Framework Integrasi *Digital Forensic Readiness* dan *Information Security Management System* di lingkungan Pemerintahan

Rico Agung Firmansyah
20917051

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer
Konsentrasi Forensika Digital
Program Studi Informatika Program Magister
Fakultas Teknologi Industri
Universitas Islam Indonesia

2024

Lembar Pernyataan Keaslian

Demi Allah, saya akui karya ini adalah hasil kerjsa saya sendiri kecuali nukilan dan ringkasan yang setiap satunya telah saya jelaskan sumbernya. Jika dikemudian hari ternyata terbukti pengakuan saya ini tidak benar dan melanggar oeraturan yang sah dalam karya tulis dan Hak Kekayaan Intelektual, maka saya bersedia ijasah yang telah saya terima untuk ditarik kembali oleh Universitas Islam Indonesia.

Yogyakarta, Maret 2025

Rico Agung Firmansyah

20917051

Lembar Pengesahan Pembimbing

***Framework* Integrasi *Digital Forensic Readiness* dan *Information Security Management System* di lingkungan Pemerintahan**

Rico Agung Firmansyah
20917051

Yogyakarta, Maret 2025

Pembimbing I	Pembimbing II
Dr. Yudi Prayudi, S.Si., M.Kom	Dr. Ahmad Luthfi, S.Kom., M.Kom

Lembar Pengesahan Penguji

***Framework* Integrasi *Digital Forensic Readiness* dan *Information Security Management System* di lingkungan Pemerintahan**

Rico Agung Firmansyah
20917051

Yogyakarta, Maret 2025

Tim Penguji,

Dr. Yudi Prayudi, S.Si., M.Kom
Ketua

Dr. Ahmad Luthfi, S.Kom., M.Kom.
Anggota I

Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D
Anggota II

11/03/2025

Mengetahui,
Ketua Program Studi Teknik Informatika Program Magister
Universitas Islam Indonesia

Ir. Irving Vitra Paputungan, S.T., M.Sc., Ph.D

Abstrak

Framework Integrasi *Digital Forensic Readiness* dan *Information Security Management System* di lingkungan Pemerintahan

Transformasi *Digital* di Indonesia dan berbagai negara telah menghadirkan manfaat signifikan dalam peningkatan layanan publik dan tata kelola pemerintahan melalui implementasi *e-Government, e-transaction, e-payment*, dan layanan *Digital* lainnya. Namun selain dampak positif, transformasi *Digital* ini juga membawa tantangan keamanan dalam pengelolaan data *Digital* yang memerlukan pendekatan komprehensif, mengingat Indonesia mengalami peningkatan yang signifikan seperti contohnya rilis dari BSSN per tahun 2022 terdapat 370,02 juta serangan (meningkat 38,72% dari 2021), dan 403,9 juta serangan pada 2023 (meningkat 9,16%) dengan beragam pola anomali serangan seperti pelanggaran data, serangan *ransomware*, eksploitasi sistem, penggunaan akses yang tidak semestinya dan pola serangan lainnya.

Untuk menjawab masalah tersebut sekaligus membangun *sustainability* pada sistem berbasis elektronik dibutuhkan kesiapan organisasi dalam hal tata kelola dan manajemen (seperti diantaranya manajemen risiko, manajemen aset, manajemen sumberdaya, manajemen SDM, manajemen pengetahuan, manajemen infrastruktur, manajemen keamanan, dan manajemen insiden). Sistem Pemerintahan Berbasis Elektronik (SPBE) telah memenuhi sebagian besar dari kebutuhan tata kelola dan manajemen tersebut, namun penerapan SMKI yang sudah dilegalkan dan diterapkan di beberapa lembaga tidak memasukkan aspek penting dalam penanganan dan investigasi jika terjadi insiden. BSSN sebagai garda keamanan *Digital* indonesia membuat, mempublikasikan, serta menghimbau penerapan *Information Security Management Systems* (ISMS) atau Sistem manajemen keamanan informasi (SMKI) dalam domain *e-governance* dengan cukup baik, bahkan terdapat *assessment tools* berupa Indeks Keamanan Informasi (IKAMI) yang dapat digunakan untuk memastikan kesiapan organisasi dalam hal keamanan data dan informasi. Namun penerapan *Digital Forensik Readiness* belum digunakan di dalam Sistem pemerintahan. DFR berperan untuk memastikan kesiapan organisasi terhadap pencegahan dan penanganan insiden keamanan informasi yang lebih terperinci. DFR dibutuhkan dalam proses investigasi yang terjadi pada ancaman maupun insiden keamanan siber seperti pengumpulan bukti *Digital*, analisis bukti *Digital*, analisis pola serangan, serta analisa pasca insiden yang dilakukan secara efektif, sistematis, terukur

dapat dibuktikan atau dapat dipertanggungjawabkan *(evidence based)*. Tidak diterapkannya DFR pada ISMS berpeluang terjadinya kegagalan pengamanan data secara komprehensif pada suatu organisasi.

