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 dokumen dan arsip secara fundamental. Praktik kearsipan yang sebelumnya berorientasi pada media fisik kini bergeser menuju pengelolaan arsip elektronik berbasis sistem digital yang menawarkan efisiensi penyimpanan, percepatan layanan informasi, dan kemudahan temu kembali arsip. Pergeseran tersebut tidak hanya merepresentasikan perubahan media penyimpanan. Transformasi ini juga mengubah paradigma organisasi dalam memandang arsip sebagai aset informasi strategis, alat bukti hukum, dan memori

kelembagaan. Dalam konteks lembaga strategis seperti Bank Indonesia, arsip elektronik memiliki nilai vital karena mendukung proses kebijakan moneter, stabilitas sistem pembayaran, dan tata kelola kelembagaan yang akuntabel (Ramudin, 2019). Oleh karena itu, keamanan, autentisitas, dan integritas arsip elektronik menjadi aspek yang tidak dapat dipisahkan dari transformasi digital pengelolaan dokumen.

Arsip elektronik memiliki fungsi yang lebih kompleks dibanding sekadar media penyimpanan informasi. Arsip berperan sebagai bukti aktivitas organisasi yang harus mampu dipertanggungjawabkan secara administratif, hukum, dan historis. ISO 15489-1:2016 menegaskan bahwa arsip yang baik harus memenuhi empat karakter utama, yaitu authenticity, reliability, integrity, dan usability (International Organization for Standardization [ISO], 2016). Keempat karakter tersebut menjadi fondasi utama dalam menjaga nilai pembuktian arsip. Namun, karakteristik arsip digital yang mudah disalin, dimodifikasi, dipindahkan, dan didistribusikan menyebabkan autentisitas dan integritas arsip elektronik lebih rentan dibanding arsip konvensional berbasis kertas. Berbeda dengan dokumen fisik yang dapat diverifikasi melalui tanda tangan basah, cap, atau karakteristik material dokumen, arsip elektronik membutuhkan mekanisme keamanan tambahan untuk memastikan bahwa dokumen tidak mengalami perubahan tidak sah selama siklus hidupnya.

Tantangan keamanan arsip elektronik saat ini semakin kompleks seiring meningkatnya ancaman siber, mobilitas kerja digital, penggunaan perangkat pribadi (bring your own device), serta integrasi layanan berbasis awan (cloud services). Risiko yang dihadapi tidak hanya berupa akses tidak sah dan kebocoran data, tetapi juga manipulasi dokumen, hilangnya jejak kustodi digital, serta lemahnya mekanisme pembuktian integritas arsip. Penelitian Mayesti dan Hanriarseto (n.d.) menunjukkan bahwa banyak institusi publik di Indonesia belum memiliki mekanisme yang memadai untuk menjaga otentisitas arsip elektronik, terutama terkait pembatasan akses, penerapan tanda tangan elektronik, dan sistem pelacakan perubahan dokumen. Permasalahan serupa juga ditemukan Marliana et al. (2024) dalam analisis kesenjangan implementasi ISO/IEC 27001:2013 pada Ina-Geoportal Badan Informasi Geospasial yang menunjukkan rendahnya tingkat pemenuhan kontrol keamanan informasi pada sistem elektronik strategis. Selain itu, Thaanyane et al. (2025) menegaskan bahwa praktik pengelolaan arsip di berbagai institusi masih belum sepenuhnya sesuai dengan prinsip ISO 15489-1:2016, khususnya pada aspek pengendalian akses, preservasi, dan integritas arsip digital.

Selain itu, pendekatan keamanan konvensional yang hanya mengandalkan autentikasi login dan Role-Based Access Control (RBAC) dinilai tidak lagi memadai untuk menghadapi dinamika ancaman digital modern. Model keamanan berbasis perimeter mengasumsikan bahwa pengguna di dalam jaringan organisasi dapat dipercaya secara implisit. Asumsi tersebut mulai kehilangan relevansinya ketika organisasi menghadapi pola kerja jarak jauh, penggunaan perangkat lintas jaringan, serta meningkatnya ancaman dari dalam (insider threats) (Rose et al., 2020). RBAC

juga bersifat statis karena keputusan akses hanya didasarkan pada peran pengguna tanpa mempertimbangkan konteks akses seperti lokasi, waktu, perangkat, atau tujuan penggunaan dokumen. Akibatnya, pengguna yang berhasil melewati autentikasi awal berpotensi memperoleh akses berlebihan terhadap arsip dengan tingkat sensitivitas yang berbeda.

