Z-ARSIP: MODEL KEAMANAN ARSIP ELEKTRONIK BERBASIS ZERO TRUST KIPLING DAN ASCON LIGHTWEIGHT CRYPTOGRAPHY UNTUK MENJAGA AUTENTISITAS DAN INTEGRITAS DOKUMEN DIGITAL

Abstrak

Transformasi digital pengelolaan arsip telah mengubah praktik kearsipan dari berbasis kertas menjadi berbasis sistem elektronik. Pergeseran ini meningkatkan efisiensi, namun memunculkan risiko baru berupa akses tidak sah, manipulasi dokumen, kebocoran data, hingga lemahnya pembuktian autentisitas dan integritas arsip digital. Pendekatan keamanan konvensional yang hanya bertumpu pada autentikasi berbasis *login* dan kontrol berbasis peran *(role-based access control)* belum cukup menjawab kompleksitas ancaman saat ini, terutama dalam konteks lembaga strategis seperti Bank Indonesia yang mengelola arsip vital bernilai pembuktian tinggi. Penelitian ini merancang Z-ARSIP, sebuah model konseptual keamanan arsip elektronik yang mengintegrasikan enam komponen utama: (1) ISO 15489-1:2016 sebagai fondasi pengelolaan arsip yang autentik, andal, utuh, dan dapat digunakan; (2) Zero Trust Kipling 5W+1H sebagai metode evaluasi konteks akses; (3) *Risk-Based Access Control* dan *Policy Engine* PIP/PAP/PDP/PEP sebagai mekanisme keputusan akses berbasis skor risiko; (4) *Zero Trust Integrity Score* (ZTIS) sebagai indikator kepercayaan integritas arsip; (5) Ascon *Lightweight Cryptography* (Ascon-AEAD128 dan Ascon-Hash256) untuk enkripsi, autentikasi, serta verifikasi *fingerprint* dokumen; dan (6) *Integrity Assurance Layer* yang mencakup *integrity check*, *tamper detection*, *chain of custody*, dan *audit log integrity*. Penelitian dilakukan dengan pendekatan kualitatif konseptual berbasis studi literatur dan pemodelan arsitektur. Hasilnya adalah sebuah kerangka keamanan arsip elektronik yang tidak hanya memverifikasi identitas pengguna, tetapi juga menilai konteks akses, menghitung risiko, mengukur tingkat kepercayaan integritas dokumen, serta menjaga jejak kustodi digital. Z-ARSIP berkontribusi pada pengembangan kajian arsip digital dengan menyatukan dimensi *policy*, *people*, dan *technology* dalam satu model keamanan terpadu.

Kata kunci: *zero trust kipling*; arsip elektronik; ISO 15489-1:2016; Ascon *lightweight cryptography*; *Zero Trust Integrity Score*; autentisitas dan integritas

1. PENDAHULUAN

Transformasi digital telah mengubah lanskap pengelolaan arsip secara fundamental. Praktik kearsipan yang dahulu didominasi oleh dokumen fisik kini bergeser menuju sistem arsip elektronik yang menjanjikan kecepatan layanan, efisiensi penyimpanan, dan kemudahan temu kembali informasi. Pergeseran ini bukan sekadar pemindahan media, melainkan perubahan paradigma dalam memperlakukan arsip sebagai aset informasi sekaligus alat bukti akuntabilitas organisasi. Dalam konteks lembaga strategis seperti Bank Indonesia, arsip elektronik menjadi tulang punggung

memori kelembagaan yang menopang kebijakan moneter, sistem pembayaran, dan stabilitas sistem keuangan, sehingga keamanan dan keandalannya menempati posisi yang sangat krusial (Ramudin, 2020).

Arsip elektronik berperan sekaligus sebagai sumber informasi, bukti hukum, dan ingatan kolektif organisasi. Standar internasional menegaskan bahwa arsip dianggap sebagai bukti otoritatif aktivitas bisnis ketika ia memiliki karakteristik *authenticity*, *reliability*, *integrity*, dan *usability* (Thaanyane et al., 2025). Karakter inilah yang membedakan arsip dari informasi biasa, dan karakter pula yang paling rentan tergerus ketika arsip berpindah ke ranah digital. Berbeda dengan dokumen kertas yang dapat ditandai dengan stempel atau tanda tangan basah, dokumen elektronik membutuhkan mekanisme khusus untuk mempertahankan keasliannya karena ia sangat mudah disalin, dimodifikasi, dan disebarkan tanpa jejak.

Tantangan terbesar dalam pengelolaan arsip digital saat ini meliputi keamanan akses, autentisitas, integritas, legalitas, perlindungan data pribadi, hingga preservasi jangka panjang. Studi pada Badan Perpustakaan dan Arsip Daerah DKI Jakarta menunjukkan bahwa banyak instansi belum siap menjaga otentisitas arsip dinamis elektronik, antara lain karena belum diterapkannya tanda tangan digital, lemahnya enkripsi, dan tidak adanya pembatasan akses berdasarkan tingkat kerahasiaan dokumen (Mayesti & Hanriarseto, n.d.). Konteks lembaga publik di Indonesia juga menunjukkan pola serupa pada level keamanan informasi. Marliana et al. (2024) dalam analisis kesenjangan ISO/IEC 27001:2013 di Badan Informasi Geospasial menemukan bahwa hanya sekitar 23 persen persyaratan utama dan 74 persen kontrol keamanan informasi yang terpenuhi pada sistem Ina-geoportal sebagai sistem elektronik strategis. Temuan serupa dilaporkan Thaanyane et al. (2025) di lingkungan perguruan tinggi, di mana praktik manajemen arsip masih jauh dari kesesuaian dengan ISO 15489-1:2016. Kondisi ini menegaskan adanya kesenjangan antara kebutuhan keamanan arsip digital dan kapasitas sistem yang berlaku di banyak organisasi.

Pendekatan keamanan konvensional yang mengandalkan *perimeter defense*, autentikasi *login*, dan *Role-Based Access Control* (RBAC) terbukti tidak memadai untuk menghadapi ancaman modern. Rose et al. (2020) menjelaskan bahwa model perimeter mengasumsikan entitas di dalam jaringan dapat dipercaya secara implisit asumsi yang runtuh ketika munculnya *bring your own device* (BYOD), kerja jarak jauh, layanan berbasis awan, dan ancaman dari dalam (*insider threats*). Tinjauan multivokal Ghasemshirazi et al. (2023) bahkan menyimpulkan bahwa kegagalan model perimeter merupakan masalah sistemik, bukan sekadar masalah implementasi, sehingga organisasi perlu menggeser paradigma keamanannya secara mendasar dari berbasis batas menjadi berbasis verifikasi berkelanjutan. RBAC bersifat statis dan tidak mampu menyesuaikan keputusan akses dengan konteks waktu, lokasi, perangkat, atau perilaku pengguna, sehingga membuka celah bagi pergerakan lateral dan penyalahgunaan hak akses. Dalam pengelolaan arsip elektronik, kelemahan ini berarti bahwa sekali pengguna berhasil masuk, ia dapat membuka berbagai dokumen lintas klasifikasi tanpa evaluasi tambahan terhadap konteks akses.

ISO 15489-1:2016 hadir sebagai standar internasional yang menggariskan prinsip pengelolaan arsip agar tetap autentik, andal, utuh, dan dapat digunakan (Thaanyane et al., 2025). Standar ini menempatkan arsip sebagai bukti aktivitas bisnis yang harus dikelola melalui kebijakan, sistem, dan proses yang terdefinisi. Bank Indonesia menjadi salah satu lembaga di Indonesia yang secara konsisten menerapkan standar ini melalui kebijakan Manajemen Dokumen Bank Indonesia (Ramudin, 2020). Meski demikian, ISO 15489-1:2016 hanya memberikan kerangka prinsip dan tidak menjabarkan mekanisme teknis untuk menjaga keempat karakter arsip tersebut di lingkungan digital, sehingga diperlukan pelapis teknologi keamanan yang relevan.