Penelitian ini dilakukan untuk mencari, menganalisa dan memastikan peranan DFR terhadap ISMS yang dapat diimplementasikan di lingkungan *e-Government* di berbagai area baik di Indonesia maupun di dunia global dengan menggunakan pendekatan analisa SLR terhadap berbagai artikel ilmiah terpublikasi di berbagai jurnal bereputasi. Selain itu, hasil analisis penelitian ini akan menjadi *output* penting dalam membangun *Framework model* pengintegrasian DFR kedalam SMKI yang telah eksisting diterapkan dilingkungan pemerintahan berbasis elektronik.

Untuk mencapai tujuan penelitian tersebut, metodologi SLR dan beberapa pendekatan validasi lainnya digunakan. SLR merupakan serangkaian proses yang ketat dan transparan dalam mengidentifikasi, memfilter, menganalisis, dan mensintesis studi-studi relevan yang diterbitkan dalam jurnal terpublikasi bereputasi dengan menerapkan kerangka kerja yang terstandarisasi secara global. Tinjauan ini berfokus pada karya-karya yang membahas integrasi kesiapan forensik dan keamanan informasi dalam konteks pemerintahan, dengan penekanan pada implementasi, tantangan, dan hasilnya. Selain pendekatan SLR metode bibliografi dan pemetaan *(mapping)* terhadap standar tertentu maupun *Framework* yang relevan juga digunakan dalam penelitian ini.

Temuan awal menunjukkan bahwa meskipun implementasi DFR dan ISMS secara terpisah cukup umum, integrasi keduanya masih kurang dieksplorasi, terutama dalam konteks *e-governance*. Penelitian ini mengidentifikasi tantangan utama, termasuk inersia organisasi, ketidakcocokan teknologi, dan kesenjangan kebijakan, sekaligus menyoroti praktek terbaik *(best practice)* dari studi kasus global. Hasil penelitian tidak hanya dapat memetakan trend dan validasi mengenai urgensi penerapan DFR kedalam ISMS, namun juga memberikan *Framework Model Integrasi* DFR bagi organisasi. Hasil penelitian diharapkan dapat memberikan wawasan yang dapat diimplementasikan bagi pembuat kebijakan, profesional TI, dan peneliti, serta membuka jalan bagi kerangka kerja terpadu yang menjembatani kesenjangan antara kesiapan forensik dan manajemen keamanan yang komprehensif. Penelitian ini menyimpulkan dengan menganjurkan integrasi DFR dan ISMS sebagai pilar utama sistem *e-governance* untuk meningkatkan kesiapan keamanan siber, memperkuat

akuntabilitas, dan mengurangi risiko yang terkait dengan transformasi *Digital* di sektor publik.

Kata kunci

Digital Forensic Readiness, Digital Forensic Framework, cyber security, information system Management system, e-governance, e-Government, systematic literature Review, Framework model

Abstract

Integration Framework of Digital Forensic Readiness and Information Security Management System in Government Environment System

Digital transformation in Indonesia and various countries has brought significant benefits in improving public services and governance through the implementation of *e-Government*, e-transactions, e-payments, and other *Digital* services. However, besides the positive *impact*s, this *Digital* transformation also brings *security Challenges* in *Digital* data *Management* that require a comprehensive approach, considering Indonesia has experienced significant increases as exemplified by BSSN's release showing 370.02 million *attack*s in 2022 (increased by 38.72% from 2021), and 403.9 million *attack*s in 2023 (increased by 9.16%) with various *attack* anomaly patterns such as data breaches, *ransomware attack*s, *system* exploitation, improper access usage, and other *attack* patterns.

