Journal of Economic and Management (JEM) Terekam Jejak, Copyright © 2025
Vol. 2, Num. 3, 2025 (Special Edition)
https://jpm.terekamjejak.com/index.php/jeh
Author: **Muhammad Munawwar Xhalil Arifin, Purwanto Putra, Viola Dwi Putri Syarif**

Analisis Tingkat Keamanan Arsip Digital dalam Menghadapi Ancaman Keamanan Siber

ABSTRACT

According to a report by the National Cyber and Crypto Agency (BSSN, 2024), there were more than 400 million cyberattack attempts targeting government institutions and the education sector in Indonesia throughout 2023. Most of these attacks involved phishing, ransomware, and data leaks. This study used a descriptive qualitative method with a literature review approach. The primary data sources came from scientific journals, official agency reports, and international standard documents published between 2020 and 2024. A high level of digital archive security is characterized by the existence of clear and structured access control mechanisms. Access control not only serves to prevent unauthorized access but also to maintain the integrity of archives from unaccountable changes. ISO/IEC 27001 emphasizes that weak access control is a major factor in information security breaches, including in digital archive systems (ISO/IEC, 2013). This study concluded that the level of digital archive security in Indonesia is still considered medium. Although encryption and backup technology have been implemented, weaknesses remain in institutional policies and human resource awareness.

Keyword: Archive security, cyber threats, digital archives

ABSTRAK

Menurut laporan Badan Siber dan Sandi Negara (BSSN, 2024), terdapat lebih dari 400 juta upaya serangan siber yang menargetkan lembaga pemerintah dan sektor pendidikan di Indonesia sepanjang tahun 2023. Sebagian besar serangan tersebut berupa phishing, ransomware, dan kebocoran data (data leak). Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi literatur (literature review). Sumber data utama berasal dari jurnal ilmiah, laporan lembaga resmi, dan dokumen standar internasional yang diterbitkan antara tahun 2020–2024. Tingkat keamanan arsip digital yang tinggi ditandai oleh adanya mekanisme pengendalian akses yang jelas dan terstruktur. Pengendalian akses tidak hanya berfungsi untuk mencegah akses tidak sah, tetapi juga untuk menjaga keutuhan arsip dari perubahan yang tidak dapat dipertanggungjawabkan. ISO/IEC 27001 menekankan bahwa lemahnya kontrol akses merupakan salah satu faktor utama terjadinya pelanggaran keamanan informasi, termasuk pada sistem arsip digital (ISO/IEC, 2013).Penelitian ini menyimpulkan bahwa tingkat keamanan arsip digital di Indonesia masih tergolong menengah. Meskipun teknologi enkripsi dan backup sudah diterapkan, masih terdapat kelemahan pada kebijakan kelembagaan dan kesadaran sumber daya manusia.

Kata Kunci: Keamanan arsip, ancaman siber, arsip digital.

PENDAHULUAN

Transformasi digital dalam kerangka Revolusi Industri 4.0 telah mendorong perubahan mendasar dalam pengelolaan informasi dan pengetahuan organisasi, termasuk dalam praktik kearsipan. Digitalisasi arsip tidak lagi semata berorientasi pada efisiensi administratif, melainkan telah bergeser menjadi isu strategis yang berkaitan dengan keamanan data, ketahanan informasi, dan tata kelola risiko (Surya & Rosana, 2021).

Dalam konteks Indonesia, mandat digitalisasi arsip dilegitimasi melalui Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan dan diperkuat secara teknis melalui Peraturan Kepala ANRI Nomor 6 Tahun 2021 tentang Pengelolaan Arsip Elektronik. Namun, sejumlah penelitian menunjukkan bahwa implementasi regulasi tersebut belum sepenuhnya disertai dengan integrasi kebijakan keamanan informasi yang memadai (Silvia & Putra, 2025).

Arsip digital memiliki karakteristik kerentanan yang berbeda dari arsip fisik karena ketergantungannya pada sistem teknologi informasi dan jaringan. Ancaman terhadap arsip digital tidak hanya berupa kehilangan data, tetapi juga manipulasi informasi, kebocoran privasi, dan gangguan terhadap keberlanjutan layanan publik (Setiawan & Yuliyanti, 2020). Kondisi ini menjadi semakin kritis ketika arsip digital menyimpan data strategis dan dokumen vital masyarakat.