Perkembangan Zero Trust Architecture (ZTA) menawarkan paradigma baru dalam keamanan informasi melalui prinsip never trust, always verify. ZTA menolak asumsi kepercayaan implisit dan menuntut setiap permintaan akses diverifikasi secara berkelanjutan berdasarkan konteks dan tingkat risiko (Rose et al., 2020). Pendekatan ini semakin relevan dalam pengelolaan arsip elektronik karena akses terhadap arsip tidak hanya perlu memverifikasi identitas pengguna, tetapi juga memastikan bahwa konteks akses sesuai dengan tingkat sensitivitas dokumen. Dalam perkembangannya, ETSI TS 104 102 memperkenalkan metodologi Zero Trust Kipling (ZT-Kipling) yang menggunakan pendekatan 5W+1H (Who, What, Why, When, Where, dan How) untuk mengevaluasi setiap interaksi terhadap aset digital (European Telecommunications Standards Institute [ETSI], 2025). Pendekatan tersebut memungkinkan proses pengambilan keputusan akses menjadi lebih kontekstual, transparan, dan adaptif.

Penerapan evaluasi kontekstual membutuhkan mekanisme pengambilan keputusan akses yang mampu menilai tingkat risiko secara dinamis. Oleh sebab itu, konsep Risk-Based Access Control dan Policy Engine menjadi elemen penting dalam Zero Trust. Shaikh et al. (2012) menjelaskan bahwa keputusan akses dapat dilakukan melalui integrasi Policy Information Point (PIP), Policy Administration Point (PAP), Policy Decision Point (PDP), dan Policy Enforcement Point (PEP) untuk menghitung tingkat risiko sebelum memberikan izin akses. Mao et al. (2025) juga menunjukkan bahwa integrasi evaluasi risiko dan kepercayaan dinamis pada kontrol akses mampu meningkatkan akurasi pengambilan keputusan hingga 96,8 persen pada lingkungan komputasi awan. Namun demikian, sebagian besar penelitian Zero Trust masih berfokus pada aspek autentikasi dan kontrol akses, sementara aspek integritas arsip digital dan pembuktian keaslian dokumen belum banyak dibahas secara spesifik dalam konteks kearsipan elektronik. Hal ini sejalan dengan temuan Mushtaq et al. (2025) dalam tinjauan sistematis terhadap 74 publikasi Zero Trust Architecture yang menunjukkan bahwa aspek auditing, orkestrasi, dan persepsi lingkungan masih kurang dieksplorasi dibanding autentikasi dan kontrol akses.

Keamanan arsip elektronik tidak hanya berkaitan dengan siapa yang dapat mengakses arsip, tetapi juga berkaitan dengan apakah arsip yang diakses masih dapat dipercaya. Oleh karena itu, penelitian ini memperkenalkan konsep Zero Trust Integrity Score (ZTIS) sebagai skor kepercayaan integritas arsip elektronik. ZTIS dirancang untuk mengevaluasi tingkat kepercayaan arsip berdasarkan hasil integrity check, konsistensi metadata, validitas chain of custody, integritas audit log, dan indikasi manipulasi dokumen (tamper indicator). Pendekatan ini memperluas paradigma Zero Trust dari sekadar verifikasi pengguna menjadi verifikasi terhadap keandalan arsip itu

sendiri. Dengan demikian, keputusan akses pada Z-ARSIP tidak hanya dipengaruhi oleh tingkat risiko pengguna, tetapi juga oleh tingkat kepercayaan integritas dokumen yang akan diakses.

Untuk memperkuat perlindungan arsip elektronik pada lapisan teknis, penelitian ini mengusulkan penggunaan Ascon sebagai algoritma lightweight cryptography. Ascon merupakan standar kriptografi ringan yang dipilih oleh National Institute of Standards and Technology (NIST) pada tahun 2023 setelah melalui proses seleksi internasional yang panjang (Dobraunig et al., 2021; Kaur et al., 2025). Ascon-AEAD128 memungkinkan proses enkripsi dan autentikasi dokumen dilakukan secara bersamaan, sedangkan Ascon-Hash256 digunakan untuk menghasilkan fingerprint dokumen sebagai dasar verifikasi integritas arsip. Dibandingkan algoritma kriptografi konvensional, Ascon memiliki keunggulan dalam efisiensi komputasi, konsumsi sumber daya yang rendah, dan ketahanan terhadap side-channel attack sehingga relevan diterapkan pada sistem pengelolaan arsip elektronik yang melibatkan banyak titik akses dan perangkat dengan kapasitas beragam (Khan et al., 2024; Sarasa Laborda et al., 2025).