To address these issues while building sustainability in electronic-based *system*s, *Organizationa*l *Readiness* is required in terms of governance and *Management* (including risk *Management*, asset *Management*, resource *Management*, human resource *Management*, knowledge *Management*, infrastructure *Management*, *security Management*, and *Incident Management*). The Electronic-Based *Government System* (SPBE) has fulfilled most of these governance and *Management* needs, however, the implementation of ISMS that has been legalized and implemented in several institutions does not *include* important aspects in handling and investigating *Incident*s. BSSN as Indonesia's *Digital security* guard creates, publishes, and encourages the implementation of *Information Security Management System*s (ISMS) in the *e-governance* domain quite well, even providing *assessment tools* in the form of *Information Security Index* (IKAMI) that can be used to ensure *Organizationa*l *Readiness* in terms of data and *information security*. However, *Digital Forensic Readiness* has not been implemented in the *Government system*. DFR serves to ensure *Organizationa*l *Readiness* for more detailed prevention and handling of *information security Incident*s. DFR is needed in the investigation process that occurs in *cyber security* threats and *Incident*s such as *Digital* evidence *collection*, *Digital* evidence analysis, *attack* pattern analysis, and post-*Incident* analysis conducted effectively, *systematic*ally, measurably, and can be proven or accountable (evidence-based). The non-implementation of DFR in ISMS creates opportunities for comprehensive data *security* failures in an *Organization*.

This *research* is conducted to find, analyze, and ensure the role of DFR in ISMS that can be implemented in *e-Government* environments across various areas both in Indonesia and globally using SLR analysis approach on various scientific articles published in reputable journals. Furthermore, the results of this *research* analysis will become an important output in building a *Framework model* for integrating DFR into existing ISMS implemented in electronic-based *Government* environments.

To achieve these *research* objectives, SLR *Methodology* and several other validation *Approaches* are used. SLR is a rigorous and transparent process in identifying, filtering, analyzing, and synthesizing relevant studies published in reputable published journals by applying globally standardized *Framework*s. This *Review* focuses on works discussing the integration of *Forensic Readiness* and *information security* in the governance context, emphasizing implementation, *Challenges*, and outcomes. Besides the SLR approach, bibliographic methods and mapping against certain standards or relevant *Framework*s are also used in this *research*.

Initial findings indicate that while the implementation of DFR and ISMS separately is quite common, their integration remains underexplored, especially in the *e-governance* context. This *research* identifies key *Challenges*, including *Organization*al inertia, technological incompatibility, and *Policy* gaps, while highlighting best practices from global case studies. The *research* results not only map trends and validate the urgency of implementing DFR into ISMS but also provide an Integration *Framework Model* of DFR for *Organization*s. The findings are expected to provide implementable insights for *Policy*makers, IT professionals, and *research*ers, as well as pave the way for an integrated *Framework* that bridges the gap between *Forensic Readiness* and comprehensive *security Management*. This *research* concludes by advocating the integration of DFR and ISMS as main pillars of *e-governance system*s to enhance *cyber security Readiness*, strengthen accountability, and mitigate risks associated with *Digital* transformation in the public sector.

Keywords

Digital Forensic Readiness, Digital Forensic Framework, cyber security, information system Management system, e-governance, e-Government, systematic literature Review, Framework model

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak cipta yang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Januari 2024

Rico Agung Firmansyah, S.Kom

Daftar Publikasi

Publikasi yang menjadi bagian dari tesis

Publikasi berikut menjadi bagian dari Bab 2, 3 dan 4

Firmansyah, R. A., Prayudi, Y., & Luthfi, A. (2025). Integrasi Digital Forensic Readiness dan Information Security Management System pada Organisasi Pemerintahan: Systematic Literature Review. JATI (Jurnal Mahasiswa Teknik Informatika), 9(2). doi.org/10.36040/jati.v9i2.13126.

https://ejournal.itn.ac.id/index.php/jati/article/view/13126

Kontributor	Jenis Kontribusi
Rico Agung Firmansyah	Mendesain eksperimen (70%) Menulis *paper* (70%)
Dr. Yudi Prayudi, S.Si., M. Kom	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (20%)
Dr. Ahmad Luthfi, S.Kom., M.Kom	Mendesain eksperimen (20%) Menulis dan mengedit *paper* (20%)

Halaman Kontribusi

Dr. Yudi Prayudi, S.Si., M.Kom selaku Pembimbing I dan Bapak Dr. Ahmad Luthfi, S.Kom., M.Kom selaku Pembimbing II yang telah memberikan arahan-arahannya kepada penulis, sehingga penulisan tesis ini bisa selesai dengan baik.

Halaman Persembahan

Ku persembahkan tesis ku ini untuk :

Ibunda tercinta dan Almarhum Ayah tersayang, akan aku dedikasikan ilmu dan segenap daya upayaku untuk kebahagiaan kalian berdua.

Istri tercinta yang selalu mendampingi lahir batinku dalam kondisi apapun.