Penelitian Yuniastriana dan Putra (2025) menunjukkan bahwa digitalisasi arsip keluarga mampu berfungsi sebagai strategi mitigasi bencana non-fisik, terutama dalam melindungi dokumen vital dari risiko kehilangan total akibat bencana alam. Temuan ini menegaskan bahwa digitalisasi arsip memiliki dimensi perlindungan sosial dan ketahanan informasi, bukan sekadar efisiensi teknis. Namun, penelitian yang sama juga mengindikasikan bahwa praktik digitalisasi berbasis teknologi sederhana dan layanan cloud publik menyimpan potensi risiko keamanan apabila tidak didukung oleh kerangka pengamanan data yang sistematis (Yuniastriana & Putra, 2025).

Pada level institusi, kelemahan tata kelola arsip turut berkontribusi terhadap rendahnya tingkat keamanan arsip digital. Studi Silvia dan Putra (2025) menemukan bahwa keterbatasan kompetensi sumber daya manusia kearsipan,

belum optimalnya penerapan klasifikasi dan Jadwal Retensi Arsip (JRA), serta minimnya fasilitas preservasi berdampak pada kerentanan arsip, baik fisik maupun digital. Temuan ini memperkuat argumen bahwa keamanan arsip digital tidak dapat dipisahkan dari kapasitas organisasi dan kualitas manajemen arsip secara keseluruhan.

Ancaman siber terhadap sistem informasi publik semakin nyata dengan meningkatnya intensitas serangan digital. Laporan BSSN (2024) mencatat ratusan juta upaya serangan siber terhadap lembaga pemerintah dan sektor pendidikan, yang sebagian besar menargetkan sistem penyimpanan data dan informasi. Dalam konteks ini, arsip digital menjadi target strategis karena nilai informasinya yang tinggi dan sifatnya yang terpusat.

Dari perspektif kebijakan, lemahnya komunikasi publik dan absennya pendekatan kebijakan yang adaptif terhadap perkembangan teknologi dapat memperburuk risiko implementasi sistem digital. Ernawati et al. (2025) menunjukkan bahwa kebijakan teknologi yang tidak disertai strategi komunikasi yang efektif berpotensi menimbulkan resistensi dan persepsi negatif di kalangan masyarakat digital. Temuan ini relevan dalam pengelolaan arsip digital, khususnya ketika kebijakan keamanan arsip tidak diiringi dengan peningkatan literasi dan pemahaman pengguna.

Selain faktor kebijakan dan teknologi, dimensi manusia juga berperan penting dalam keamanan informasi. Studi Wiendari et al. (2025) menegaskan bahwa kesadaran, refleksi intrapersonal, dan kemampuan pengelolaan emosi berkontribusi terhadap pengambilan keputusan individu dalam menghadapi tekanan peran dan risiko. Dalam konteks organisasi, aspek ini berkorelasi dengan kesadaran keamanan (security awareness) dan kepatuhan terhadap prosedur pengelolaan arsip digital.

Berdasarkan state of the art tersebut, terlihat bahwa kajian kearsipan digital di Indonesia masih cenderung menempatkan aspek keamanan sebagai isu sekunder. Padahal, meningkatnya ancaman siber, kompleksitas tata kelola arsip, dan ketergantungan pada sistem digital menuntut pendekatan keamanan arsip yang lebih holistik dan terintegrasi. Kesenjangan inilah yang menjadi novelty

penelitian ini, yaitu dengan memosisikan keamanan arsip digital sebagai elemen inti dalam transformasi kearsipan digital.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan desain tinjauan literatur naratif terarah (directed narrative literature review) untuk menganalisis tingkat keamanan arsip digital, faktor kerentanan, serta strategi penguatan keamanan di lingkungan organisasi. Pendekatan ini dipilih karena fokus penelitian berada pada pemetaan temuan ilmiah (state of the art) dan penyusunan sintesis konseptual mengenai keamanan arsip digital, bukan pada pengujian hubungan kausal melalui statistik inferensial atau eksperimen. Selain itu, model tinjauan literatur memungkinkan peneliti mengidentifikasi pola argumentasi, kesenjangan riset (research gap), dan rekomendasi strategis yang dapat diturunkan dari studi-studi terdahulu (Putra, 2023; Wibowo & Putra, 2025).