Selain perlindungan kriptografis, integritas arsip juga memerlukan mekanisme pembuktian dan pelacakan aktivitas arsip secara berkelanjutan. Oleh karena itu, penelitian ini menambahkan Integrity Assurance Layer yang mencakup integrity check, tamper detection, chain of custody, dan audit log integrity. Lapisan ini berfungsi menjaga jejak perubahan dokumen dan memastikan bahwa seluruh aktivitas terhadap arsip dapat ditelusuri secara akuntabel. Keberadaan audit trail dan chain of custody menjadi penting karena arsip elektronik tidak hanya harus aman, tetapi juga harus dapat dibuktikan keaslian dan riwayat pengelolaannya ketika digunakan sebagai alat bukti.

Berdasarkan penelusuran literatur, penelitian mengenai keamanan arsip elektronik umumnya masih membahas aspek autentikasi pengguna, penyimpanan digital, atau penerapan standar pengelolaan arsip secara terpisah. Belum banyak penelitian 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 dalam satu model keamanan arsip elektronik yang terpadu. Kesenjangan inilah yang menjadi dasar pengembangan Z-ARSIP.

Dengan demikian, penelitian ini bertujuan merancang Z-ARSIP sebagai model konseptual keamanan arsip elektronik berbasis Zero Trust Kipling dan Ascon Lightweight Cryptography untuk menjaga autentisitas, integritas, kerahasiaan, dan akuntabilitas dokumen digital. Model ini diharapkan dapat memberikan kontribusi konseptual dan metodologis dalam pengembangan kajian keamanan arsip elektronik, khususnya pada lembaga strategis yang mengelola arsip vital bernilai pembuktian tinggi.

2. METODE PENELITIAN

2.1 Pendekatan dan Jenis Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan jenis conceptual research yang bertujuan merancang model keamanan arsip elektronik berbasis Zero Trust. Pendekatan kualitatif dipilih karena penelitian berfokus pada analisis konseptual terhadap pengelolaan arsip elektronik, keamanan informasi, dan integrasi teknologi keamanan digital dalam satu kerangka model terpadu (Mayesti & Hanriarseto, n.d.; Ramudin, 2019). Z-ARSIP diposisikan sebagai model konseptual atau prototipe akademik yang dirancang untuk menjawab tantangan autentisitas, integritas, dan keamanan arsip elektronik pada lembaga strategis pengelola arsip vital. Kerangka penelitian mengadopsi logika design science research, yaitu perancangan artefak konseptual sebagai solusi atas masalah yang teridentifikasi melalui studi literatur dan analisis teoretis (Mushtaq et al., 2025). Artefak yang dihasilkan meliputi arsitektur Z-ARSIP, formula Risk Score, formula Zero Trust Integrity Score (ZTIS), serta alur pengambilan keputusan akses berbasis Zero Trust Kipling 5W+1H.

2.2 Sumber Data

Penelitian menggunakan data sekunder yang diperoleh melalui studi literatur dan studi dokumen. Literatur yang digunakan terdiri atas tiga kelompok utama. Pertama, standar dan regulasi, meliputi ISO 15489-1:2016, NIST SP 800-207 tentang Zero Trust Architecture, ETSI TS 104 102 tentang ZT-Kipling Methodology, serta regulasi nasional seperti Undang-Undang Nomor 43 Tahun 2009 tentang Kearsipan, Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik beserta perubahannya, dan Undang-Undang Nomor 27 Tahun 2022 tentang Pelindungan Data Pribadi. Kedua, literatur ilmiah yang membahas Zero Trust Architecture, Risk-Based Access Control, Policy Engine, dan lightweight cryptography (Dobraunig et al., 2021; Kaur et al., 2025; Mao et al., 2025; Rose et al., 2020). Ketiga, literatur kearsipan dan keamanan informasi terkait autentisitas, integritas, serta pengelolaan arsip digital di Indonesia (Ismayati, 2014; Marliana et al., 2024; Ramudin, 2019). Data dokumen juga diperoleh dari publikasi resmi mengenai penerapan pengelolaan arsip berbasis ISO 15489-1:2016 pada lembaga strategis.