Kakak, adik serta semua Keluarga besar kami,

Sahabat dan Rekan-rekan ku Forensika *Digital* angkatan XX,

Tim Konsultan Amanin & MMM yang berkontribusi dalam penatnya tekanan pekerjaan dan profesionalisme serta ketabahan dalam berkah yang tak ternilai.

Semua pihak yang telah berkontribusi secara langsung maupun tak langsung sehingga tesis ini terselesaikan dengan baik.

Semua pihak yang merasa mendapatkan manfaat dari hasil penelitian, tulisan, ataupun data-data yang ada dalam dokumen ini, semoga jadi manfaat dan berkah untuk kita semua. Aamiin.

Kata Pengantar

Puji syukur kehadirat Allah SWT atas limpahan rahmat dan karunia-Nya sehingga penulis dapat menyelesaikan tesis berjudul "*Framework* Integrasi *Digital Forensic Readiness* dan *Information Security Management System* di Lingkungan Pemerintahan" sebagai salah satu syarat untuk memperoleh gelar Magister Komputer pada Program Studi Informatika Program Magister, Fakultas Teknologi Industri, Universitas Islam Indonesia.

Tesis ini disusun dengan tujuan untuk memberikan kontribusi ilmiah terkait integrasi *Digital Forensic Readiness* (DFR) dan *Information Security Management System* (ISMS) dalam mendukung keamanan informasi di sistem pemerintahan berbasis elektronik *(e-Government).* Dalam proses penyusunan tesis ini, penulis mendapatkan banyak dukungan, arahan, dan motivasi dari berbagai pihak yang tidak dapat disebutkan satu per satu. Oleh karena itu, pada kesempatan ini, penulis ingin menyampaikan penghargaan dan ucapan terima kasih yang sebesar-besarnya kepada:

1. Dr. Yudi Prayudi, S.Si., M.Kom, selaku pembimbing utama, dan Dr. Ahmad Luthfi, S.Kom., M.Kom, selaku pembimbing pendamping, atas bimbingan, arahan, serta dukungan yang luar biasa selama proses penyusunan tesis ini.
2. Seluruh dosen dan staf pengajar di Program Magister Informatika, Universitas Islam Indonesia, yang telah memberikan ilmu dan wawasan selama masa studi.
3. Keluarga tercinta yang selalu memberikan doa, semangat, dan dukungan moral maupun material tanpa henti.
4. Rekan-rekan mahasiswa Program Magister Informatika atas diskusi dan kebersamaan yang menjadi motivasi selama menyelesaikan studi.

Penulis menyadari bahwa tesis ini masih memiliki keterbatasan. Oleh karena itu, kritik dan saran yang membangun sangat diharapkan untuk penyempurnaan di masa mendatang. Penulis berharap tesis ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya dalam bidang keamanan informasi dan *Digital* forensik, serta dapat menjadi referensi bagi peneliti, praktisi, dan pembuat kebijakan.

Yogyakarta, Januari 2025

Rico Agung Firmansyah

Daftar Isi

Daftar Tabel

D**aftar Gambar**

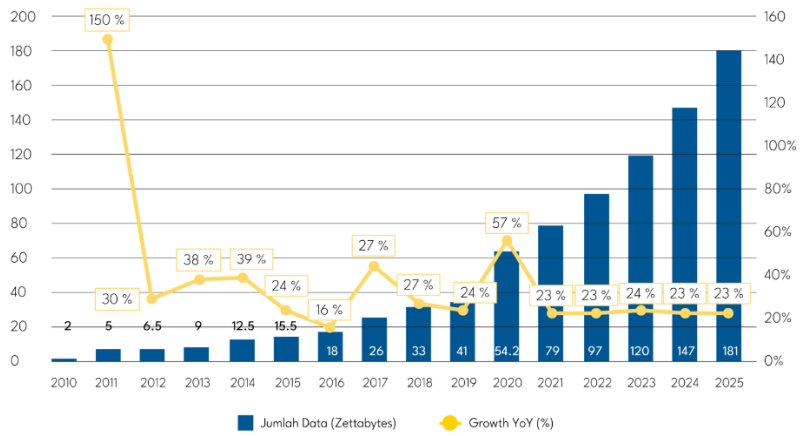
Glosarium

CSPCR	- *Cloud Security*, *Privacy* and *Compliance Readiness*
DF	- *Digital Forensic*
DFR	- *Digital Forensic Readiness*
DFRF	- *Digital Forensic Readiness Framework*
DFRI	- *Digital Forensic Readiness Index*
DSRM	- *Design* Science *Research Methodology*
e-Gov	- electronic-*Government*, *e-governance*
IKAMI	- Indeks Keamanan Informasi
ISMS	- *Information Security Management System*
ISO/IEC	- *International Organization for Standardization / International Electrotechnical Commission*
RQ	- *Research Question*
SMKI	- Sistem Manajemen Keamanan Informasi
SDM	- Sumber Daya Manusia
SLR	- *Systematic Literature Review*
SPBE	- Sistem Pemerintahan Berbasis Elektronik