Sumber data penelitian berupa artikel jurnal, buku, dan dokumen regulasi yang relevan dengan tema arsip digital, keamanan informasi, serta tata kelola kearsipan. Penelusuran literatur dilakukan melalui basis data akademik (misalnya Google Scholar) dengan kata kunci dalam bahasa Indonesia dan Inggris, seperti: *arsip digital*, *keamanan arsip*, *electronic records management*, *cloud storage*, *cyber security*, *data breach*, serta *kebijakan kearsipan elektronik*. Selain literatur ilmiah, penelitian juga menggunakan dokumen kebijakan sebagai rujukan normatif, terutama Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan yang menjadi landasan institusional pengelolaan arsip, termasuk pengamanan dan keberlanjutan arsip dalam konteks organisasi publik (Pemerintah Republik Indonesia, 2009).

Literatur dipilih menggunakan kriteria inklusi: (1) membahas pengelolaan arsip elektronik/digital pada organisasi publik/pendidikan/layanan; (2) memuat isu keamanan data (kerahasiaan,

integritas, ketersediaan), risiko kehilangan, atau ancaman pada penyimpanan digital/awan; (3) terbit pada rentang waktu yang relevan untuk menangkap dinamika transformasi digital kearsipan; dan (4) memiliki relevansi langsung dengan rumusan masalah penelitian. Literatur dikeluarkan (eksklusi) bila hanya membahas kearsipan fisik tanpa kaitan dengan sistem digital, atau tidak memberikan kontribusi konseptual terhadap dimensi keamanan.

Unit analisis penelitian adalah tema-tema temuan dalam literatur terkait keamanan arsip digital. Untuk menjaga konsistensi analisis, peneliti menggunakan kerangka analitis yang mengelompokkan temuan ke dalam tiga dimensi utama keamanan informasi: kerahasiaan (confidentiality), integritas (integrity), dan ketersediaan (availability), serta dimensi tata kelola kearsipan (kebijakan, prosedur, SDM, dan infrastruktur). Kerangka ini dipadukan dengan perspektif kearsipan tentang siklus hidup/rekod kontinum untuk menilai bagaimana risiko keamanan dapat muncul pada tahap penciptaan, penggunaan, penyimpanan, pemindahan, hingga preservasi jangka panjang (Putra, 2023; Schellenberg, 1956).

Analisis data dilakukan dengan analisis tematik melalui tahapan: (1) pengumpulan literatur dan ekstraksi informasi kunci; (2) pengkodean awal berdasarkan kategori: jenis risiko (phishing, ransomware, kebocoran data), titik rawan (akses, penyimpanan cloud, backup), serta faktor organisasi (SOP, kompetensi, infrastruktur); (3) pengelompokan kode menjadi tema besar; dan (4) sintesis tematik untuk merumuskan peta tingkat keamanan, faktor kerentanan, dan strategi perbaikan.

Dalam proses sintesis, penelitian juga membandingkan temuan lintas konteks: (a) konteks rumah tangga/komunitas sebagai mitigasi bencana melalui digitalisasi arsip keluarga—yang menekankan aspek penyelamatan dokumen vital namun rentan jika prosedur pengamanan cloud tidak sistematis (Apriani & Putra, 2025); (b) konteks organisasi layanan/publik yang menerapkan arsip elektronik untuk administrasi dan layanan, namun menghadapi tantangan integrasi prosedur dan pengamanan sistem (Wibowo & Putra, 2025; Putra et al., 2025); dan (c) konteks tata kelola kelembagaan yang menunjukkan bahwa keterbatasan SDM, SOP, dan sarana prasarana berkontribusi pada lemahnya

pengendalian arsip dan potensi risiko keamanan (Rahmad Harahap, 2020; Mutmainnah et al., 2020).

Untuk menjaga kredibilitas, penelitian menerapkan triangulasi sumber dengan membandingkan temuan dari berbagai jenis literatur (artikel empiris, buku rujukan, dan regulasi). Selain itu, peneliti melakukan *peer-checking* internal pada tahap kategorisasi tema dengan memastikan kesesuaian antara kutipan, kode, dan tema yang disusun. Ketepatan simpulan dijaga melalui prinsip keterlacakan argumen, yaitu setiap rekomendasi strategis harus diturunkan dari temuan literatur dan koheren dengan kerangka kearsipan (Putra, 2023; Sattar, 2021).

Hasil penelitian disajikan secara deskriptif-analitis dalam bentuk: (1) peta tema risiko dan kerentanan keamanan arsip digital; (2) matriks ringkas "kondisi yang dilaporkan literatur–titik rawan–dampak–mitigasi"; dan (3) rekomendasi strategi penguatan keamanan arsip digital yang mencakup kebijakan, prosedur, SDM, dan infrastruktur. Format ini dipilih agar pembaca memperoleh gambaran yang sistematis tentang kondisi keamanan arsip digital sekaligus langkah perbaikan yang dapat diadopsi secara bertahap.

