalui wawancara dengan staf teknis serta telaah dokumen prosedur operasional terkait perlindungan data. Hasil penelitian menunjukkan bahwa perusahaan telah menjalankan fungsi inti NIST Cybersecurity Framework (CSF) melalui pengendalian akses, pemantauan sistem, penanganan insiden, dan pemulihan data yang mendukung keberlangsungan layanan. Temuan juga menunjukkan perlunya peningkatan pada

aspek penilaian risiko yang lebih terstruktur, pelatihan keamanan yang dilakukan secara berkala, serta pendokumentasian insiden yang lebih lengkap dan konsisten. Selain itu, penelitian menemukan bahwa penguatan koordinasi antarunit kerja dan penyempurnaan prosedur respons insiden dapat membantu perusahaan lebih siap menghadapi perkembangan ancaman digital. Secara keseluruhan, penelitian ini menyimpulkan bahwa penerapan keamanan informasi di perusahaan telah berjalan dengan arah yang tepat, namun masih memerlukan penguatan berkelanjutan agar dapat mengikuti dinamika ancaman digital dan menjaga keandalan layanan penyimpanan arsip bagi seluruh pengguna layanan dalam operasional sehari-hari secara konsisten.

Kata Kunci : keamanan informasi; arsip digital; NIST Cybersecurity Framework (CSF)

Pendahuluan

Perkembangan teknologi informasi yang pesat telah mendorong organisasi untuk beralih dari sistem kearsipan konvensional menuju pengelolaan arsip digital. Digitalisasi arsip memberikan berbagai manfaat, seperti efisiensi ruang penyimpanan, kemudahan akses, serta percepatan proses temu kembali informasi (Azahra & Putra, 2024). Namun, transformasi ini juga membawa risiko baru karena arsip digital rentan terhadap akses tidak sah, kebocoran data, gangguan sistem, dan kerusakan infrastruktur teknologi apabila tidak didukung oleh sistem pengamanan yang memadai (Bawono, 2022; Nurkarimah, 2025). Selain itu, pengelolaan arsip digital menuntut perancangan sistem penyimpanan yang konsisten agar keaslian dan integritas dokumen tetap terjaga dalam jangka panjang (Meghanandha & Naik, 2025). Seiring dengan meningkatnya volume data, beragamnya format arsip digital, serta tingginya tuntutan terhadap keamanan dan integritas informasi, organisasi dituntut untuk menerapkan strategi pengelolaan arsip digital yang lebih komprehensif dan terintegrasi (Rahmaeisa & Kurniawan, 2025).

Dalam pengelolaan arsip digital, keamanan informasi menjadi aspek fundamental karena arsip tidak hanya berfungsi sebagai sumber informasi operasional, tetapi juga sebagai bukti hukum dan aset strategis organisasi. Berbagai penelitian menunjukkan bahwa lemahnya pengamanan sistem arsip digital dapat berdampak pada gangguan layanan, hilangnya kepercayaan pengguna, serta meningkatnya risiko pelanggaran perlindungan data (Tekle, 2024; Nemec Zlatolas dkk., 2024). Risiko tersebut dapat semakin diperbesar oleh kesalahan prosedural dan faktor sumber daya manusia, meskipun teknologi yang digunakan telah memadai (Kishani & Asadi, 2018). Kondisi ini menegaskan bahwa keamanan arsip digital tidak dapat dipahami semata-mata sebagai persoalan teknis, melainkan sebagai bagian dari tata kelola organisasi secara menyeluruh.

Di Indonesia, peningkatan digitalisasi layanan publik dan swasta belum selalu diimbangi dengan penerapan sistem keamanan informasi yang terstruktur dan terukur. Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 mewajibkan penyelenggara sistem elektronik untuk menjamin kerahasiaan, integritas, dan ketersediaan data. Namun, sejumlah penelitian menunjukkan bahwa masih banyak organisasi yang menghadapi kesulitan dalam mengelola risiko keamanan informasi secara berkelanjutan akibat lemahnya perencanaan keamanan dan minimnya penerapan kerangka kerja yang terstandar (Sama dkk., 2021; Frank, 2021). Hal ini menunjukkan adanya kesenjangan antara tuntutan regulasi dan praktik pengamanan informasi yang dijalankan di lapangan.

Dalam konteks tersebut, PT Putraduta Buanasentosa (Indoarsip) sebagai penyedia layanan penyimpanan arsip digital memiliki tingkat urgensi keamanan informasi yang tinggi. Perusahaan ini mengelola arsip digital milik berbagai klien lintas sektor dengan tingkat sensitivitas data yang beragam, sehingga keamanan informasi tidak hanya menjadi persoalan teknis internal, tetapi juga bagian dari tanggung jawab profesional dalam menjaga kepercayaan pengguna layanan. Penyedia layanan arsip digital memiliki tanggung jawab yang lebih besar dibandingkan organisasi yang hanya mengelola data internal, karena stabilitas sistem dan keamanan informasi secara langsung memengaruhi keberlanjutan operasional klien (Repetto et al., 2021).

Sejumlah penelitian sebelumnya telah membahas keamanan informasi dan pengelolaan arsip digital dari berbagai perspektif, termasuk teknologi dan kebijakan organisasi (Tan & Soewito, 2022; Mahendra & Soewito, 2023). Namun, sebagian besar penelitian tersebut berfokus pada institusi yang mengelola arsip internal dan belum banyak mengkaji penerapan keamanan informasi berbasis kerangka kerja standar pada penyedia layanan arsip digital komersial di Indonesia. Selain itu, kajian yang secara khusus menganalisis implementasi keamanan informasi arsip digital menggunakan NIST Cybersecurity Framework (CSF) dalam konteks layanan penyimpanan arsip digital masih relatif terbatas.