Di sinilah Zero Trust Architecture (ZTA) menjadi sangat relevan. ZTA adalah paradigma keamanan yang berpegang pada prinsip "*never trust, always verify*", yaitu tidak ada pengguna, perangkat, atau sistem yang dipercaya secara implisit, baik di dalam maupun di luar perimeter organisasi (Rose et al., 2020). Tinjauan sistematis Mushtaq et al. (2025) atas 74 publikasi ZTA lintas domain mencatat bahwa kontrol akses, autentikasi, dan otorisasi merupakan komponen ZTA yang paling matang penerapannya, sementara aspek auditing, orkestrasi, dan persepsi lingkungan masih kurang dieksplorasi—celah yang justru menjadi titik fokus penelitian ini. Prinsip ZTA diperkuat oleh metodologi Zero Trust Kipling (ZT-Kipling) yang dirumuskan dalam ETSI TS 104 102 (2025), yaitu pendekatan yang mewajibkan setiap permintaan akses dievaluasi melalui enam pertanyaan klasik *what*, *why*, *when*, *how*, *where*, dan *who* untuk memberikan transparansi dan eksplikabilitas atas setiap interaksi terhadap aset yang dilindungi. Penerapan ZTA pada lembaga dengan tingkat sensitivitas data tinggi telah terbukti dalam berbagai konteks; Chen et al. (2021) merancang sistem keamanan berbasis Zero Trust untuk layanan kesehatan pintar berbasis 5G dengan empat dimensi (subjek, objek, perilaku, lingkungan) yang menghasilkan autentikasi berkelanjutan dan kontrol akses granular pada data dan layanan kritis. Pengalaman ini menunjukkan bahwa ZTA dapat diadaptasi untuk lembaga lain dengan profil aset bernilai tinggi, termasuk lembaga kearsipan.

Untuk menerjemahkan evaluasi kontekstual menjadi keputusan akses yang konkret, dibutuhkan *Risk-Based Access Control* yang ditopang oleh *Policy Engine*. Shaikh et al. (2012) memperlihatkan bahwa Policy Decision Point (PDP) dapat mengintegrasikan informasi dari Policy Information Point (PIP) untuk menghitung skor kepercayaan dan risiko sebelum memberikan keputusan kepada Policy Enforcement Point (PEP). Mao et al. (2025) lebih lanjut menunjukkan bahwa integrasi Attribute-Based Access Control dengan evaluasi kepercayaan dinamis pada ZTA mampu meningkatkan akurasi kontrol akses hingga 96,8 persen pada lingkungan awan. Kerangka PIP/PAP/PDP/PEP karenanya menjadi tulang punggung keputusan akses arsip yang dapat menyesuaikan diri dengan konteks dan klasifikasi dokumen.

Namun, keamanan arsip tidak berhenti pada pengaturan akses. Aspek lain yang sama pentingnya adalah kepercayaan terhadap integritas arsip itu sendiri. Atas dasar itu penelitian ini memperkenalkan *Zero Trust Integrity Score* (ZTIS), sebuah skor kepercayaan integritas yang dihitung dari hasil *integrity check*, konsistensi metadata, validitas *chain of custody*, integritas *audit log*, dan indikasi *tampering*. ZTIS

memberikan dimensi baru: bukan hanya menanyakan "apakah pengguna berhak mengakses?" tetapi juga "apakah arsip yang akan diakses masih dapat dipercaya?". Kehadiran ZTIS menjadikan integritas arsip sebagai variabel dinamis dalam proses pengambilan keputusan akses, bukan sekadar atribut pasif yang diasumsikan selalu valid. Dalam model Z-ARSIP, akses arsip hanya diberikan apabila nilai Risk Score berada di bawah ambang risiko yang ditentukan dan nilai ZTIS menunjukkan arsip berada pada status terpercaya *(trusted record)*. Untuk mendukungnya, dibutuhkan *Integrity Assurance Layer* yang menggabungkan *tamper detection*, pencatatan *chain of custody* yang konsisten, dan *audit log* yang dapat diverifikasi (Daah et al., 2026).

Pada lapis kriptografi, penelitian ini mengusulkan penggunaan Ascon, algoritma *lightweight cryptography* yang dipilih NIST sebagai standar pada tahun 2023 setelah seleksi panjang terhadap berbagai kandidat (Dobraunig et al., 2021; Kaur et al., 2025). Ascon-AEAD128 menyediakan enkripsi sekaligus autentikasi data, sementara Ascon-Hash256 dapat dimanfaatkan untuk verifikasi *fingerprint* dokumen. Keunggulan Ascon terletak pada efisiensi komputasi, konsumsi sumber daya rendah, serta ketahanannya terhadap *side-channel attack*, sehingga relevan diterapkan pada sistem kearsipan yang melibatkan banyak titik akses dan perangkat dengan kapasitas beragam (Khan et al., 2024; Sarasa Laborda et al., 2025).

Di tengah berbagai studi tentang ZTA, kontrol akses berbasis risiko, *lightweight cryptography*, dan pengelolaan arsip, belum banyak penelitian yang mengintegrasikan keseluruhan komponen tersebut secara terpadu dalam satu model keamanan arsip elektronik. Inilah celah yang ingin diisi oleh Z-ARSIP. Tujuan penelitian ini adalah merancang model konseptual keamanan arsip elektronik yang mengintegrasikan ISO 15489-1:2016, Zero Trust Kipling 5W+1H, *Risk-Based Access Control*, *Policy Engine* PIP/PAP/PDP/PEP, *Zero Trust Integrity Score*, Ascon *Lightweight Cryptography*, dan *Integrity Assurance Layer* untuk menjaga autentisitas, integritas, kerahasiaan, dan akuntabilitas dokumen digital pada lembaga strategis, dengan Bank Indonesia sebagai konteks ilustratif.

2. METODE PENELITIAN

2.1 Pendekatan dan Jenis Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian *conceptual research* yang bertujuan menghasilkan rancangan model keamanan arsip elektronik. Pendekatan kualitatif dipilih karena penelitian berfokus pada pemahaman mendalam terhadap pokok permasalahan dan informasi terkait pengelolaan arsip elektronik, sebagaimana digunakan dalam kajian-kajian kearsipan lain yang sejenis (Mayesti & Hanriarseto, 2015; Ramudin, 2019). Penelitian konseptual diarahkan untuk menyusun kerangka teoretis dan arsitektural yang mengintegrasikan beberapa standar dan teknologi keamanan ke dalam satu model terpadu, bukan untuk menguji implementasi sistem secara empiris pada lingkungan operasional. Z-ARSIP, dengan demikian, diposisikan sebagai model konseptual atau prototipe akademik yang dapat menjadi rujukan bagi lembaga strategis pengelola arsip vital, dengan Bank Indonesia

digunakan sebagai konteks ilustratif karena lembaga ini telah menerapkan ISO 15489-1:2016 dan memiliki kompleksitas pengelolaan arsip yang representatif (Ramudin, 2019).

Kerangka berpikir penelitian mengikuti logika *design science research* yang lazim digunakan dalam kajian sistem informasi dan keamanan siber, yaitu perancangan artefak konseptual sebagai jawaban atas suatu masalah yang teridentifikasi, kemudian dianalisis kelayakannya melalui pendekatan teoretis dan logis (Mushtaq et al., 2025). Artefak yang dihasilkan dalam penelitian ini berupa kerangka arsitektur Z-ARSIP, formula skor risiko *(risk score)*, formula *Zero Trust Integrity Score* (ZTIS), dan alur pengambilan keputusan akses berbasis 5W+1H.

2.2 Sumber Data

Sumber data terdiri atas data sekunder yang diperoleh melalui studi literatur dan studi dokumen. Studi literatur merupakan metode pengumpulan data yang umum digunakan dalam penelitian sosial dan kearsipan untuk menelusuri data historis maupun perkembangan teoretis suatu kajian (Kuswantoro, 2018). Literatur yang digunakan mencakup tiga kelompok besar. Pertama, literatur regulasi dan standar yang meliputi ISO 15489-1:2016, NIST Special Publication 800-207 tentang Zero Trust Architecture, ETSI TS 104 102 tentang ZT-Kipling Methodology, NIST Lightweight Cryptography Standard untuk Ascon, Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, serta Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi.

Kedua, literatur ilmiah berupa artikel jurnal terindeks yang membahas Zero Trust Architecture, *risk-based access control*, *attribute-based access control*, *policy engine*, *lightweight cryptography*, dan integrasi *blockchain* untuk *audit log* (Buck et al., 2021; Daah et al., 2026; Dobraunig et al., 2021; Kaur et al., 2025; Mao et al., 2025; Rose et al., 2020). Ketiga, literatur kearsipan dan keamanan informasi yang membahas autentisitas, integritas, dan pengelolaan arsip digital di Indonesia (Ismayati, 2014; Marliana et al., 2024; Mayesti & Hanriarseto, 2015; Ramudin, 2019). Data dokumen diperoleh dari publikasi resmi terkait pengelolaan arsip pada lembaga negara, khususnya yang menerapkan standar internasional ISO 15489-1:2016.