HASIL DAN PEMBAHASAN

Peta Konseptual Keamanan Arsip Digital: Dari Rekod ke Risiko

Temuan literatur menunjukkan bahwa arsip digital bukan sekadar "file elektronik", melainkan rekod yang harus mempertahankan konteks penciptaan, struktur, serta relasi fungsionalnya. Karena itu, keamanan arsip digital tidak cukup dipahami sebagai keamanan *data*, tetapi juga keamanan nilai bukti dan keautentikan rekod (Duranti, 1998; Yusup & Subekti, 2021). Literatur kearsipan digital di Indonesia menegaskan bahwa transformasi pengelolaan arsip—termasuk penggunaan aplikasi kearsipan pemerintah seperti SRIKANDI—mempercepat layanan dan efisiensi, namun pada saat yang sama memperluas permukaan risiko, terutama terkait kontrol akses, integrasi SOP, dan disiplin

pencatatan metadata (Aprilia et al., 2025; Fadilah & Putra, 2024; Sari et al., 2024).

Pada dimensi standar, literatur memperlihatkan kecenderungan bahwa organisasi yang mengadopsi kerangka manajemen keamanan (mis. prinsip CIA triad dalam ISO/IEC 27001) memiliki struktur kontrol yang lebih jelas—mulai dari kebijakan, manajemen risiko, hingga pengendalian akses—dibanding organisasi yang hanya mengandalkan perlindungan teknis "seadanya" (ISO/IEC 27001, 2022; Stallings, 2021). Di ranah kearsipan, kerangka keamanan ini perlu diperluas dengan penekanan pada autentisitas dan integritas rekod sepanjang siklus hidupnya (Duranti, 1998; Putra et al., 2023).

Pembahasan terhadap hipotesis konseptual penelitian: Temuan di atas mendukung hipotesis bahwa kerentanan meningkat saat keamanan tidak diintegrasikan sebagai komponen inti sistem kearsipan, melainkan ditempatkan sebagai "tambahan teknis" pasca implementasi digital. Ketika digitalisasi dipahami hanya sebagai proses migrasi media (kertas → file), organisasi cenderung mengabaikan pengendalian akses berbasis fungsi, tata kelola retensi, dan audit trail—padahal ketiganya penting untuk menjaga integritas dan reliabilitas arsip (Siregar, 2021; Wahyuni, 2022).

Tingkat Penerapan Keamanan dan Titik Lemah Dominan

Berdasarkan sintesis 10 literatur (Tabel 1), tingkat keamanan arsip digital pada banyak organisasi cenderung berada pada level "proteksi dasar", yakni penggunaan firewall, enkripsi terbatas, dan backup, tetapi belum konsisten pada aspek kontrol berlapis seperti multi-factor authentication (MFA), *security monitoring* berbasis log, uji pemulihan (*disaster recovery test*), dan audit keamanan berkala (ISO/IEC 27001, 2022; Priyanto, 2020). Studi implementasi sistem e-arsip di satuan pendidikan menunjukkan bahwa adopsi aplikasi memang memperbaiki kerapian proses simpan-temu balik, tetapi sering diiringi kendala kapasitas operator, standar prosedur yang belum seragam, dan ketergantungan pada penyimpanan daring tanpa desain kontrol yang matang (Setiawan et al., 2025; Wulandari & Putra, 2024).

Temuan paling konsisten terkait titik lemah muncul pada tiga ranah berikut.