2.3 Tahapan Penelitian

Penelitian dilaksanakan melalui lima tahapan. Tahap pertama adalah problem identification, yaitu identifikasi kesenjangan penelitian terkait keterbatasan keamanan arsip elektronik konvensional yang umumnya masih terpisah antara pengelolaan arsip, kontrol akses, dan perlindungan integritas dokumen.

Tahap kedua adalah requirement formulation, yaitu perumusan kebutuhan model berdasarkan prinsip ISO 15489-1:2016 dan Zero Trust Architecture. Pada tahap ini ditetapkan bahwa model harus mampu menjaga autentisitas, integritas, akuntabilitas, dan keamanan akses arsip secara bersamaan.

Tahap ketiga adalah conceptual design, yaitu perancangan arsitektur Z-ARSIP yang mengintegrasikan enam komponen utama: ISO 15489-1:2016, Zero Trust Kipling 5W+1H, Risk-Based Access Control dan Policy Engine, ZTIS, Ascon Lightweight Cryptography, serta Integrity Assurance Layer. Pada tahap ini dirumuskan formula Risk Score dan ZTIS sebagai dasar pengambilan keputusan akses dan evaluasi integritas arsip.

Tahap keempat adalah workflow design, yaitu penyusunan alur sistem mulai dari permintaan akses arsip, evaluasi konteks 5W+1H, perhitungan Risk Score dan ZTIS oleh Policy Decision Point (PDP), penegakan keputusan akses oleh Policy Enforcement Point (PEP), hingga pencatatan audit log dan chain of custody.

Tahap kelima adalah conceptual validation, yaitu validasi konseptual model melalui penyandingan dengan standar, regulasi, dan penelitian terdahulu. Validasi dilakukan dengan menilai kesesuaian model terhadap prinsip ISO 15489-1:2016, Zero Trust Architecture, dan kebutuhan keamanan arsip elektronik pada organisasi strategis.

2.4 Teknik Analisis Data

Analisis data dilakukan menggunakan teknik content analysis dan analisis komparatif. Content analysis digunakan untuk mengekstrak prinsip-prinsip utama dari standar, regulasi, dan literatur ilmiah terkait pengelolaan arsip elektronik dan keamanan informasi. Sementara itu, analisis komparatif digunakan untuk membandingkan Z-ARSIP dengan model keamanan lain seperti risk-based access control dan Zero Trust access control pada lingkungan komputasi awan (Alharbe et al., 2023; Mao et al., 2025). Hasil analisis kemudian disintesiskan ke dalam model konseptual yang menghubungkan aspek kebijakan, manusia, dan teknologi dalam pengelolaan arsip elektronik berbasis Zero Trust.