2.3 Tahapan Penelitian

Penelitian dilaksanakan dalam lima tahap yang saling terhubung secara iteratif. Tahap pertama adalah *problem identification*, yaitu identifikasi celah penelitian berdasarkan studi literatur tentang keterbatasan pendekatan keamanan arsip elektronik konvensional. Tahap ini menghasilkan rumusan masalah berupa lemahnya integrasi antara prinsip pengelolaan arsip, evaluasi konteks akses, kontrol akses berbasis risiko, penilaian integritas arsip, dan kriptografi ringan dalam satu model.

Tahap kedua adalah *requirement formulation*, yakni perumusan kebutuhan model berdasarkan keempat karakter arsip dalam ISO 15489-1:2016 (autentik, andal, utuh, dan dapat digunakan) serta tujuh prinsip Zero Trust Architecture (Rose et al.,

2020). Pada tahap ini ditetapkan bahwa model harus mampu menjawab persoalan akses, integritas, dan akuntabilitas secara bersamaan.

Tahap ketiga adalah *conceptual design*, yaitu perancangan arsitektur Z-ARSIP yang terdiri atas enam lapisan, yakni *records management layer*, *context awareness layer*, *policy and decision layer*, *integrity layer* (ZTIS), *cryptographic layer* (Ascon), dan *integrity assurance layer*. Pada tahap ini dirumuskan formula skor risiko sebagai penjumlahan bobot enam komponen kontekstual (sensitivitas dokumen, peran pengguna, perangkat, lokasi, waktu, dan aksi) serta formula ZTIS sebagai penjumlahan empat indikator integritas dikurangi indikator manipulasi.

Tahap keempat adalah *workflow design*, yakni penyusunan alur sistem dari permintaan akses, pengisian kuesioner ZT-Kipling 5W+1H, evaluasi PIP, perhitungan PDP, eksekusi PEP, perlindungan kriptografis melalui Ascon, hingga pencatatan *audit log* dan pemantauan *integrity assurance layer*. Alur ini mengadaptasi kerangka XACML yang umum digunakan dalam sistem ABAC dan ZTA (Mao et al., 2025).

Tahap kelima adalah *conceptual validation*, yaitu validasi konseptual model melalui penyandingan dengan literatur dan standar yang relevan. Validasi dilakukan dengan menilai kesesuaian model terhadap empat karakter arsip ISO 15489-1:2016, tujuh prinsip ZTA, kriteria ZT-Kipling, dan ketentuan hukum nasional (UU Kearsipan, UU ITE, UU PDP). Pendekatan validasi ini sejalan dengan praktik *systematic literature review* yang digunakan untuk menilai kematangan ZTA lintas domain (Mushtaq et al., 2025).

2.4 Teknik Analisis Data

Analisis data dilakukan dengan teknik analisis isi *(content analysis)* terhadap literatur dan teknik analisis komparatif terhadap model-model keamanan yang sudah ada. Analisis isi digunakan untuk mengekstrak prinsip-prinsip kunci dari standar dan literatur, sedangkan analisis komparatif digunakan untuk memetakan posisi Z-ARSIP terhadap model-model sejenis seperti AT-ZTAC (Mao et al., 2025), AI-ZTB (Daah et al., 2026), dan kerangka kontrol akses berbasis risiko untuk lingkungan awan (Alharbe et al., 2023). Hasil analisis kemudian disintesiskan ke dalam matriks integrasi yang menghubungkan setiap komponen Z-ARSIP dengan literatur pendukung, prinsip ISO 15489-1:2016, dan tujuh prinsip ZTA.

2.5 Batasan Penelitian

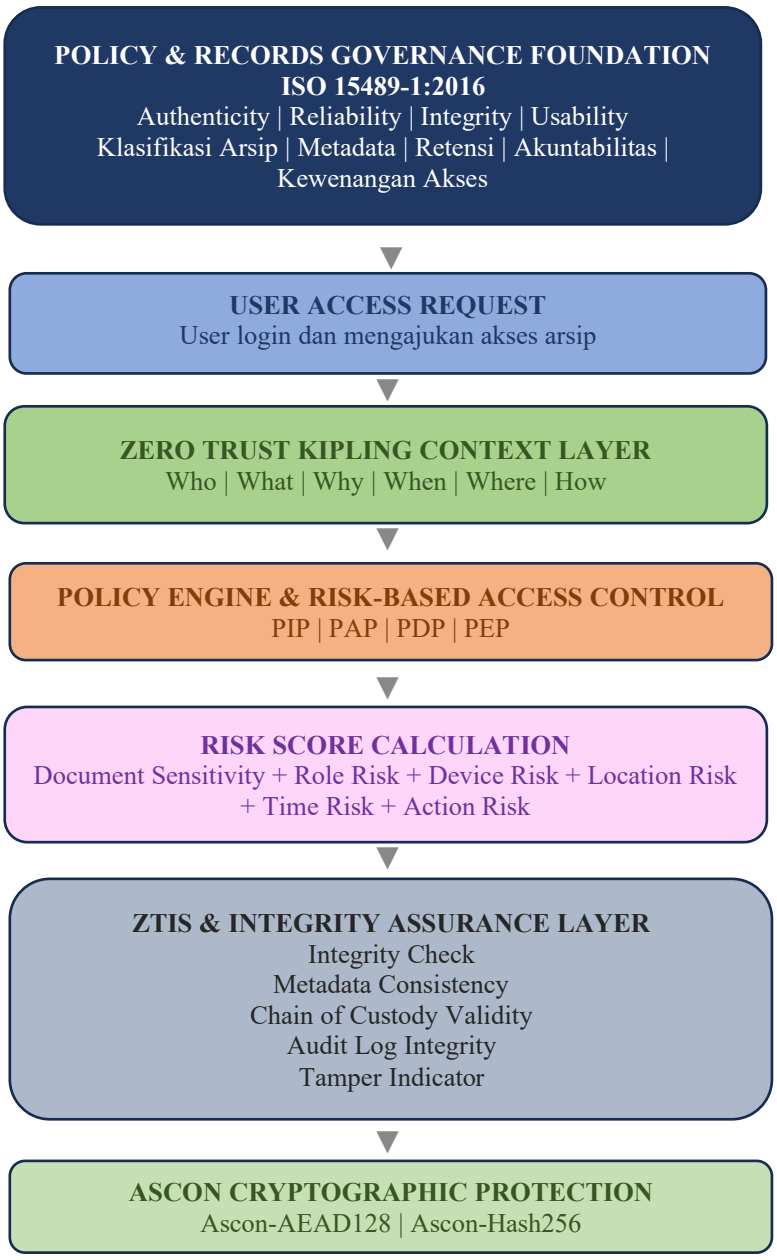
Penelitian ini memiliki tiga batasan yang perlu ditegaskan. Pertama, Z-ARSIP merupakan model konseptual yang belum diimplementasikan dalam sistem operasional Bank Indonesia atau lembaga lain; lembaga tersebut digunakan sebagai konteks ilustratif untuk menggambarkan kompleksitas pengelolaan arsip vital. Kedua, simulasi Ascon dibahas pada tataran rancangan, bukan pengukuran kinerja pada perangkat keras tertentu, sehingga aspek *throughput*, konsumsi daya, dan ketahanan terhadap *side-channel attack* dirujuk dari penelitian terdahulu (Khan et al., 2024; Sarasa Laborda et al., 2025; Widodo et al., 2025). Ketiga, evaluasi model dilakukan secara konseptual dan logis, sedangkan pengujian empiris terhadap pengguna dan

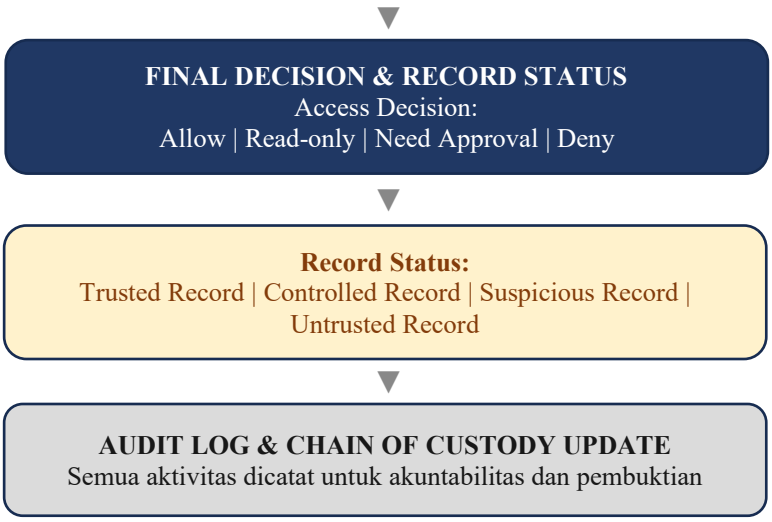
ancaman nyata berada di luar lingkup penelitian ini dan menjadi rekomendasi penelitian lanjutan.