1. Faktor manusia (security awareness dan kepatuhan prosedur). Literatur menempatkan manusia sebagai titik rawan utama: kebiasaan kata sandi lemah, *phishing susceptibility*, dan keterlambatan pembaruan sistem. Rendahnya kesadaran keamanan membuat kontrol teknis yang baik sekalipun bisa dilompati melalui kesalahan pengguna (Simanjuntak, 2022). Temuan ini selaras dengan literatur organisasi yang menekankan perlunya penguatan kompetensi SDM kearsipan dan infrastruktur sebagai determinan kualitas pengelolaan arsip, termasuk ketika sistem bergerak ke digital (Wulandari & Putra, 2024). Dalam praktik kearsipan dinamis, berbagai studi juga menunjukkan bahwa keterbatasan SDM dan ketidakseragaman prosedur menurunkan konsistensi tata kelola arsip (Miharja & Putra, 2024; Herlinda & Haderiyah, 2023).
2. Kebijakan dan tata kelola (SOP, retensi, klasifikasi, audit). Sebagian instansi belum memiliki regulasi internal yang secara khusus mengatur keamanan arsip digital (Hidayat, 2022). Ketika organisasi menerapkan sistem digital tanpa SOP yang operasional, efeknya adalah praktik berbeda-beda antar unit, minim audit trail, dan kontrol akses yang tidak berbasis fungsi. Studi tentang kearsipan dinamis berbasis SRIKANDI memperlihatkan bahwa peningkatan efisiensi akan maksimal jika diikuti standardisasi prosedur, pembenahan tata kelola, dan dukungan manajerial (Fadilah & Putra, 2024; Sari et al., 2024). Hal ini juga sejalan dengan prinsip pengelolaan arsip vital dan dinamis yang menuntut disiplin retensi dan perlindungan aset informasi strategis (Makmur & Zuraida, 2023; Putra et al., 2020).
3. Infrastruktur dan teknologi (cloud, enkripsi, pemulihan bencana). Literatur menegaskan bahwa enkripsi dan tanda tangan digital efektif untuk menjaga kerahasiaan serta mencegah modifikasi tidak sah (Kurniawan & Rahmawati, 2021). Namun, ketergantungan pada *cloud* tanpa kontrol berlapis meningkatkan risiko kebocoran, terutama bila tidak ada MFA, manajemen hak akses, dan kebijakan *backup* off-site yang diuji secara berkala (ISO/IEC 27001, 2022; Nugroho et al., 2023). Dalam

konteks mitigasi bencana, praktik digitalisasi arsip keluarga (pemindaian + duplikasi ke Google Drive) terbukti bermanfaat melindungi dokumen vital dari kehilangan fisik, tetapi tetap perlu kerangka pengamanan agar "aman" tidak berhenti pada "tersalin", melainkan "terlindungi" (Apriani & Putra, 2025; Yuniastriana & Putra, 2025). Sejalan dengan itu, pendekatan mitigasi berbasis arsip (enkapsulasi, digital backup) diposisikan sebagai bagian dari strategi resiliensi komunitas yang memerlukan tata kelola penyimpanan dan akses yang jelas (Windah et al., 2024).

Pembahasan (mengikat ke tujuan 1 & 2): Temuan ini menjelaskan bahwa tingkat keamanan arsip digital ditentukan oleh keseimbangan antara kontrol teknis (enkripsi, akses), kontrol organisasi (SOP, audit, retensi), dan kontrol manusia (literasi keamanan). Ketidakseimbangan pada salah satu sisi menciptakan "celah dominan" yang dapat dimanfaatkan ancaman seperti ransomware dan phishing (Priyanto, 2020; ENISA, 2022).

Strategi Penguatan dan Model Integratif Keamanan Arsip Digital

Sintesis literatur memperlihatkan bahwa strategi peningkatan keamanan arsip digital paling efektif bila dirancang sebagai program berkelanjutan yang mengintegrasikan tata kelola dan teknologi, bukan respons insidental setelah terjadi insiden. Literatur keamanan informasi menekankan pendekatan berbasis risiko dan siklus perbaikan terus-menerus (Plan–Do–Check–Act) sebagaimana ditekankan dalam ISMS ISO/IEC 27001 (ISO/IEC 27001, 2022; Von Solms & Van Niekerk, 2013). Sementara itu, literatur kearsipan menegaskan bahwa strategi pengamanan harus melindungi autentisitas, reliabilitas, integritas, dan kegunaan rekod dalam jangka panjang (Duranti, 1998; Bawono, 2022).

Berdasarkan temuan (Sub-bab 4.1–4.2), artikel ini merumuskan model integratif yang terdiri dari tiga lapisan—teknologi, kebijakan, dan manusia—dengan rincian strategi sebagai berikut.

(a) Lapisan Kebijakan dan Tata Kelola

1. Adopsi ISMS berbasis ISO/IEC 27001 sebagai kerangka kerja manajemen risiko, disertai penetapan peran, proses audit, dan kontrol akses. (ISO/IEC 27001, 2022).
2. Standardisasi SOP kearsipan digital: klasifikasi, retensi, prosedur akses, audit trail, dan mekanisme pemulihan bencana. Temuan implementasi SRIKANDI menunjukkan bahwa SOP yang operasional menjadi kunci konsistensi lintas unit (Aprilia et al., 2025; Sari et al., 2024).
3. Penguatan tata kelola arsip vital dan dinamis agar keamanan tidak hanya melindungi "arsip lama", tetapi melindungi rekod aktif yang bernilai strategis dan rawan disalahgunakan (Makmur & Zuraida, 2023; Putra et al., 2020).