Berdasarkan kondisi tersebut, terdapat celah penelitian terkait bagaimana penerapan keamanan informasi berbasis NIST Cybersecurity Framework (CSF) dijalankan secara operasional oleh penyedia layanan arsip digital di Indonesia serta sejauh mana kerangka kerja tersebut mendukung kematangan keamanan layanan arsip digital. Penelitian ini hadir untuk mengisi celah tersebut dengan menjadikan Indoarsip sebagai studi kasus.

Penelitian ini bertujuan untuk menganalisis penerapan keamanan informasi pada penyimpanan arsip digital di Indoarsip berdasarkan NIST Cybersecurity Framework (CSF). Secara teoretis, penelitian ini diharapkan dapat memperkaya kajian keamanan arsip digital berbasis kerangka kerja standar dalam konteks penyedia layanan arsip. Secara praktis, hasil penelitian ini diharapkan dapat menjadi bahan evaluasi bagi penyedia layanan arsip digital dalam meningkatkan kematangan sistem keamanan informasi secara berkelanjutan.

Metode

Penelitian ini menggunakan pendekatan deskriptif kualitatif. Pendekatan ini dipilih karena memungkinkan peneliti memahami fenomena secara mendalam berdasarkan kondisi nyata di lapangan. Yuliani (2018), mengadaptasi pemikiran Mohajan dan Haradhan (2018), menjelaskan bahwa penelitian kualitatif bertujuan mengkaji peristiwa dan tindakan sosial dalam konteks alaminya dengan menekankan pada cara individu menafsirkan pengalaman mereka untuk memahami realitas dan memecahkan permasalahan. Dengan demikian, metode ini sesuai untuk menggambarkan bagaimana Indoarsip menerapkan keamanan informasi dalam pengelolaan arsip digital.

1. Desain Penelitian

   Pendekatan deskriptif kualitatif dipilih secara spesifik karena penelitian ini merupakan studi kasus di PT Putraduta Buanasentosa (Indoarsip). Desain ini memungkinkan peneliti melakukan analisis mendalam terhadap prosedur, kebijakan, dan praktik nyata keamanan informasi dalam konteks operasional penyedia layanan arsip digital. Pendekatan ini memungkinkan analisis tidak hanya berdasarkan data kuantitatif atau angka, tetapi juga berdasarkan realitas organisasi. Dalam hal ini, kerangka seperti NIST Cybersecurity Framework (CSF) memberi landasan untuk mengevaluasi kematangan keamanan secara menyeluruh, meliputi aspek teknis, prosedural, dan manajerial, sebagaimana dijelaskan dalam penelitian terkait di Indonesia (Balafif, 2023).

2. Informan Penelitian dan Teknik Penentuan

   Informan utama dalam penelitian ini adalah staf di bagian System & Application PT Putraduta Buanasentosa (Indoarsip) yang bertanggung jawab langsung terhadap pengelolaan sistem penyimpanan arsip digital. Hanya satu informan yang dipilih karena merupakan orang yang paling memahami prosedur, kebijakan, dan praktik keamanan informasi di bagian tersebut. Pemilihan informan dilakukan menggunakan purposive sampling. Menurut Sugiyono (2019), purposive sampling adalah teknik pemilihan sampel berdasarkan pertimbangan tertentu, yaitu memilih informan yang dianggap paling memahami konteks penelitian sesuai kriteria yang ditetapkan. Informan dipilih karena terlibat langsung dalam penerapan kontrol NIST Cybersecurity Framework (CSF) dan penanganan insiden siber, sehingga data yang diperoleh bersifat relevan, dan valid untuk menggambarkan praktik keamanan informasi di Indoarsip.

3. Teknik Pengumpulan Data

   Pengumpulan data dalam penelitian ini dilakukan melalui wawancara terstruktur yang disusun berdasarkan lima fungsi inti NIST Cybersecurity Framework, yaitu Identify, Protect, Detect, Respond, dan Recover. Wawancara bertujuan untuk memperoleh gambaran mengenai kebijakan, prosedur, serta mekanisme pengelolaan keamanan informasi arsip digital yang diterapkan di Indoarsip.

Selain wawancara, penelitian ini didukung oleh studi dokumentasi terhadap Standar Operasional Prosedur (SOP) Keamanan Informasi sebagai data pendukung. Dokumen SOP dianalisis untuk menelaah kesesuaian kebijakan tertulis dengan fungsi-fungsi keamanan informasi dalam NIST CSF.

Kombinasi wawancara dan studi dokumentasi memungkinkan triangulasi sumber data dalam menilai kesiapan dan kerangka pengelolaan keamanan informasi arsip digital. Namun, pengumpulan data dalam penelitian ini terbatas pada dokumen internal dan informasi naratif, sehingga analisis difokuskan pada aspek kebijakan dan perencanaan keamanan informasi, serta belum mencakup pengamatan langsung terhadap implementasi teknis maupun simulasi insiden keamanan.