BAB 1
Pendahuluan

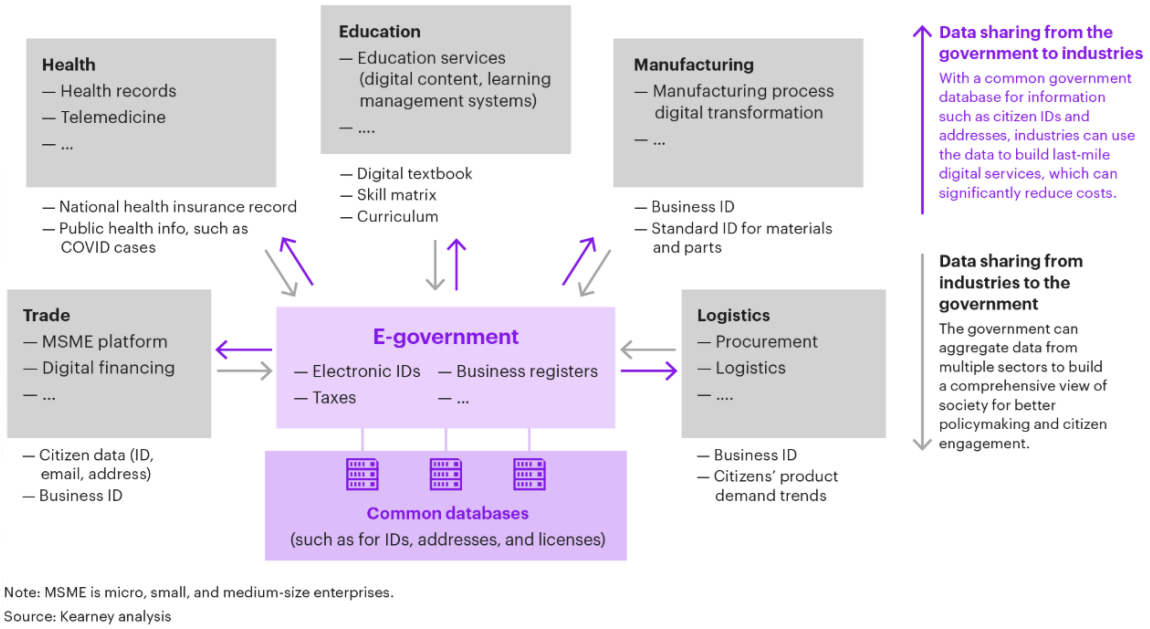
1.1 Latar Belakang

Transformasi *Digital* yang diterapkan di banyak negara, termasuk juga di indonesia diterapkan guna menjawab tantangan kebutuhan global telah membawa manfaat signifikan dalam banyak hal seperti peningkatan akurasi, performa, efisiensi dan aksesibilitas di banyak lini kehidupan mulai dari aspek finansial, perdagangan, pendidikan, pertanian, keamanan, legal hukum, tata kota, transportasi dan banyak lagi lainnya termasuk dalam hal layanan publik di sistem pemerintahan (Gusman, S. W., 2022 & Mangindaan, D., Adib, A., Febrianta, H., & Hutabarat, D. J. C., 2024). Salah satu contoh penerapan Transformasi *Digital* yaitu Sistem Pemerintahan Berbasis Elektronik (SPBE) yang merupakan ruh dari *E-Government*. SPBE merupakan sebuah konsep yang merujuk pada penggunaan teknologi informasi dan komunikasi (TIK) oleh pemerintah untuk meningkatkan efektivitas dan efisiensi pelayanan publik (Hidayat, T., & Putri, R. A, 2023 & Hidayat, E. D., & Purwaningsih, S. B, 2024). Dalam era *Digital*, keamanan informasi menjadi sangat krusial, karena data dan informasi yang dikelola oleh pemerintah sangat sensitif dan penting untuk keamanan negara, kepercayaan publik, dan kelancaran operasional pemerintahan. SPBE merupakan sistem yang terhubung dengan berbagai layanan publik berdasarkan arsitektur sistem, arsitektur aplikasi, arsitektur data, arsitektur infrastruktur *Digital*, serta arsitektur keamanan data dan informasi. Penerapan transformasi *Digital* dalam organisasi bisa dilihat dari berbagai wujud nyata yang dirasakan oleh penggunanya, seperti *e-Government/e-governance*, *e-transaction*, *e-payment*, dan sebagainya seperti yang disajikan pada perpespektif gambar 1 dan gambar 2 berikut ini.