(b) Lapisan Teknologi dan Infrastruktur

1. Enkripsi kuat dan manajemen kunci untuk melindungi kerahasiaan dan mengurangi dampak kebocoran data (Kurniawan & Rahmawati, 2021).
2. MFA dan prinsip least privilege pada seluruh akun pengelola arsip digital, terutama bila memanfaatkan penyimpanan cloud (ISO/IEC 27001, 2022; Nugroho et al., 2023).
3. Backup 3-2-1 dan uji pemulihan berkala (tiga salinan, dua media berbeda, satu off-site) untuk menghadapi ransomware dan kegagalan sistem—serangan yang diidentifikasi sebagai ancaman utama terhadap arsip digital (Priyanto, 2020; Behl & Behl, 2017).
4. Monitoring berbasis log dan deteksi anomali; pemanfaatan AI dapat membantu mendeteksi aktivitas mencurigakan secara real-time, namun tetap harus ditopang kebijakan akses dan respons insiden (Rahardjo, 2023; ISO/IEC 27001, 2022).

(c) Lapisan Manusia dan Budaya Keamanan

1. Pelatihan rutin keamanan siber (phishing drill, password hygiene, manajemen perangkat) untuk menaikkan *security awareness* dan kepatuhan pengguna (Simanjuntak, 2022).

2. Penguatan kompetensi SDM dan dukungan organisasi, karena kualitas pengelolaan arsip digital sangat dipengaruhi kapasitas SDM dan kesiapan infrastruktur (Wulandari & Putra, 2024; Kuswantoro & Utami, 2025).
3. Literasi informasi dan manajemen pengetahuan sebagai basis budaya organisasi: pemahaman nilai arsip, risiko informasi, dan disiplin dokumentasi untuk menjaga kualitas rekod dan keamanannya (Hendrawan & Putra, 2022; Wahyuni, 2022).

Pembahasan (mengikat ke tujuan 3): Model integratif ini memperkuat hipotesis penelitian bahwa penguatan keamanan arsip digital harus bersifat holistik. Literatur mitigasi bencana berbasis arsip keluarga memperlihatkan bahwa keberhasilan digitalisasi sebagai perlindungan sangat ditentukan oleh praktik pengelolaan (klasifikasi, duplikasi) dan tata kelola akses (Apriani & Putra, 2025; Yuniastriana & Putra, 2025). Dengan analogi yang sama, pada level institusi, keamanan arsip digital akan efektif ketika digitalisasi disertai tata kelola, kontrol akses, dan budaya keamanan sebagai kebiasaan kerja.

KESIMPULAN

Transformasi kearsipan menuju arsip digital terbukti membawa manfaat efisiensi dan aksesibilitas, tetapi sekaligus memperluas spektrum risiko karena arsip digital tetap harus memenuhi prinsip kearsipan—autentisitas, reliabilitas, integritas, dan kegunaan—sepanjang siklus hidupnya. Sintesis literatur menunjukkan bahwa keamanan arsip digital tidak cukup dipahami sebagai proteksi file, melainkan perlindungan nilai-bukti rekod melalui tata kelola, standar, dan kontrol yang menjaga konteks serta jejak perubahan arsip. Dengan demikian, keamanan arsip digital harus diposisikan sebagai komponen inti transformasi digital kearsipan, bukan pelengkap teknis setelah sistem berjalan.

Hasil kajian memperlihatkan bahwa tingkat keamanan di banyak organisasi masih berada pada level proteksi dasar (misalnya backup dan pengamanan umum), sementara kontrol berlapis seperti MFA, audit berkala,

pengelolaan akses berbasis fungsi, serta pemantauan log belum konsisten diterapkan. Titik lemah dominan muncul pada tiga ranah yang saling menguatkan: faktor manusia (kesadaran dan kepatuhan keamanan rendah), kelemahan kebijakan-tata kelola (SOP, retensi, klasifikasi, audit trail belum operasional), serta ketergantungan infrastruktur (terutama cloud) tanpa desain pengamanan berlapis dan uji pemulihan yang memadai. Pola ini menjelaskan mengapa ancaman seperti phishing dan ransomware berpotensi berdampak serius pada kerahasiaan, integritas, dan ketersediaan arsip digital.