4. Teknik Analisis Data

Analisis data dilakukan menggunakan analisis interaktif, sebuah pendekatan yang dikembangkan oleh Miles dan Huberman (1994; sebagaimana dikutip dalam Zulfirman, 2022). Pendekatan ini meliputi tiga tahap utama, yaitu reduksi data, penyajian data, dan penarikan kesimpulan. Pada tahap reduksi data, informasi dari transkrip wawancara dan SOP dipilah dan dikelompokkan ke dalam tema utama sesuai lima fungsi NIST Cybersecurity Framework (CSF). Setiap bagian data kemudian diberi kode agar lebih mudah dianalisis. Data selanjutnya dianalisis secara deskriptif untuk mengenali pola, praktik, dan tingkat kematangan penerapan kontrol keamanan di Indoarsip.

Untuk menjaga validitas data, peneliti menggunakan triangulasi sumber, yaitu membandingkan informasi dari wawancara dengan dokumen SOP. Triangulasi pada dasarnya adalah pendekatan yang menggunakan beberapa metode untuk membantu peneliti mengumpulkan dan menganalisis data secara lebih menyeluruh (Nurfajriani dkk., 2024). Dengan cara ini, hasil analisis dapat mencerminkan kondisi nyata secara akurat dan dapat dipertanggungjawabkan.

Hasil dan Pembahasan

Hasil penelitian yang diperoleh melalui wawancara dengan staf bagian System & Application serta analisis terhadap dokumen SOP keamanan informasi menunjukkan bahwa PT Putraduta Buanasentosa (Indoarsip) telah menerapkan berbagai langkah pengamanan dalam pengelolaan arsip digital. Untuk memetakan implementasi tersebut secara lebih terstruktur, penelitian ini menggunakan lima fungsi utama NIST Cybersecurity Framework (CSF), yaitu Identify, Protect, Detect, Respond, dan Recover. Framework ini dipilih karena sesuai untuk organisasi yang menyediakan layanan berbasis digital, termasuk penyimpanan arsip, di mana keberlangsungan layanan dan keamanan informasi menjadi prioritas utama.

NIST Cybersecurity Framework (CSF) dirancang sebagai pedoman komprehensif yang membantu organisasi memahami, mengelola, dan menurunkan risiko keamanan siber melalui pendekatan yang bertahap dan sistematis. Framework ini dapat diterapkan oleh berbagai jenis organisasi karena sifatnya yang mudah disesuaikan, sehingga perusahaan dengan kapasitas berbeda tetap dapat menyesuaikan penerapannya sesuai kebutuhan operasional. Dengan struktur lima fungsinya, NIST Cybersecurity Framework (CSF) memberikan panduan mengenai bagaimana proses keamanan informasi dapat dibangun secara berlapis, mulai dari identifikasi aset hingga pemulihan setelah insiden. Kerangka ini membantu Indoarsip karena perusahaan mengelola arsip digital bernilai tinggi yang memerlukan perlindungan berkelanjutan dan tata kelola yang konsisten.

Penerapan NIST Cybersecurity Framework (CSF) memberikan gambaran menyeluruh mengenai hubungan antara kebijakan perusahaan, perlindungan teknis, dan praktik operasional dalam menjaga keamanan arsip digital. Melalui pendekatan ini, penelitian dapat melihat bagian-bagian yang sudah berjalan dengan baik serta bagian yang masih memerlukan penguatan agar sistem keamanan informasi berkembang lebih stabil.

Gambar 1. Kerangka Kerja NIST Cybersecurity Framework (CSF)

Sumber: Website Device42

1. Identify

Pada fungsi Identify dalam NIST Cybersecurity Framework, Indoarsip telah memiliki landasan awal dalam mengenali aset informasi dan struktur pendukung operasional pengelolaan arsip digital. Berdasarkan hasil wawancara dan analisis dokumen, proses identifikasi aset dilakukan oleh departemen Information Technology (IT), khususnya bagian System & Application, yang bertanggung jawab atas pengelolaan server, aplikasi penyimpanan arsip digital, serta infrastruktur teknis pendukung lainnya.

Identifikasi aset dilakukan melalui pencatatan dan pemeriksaan berkala terhadap perangkat keras dan perangkat lunak yang digunakan. Proses ini mencakup pemantauan kondisi server, kapasitas penyimpanan data, serta performa sistem secara umum. Selain itu, pengelolaan sistem dilakukan dengan memastikan perangkat lunak keamanan pada server diperbarui secara berkala sebagai bagian dari upaya perlindungan terhadap potensi ancaman keamanan informasi. Praktik ini menunjukkan adanya kesadaran terhadap pentingnya identifikasi aset sebagai langkah awal dalam pengelolaan keamanan informasi.

Hasil wawancara menunjukkan bahwa identifikasi risiko keamanan informasi di Indoarsip masih didasarkan pada pengalaman operasional staf IT dalam mengelola sistem dan infrastruktur pendukung. Pemahaman terhadap karakteristik sistem serta permasalahan yang pernah muncul dalam operasional sehari-hari menjadi dasar dalam mengenali potensi risiko yang dapat memengaruhi keberlangsungan layanan arsip digital.

Pendekatan berbasis pengalaman tersebut memungkinkan organisasi untuk merespons risiko yang bersifat langsung dan operasional. Namun, jika dikaitkan dengan kerangka NIST CSF, kondisi ini berimplikasi pada keterbatasan dalam pemetaan risiko secara sistematis, sehingga penentuan prioritas pengamanan dan pengambilan keputusan keamanan masih sangat dipengaruhi oleh kebutuhan operasional jangka pendek. Dengan demikian, fungsi Identify di Indoarsip telah berjalan secara praktis, tetapi tingkat kematangannya masih berada pada tahap awal karena proses identifikasi risiko belum sepenuhnya terintegrasi dalam kerangka manajemen risiko keamanan informasi yang komprehensif.