3. PEMBAHASAN

3.1 Arsitektur Z-ARSIP: Enam Lapisan Keamanan Arsip Elektronik

Z-ARSIP dirancang sebagai model keamanan arsip elektronik berlapis yang memadukan prinsip pengelolaan arsip dan keamanan informasi modern. Arsitektur ini terdiri atas enam lapisan yang bekerja secara sinergis, yaitu *records management layer*, *context awareness layer*, *policy and decision layer*, *integrity layer*, *cryptographic layer*, dan *integrity assurance layer*. Setiap lapisan memiliki peran spesifik namun saling melengkapi untuk menjawab kebutuhan akan arsip yang autentik, andal, utuh, dan dapat digunakan.





Gambar 1. Arsitektur Model Keamanan Arsip Elektronik Z-ARSIP

Lapisan pertama, *records management layer*, mengadopsi prinsip ISO 15489-1:2016 sebagai fondasi pengelolaan arsip elektronik. Standar ini menempatkan arsip sebagai bukti otoritatif aktivitas bisnis yang harus memiliki karakter *authenticity*, *reliability*, *integrity*, dan *usability* (Thaanyane et al., 2025). Lapisan ini menetapkan kebijakan, sistem, dan proses pengelolaan arsip mulai dari penciptaan, penangkapan, klasifikasi, akses, hingga penyusutan. Pada konteks Bank Indonesia, pendekatan ini sejalan dengan kebijakan Manajemen Dokumen Bank Indonesia yang menjadikan ISO 15489-1:2016 sebagai rujukan utama (Ramudin, 2019).

Lapisan kedua, *context awareness layer*, menerapkan metodologi Zero Trust Kipling sebagai mekanisme evaluasi konteks akses berbasis enam pertanyaan klasik *what*, *why*, *when*, *how*, *where*, dan *who* (ETSI, 2025). Lapisan ketiga, *policy and decision layer*, mengoperasionalkan keputusan akses melalui *Policy Engine* yang terdiri atas Policy Information Point (PIP), Policy Administration Point (PAP), Policy Decision Point (PDP), dan Policy Enforcement Point (PEP), dengan tambahan *Risk-Based Access Control* (Mao et al., 2025; Shaikh et al., 2012). Lapisan keempat, *integrity layer*, memperkenalkan *Zero Trust Integrity Score* (ZTIS) sebagai indikator kepercayaan integritas arsip. Lapisan kelima, *cryptographic layer*, memanfaatkan Ascon *Lightweight Cryptography* untuk enkripsi, autentikasi, dan verifikasi *fingerprint* dokumen (Dobraunig et al., 2021). Lapisan keenam, *integrity assurance layer*, menutup arsitektur dengan *integrity check*, *tamper detection*, *chain of custody*, dan *audit log integrity*.

Pendekatan berlapis ini bersifat saling melengkapi dan tidak saling menggantikan. ISO 15489-1:2016 memberi kerangka pengelolaan, ZTA memberi prinsip kontrol akses, ZTIS memberi indikator integritas, dan Ascon memberi pelindung kriptografis. Inilah yang menjadi pembeda Z-ARSIP dari model-model sebelumnya yang umumnya hanya berfokus pada salah satu dimensi.

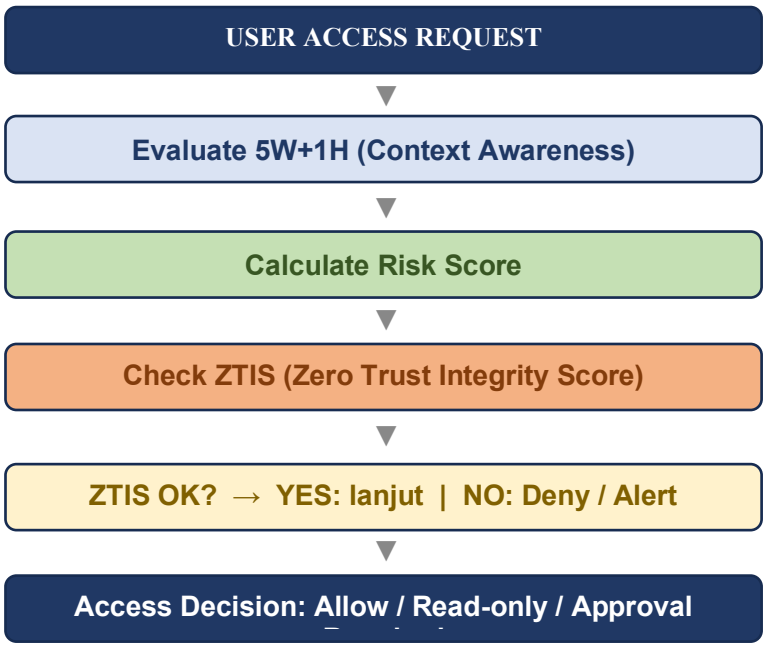
3.2 Penerapan ZT-Kipling 5W+1H pada Akses Arsip Elektronik

Pendekatan ZT-Kipling memungkinkan setiap permintaan akses arsip dievaluasi secara kontekstual dan eksplisit. Pada Z-ARSIP, keenam pertanyaan Kipling diterjemahkan ke dalam variabel akses arsip sebagai berikut. *Who* mengacu pada identitas pengguna beserta peran (arsiparis, pejabat, auditor, pihak ketiga). *What* merujuk pada arsip spesifik yang diminta beserta klasifikasi keamanannya. *Why* menanyakan tujuan akses, misalnya pemeriksaan internal, layanan publik, atau riset. *When* menilai waktu akses, apakah dalam jam kerja resmi atau di luar jam kerja. *Where* menilai lokasi dan perangkat akses, termasuk apakah menggunakan jaringan internal lembaga atau jaringan publik. *How* menilai aksi yang akan dilakukan terhadap arsip, seperti melihat *(read)*, mengunduh *(download)*, mencetak *(print)*, atau menyunting *(edit)*.

Penerapan Kipling pada akses arsip memberi tiga keuntungan. Pertama, ia membuat keputusan akses transparan dan dapat dijelaskan, sebagaimana ditekankan ETSI (2025) sebagai prinsip utama ZT-Kipling. Kedua, ia memungkinkan pengelolaan akses yang granular dan adaptif, tidak lagi hanya berbasis peran statis seperti pada RBAC konvensional. Ketiga, ia membuka peluang penegakan prinsip *least privilege* dan *least persistence* yang menjadi inti Zero Trust (Rose et al., 2020).

Ilustrasinya, seorang arsiparis pusat yang mengakses arsip *internal* dari komputer kantor pada jam kerja akan dievaluasi berbeda dengan arsiparis yang sama ketika mencoba mengakses arsip *highly confidential* dari perangkat pribadi pada tengah malam. Pada model konvensional kedua skenario diperlakukan sama selama identitas dan peran terverifikasi; pada Z-ARSIP keduanya menghasilkan keputusan akses yang berbeda karena konteksnya berbeda.

3.3 Risk-Based Access Control dan Policy Engine PIP/PAP/PDP/PEP



Gambar 2. Alur Keputusan Akses Berbasis Risk Score dan ZTIS

Untuk mengubah evaluasi kontekstual menjadi keputusan akses, Z-ARSIP mengadopsi *Risk-Based Access Control* yang dikelola oleh *Policy Engine*. Pendekatan ini sejalan dengan model XACML yang lazim digunakan dalam ABAC dan ZTA (Mao et al., 2025), serta diperkuat oleh Shaikh et al. (2012) yang memperkenalkan PDP berbasis nilai kepercayaan dan risiko sebelum mengambil keputusan. Pendekatan tersebut diperluas oleh Alharbe et al. (2023) yang mengembangkan model kontrol akses berbasis risiko dengan asesmen *fuzzy AHP* untuk lingkungan awan, dengan hasil eksperimen menunjukkan kemampuan sistem memberikan keputusan akses dinamis terhadap data sensitif sesuai konteks subjek, sumber daya, dan lingkungan. Pengalaman ini relevan bagi rancangan Z-ARSIP karena arsip elektronik lembaga strategis menghadapi karakteristik akses yang serupa: dinamis, lintas perangkat, dan sensitif.