Berdasarkan temuan tersebut, strategi peningkatan keamanan arsip digital perlu dirancang secara holistik melalui model integratif tiga lapisan: kebijakan-tata kelola (ISMS/ISO 27001, SOP, audit, retensi), teknologi (enkripsi, MFA, backup 3-2-1, monitoring dan deteksi anomali), serta manusia (pelatihan rutin, budaya keamanan, penguatan kompetensi SDM). Implementasi strategi ini diharapkan tidak hanya menutup celah teknis, tetapi juga memperkuat ketahanan arsip digital sebagai infrastruktur informasi yang kredibel, aman, dan berkelanjutan. Ke depan, penelitian empiris pada konteks lembaga tertentu diperlukan untuk menguji efektivitas model integratif ini dan memetakan prioritas kontrol keamanan yang paling berdampak.

DAFTAR PUSTAKA

Apriani, R., & Putra, P. (2025). Pentingnya menjaga arsip keluarga serta tempat yang sesuai untuk menyimpan arsip keluarga. *Journal of GLAM Terekam Jejak, 1*(2), 118–133.

Aprilia, A., Dakir, D., & Riyadi, S. (2025). Pengelolaan kearsipan dinamis berbasis aplikasi SRIKANDI pada bidang pendidikan madrasah di Kanwil Kemenag Provinsi Kalimantan Tengah. *Jurnal Pendidikan Indonesia (JAPENDI), 6*(3), 1615–1624.

Bawono, H. (2022). Digital preservation and digital records and archives management in Indonesia: Contextualization-synthesis of two models digital preservation. *Jurnal Kearsipan, 17*(2), 121–135.

Behl, A., & Behl, K. (2017). Ransomware: A growing menace to digital information assets. *Computers & Security*.

Duranti, L. (1998). *Diplomatics: New uses for an old science*. Scarecrow Press.

ENISA. (2022). *Threat landscape for the public sector*. European Union Agency for Cybersecurity.

Ernawati, L., Kartika, T., Utaridah, N., Putra, P., & Besar, I. (2025). Kebijakan TKDN dan IMEI dalam sorotan media: Studi framing dan persepsi milenial terhadap iPhone 16. *J-IKA: Jurnal Ilmu Komunikasi Fakultas Ilmu Komunikasi Universitas BSI Bandung, 12*(2), 70–77.

Fadilah, M., & Putra, P. (2024). Transformasi praktik pengelolaan arsip dinamis melalui aplikasi SRIKANDI: Studi kualitatif efek implementasi pada efisiensi dan persepsi pengguna. *Prosiding Seminar Nasional Hukum Ilmu Sosial dan Ilmu Politik*, 1, 282–295.

Hendrawan, M. R., & Putra, P. (2022). *Integrasi manajemen pengetahuan dan literasi informasi: Pendekatan konsep dan praktik*. Universitas Brawijaya Press.

Herlinda, S. A. A., & Haderiyah. (2023). Pengelolaan arsip dinamis pada Dinas Pendidikan dan Kebudayaan Kabupaten Balangan. *Sentri: Jurnal Riset Ilmiah, 3*(4), 214–224.

ISO/IEC. (2022). *ISO/IEC 27001:2022 Information security management systems—Requirements*. International Organization for Standardization.

Kurniawan, A., & Rahmawati, S. (2021). Enkripsi data dan tanda tangan digital dalam perlindungan arsip. *Jurnal Keamanan Informasi*.

Kuswantoro, A., & Utami, L. P. T. (2025). Records management at the Archives and Library Service of Kebumen Regency: Its maintenance, utilization,

and challenges. *Khizanah Al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, dan Kearsipan, 13*(1), 113–125.

Makmur, S., & Zuraida, S. (2023). *Penyelenggaraan kearsipan dinamis: Pengelolaan arsip aktif, in-aktif dan arsip vital pejabat negara hasil pilkada 2020*. Diva Pustaka.

Miharja, J., & Putra, P. (2024). Pengelolaan arsip dinamis pada Sub Bagian Tata Usaha Cabang Dinas Kehutanan Wilayah II Purwakarta. *Journal of Economic and Management (JEM) Terekam Jejak, 1*(1), 1–12.

Muhidin, S. A., & Winata, H. (2016). *Manajemen kearsipan: Untuk organisasi publik, bisnis, sosial, politik, dan kemasyarakatan*. PT Gramedia Pustaka Utama.

Mutmainnah, S., et al. (2020). Manajemen arsip perguruan tinggi dilengkapi dengan jadwal retensi arsip perguruan tinggi. *Jurnal Manajemen Kearsipan Perguruan Tinggi, 10*(2), 34–46.