2. Protect

Pada fungsi Protect dalam NIST Cybersecurity Framework, Indoarsip menerapkan berbagai langkah perlindungan yang mencakup aspek administratif, teknis, dan pengaturan perilaku kerja guna menjaga keamanan informasi arsip digital. Berdasarkan hasil wawancara dan analisis dokumen, langkah-langkah perlindungan tersebut dirancang untuk mencegah akses tidak sah, kebocoran data, serta gangguan terhadap sistem penyimpanan arsip digital.

Pada aspek administratif, pengendalian akses sistem dilakukan dengan memberikan hak akses hanya kepada pegawai yang memiliki kewenangan tertentu sesuai dengan tugas dan tanggung jawabnya. Penggunaan akun individual memungkinkan pengelolaan akses yang lebih terkontrol dan meminimalkan risiko penyalahgunaan hak akses. Selain itu, pembatasan penggunaan perangkat penyimpanan eksternal, seperti flashdisk, diterapkan untuk mengurangi potensi transfer data tanpa pengawasan serta mencegah masuknya file berbahaya ke dalam sistem.

Dari sisi teknis, perlindungan jaringan didukung oleh penggunaan firewall sebagai lapisan utama pengamanan lalu lintas data. Firewall berfungsi untuk mengatur dan memfilter aktivitas

jaringan berdasarkan aturan tertentu sehingga potensi ancaman dapat dibatasi sejak awal. Selain itu, staf IT melakukan pemantauan terhadap kinerja server, kapasitas penyimpanan, penggunaan sumber daya sistem, serta kestabilan aplikasi penyimpanan arsip digital. Kegiatan pemantauan ini menunjukkan adanya upaya perlindungan yang bersifat preventif, di mana potensi gangguan dapat dikenali sebelum berdampak pada layanan.

Perusahaan juga menerapkan kebijakan kerja yang mendukung perlindungan sistem, seperti larangan mengakses situs tidak aman, pembatasan pemasangan aplikasi yang tidak berkaitan dengan operasional, serta pembaruan firmware perangkat jaringan secara berkala. Kebijakan tersebut berperan dalam membentuk perilaku kerja yang selaras dengan upaya perlindungan keamanan informasi.

Jika dikaitkan dengan karakteristik data arsip klien yang memiliki tingkat sensitivitas yang beragam, langkah-langkah perlindungan yang diterapkan Indoarsip dapat dinilai memadai untuk memberikan perlindungan dasar terhadap risiko keamanan informasi secara umum. Namun, hasil analisis menunjukkan bahwa penerapan kontrol keamanan masih bersifat seragam dan belum secara eksplisit dibedakan berdasarkan tingkat sensitivitas data arsip yang dikelola. Kondisi ini berimplikasi pada perlunya penguatan pendekatan perlindungan yang lebih adaptif agar kontrol keamanan dapat disesuaikan dengan risiko dan tingkat kepentingan masing-masing data arsip.

3. Detect

Pada fungsi Detect dalam NIST Cybersecurity Framework, Indoarsip menerapkan mekanisme deteksi melalui pemantauan rutin terhadap aktivitas sistem dan jaringan. Berdasarkan hasil wawancara, staf IT secara berkala memeriksa log server, laporan firewall, serta aktivitas jaringan untuk mengidentifikasi indikasi awal yang berpotensi mengganggu operasional layanan arsip digital. Pemantauan ini mencakup pencarian pola aktivitas yang tidak wajar, seperti percobaan login berulang, akses dari alamat IP yang tidak dikenal, peningkatan trafik secara tiba-tiba, atau perubahan perilaku sistem yang menyimpang dari kondisi normal.

Selain pemantauan aktivitas keamanan, staf IT juga melakukan pengawasan terhadap indikator performa sistem, seperti penggunaan memori, aktivitas prosesor, respons aplikasi, dan kestabilan basis data. Ketika teridentifikasi adanya penurunan performa, staf menilai apakah kondisi tersebut masih berada dalam batas operasional normal atau merupakan indikasi awal gangguan sistem maupun potensi ancaman keamanan informasi. Pendekatan ini memungkinkan deteksi dini terhadap permasalahan teknis yang dapat berdampak pada layanan.

Sistem yang digunakan Indoarsip juga didukung oleh pembaruan informasi ancaman siber secara berkala, yang membantu sistem mengenali pola ancaman yang berkembang. Pembaruan tersebut memperkuat kemampuan deteksi awal, khususnya terhadap ancaman yang bersifat umum atau telah dikenal. Meskipun demikian, proses deteksi masih sangat bergantung pada pemantauan manual dan interpretasi staf IT terhadap informasi yang tersedia.

Jika dikaitkan dengan peningkatan skala data arsip dan aktivitas sistem seiring bertambahnya jumlah klien, ketergantungan pada monitoring manual berimplikasi pada potensi keterlambatan dalam mendeteksi ancaman keamanan yang bersifat kompleks atau terjadi secara simultan. Pada kondisi beban sistem yang meningkat, volume log dan aktivitas jaringan yang besar dapat menyulitkan proses identifikasi pola anomali secara cepat. Oleh karena itu, meskipun mekanisme deteksi yang diterapkan saat ini dinilai cukup untuk kebutuhan operasional dasar, peningkatan skala layanan menuntut penguatan kemampuan deteksi agar proses identifikasi ancaman dapat dilakukan secara lebih responsif dan konsisten.