Gambar 1.1. Data Tren Pertumbuhan Data *Center* di Indonesia 2010-2025,

(Sumber: https://www.arghajata.com/id/insight/2024/05/*Digital*-transformation-trends, diakses 24/12/2024)

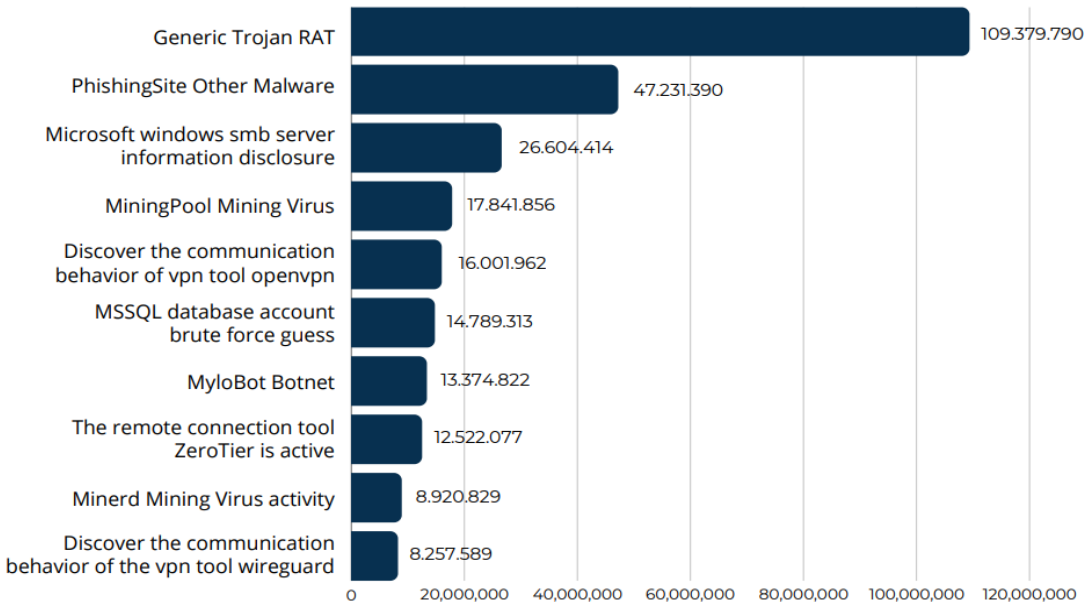


Gambar 1.2. *Digital Transformation Landscape Impact Area*, (sumber: https://www.kearney.com/industry/public-sector/article/-/insights/transforming-indonesia-s-*e-Government*-landscape, diakses 24/12/2024)

Penjabaran penggunaan sistem *Digital*isasi yang kompleks dalam suatu organisasi tersebut diatas sering juga disebut dengan Sistem *Enterprise* atau *Enterprise Architecture* dimana dalam satu organisasi terdapat banyak layanan, banyak aplikasi, banyak data, banyak infrastruktur yang saling terintegrasi untuk memproses data dan informasi tertentu baik internal organisasi maupun eksternal organisasi (Suryono, R. R., Budi, I., & Purwandari, B, 2020 & Zulfikar,F & Wahyu, W.W, 2023). Sistem yang kompleks ini menjadi dampak positif sekaligus negatif bagi organisasi, stakeholder dan penggunanya. Kemudahan, kecepatan, keakuratan, serta efektivitas dan efisiensi pemrosesan data dan informasi menjadi dampak positif yang diharapkan. Namun dampak negatif atau konsekuensi terhadap pemrosesan dan pengolahan data yang kompleks tersebut baik di area privat maupun publik menjadikan urgensi yang perlu dijaga dengan baik keamanannya yaitu keutuhan data, integritas data dan ketersediaan akses data berdasarkan perspektif teknis maupun non teknis, karena hal tersebut membawa dampak yang cukup signifikan. Beberapa contoh insiden ancaman siber di indonesia terhadap sektor publik (sistem pemerintahan berbasis elektronik) maupun sektor privat (korporasi, organisasi, swasta) pada dekade terakhir ini menunjukan

bahwa perubahan pola kehidupan *Digital*isasi membutuhkan kesiapan pengamanan data dan sistem yang serius Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N, 2019). Seperti contohnya rilis dari BSSN per tahun 2022 terdapat 370,02 juta serangan (meningkat 38,72% dari 2021), dan 403,9 juta serangan pada 2023 (meningkat 9,16%) dengan beragam pola anomali serangan seperti pelanggaran data, serangan *ransomware*, eksploitasi sistem, penggunaan akses yang tidak semestinya dan pola serangan lainnya. Gambar berikut ini menjelasakan trafik anomali data yang dirilis BSSN selama tahun 2023 saja.