Pemerintah Republik Indonesia. (2009). *Undang-Undang Republik Indonesia Nomor 43 Tahun 2009 tentang Kearsipan*. Kementerian Hukum dan HAM.

Priyanto. (2020). Analisis ransomware sebagai ancaman utama arsip digital. *Jurnal Keamanan Siber*.

Putra, P. (2023). Memahami lebih dalam tentang teori siklus hidup, model kontinum rekod dan konsep arsip total. *Jurnal Ilmu Informasi, Perpustakaan dan Kearsipan, 25*(2).

Putra, P., Khairunnisa, M., & Putri, I. (2025). Perbandingan efisiensi dan efektivitas pengelolaan rekod elektronik dan konvensional di UPT Perpustakaan Universitas Lampung. *JEVIEF, 4*(1), 10–19.

Putra, P., Purnamayanti, A., & Maryani, E. (2020). Efisiensi penyimpanan dan aksesibilitas arsip vital dalam penyelenggaraan kearsipan universitas di UPT Kearsipan UNILA. *Journal of Documentation and Information Science*, 6003.

Rahardjo. (2023). Pemanfaatan kecerdasan buatan untuk deteksi ancaman siber. *Jurnal Teknologi Informasi*.

Rahmad Harahap, W. (2020). Profesi arsiparis sebagai sumber daya manusia dalam mengelola arsip statis. *Jurnal Pengelolaan Arsip dan Informasi, 12*(5), 56–71.

Sari, A. S., Ruhana, F., & Karno, K. (2024). Implementasi kebijakan sistem informasi kearsipan dinamis terintegrasi (SRIKANDI) di Komisi Pemberantasan Korupsi Republik Indonesia. *Syntax Literate: Jurnal Ilmiah Indonesia, 9*(1), 55–68.

Setiawan, A., & Yuliyanti, D. (2020). Keamanan informasi dalam pengelolaan arsip digital. *Jurnal Kearsipan dan Informasi, 5*(2), 45–58.

Setiawan, U. S. M. A., Putra, P., & Syarif, V. D. P. (2025). Implementasi aplikasi E-Arsip di lingkungan SMAN 2 Mesuji Raya. *Journal of GLAM Terekam Jejak, 1*(1), 105–113.

Simanjuntak. (2022). Faktor manusia sebagai titik lemah keamanan arsip digital. *Jurnal Keamanan Informasi*.

Siregar, D. R. (2021). *Pengelolaan arsip berbasis teknologi informasi*. Remaja Rosdakarya.

Stallings, W. (2021). *Effective cybersecurity: A guide to using best practices and standards*. Addison-Wesley.

Surya, R., & Rosana, E. (2021). Transformasi digital dalam pengelolaan arsip organisasi. *Jurnal Administrasi Publik dan Informasi, 9*(1), 23–34.

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers & Security, 38*, 97–102.

Wahyuni, E. (2022). *Manajemen kearsipan digital di era e-government*. Deepublish.

Wibowo, M. S., & Putra, P. (2025). Manajemen arsip elektronik pada CV Ayasha Hijab. *Jurnal Pengabdian Masyarakat (JPM) Terekam Jejak, 2*(3), 80–98.

Wiendari, N., Kartika, T., Ashaf, A. F., Putra, P., & Utaridah, N. (2025). A phenomenological study of women's expectations: Intrapersonal communication in living dual roles. *Jurnal Hawa: Studi Pengarusutamaan Gender dan Anak, 7*(2).

Windah, A., Putra, P., Purnamayanti, A., & Maryani, E. (2024). Penguatan resiliensi komunitas melalui enkapsulasi arsip: Strategi integral mitigasi bencana dan adaptasi terhadap perubahan iklim di Desa Negeri Katon. *Jurnal Pengabdian Masyarakat (JPM) Terekam Jejak, 1*(1), 1–15.

Wulandari, T. W., & Putra, P. (2024). Analisis peran kompetensi SDM dan infrastruktur teknologi terhadap kualitas pengelolaan arsip dinamis. *Journal of Economic and Management (JEM) Terekam Jejak, 1*(1), 1–17.

Yuniastriana, K., & Putra, P. (2025). Digitalisasi arsip keluarga dalam upaya mitigasi bencana longsor di Kabupaten Temanggung. *Journal of Education and Humanities (JEH) Terekam Jejak, 1*(3), 129–141.

Yusup, M., & Subekti, A. (2021). Konsep dan manajemen arsip digital. *Jurnal Kearsipan*.