4. Respond

Pada fungsi Respond, Indoarsip berupaya memastikan bahwa setiap insiden yang berpotensi mengancam keamanan informasi dapat ditangani secara cepat, terarah, dan terkoordinasi. Penanganan biasanya diawali dengan komunikasi langsung antara staf IT dan unit terkait ketika terdeteksi gangguan pada server, ketidakteraturan pada aktivitas jaringan, atau aktivitas akses yang tidak wajar. Langkah awal umumnya dilakukan dengan membatasi bagian yang dianggap menjadi sumber permasalahan sambil meninjau log dan kondisi sistem untuk mengetahui penyebab utama terjadinya gangguan.

Indoarsip telah memiliki dokumen formal berupa SOP *Policy*, SOP *Disaster Recovery Plan* (DRP), dan SOP Pelindungan Data Pribadi (PDP). Ketiga dokumen ini menjadi acuan penting dalam menentukan langkah respons ketika insiden terjadi. Meskipun implementasinya masih terus

diperkuat, keberadaan SOP tersebut membantu memastikan bahwa penanganan tidak dilakukan secara spontan semata, tetapi mengikuti alur kerja yang terstruktur. Prosedur meliputi tindakan dasar seperti pembatasan akses sementara, pemeriksaan sistem yang terdampak, pemulihan layanan, serta penyampaian informasi kepada pihak yang berkepentingan.

Setelah insiden dapat ditangani, staf IT melakukan evaluasi internal untuk meninjau penyebab, dampak, dan efektivitas langkah respons yang telah diambil. Evaluasi ini penting sebagai proses pembelajaran agar konfigurasi, kebijakan, atau prosedur dapat diperbaiki apabila ditemukan celah pada penanganan sebelumnya. Dengan cara ini, Indoarsip membangun siklus peningkatan berkelanjutan dalam menghadapi insiden keamanan.

Koordinasi antarunit juga menjadi bagian yang tidak terpisahkan dalam fungsi Respond. Apabila gangguan berdampak pada banyak pengguna, komunikasi antarunit dilakukan untuk menyampaikan kondisi terkini sehingga setiap unit dapat menyesuaikan aktivitas operasionalnya. Mekanisme koordinasi ini membantu meminimalkan gangguan layanan dan mempercepat proses pemulihan.

Untuk peningkatan di masa mendatang, dokumentasi insiden dan penyusunan prosedur yang lebih rinci dapat membantu memastikan konsistensi dalam penanganan respons, sehingga tidak hanya bergantung pada pengalaman individu staf IT. Adanya panduan yang lebih lengkap akan memperkuat kesiapan perusahaan dalam menghadapi insiden yang lebih kompleks dan menjaga ketahanan keamanan informasi secara lebih optimal.

5. Recover

Pada fungsi Recover, Indoarsip berupaya memastikan bahwa layanan dapat kembali berjalan normal setelah insiden terjadi. Pemulihan dilakukan secara bertahap, dimulai dari memulihkan layanan inti seperti akses server, aplikasi penyimpanan arsip, serta koneksi jaringan yang terdampak. Staf IT meninjau ulang konfigurasi sistem untuk memastikan tidak ada komponen yang tertinggal dalam kondisi tidak stabil setelah penanganan insiden, sehingga risiko gangguan lanjutan dapat diminimalkan.

Proses pemulihan ini juga berkaitan dengan keberadaan SOP *Disaster Recovery Plan* (DRP) yang menjadi pedoman ketika terjadi gangguan besar. Dokumen tersebut mengatur urutan prioritas pemulihan, termasuk langkah-langkah yang harus dilakukan jika terjadi kejadian yang menyebabkan *downtime* lebih lama dari biasanya. Meskipun penerapannya masih terus diperkuat, SOP tersebut memberikan struktur yang jelas sehingga proses pemulihan tidak semata-mata bergantung pada pengalaman teknis individu.

Selain memulihkan layanan teknis, Indoarsip juga melakukan pengecekan berulang terhadap stabilitas sistem setelah pemulihan dilakukan. Staf IT meninjau performa server, memastikan aplikasi berjalan dalam kondisi stabil, serta mengevaluasi apakah pengguna dapat kembali mengakses layanan secara normal. Pemantauan pascapemulihan ini penting untuk memastikan bahwa gangguan tidak muncul kembali dalam waktu dekat.

Selanjutnya, perusahaan juga melakukan penyesuaian jika ditemukan area yang dinilai perlu diperbaiki agar proses pemulihan pada insiden berikutnya dapat berjalan lebih cepat. Penyesuaian ini dapat mencakup pembaruan prosedur, penguatan konfigurasi keamanan, atau peningkatan kapasitas perangkat yang dianggap sudah mendekati batas kemampuan. Upaya seperti ini membantu membangun ketahanan sistem jangka panjang.

Untuk mendukung tingkat pemulihan yang lebih baik, Indoarsip mendorong adanya dokumentasi pasca-insiden sebagai bahan evaluasi berkala. Dokumentasi tersebut memungkinkan perusahaan melihat pola insiden yang berulang dan merumuskan langkah pencegahan yang lebih efektif. Dengan demikian, fungsi Recover tidak hanya berfokus pada pemulihan layanan, tetapi juga pada penguatan kesiapan perusahaan agar lebih tangguh dalam menghadapi gangguan di masa mendatang.