2.5 Batasan Penelitian

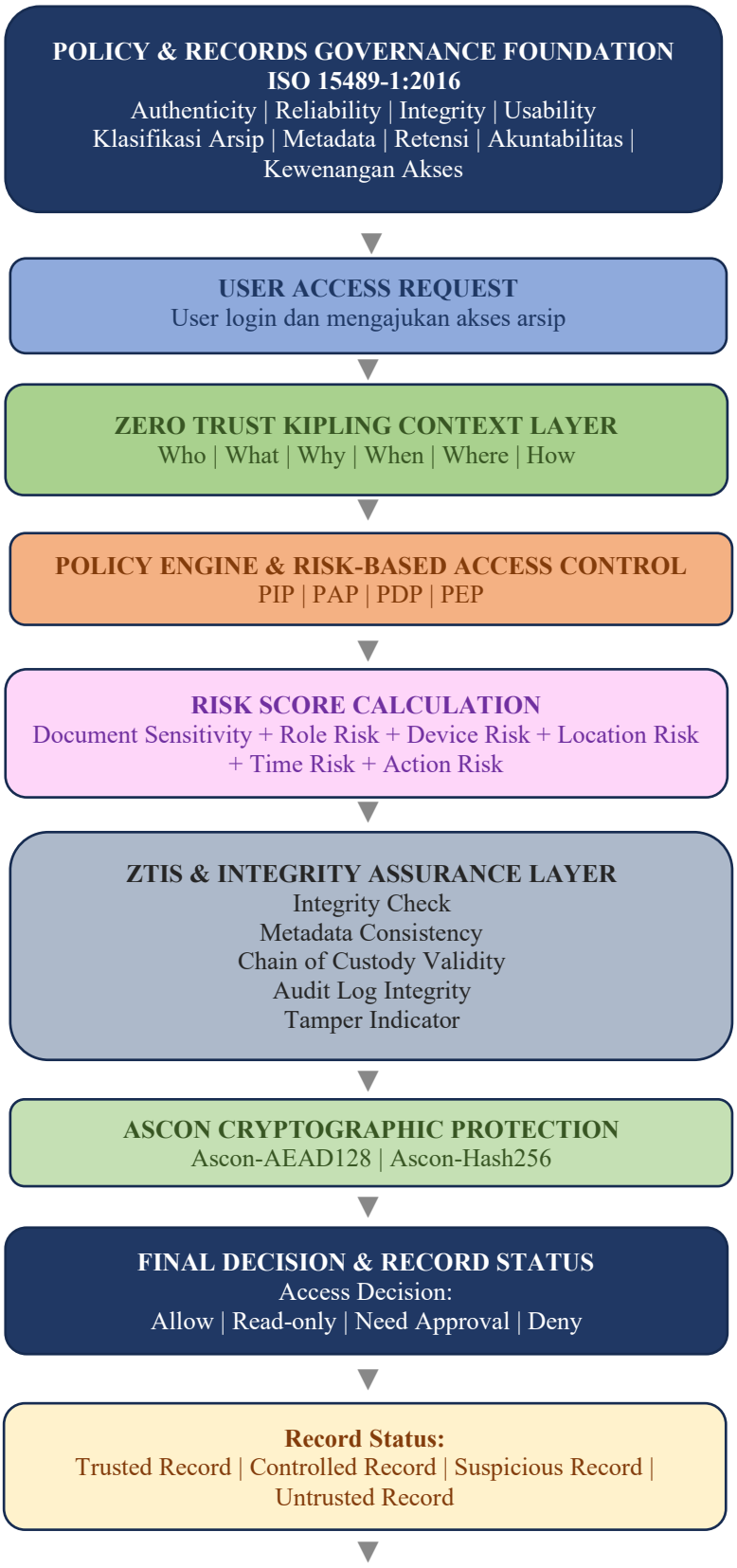
Penelitian ini memiliki beberapa batasan. Pertama, Z-ARSIP merupakan model konseptual dan belum diimplementasikan pada sistem operasional lembaga tertentu. Kedua, penggunaan Ascon dibahas pada tataran rancangan konseptual sehingga pengujian performa teknis, seperti throughput dan konsumsi daya, tidak dilakukan secara empiris. Ketiga, evaluasi model dilakukan melalui pendekatan konseptual dan literatur, sedangkan pengujian langsung terhadap pengguna dan skenario ancaman nyata menjadi ruang pengembangan penelitian selanjutnya.

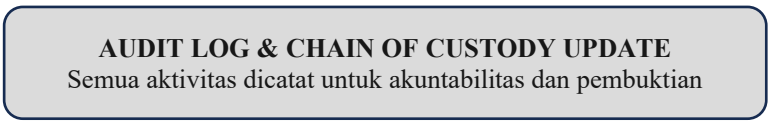
3. PEMBAHASAN

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*

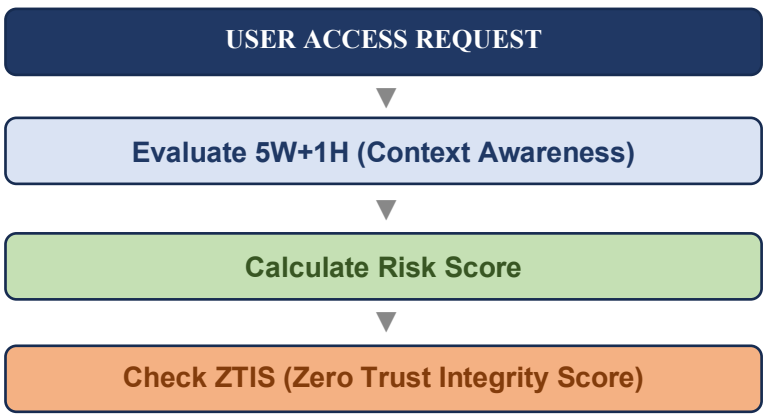
3.2 Penerapan ZT-Kipling 5W+1H pada Akses Arsip Elektronik