Gambar 1.3. Data Trafik Anomali di Indonesia per 2023 rilis versi BSSN (Sumber: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf , diakses 24/12/2024)



Gambar 1.4. Data 10 Jenis serangan keamanan siber di indonesia tahun 2023

(Sumber: https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf , diakses 24/12/2024)

Ancaman seperti pelanggaran data, serangan *ransomware*, virus, *phising*, eksploitasi sistem, penggunaan akses yang tidak semestinya, dan beragam pola serangan lainnya seringkali memanfaatkan celah data, celah sistem, ataupun celah dalam merespon suatu insiden atau proses penanganan insiden tertentu. Kerugian dari insiden keamanan data dan informasi tersebut juga dinilai sangat besar baik bagi organisasi maupun bagi penggunanya.

Untuk menjawab masalah tersebut sekaligus membangun *sustainability* pada sistem berbasis elektronik dibutuhkan kesiapan organisasi dalam hal tata kelola dan manajemen (seperti diantaranya manajemen risiko, manajemen aset, manajemen sumberdaya, manajemen SDM, manajemen pengetahuan, manajemen infrastruktur, manajemen keamanan, dan manajemen insiden). Sistem Pemerintahan Berbasis Elektronik (SPBE) telah memenuhi sebagian besar dari kebutuhan tata kelola dan manajemen tersebut, namun penerapan Sistem Manajemen Keamanan Informasi (SMKI) yang sudah dilegalkan dan diterapkan di beberapa lembaga tidak memasukkan aspek penting dalam penanganan dan investigasi jika terjadi insiden pada sistem. SMKI adalah serangkaian kebijakan dan prosedur yang dirancang untuk mengelola dan melindungi data dan informasi dalam organisasi. SMKI merupakan standar sekaligus *Framework* dalam tata kelola dan manajemen data dan informasi yang ingin dicapai oleh organisasi baik organisasi pemerintah maupun sektor swasta. Dalam konteks pemerintahan berbasis elektronik, SMKI berfungsi untuk melindungi aset yang dikelola organisasi, mulai dari data sensitif, informasi yang

dimiliki organisasi, serta infrastruktur penopang layanan publik. SMKI memberikan pendekatan yang terstruktur untuk menilai risiko keamanan, menerapkan kebijakan keamanan, dan menanggapi ancaman yang ada dengan kemampuan dan kesiapan organisasi.

BSSN sebagai garda keamanan *Digital* indonesia membuat, mempublikasikan, serta menghimbau penerapan *Information Security Management Systems* (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) dalam domain *e-governance* dengan cukup baik, bahkan terdapat *assessment tools* berupa Indeks Keamanan Informasi (IKAMI) yang dapat digunakan untuk memastikan kesiapan organisasi dalam hal keamanan data dan informasi. Namun penerapan *Digital Forensik Readiness* belum digunakan di dalam Sistem pemerintahan. DFR berperan untuk memastikan kesiapan organisasi terhadap pencegahan dan penanganan insiden keamanan informasi yang lebih terperinci. DFR Dibutuhkan dalam proses investigasi yang terjadi pada ancaman maupun insiden keamanan siber seperti pengumpulan bukti *Digital*, analisis bukti *Digital*, analisis pola serangan, serta analisa pasca insiden yang dilakukan secara efektif, sistematis, terukur dapat dibuktikan atau dapat dipertanggungjawabkan *(evidence based)* (Ariffin, K.A.Z., & Ahmad, F.H, 2021). DFR berperan penting dalam memastikan bahwa ketika terjadi pelanggaran atau insiden siber, bukti dapat dikumpulkan dan dianalisis dengan cara yang sah dan efisien. Tidak diterapkannya DFR pada ISMS berpeluang terjadinya kegagalan pengamanan data secara komprehensif pada suatu organisasi.