Pada Z-ARSIP, PIP mengumpulkan informasi konteks (pengguna, peran, perangkat, lokasi, waktu, klasifikasi arsip, dan aksi akses). PAP menjadi tempat administrator menetapkan kebijakan akses, termasuk ambang batas risiko untuk tiap klasifikasi arsip. PDP menghitung skor risiko berdasarkan input PIP dan kebijakan PAP, sedangkan PEP menegakkan keputusan akses berupa *allow*, *read-only*, *need approval*, atau *deny*.

Penilaian sensitivitas arsip dirumuskan dalam lima tingkat klasifikasi sebagaimana disajikan pada Tabel 1.

Tabel 1. Klasifikasi Dokumen dan Bobot Risiko pada Z-ARSIP

Tingkat	Klasifikasi	Bobot Risiko
1	*Public*	5
2	*Internal*	20
3	*Restricted*	30
4	*Confidential*	40
5	*Highly Confidential* / Arsip Vital	55

Risk Score dihitung sebagai penjumlahan bobot enam komponen kontekstual:

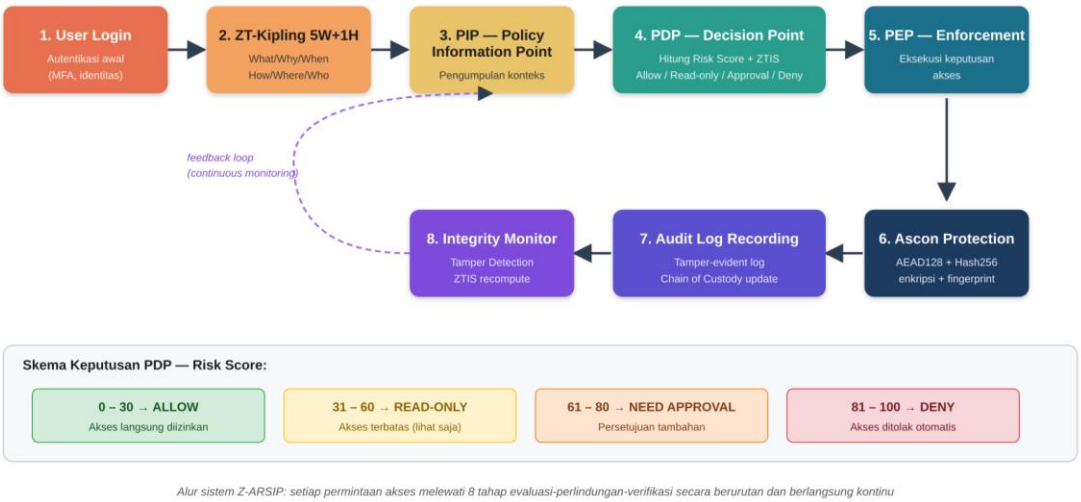
$$Risk\ Score = Document\ Sensitivity + Role\ Risk + Device\ Risk + Location\ Risk + Time\ Risk + Action\ Risk$$

Bobot dalam model ini bersifat konseptual dan dapat dikalibrasi lebih lanjut sesuai kebijakan risiko organisasi, tingkat sensitivitas arsip, serta kebutuhan keamanan masing-masing institusi. Pendekatan ini memungkinkan organisasi menyesuaikan toleransi risiko dan ambang keputusan akses berdasarkan karakteristik lingkungan kerjanya. Hasil perhitungan menentukan keputusan akses, yang dipetakan dalam empat kategori sebagaimana terlihat pada Tabel 2.

Tabel 2. Pemetaan Risk Score terhadap Keputusan Akses

Rentang *Risk Score*	Kategori Risiko	Keputusan Akses
0–30	*Low Risk*	*Allow*
31–60	*Medium Risk*	*Read-only*
61–80	*High Risk*	*Need Approval*
81–100	*Critical Risk*	*Deny*

Untuk memberikan gambaran utuh tentang bagaimana komponen-komponen di atas bekerja secara terpadu dari permintaan akses pertama hingga audit dan pemantauan integritas, alur sistem Z-ARSIP disajikan pada Gambar 2.



Gambar 2. Alur Sistem Z-ARSIP — Dari Permintaan Akses Hingga Audit dan Pemantauan Integritas

Melalui mekanisme ini, akses terhadap arsip *highly confidential* dari perangkat pribadi pada tengah malam akan menghasilkan skor risiko yang tinggi sehingga otomatis ditolak atau memerlukan persetujuan tambahan, sedangkan akses arsip *public* dari perangkat kantor pada jam kerja akan langsung diizinkan. Pendekatan ini selaras dengan praktik *risk-adaptive access control* yang dikembangkan Alharbe et al. (2023), Li et al. (2024), dan Mao et al. (2025), namun diadaptasi spesifik untuk konteks arsip elektronik.

3.4 Zero Trust Integrity Score (ZTIS) dan Integrity Assurance Layer

Pengaturan akses saja tidak cukup untuk menjamin keamanan arsip; sistem juga perlu memastikan bahwa arsip yang diakses memang masih dapat dipercaya. Untuk menjawab kebutuhan ini, Z-ARSIP memperkenalkan *Zero Trust Integrity Score*

(ZTIS), yaitu skor kepercayaan integritas arsip yang dihitung secara dinamis. ZTIS dirumuskan sebagai berikut:

$$\text{ZTIS} = \textit{Integrity Check} + \textit{Metadata Consistency} + \textit{Chain of Custody} + \textit{Audit Log Integrity} - \textit{Tamper Indicator}$$

Formula ZTIS pada penelitian ini digunakan sebagai model konseptual untuk menggambarkan tingkat kepercayaan integritas arsip elektronik. Nilai tiap komponen dapat disesuaikan lebih lanjut berdasarkan kebijakan preservasi, mekanisme audit, dan kebutuhan validasi integritas pada masing-masing organisasi.

Komponen *integrity check* dihitung dari hasil verifikasi *hash*/*fingerprint* dokumen terhadap nilai referensi yang tercatat saat penciptaan arsip. *Metadata consistency* menilai konsistensi metadata kunci seperti pencipta, tanggal pembuatan, klasifikasi, dan jadwal retensi. *Chain of custody* menilai kelengkapan jejak kustodi digital, yakni siapa saja yang pernah memegang, menyalin, atau memodifikasi arsip. *Audit log integrity* menilai keutuhan rekam aktivitas akses arsip. *Tamper indicator* dikurangkan dari total skor karena bersifat indikasi negatif.

Hasil ZTIS dikategorikan ke dalam empat tingkat 85–100 sebagai *Trusted Record*, 70–84 sebagai *Controlled Record*, 50–69 sebagai *Suspicious Record*, dan kurang dari 50 sebagai *Untrusted Record*. Arsip dengan kategori *Suspicious* atau *Untrusted* memicu peringatan dan investigasi, bahkan bisa membatalkan keputusan akses meskipun pengguna lolos uji *Risk Score*. Pendekatan ini mengisi celah penelitian Mayesti dan Hanriarseto (2015) yang menunjukkan bahwa banyak instansi belum memiliki *tracking system* memadai untuk memastikan integritas arsip dinamis elektronik.

ZTIS ditopang oleh *Integrity Assurance Layer* yang memuat empat fungsi utama: *integrity check* berkala, *tamper detection* otomatis, pencatatan *chain of custody* yang konsisten, dan jaminan *audit log integrity*. Fungsi-fungsi ini mengadaptasi praktik *tamper-evident audit trail* yang dikembangkan dalam riset Daah et al. (2026), namun diterapkan pada domain arsip elektronik. Dengan kombinasi ZTIS dan *Integrity Assurance Layer*, Z-ARSIP tidak hanya menjawab pertanyaan "siapa yang berhak mengakses" tetapi juga "apakah yang diakses masih utuh dan dapat dipercaya".