Selain temuan mengenai penerapan kontrol keamanan berdasarkan lima fungsi NIST Cybersecurity Framework (CSF) tersebut, analisis lebih dalam menunjukkan bahwa posisi keamanan informasi Indoarsip tidak dapat dilihat hanya dari ketersediaan kendali teknis, tetapi juga dari bagaimana penerapan tersebut sejalan dengan perkembangan praktik keamanan arsip digital terkini. Kondisi ini memberikan ruang untuk menilai apakah sistem keamanan yang berjalan saat ini sekadar memenuhi kebutuhan operasional atau

sudah bergerak menuju kematangan keamanan jangka panjang. Dibandingkan dengan studi terdahulu, Indoarsip tampak memiliki fondasi pengamanan yang kuat, namun konsistensi pembaruan dan peningkatan kapasitas SDM masih menjadi faktor penentu keberlangsungan sistem ke depannya. Hal ini sejalan dengan pandangan bahwa organisasi penyedia layanan digital harus menyeimbangkan kendali teknis dan kemampuan manusia untuk menghindari risiko tersembunyi dalam jangka panjang (Evitha, 2024).

Kesesuaian praktik Indoarsip dengan literatur juga tampak pada pola penguatan kebijakan teknis yang bersifat berlapis. Firewall berperan sebagai garis perlindungan pertama, monitoring server sebagai garis kedua, dan pembatasan perangkat eksternal sebagai garis ketiga. Pendekatan multilayer ini serupa dengan praktik institusi layanan digital skala menengah yang menggabungkan kendali administratif dan teknis untuk mencegah kebocoran data; model keamanan yang terdiri dari lapisan proteksi berjenjang seperti firewall, pemantauan jaringan, dan deteksi intrusi dapat meningkatkan ketahanan sistem terhadap berbagai jenis serangan siber (Ryu & Lee, 2024). Namun Indoarsip belum menjalankan program peningkatan kesadaran keamanan secara sistematis, sementara berbagai penelitian menunjukkan bahwa risiko keamanan tidak hanya berasal dari serangan eksternal, tetapi juga dari kesalahan manusia akibat rendahnya literasi keamanan. Penelitian internasional menunjukkan bahwa perilaku pengguna dan kesalahan manusia masih menjadi penyebab utama terjadinya insiden keamanan informasi, sehingga pendekatan keamanan tidak cukup hanya mengandalkan solusi teknis, tetapi juga perlu didukung oleh program edukasi dan peningkatan kesadaran keamanan yang berkelanjutan (Khadka & Ullah, 2025).

Peningkatan kebutuhan deteksi juga terlihat ketika membandingkan temuan penelitian ini dengan literatur terkait penguatan monitoring dalam layanan digital. Meskipun deteksi berbasis server dan firewall yang diterapkan Indoarsip sudah berjalan konsisten, pertumbuhan jumlah arsip digital dan meningkatnya aktivitas pengguna berpotensi membuat monitoring manual menjadi kurang optimal pada beban kerja yang lebih tinggi. Studi terdahulu menekankan bahwa organisasi perlu memastikan kemampuan deteksi yang lebih cepat dan menyeluruh dengan memaksimalkan fitur pemantauan yang sudah tersedia pada perangkat jaringan dan server, termasuk sistem peringatan otomatis yang mampu mengidentifikasi aktivitas tidak biasa sejak tahap awal. Temuan Vervaet (2023) turut mendukung hal tersebut dengan menunjukkan bahwa sistem deteksi otomatis berbasis log dapat mengolah volume data yang besar secara real time sehingga potensi keterlambatan dan keterbatasan monitoring manual dapat diminimalkan. Dengan kata lain, Indoarsip telah berada pada jalur yang tepat dalam manajemen deteksi ancaman, namun peningkatan kapasitas pada fitur deteksi yang sudah dimiliki perusahaan dapat menjadi langkah lanjutan yang realistis untuk memperkuat ketahanan sistem seiring pertumbuhan klien dan volume arsip digital.

Dari sisi respons dan pemulihan, Indoarsip sudah memiliki SOP yang cukup jelas sebagai pedoman ketika insiden terjadi. Keberadaan SOP DRP dan PDP menunjukkan bahwa arah perusahaan sudah sesuai dengan tren tata kelola keamanan digital modern yang menempatkan respons cepat sebagai bagian dari kesinambungan layanan. Namun, efektivitas prosedur respons tidak hanya bergantung pada dokumen, tetapi juga pada latihan teknis dan pelatihan tim untuk menguji kesiapan menghadapi skenario insiden nyata. Penelitian internasional menunjukkan bahwa pelatihan berbasis skenario dapat meningkatkan keterampilan tim respons insiden dan mengatasi hambatan sosial-teknis dalam keterlibatan tim (O'Neill, Ahmad, & Maynard, 2021). Indoarsip belum melakukan simulasi pemulihan secara berkala, sehingga masih terdapat kemungkinan ketidaksesuaian antara dokumen prosedural dan praktik teknik di lapangan. Praktik recovery drill, yakni simulasi pemulihan sistem yang dilakukan untuk memastikan prosedur respons benar-benar dapat dijalankan ketika insiden terjadi, menjadi penting bukan hanya untuk menilai kesiapan teknis, tetapi juga untuk membentuk budaya respons yang adaptif terhadap perubahan ancaman.

Penilaian risiko juga menjadi komponen yang layak diperhatikan. Identifikasi risiko di Indoarsip saat ini bergantung pada pengalaman staf teknis, sedangkan standar penelitian terbaru menekankan perlunya penilaian risiko berbasis metode formal agar keputusan pengamanan dapat diprioritaskan berdasarkan tingkat risiko terbesar, bukan persepsi pengalaman (Muliati dkk., 2025). Karena volume arsip digital cenderung meningkat setiap tahun, penilaian risiko terstruktur dapat membantu perusahaan memprediksi kebutuhan infrastruktur, kapasitas server, dan jalur mitigasi sebelum ancaman terjadi. Pemahaman teoretis ini penting tidak hanya bagi Indoarsip, tetapi juga untuk memperkaya literatur keamanan arsip digital di Indonesia, karena penelitian mengenai manajemen risiko berbasis framework dalam konteks penyedia layanan arsip masih tergolong terbatas.