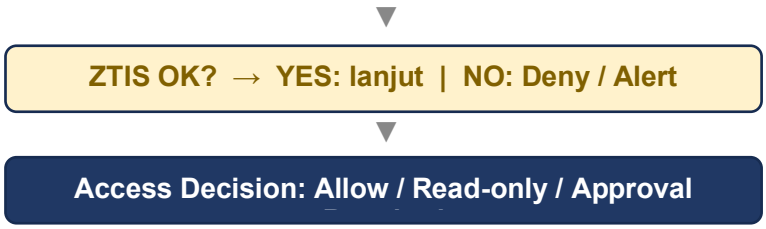
Pendekatan ZT-Kipling memungkinkan setiap permintaan akses arsip dievaluasi secara kontekstual dan eksplisit. Pada Z-ARSIP, keenam pertanyaan Kipling diterjemahkan ke dalam variabel akses arsip sebagai berikut. Who mengacu pada identitas pengguna beserta peran (arsiparis, pejabat, auditor, pihak ketiga). 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:

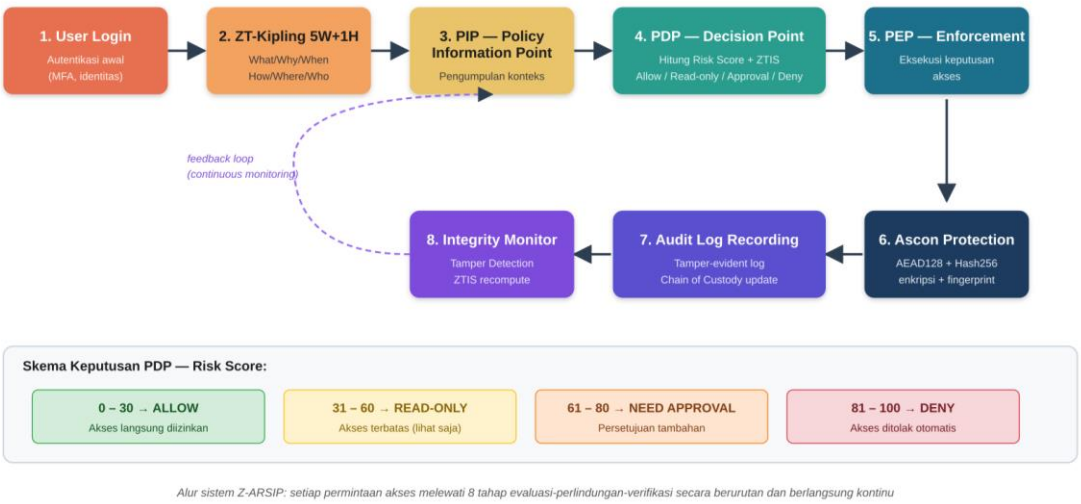
$$Risk\ Score = Document\ Sensitivity + Role\ Risk + Device\ Risk + Location\ Risk + Time\ Risk + Action\ Risk$$

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 3. *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 penggguna 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 perangkat terdaftar	**Who:** auditor; **What:** arsip confidential; **Why:** pemeriksaan; **When:** luar jam kerja; **Where:** VPN	Document Sensitivity 40 + Role Risk 5 + Device Risk 0 + Location Risk 5 + Time Risk	70	82	Need Approval	Akses memerlukan persetujuan tambahan karena dokumen bersifat

		resmi; **How:** mengunduh dokumen	10 + Action Risk 10				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 mendeteksi perubahan hash	**Who:** arsiparis; **What:** arsip restricted; **Why:** validasi retensi; **When:** jam kerja; **Where:** jaringan kantor; **How:**	Document Sensitivity 30 + Role Risk 0 + Device Risk 0 + Location Risk 0 + Time Risk 0 + Action Risk 5	35	58	Read-only + Integrity Alert	Akses dibatasi karena ZTIS berada pada kategori **Suspicious Record**. Sistem memberi

		membuka dan memverifikasi metadata					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 4.

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