Tabel 3. Simulasi Komponen Akses Arsip Pada Model Z-ARSIP

No.	Skenario Akses	Konteks Zero Trust Kipling 5W+1H	Komponen Risiko	Risk Score	ZTIS	Keputusan Akses	Interpretasi

1.	Pegawai internal mengakses arsip internal dari perangkat resmi pada jam kerja	**Who:** pegawai unit terkait; **What:** arsip internal; **Why:** tugas rutin; **When:** jam kerja; **Where:** jaringan kantor; **How:** membaca dokumen	Document Sensitivity 20 + Role Risk 0 + Device Risk 0 + Location Risk 0 + Time Risk 0 + Action Risk 5	25	92	Allow	Akses diberikan karena konteks sesuai kewenangan, perangkat resmi, waktu normal, dan arsip memiliki status **Trusted Record**.
2.	Pegawai lintas unit mengakses arsip restricted dari perangkat resmi	**Who:** pegawai lintas unit; **What:** arsip restricted; **Why:** koordinasi pekerjaan; **When:** jam kerja; **Where:** jaringan kantor; **How:** membaca dokumen	Document Sensitivity 30 + Role Risk 10 + Device Risk 0 + Location Risk 0 + Time Risk 0 + Action Risk 5	45	87	Read-only	Akses dibatasi karena pengguna bukan dari unit pemilik arsip, meskipun perangkat dan waktu akses valid. Dokumen tetap dapat dibaca, tetapi tidak dapat diunduh atau diubah.
3.	Auditor mengakses arsip confidential melalui VPN dari	**Who:** auditor; **What:** arsip confidential; **Why:** pemeriksaan;	Document Sensitivity 40 + Role Risk 5 + Device Risk 0 +	70	82	Need Approval	Akses memerlukan persetujuan tambaha

	perangkat terdaftar	**When:** luar jam kerja; **Where:** VPN resmi; **How:** mengunduh dokumen	Location Risk 5 + Time Risk 10 + Action Risk 10				n karena dokumen bersifat rahasia dan tindakan unduh dilakukan di luar jam kerja. Status arsip masih **Controlled Record**, sehingga perlu pengawasan.
4.	User eksternal terbatas mencoba mengakses arsip vital dari perangkat tidak dikenal	**Who:** user eksternal; **What:** highly confidential/ arsip vital; **Why:** tidak jelas; **When:** malam hari; **Where:** lokasi tidak dikenal; **How:** mengunduh dan membagikan	Document Sensitivity 55 + Role Risk 15 + Device Risk 10 + Location Risk 10 + Time Risk 10 + Action Risk 15	110	90	Deny	Akses ditolak karena risiko kritis. Meskipun arsip berstatus **Trusted Record**, konteks akses tidak sah dan berpotensi membahayakan arsip vital.
5.	Arsiparis mengakses arsip restricted, tetapi sistem	**Who:** arsiparis; **What:** arsip restricted; **Why:** validasi retensi;	Document Sensitivity 30 + Role Risk 0 + Device Risk 0 +	35	58	Read-only + Integrity Alert	Akses dibatasi karena ZTIS berada pada

	mendeteksi perubahan hash	**When:** jam kerja; **Where:** jaringan kantor; **How:** membuka dan memverifikasi metadata	Location Risk 0 + Time Risk 0 + Action Risk 5				kategori **Suspicious Record**. Sistem memberi peringatan untuk pemeriksaan integrity check, metadata, dan chain of custody.

3.5 Penerapan Ascon Lightweight Cryptography pada Arsip Elektronik

Lapisan kriptografi Z-ARSIP memanfaatkan Ascon, algoritma *lightweight cryptography* yang ditetapkan NIST sebagai standar pada tahun 2023 setelah seleksi panjang terhadap berbagai kandidat (Dobraunig et al., 2021; Kaur et al., 2025). Ascon-AEAD128 digunakan untuk enkripsi sekaligus autentikasi data arsip, sedangkan Ascon-Hash256 digunakan untuk menghasilkan *fingerprint* dokumen yang menjadi acuan bagi *integrity check* dalam ZTIS.

Pemilihan Ascon dilatarbelakangi tiga keunggulan. Pertama, efisiensi komputasi. Studi Sarasa Laborda et al. (2025) menunjukkan bahwa Ascon-128a memiliki performa siklus yang lebih baik dibandingkan varian lain pada platform Arduino, sehingga cocok untuk perangkat dengan keterbatasan sumber daya. Survei Soto-Cruz et al. (2025) atas algoritma kriptografi ringan untuk mikrokontroler berdaya rendah juga menempatkan Ascon di antara pilihan paling efisien dari sisi konsumsi memori, latensi, dan energi. Kedua, keseimbangan keamanan dan efisiensi. Radhakrishnan et al. (2024) menyimpulkan bahwa Ascon memberikan jaminan keamanan kuat terhadap serangan kerahasiaan dan integritas dengan *overhead* rendah, dengan ketahanan menonjol terhadap serangan kriptografi dibandingkan AES-128 dan SPECK pada perangkat IoT. Ketiga, dukungan terhadap autentikasi terautentikasi *(authenticated encryption)*. Kombinasi enkripsi dan autentikasi pada satu algoritma menyederhanakan arsitektur sistem dan mengurangi risiko inkonsistensi antarlapis kriptografi (Khan et al., 2024).

Tinjauan Konstantopoulou et al. (2025) terhadap implementasi FPGA dan ASIC dari para finalis NIST *Lightweight Cryptography* menyimpulkan bahwa Ascon menawarkan keseimbangan optimal antara *throughput* dan area, dengan ketahanan yang baik terhadap *fault injection*. Pengembangan terbaru Öztürk et al. (2025) bahkan memperluas Ascon-AEAD128 dengan integrasi peta chaos Zaslavsky untuk Internet

of Robotic Things, yang menghasilkan ketahanan tinggi terhadap serangan pasif maupun aktif sembari tetap kompatibel dengan platform berdaya rendah seperti Raspberry Pi 3B. Bukti-bukti ini memperkuat posisi Ascon sebagai algoritma yang adaptif untuk berbagai skenario, termasuk pengelolaan arsip elektronik lintas perangkat.

Untuk konteks arsip elektronik lembaga strategis seperti Bank Indonesia, Ascon menjadi pilihan strategis karena beberapa alasan operasional. Sistem pengelolaan arsip lembaga besar melibatkan banyak titik akses, perangkat, dan kantor cabang dengan kapasitas perangkat yang beragam. Bila kriptografi yang digunakan terlalu berat, sistem akan melambat dan mengganggu produktivitas. Studi Widodo et al. (2025) menunjukkan bahwa walau Ascon memerlukan energi sedikit lebih tinggi dibanding Speck dan Simon pada simulasi WSN, ia memberi jaminan keamanan yang jauh lebih kuat dengan tetap berstatus *lightweight*. Untuk arsip vital, *trade-off* tersebut sangat bisa diterima karena nilai kebuktian arsip jauh lebih penting daripada selisih konsumsi energi.

Pada Z-ARSIP, Ascon-AEAD128 dijalankan secara konseptual pada tiga titik kritis: (1) saat arsip pertama kali dibuat atau dialih-mediakan, untuk melindungi konten dan menambahkan tag autentikasi; (2) saat arsip ditransfer antarsatuan kerja, untuk mencegah penyadapan; dan (3) saat arsip disimpan dalam *storage* jangka panjang, untuk mencegah pembacaan tidak sah. Sementara itu, Ascon-Hash256 menghasilkan *digital fingerprint* yang menjadi referensi *integrity check* dalam ZTIS. Dengan demikian, lapisan kriptografi Ascon menjadi tulang punggung teknis bagi prinsip autentisitas dan integritas arsip yang digariskan ISO 15489-1:2016.

3.6 Integrasi Policy, People, dan Technology

Z-ARSIP tidak akan efektif jika hanya dipandang sebagai konstruksi teknologi. Keamanan arsip elektronik adalah isu sosioteknis yang menuntut keseimbangan antara *policy*, *people*, dan *technology*. Dimensi *policy* terwujud dalam kebijakan kearsipan yang merujuk pada UU No. 43 Tahun 2009, UU ITE, UU No. 27 Tahun 2022 tentang PDP, ISO 15489-1:2016, dan NIST SP 800-207. Pada lembaga seperti Bank Indonesia, kebijakan internal menjadi penerjemah aturan-aturan tersebut ke dalam praktik operasional (Ramudin, 2019).

Dimensi *people* mencakup arsiparis, pejabat administrator, pengguna umum, dan pemangku kebijakan. Kuswantoro (2018) mengingatkan bahwa di era disrupsi, kompetensi arsiparis tidak cukup berbasis kearsipan tradisional, melainkan harus mencakup penguasaan TIK dan sistem informasi manajemen. Z-ARSIP menuntut arsiparis yang mampu memahami konsep risiko, kontrol akses kontekstual, integritas digital, serta kriptografi pada level konseptual. Studi Marliana et al. (2024) di Badan Informasi Geospasial juga menegaskan bahwa keberhasilan implementasi sistem manajemen keamanan informasi sangat bergantung pada komitmen manajemen, budaya organisasi, dan kapasitas SDM, bukan semata-mata pada kelengkapan teknologi. Tanpa peningkatan kapasitas SDM, *Policy Engine* secanggih apa pun akan

kehilangan makna karena tidak ada operator yang mampu menjalankannya secara konsisten.