Temuan penelitian ini memberikan implikasi teoretis bahwa NIST Cybersecurity Framework (CSF) bersifat adaptif dan dapat diterapkan bertahap oleh organisasi berskala menengah tanpa harus

menerapkan semua kontrol secara penuh sekaligus. Selama praktik operasional konsisten dan risiko dipetakan secara berkelanjutan, organisasi tetap dapat mencapai keamanan sistem yang stabil. Implikasi praktisnya adalah Indoarsip dan penyedia arsip digital lainnya dapat mempertimbangkan beberapa pendekatan untuk meningkatkan kematangan keamanan: (1) membangun sistem pelatihan keamanan siber berkala; (2) melakukan penilaian risiko formal berbasis metode; (3) mengoptimalkan fitur deteksi dan peringatan otomatis yang sudah tersedia pada perangkat jaringan dan server untuk memperkuat kemampuan pemantauan; (4) memperkuat dokumentasi insiden sebagai rekam jejak peningkatan keamanan; dan (5) melaksanakan recovery drill secara berkala untuk menyelaraskan SOP dan praktik teknis. Pendekatan ini selaras dengan perspektif yang menekankan bahwa keamanan informasi harus dilihat sebagai proses berkelanjutan, bukan kondisi statis (Tarumingkeng, 2025).

Keterbatasan penelitian ini juga perlu dicatat agar temuan tidak digeneralisasi secara luas. Penelitian hanya melibatkan satu informan dan bersandar pada dokumen internal yang disediakan perusahaan, sehingga variasi perspektif dari divisi lain belum tergambarkan. Selain itu, ketiadaan observasi langsung terhadap sistem juga membatasi pemahaman mengenai bagaimana mekanisme keamanan berjalan pada kondisi insiden sebenarnya. Untuk itu penelitian selanjutnya dianjurkan memperluas partisipasi informan, melakukan observasi teknis secara langsung, dan membandingkan beberapa penyedia arsip digital agar dapat memetakan tingkat keamanan informasi di sektor ini secara lebih komprehensif.

Simpulan

Penelitian ini menyimpulkan bahwa pengelolaan keamanan informasi pada penyimpanan arsip digital di PT Putraduta Buanasentosa (Indoarsip) telah mencakup seluruh fungsi inti dalam NIST Cybersecurity Framework (CSF), yaitu Identify, Protect, Detect, Respond, dan Recover, yang tercermin melalui kebijakan internal, pembagian peran teknis, mekanisme perlindungan sistem, pemantauan aktivitas, serta prosedur penanganan dan pemulihan insiden guna mendukung keberlangsungan operasional arsip digital. Namun demikian, penelitian ini memiliki keterbatasan metodologis karena menggunakan pendekatan deskriptif kualitatif berbasis wawancara dan dokumen SOP internal, sehingga analisis lebih menekankan pada kesiapan kebijakan dan praktik yang dilaporkan dibandingkan pengukuran empiris efektivitas kontrol keamanan secara teknis, dan belum dapat menilai tingkat ketahanan sistem secara kuantitatif maupun dampak langsung terhadap pencegahan insiden siber. Oleh karena itu, simpulan penelitian ini dipahami sebagai gambaran tingkat kematangan pengelolaan keamanan informasi berdasarkan kerangka kerja standar, bukan sebagai hasil audit teknis menyeluruh, meskipun tetap memberikan kontribusi dalam menunjukkan implementasi NIST Cybersecurity Framework (CSF) pada penyedia layanan arsip digital di Indonesia. Penelitian selanjutnya disarankan mengombinasikan pendekatan kualitatif dengan observasi teknis atau pengukuran kuantitatif guna memperoleh pemahaman yang lebih komprehensif mengenai efektivitas dan ketahanan sistem keamanan informasi.

Pengakuan

Penulis menyampaikan terima kasih kepada PT Putraduta Buanasentosa (Indoarsip) atas kesempatan dan dukungan selama proses penelitian serta kepada staf bagian System & Application yang telah bersedia memberikan data, informasi, dan penjelasan terkait mekanisme pengelolaan keamanan arsip digital. Ucapan terima kasih juga diberikan kepada dosen pembimbing yang telah memberikan arahan dan masukan sepanjang penyusunan artikel ini. Tidak lupa penulis menyampaikan apresiasi kepada keluarga dan rekan-rekan yang telah memberikan dorongan moral sehingga penelitian dan penulisan artikel ini dapat diselesaikan dengan baik.

Daftar Pustaka

Azahra, M. F., & Putra, P. (2024). Implementasi arsip digital dalam efisiensi penyimpanan. *Journal of Economic and Management (JEM) Terekam Jejak, 1*(1).

Balafif, S. (2023). Penyesuaian model ketahanan siber UMKM di Indonesia dengan NIST Cybersecurity Framework. *Jurnal Informatika: Jurnal Pengembangan IT (JPIT), 8*(3).