Dimensi *technology* mencakup *Policy Engine*, ZTIS, Ascon, dan sistem *audit log*. Teknologi ini bukan tujuan akhir, melainkan alat yang mendukung kepatuhan terhadap kebijakan dan memberdayakan SDM. Integrasi ketiga dimensi inilah yang memberi Z-ARSIP karakter sebagai model sosioteknis, bukan semata-mata model teknis.

3.7 Landasan Hukum dan Kebaruan Z-ARSIP

Z-ARSIP berpijak pada landasan hukum yang kokoh. Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan menjamin arsip harus autentik, utuh, dan dapat dipertanggungjawabkan. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik memberikan legalitas dokumen elektronik dan tanda tangan elektronik (Mayesti & Hanriarseto, 2015). Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi mengatur perlindungan data dan kontrol akses informasi pribadi. Pada level standar internasional, Z-ARSIP mengacu pada ISO 15489-1:2016, NIST SP 800-207, ETSI TS 104 102, dan NIST Lightweight Cryptography Standard untuk Ascon.

Kebaruan Z-ARSIP terletak pada integrasi ISO 15489-1:2016, Zero Trust Kipling 5W+1H, *Risk-Based Access Control*, *Policy Engine* PIP/PAP/PDP/PEP, *Zero Trust Integrity Score*, Ascon *Lightweight Cryptography*, dan *Integrity Assurance Layer* dalam satu model keamanan arsip elektronik. Sepanjang penelusuran literatur, belum ditemukan model yang mengintegrasikan keseluruhan komponen tersebut secara terpadu. Beberapa studi seperti AT-ZTAC (Mao et al., 2025) berfokus pada ABAC dengan evaluasi kepercayaan dinamis, AI-ZTB (Daah et al., 2026) menggabungkan ZTA dengan *blockchain* dan AI untuk *EV charging*, sedangkan kerangka Chen et al. (2021) berfokus pada layanan kesehatan 5G. Z-ARSIP menempatkan pengelolaan arsip sebagai pusat perhatian, bukan sebagai bagian sampingan, sehingga relevan langsung bagi lembaga negara dan lembaga strategis yang mengelola arsip vital bernilai pembuktian tinggi. Perbandingan karakteristik Z-ARSIP dengan pendekatan keamanan arsip elektronik konvensional disajikan pada Tabel 3.

Tabel 4. Perbandingan Kapabilitas Keamanan Sistem Konvensional dengan Z-ARSIP

Aspek keamanan	Sistem konvensional	Z-ARSIP
Akses berbasis konteks	Tidak ada	Ada
Penilaian integritas (ZTIS)	Tidak ada	Ada
Pelacakan rantai kepemilikan	Terbatas	Ada
Kontrol akses berbasis risiko	Tidak ada	Ada

Kriptografi ringan	Tidak ada	Ada
Deteksi manipulasi dokumen	Terbatas	Ada
Kepatuhan ISO 15489-1:2016	Terbatas	Ada
Integrasi kepatuhan hukum	Tidak ada	Ada

Kontribusi Z-ARSIP karenanya bersifat empat dimensi. Secara konseptual, ia mengusulkan model keamanan arsip berbasis Zero Trust kontekstual. Secara metodologis, ia menyediakan mekanisme evaluasi akses berbasis 5W+1H, *risk score*, *policy engine*, dan ZTIS. Secara teknologis, ia menerapkan Ascon untuk menjaga autentisitas dan integritas dokumen digital. Secara kearsipan, ia mendukung penerapan prinsip ISO 15489-1:2016 di lingkungan digital dan memperkuat kerangka hukum nasional di bidang arsip elektronik.

4. SIMPULAN DAN SARAN

4.1 Simpulan

Penelitian ini menghasilkan Z-ARSIP, sebuah model konseptual keamanan arsip elektronik yang mengintegrasikan enam komponen utama, yaitu ISO 15489-1:2016, Zero Trust Kipling 5W+1H, *Risk-Based Access Control* dengan *Policy Engine* PIP/PAP/PDP/PEP, *Zero Trust Integrity Score* (ZTIS), Ascon *Lightweight Cryptography*, dan *Integrity Assurance Layer*. Berdasarkan kajian yang dilakukan, terdapat empat simpulan utama yang dapat ditarik.

Pertama, model keamanan arsip elektronik konvensional yang hanya bertumpu pada autentikasi *login* dan *Role-Based Access Control* tidak memadai untuk menjaga autentisitas, integritas, dan akuntabilitas arsip digital di era ancaman siber modern. Pendekatan tersebut bersifat statis, tidak peka terhadap konteks, dan rentan terhadap pergerakan lateral serta ancaman dari dalam. Z-ARSIP menjawab kelemahan ini dengan kontrol akses kontekstual berbasis ZT-Kipling 5W+1H yang memungkinkan setiap permintaan akses dievaluasi secara granular dan adaptif terhadap perubahan kondisi.

Kedua, integrasi *Risk-Based Access Control* dengan *Policy Engine* memungkinkan keputusan akses arsip diambil secara dinamis berdasarkan skor risiko yang dihitung dari sensitivitas dokumen, peran, perangkat, lokasi, waktu, dan aksi. Pemetaan keputusan akses ke dalam empat kategori (*allow*, *read-only*, *need approval*, dan *deny*) memberi keseimbangan antara fleksibilitas kerja dan keamanan arsip. Pendekatan ini secara konsep memperkuat penerapan prinsip *least privilege* yang menjadi inti Zero Trust Architecture.

Ketiga, *Zero Trust Integrity Score* (ZTIS) memberikan dimensi baru dalam keamanan arsip elektronik dengan mengukur tingkat kepercayaan integritas dokumen, bukan hanya kelayakan akses pengguna. Skor yang dihitung dari *integrity check*,

konsistensi metadata, *chain of custody*, dan *audit log integrity*, dikurangi *tamper indicator*, memberi indikator yang dapat dipertanggungjawabkan tentang status keandalan arsip. Lapisan ini memperkuat empat karakter arsip ISO 15489-1:2016 (*authenticity*, *reliability*, *integrity*, dan *usability*) dalam lingkungan digital.

Keempat, penggunaan Ascon sebagai *lightweight cryptography* yang ditetapkan NIST sebagai standar pada tahun 2023 memberikan pelindung kriptografis yang efisien sekaligus kuat untuk arsip elektronik. Ascon-AEAD128 menyediakan enkripsi sekaligus autentikasi, sedangkan Ascon-Hash256 mendukung verifikasi *fingerprint* dokumen. Kombinasi keduanya menjadi tulang punggung teknis bagi prinsip autentisitas dan integritas yang diisyaratkan ISO 15489-1:2016. Secara keseluruhan, Z-ARSIP berkontribusi sebagai model sosioteknis yang menyatukan dimensi *policy*, *people*, dan *technology* dalam satu kerangka keamanan arsip yang sesuai dengan landasan hukum nasional dan standar internasional.

4.2 Saran

Berdasarkan simpulan di atas, terdapat tiga kelompok saran yang diajukan. Pertama, saran bagi lembaga pengelola arsip, khususnya lembaga strategis seperti Bank Indonesia. Lembaga disarankan mempertimbangkan adopsi prinsip Zero Trust Kipling secara bertahap pada sistem kearsipan elektroniknya, dimulai dari pemetaan klasifikasi dokumen dan rekayasa ulang kebijakan akses berdasarkan konteks 5W+1H. Penguatan kebijakan internal yang mengakomodasi *Risk-Based Access Control* dan ZTIS akan memperkuat akuntabilitas pengelolaan arsip vital. Selain itu, lembaga perlu meningkatkan kompetensi SDM kearsipannya melalui pelatihan tematik di bidang keamanan informasi, kriptografi terapan, dan tata kelola data, sebagaimana dianjurkan Kuswantoro (2018) untuk arsiparis era disrupsi serta Marliana et al. (2024) untuk implementasi sistem manajemen keamanan informasi di lembaga publik.

Kedua, saran bagi pembuat kebijakan dan regulator. Pemerintah disarankan mendorong harmonisasi regulasi antara UU No. 43 Tahun 2009 tentang Kearsipan, UU No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi, serta peraturan pelaksana di bidang Sistem Pemerintahan Berbasis Elektronik. Harmonisasi ini penting agar penerapan model seperti Z-ARSIP memiliki pijakan hukum yang kokoh, terutama terkait kekuatan pembuktian arsip elektronik, perlindungan data pribadi yang tersimpan dalam arsip, dan akuntabilitas digital lembaga negara. Regulator juga disarankan menyusun panduan teknis nasional tentang penerapan *lightweight cryptography* dan Zero Trust pada sistem kearsipan elektronik agar lembaga publik memiliki rujukan implementasi yang seragam.

Ketiga, saran bagi peneliti selanjutnya. Penelitian ini menghasilkan model konseptual yang masih membutuhkan validasi empiris. Riset lanjutan disarankan mengembangkan prototipe *proof-of-concept* Z-ARSIP, mengukur kinerja Ascon pada arsip dengan beragam ukuran dan format, serta menguji ketahanan model terhadap berbagai skenario serangan, termasuk *insider threat* dan *advanced persistent threat*. Penelitian lain dapat memperluas Z-ARSIP dengan mengintegrasikan teknologi

pelengkap seperti *blockchain* untuk *audit log integrity* yang sepenuhnya *tamper-proof* (Daah et al., 2026), atau memperkenalkan modul *explainable AI* pada *trust evaluation engine* sebagaimana disarankan dalam tinjauan Mushtaq et al. (2025). Pengembangan lebih lanjut juga dapat diarahkan pada penerapan model di lembaga lain di luar sektor moneter, misalnya di lembaga penegak hukum, kementerian, atau pemerintah daerah, untuk menguji generalisabilitas Z-ARSIP pada konteks pengelolaan arsip publik yang lebih luas.

DAFTAR PUSTAKA

Alharbe, N., Aljohani, A., Rakrouki, M. A., & Khayyat, M. (2023). An access control model based on system security risk for dynamic sensitive data storage in the cloud. *Applied Sciences*, *13*(5), Article 3187. https://doi.org/10.3390/app13053187

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers & Security*, *110*, Article 102436. https://doi.org/10.1016/j.cose.2021.102436

Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., Chen, H., Lu, H., & Zhai, Y. (2021). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, *8*(13), 10248–10263. https://doi.org/10.1109/JIOT.2020.3041042

Daah, C., Fallot, Y., Qureshi, A., Awan, I., & Konur, S. (2026). AI-driven zero trust and blockchain framework for secure electric vehicle infrastructure. *Expert Systems With Applications*, *312*, Article 131577. https://doi.org/10.1016/j.eswa.2026.131577

Dobraunig, C., Eichlseder, M., Mendel, F., & Schläffer, M. (2021). Ascon v1.2: Lightweight authenticated encryption and hashing. *Journal of Cryptology*, *34*(3), Article 33. https://doi.org/10.1007/s00145-021-09398-9

European Telecommunications Standards Institute. (2025). *ETSI TS 104 102 V1.1.1: Cyber security (CYBER); Methods and protocols for the application of Zero Trust principles using the Kipling methodology (ZT-Kipling)*. ETSI.

International Organization for Standardization. (2016). *ISO 15489-1:2016 — Information and documentation: Records management — Part 1: Concepts and principles*. ISO.

Ismayati, N. (2014). Preservasi arsip vital perguruan tinggi: Studi kasus di Universitas X. *Jurnal Pustakawan Indonesia*, *13*(2), 59–68.

Kaur, J., Cintas Canto, A., Mozaffari Kermani, M., & Azarderakhsh, R. (2025). A survey on the implementations, attacks, and countermeasures of the NIST lightweight cryptography standard: ASCON. *ACM Computing Surveys*, *58*(1), Article 6. https://doi.org/10.1145/3744640

Khan, S., Inayat, K., Muslim, F. B., Shah, Y. A., Ur Rehman, M. A., Khalid, A., Imran, M., & Abdusalomov, A. (2024). Securing the IoT ecosystem: ASIC-based hardware realization of Ascon lightweight cipher. *International Journal of Information Security*, *23*, 3653–3664. https://doi.org/10.1007/s10207-024-00904-1

Konstantopoulou, E., Sklavos, N., Christodoulou, P., & Lalos, A. S. (2025). Advances in performance and allocated resources of NIST lightweight cryptography finalists' implementations. *ACM Computing Surveys*, *57*(10), Article 246. https://doi.org/10.1145/3721122

Kuswantoro, A. (2018). Kompetensi arsiparis pada era disrupsi di Universitas Negeri Semarang (UNNES). *Jurnal Pustakawan Indonesia*, *17*(1), 19–24.

Li, B., Yang, F., & Zhang, S. (2024). Context-aware risk attribute access control. *Mathematics*, *12*(16), Article 2541. https://doi.org/10.3390/math12162541

Mao, Y., Fu, W., Zhao, Y., Yuan, Z., Sun, Z., & Zhao, Y. (2025). A zero-trust access control model based on attribute and dynamic trust evaluation for cloud environments. *Symmetry*, *17*(12), Article 2059. https://doi.org/10.3390/sym17122059

Marliana, E., Nurhadryani, Y., & Hermadi, I. (2024). Analisis kesenjangan pemenuhan standar sistem manajemen keamanan informasi pada Ina-Geoportal. *JIKA: Jurnal Ilmu Komputer dan Agri-Informatika*, *11*(1), 27–38.

Mayesti, N., & Hanriarseto, T. (2015). Otentisitas dalam pengelolaan arsip elektronik: Studi kasus di Badan Perpustakaan dan Arsip Daerah (BPAD) Pemerintah Provinsi DKI Jakarta. *Jurnal Ilmu Informasi, Perpustakaan, dan Kearsipan*, *17*(2), 121–146.

Mushtaq, S., Mohsin, M., & Mushtaq, M. M. (2025). A systematic literature review on the implementation and challenges of Zero Trust Architecture across domains. *Sensors*, *25*(19), Article 6118. https://doi.org/10.3390/s25196118

Öztürk, G., Çimen, M. E., Çavuşoğlu, Ü., Eldoğan, O., & Karayel, D. (2025). Secure and efficient data encryption for Internet of Robotic Things via chaos-based Ascon. *Applied Sciences*, *15*(19), Article 10641. https://doi.org/10.3390/app151910641

Radhakrishnan, I., Jadon, S., & Honnavalli, P. B. (2024). Efficiency and security evaluation of lightweight cryptographic algorithms for resource-constrained IoT devices. *Sensors*, *24*(12), Article 4008. https://doi.org/10.3390/s24124008

Ramudin, R. P. (2019). Perkembangan pengelolaan arsip sesuai standar internasional (ISO 15489-1:2016): Studi kasus pengelolaan arsip Bank Indonesia. *Diplomatika: Jurnal Kearsipan Terapan*, *3*(1), 14–25.

Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207

Sarasa Laborda, V., Hernández-Álvarez, L., Hernández Encinas, L., Sánchez García, J. I., & Queiruga-Dios, A. (2025). Study about the performance of Ascon in Arduino devices. *Applied Sciences*, *15*(7), Article 4071. https://doi.org/10.3390/app15074071

Shaikh, R. A., Adi, K., & Logrippo, L. (2012). Dynamic risk-based decision methods for access control systems. *Computers & Security*, *31*(4), 447–464. https://doi.org/10.1016/j.cose.2012.02.006

Soto-Cruz, J., Ruiz-Ibarra, E., Vázquez-Castillo, J., Espinoza-Ruiz, A., Castillo-Atoche, A., & Mass-Sanchez, J. (2025). A survey of efficient lightweight cryptography for power-constrained microcontrollers. *Technologies*, *13*(1), Article 3. https://doi.org/10.3390/technologies13010003

Thaanyane, T. A., Lefika, P. T., & Khumalo, S. (2025). Evaluating the National University of Lesotho's records management practices with the ISO 15489. *South African Journal of Information Management*, *27*(1), Article a1955. https://doi.org/10.4102/sajim.v27i1.1955

Undang-Undang Republik Indonesia Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. (2008). *Lembaran Negara Republik Indonesia Tahun 2008 Nomor 58*.

Undang-Undang Republik Indonesia Nomor 43 Tahun 2009 tentang Kearsipan. (2009). *Lembaran Negara Republik Indonesia Tahun 2009 Nomor 152*.

Undang-Undang Republik Indonesia Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. (2022). *Lembaran Negara Republik Indonesia Tahun 2022 Nomor 196*.

Widodo, B., Fazrie, M., & Parulian, D. (2025). Lightweight cryptography for IoT in wireless sensor networks: Evaluating Speck, Simon, and Ascon using NS-3. *Electronic Journal of Education, Social Economics and Technology*, *6*(2), Article 1161. https://doi.org/10.33122/ejeset.v6i2.1161