Bawono, H. (2022). *Digital Preservation and Digital Records and Archives Management in Indonesia: Contextualization-Synthesis of Two Models Digital Preservation*. Jurnal Kearsipan, 17(2). https://doi.org/10.46836/jk.v17i2.257

Evitha, Y. (2024). Leading digital transformation: Strategies for higher education leaders in navigating online platforms, administrative services, and cybersecurity. *Al-Ishlah: Jurnal Pendidikan, 16*(2), 2645–2656. https://doi.org/10.35445/alishlah.v16i2.5614

Frank, R. D. (2021). Risk in trustworthy digital repository audit and certification. *Archival Science, 22*, 43–73. https://doi.org/10.1007/s10502-021-09366-z

Khadka, K., & Ullah, A. B. (2025). *Human factors in cybersecurity: An interdisciplinary review and framework proposal. International Journal of Information Security, 24*(3), Article 119. https://doi.org/10.1007/s10207-025-01032-0

Mahendra, V., & Soewito, B. (2023). Penerapan kerangka kerja NIST Cybersecurity dan CIS Controls sebagai manajemen risiko keamanan siber. *Techno.COM, 22*(3), 527–538.

Meghanandha, & Naik, U. (2025). *A comparative review of metadata, communication, content, and digital preservation standards in modern libraries*. *American Journal of Information Science and Technology, 9*(1), 24–33. https://doi.org/10.11648/j.ajist.20250901.13

Muliati, S. F., Supriadi, F., & Junaedi, D. I. (2025). Strategi manajemen risiko teknologi informasi berbasis studi literatur. *Jupiter: Publikasi Ilmu Keteknikan Industri, Teknik Elektro dan Informatika, 3*(2), 27–39. https://doi.org/10.61132/jupiter.v3i2.780

Nemec Zlatolas, L., Welzer, T., & Lhotska, L. (2024). *Data breaches in healthcare: Security mechanisms for attack mitigation*. *Cluster Computing, 27*(7), 8639–8654. https://doi.org/10.1007/s10586-024-04507-2

Nurfajriani, W. V., Ilhami, M. W., Mahendra, A., Sirodj, R. A., & Afgani, M. W. (2024). Triangulasi data dalam analisis data kualitatif. *Jurnal Ilmiah Wahana Pendidikan, 10*(17), 826–833. https://doi.org/10.5281/zenodo.13929272

Nurkarimah, I. (2025). Pengelolaan arsip digital: Tantangan dan strategi di era transformasi digital. *Maliki Interdisciplinary Journal (MIJ), 3*(6), 1625–1629.

O'Neill, A., Ahmad, A., & Maynard, S. (2021). *Cybersecurity incident response in organisations: A meta-level framework for scenario-based training*. arXiv. https://arxiv.org/abs/2108.04996

Peraturan Menteri Komunikasi dan Informatika Republik Indonesia Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. (2016). Kementerian Komunikasi dan Informatika.

Rahmaeisa, U. I., & Kurniawan, K. (2025). *Kearsipan digital: Transformasi dan tantangan di era teknologi informasi*. JIIP – Jurnal Ilmiah Ilmu Pendidikan, 8(11), 12852–12856. https://doi.org/10.54371/jiip.v8i11.9923

Repetto, M., Striccoli, D., Piro, G., & Santoro, F. (2021). *An autonomous cybersecurity framework for next-generation digital service chains*. Journal of Network and Systems Management, 29, Article 37. https://doi.org/10.1007/s10922-021-09607-7

Ryu, D., & Lee, S. (2024). *Enhancing cybersecurity in energy IT infrastructure through a layered defense approach to major malware threats.* Applied Sciences, 14(22), Article 10342. https://www.mdpi.com/2076-3417/14/22/10342

Sama, H., Licen, Saragi, J. S. D., Erline, M., Kelvin, Hartanto, Y., Winata, J., & Devalia, M. (2021). Studi komparasi framework NIST dan ISO 27001 sebagai standar audit dengan metode deskriptif studi pustaka. *RABIT: Jurnal Teknologi dan Sistem Informasi Univrab, 6*(2), 116–121. https://doi.org/10.36341/rabit.v6i2.1752

Sugiyono. (2019). *Metode penelitian kuantitatif, kualitatif, dan R&D*. Alfabeta.

Tan, T., & Soewito, B. (2022). Manajemen risiko serangan siber menggunakan framework NIST Cybersecurity di Universitas ZXC. *Journal of Information System, Applied, Management, Accounting and Research (JISAMAR), 6*(2), 411–422.

Tarumingkeng, R. C. (2025). Pelatihan dan pengembangan keahlian cybersecurity untuk SDM: Strategi, tantangan dan implementasi. *RUDYCT e-PRESS*.

Tekle, K. (2024). Barriers to effective electronic records management in public sector organizations in East Africa. *African Journal of Information and Knowledge Management, 2*(2), 45–55. https://doi.org/10.47604/ajikm.2733

Vervaet, A. (2023). MoniLog: An automated log-based anomaly detection system for cloud computing infrastructures. *arXiv*. https://arxiv.org/abs/2304.11940

Yuliani, W. (2018). *Metode penelitian deskriptif kualitatif dalam perspektif bimbingan dan konseling*. Quanta: Kajian Bimbingan dan Konseling dalam Pendidikan, 2(2), 83–91. https://doi.org/10.22460/q.v2i2p83-91.1641

Zulfirman, R. (2022). Implementasi metode outdoor learning dalam peningkatan hasil belajar siswa pada mata pelajaran Pendidikan Agama Islam di MAN 1 Medan. *Jurnal Penelitian, Pendidikan dan Pengajaran, 3*(2). https://doi.org/10.30596/jppp.v3i2.11758