DFR dan SMKI saling mendukung dalam membangun sistem keamanan informasi yang komprehensif. DFR memastikan bahwa data yang relevan untuk investigasi tersedia dan dapat diakses, sedangkan ISMS membantu dalam pengelolaan dan perlindungan data tersebut (Ariffin, K.A.Z., & Ahmad, F.H, 2021). Dalam konteks pemerintahan berbasis elektronik, hubungan antara keduanya sangat penting untuk menciptakan lingkungan yang aman bagi data dan informasi yang dikelola oleh organisasi. ISMS digunakan untuk memastikan bahwa aset dapat terlindungi secara proaktif dari berbagai serangan/ancaman yang ada, atau dengan kata lain sebelum terjadinya insiden (pra-*Incident*) (Karokola, G. R. (2012). Sedangkan DFR memastikan bahwa sistem yang ada dapat bereaksi secara cepat dan efektif terhadap insiden keamanan informasi, serta memastikan data dan informasi tercadangkan dan dapat direstorasi dengan baik setelah insiden terjadi *(pasca-Incident)*.

DFR tidak hanya mencakup investigasi reaktif setelah kejadian insiden, tetapi juga pendekatan proaktif yang memastikan bahwa organisasi siap mengumpulkan bukti *Digital* yang diperlukan untuk investigasi dengan minim gangguan pada proses bisnis, namun juga memperkuat kebijakan dan prosedur ISMS yang sudah ada, sehingga organisasi dapat

melanjutkan operasional dengan gangguan minimal sambil tetap mematuhi regulasi hukum yang ada (T Gobler, et.al, 2007 & Pangalos, G.,). Selain itu, DFR menjadi bagian dari praktik terbaik ISMS karena dapat membantu memastikan keamanan yang lebih baik dengan menyarankan agar kontrol keamanan, kebijakan, dan prosedur diintegrasikan ke dalam strategi ISMS untuk memfasilitasi investigasi yang sukses ketika insiden terjadi. Proses DFR yang matang memungkinkan organisasi untuk menangani insiden keamanan dengan lebih efektif, sambil tetap menjaga keutuhan dan keabsahan bukti *Digital* untuk tindakan hukum. DFR memengaruhi seluruh siklus manajemen IS, mulai dari perencanaan hingga evaluasi (T Gobler, et.al, 2007).. Hal ini berarti bahwa dengan mengintegrasikan teknik forensik *Digital* ke dalam ISMS, organisasi dapat menilai kerentanannya lebih baik, melakukan penetration testing, dan audit untuk menilai keamanan sistem yang ada. DFR menambahkan kontrol dan prosedur yang diperlukan untuk melakukan investigasi yang sukses, sehingga memperkuat postur keamanan ISMS yang sudah ada (T Gobler, et.al, 2007 & Pangalos, G.,).

Sayangnya, penerapan ISMS dan DFR dalam organisasi menjadi hal yang belum banyak digunakan. Sebagai contoh di indonesia, landasan hukum penerapan DFR terhadap SPBE belum dibentuk meskipun regulasi tentang SMKI sudah diterapkan (Prawiranata, R. T. A, 2024). Oleh karena itu, penelitian ini perlu dilakukan untuk mencari, menganalisa dan memastikan peranan DFR terhadap ISMS yang dapat diimplementasikan di lingkungan *e-Government* di berbagai area baik di Indonesia maupun di dunia global dengan menggunakan pendekatan analisa SLR terhadap berbagai artikel ilmiah terpublikasi di berbagai jurnal bereputasi. Hasil penelitian tidak hanya dapat memetakan trend dan validasi mengenai urgensi penerapan DFR kedalam ISMS, namun juga memberikan *Framework Model* Integrasi DFR bagi organisasi.

Untuk mencapai tujuan penelitian tersebut, metodologi SLR dan beberapa pendekatan validasi lainnya digunakan. SLR merupakan serangkaian proses yang ketat dan transparan dalam mengidentifikasi, memfilter, menganalisis, dan mensintesis studi-studi relevan yang diterbitkan dalam jurnal terpublikasi bereputasi dengan menerapkan kerangka kerja yang terstandarisasi secara global (Triandini, E., Jayanatha, S., Indrawan, A., Putra, G. W., & Iswara, B. 2019). Tinjauan ini berfokus pada karya-karya yang membahas integrasi kesiapan forensik dan keamanan informasi dalam konteks pemerintahan, dengan penekanan pada implementasi, tantangan, dan hasilnya. Selain pendekatan SLR metode bibliografi dan pemetaan *(mapping)* terhadap standar tertentu maupun *Framework* yang relevan juga digunakan dalam penelitian ini.

1.2 Rumusan Masalah

Berdasarkan latar belakang tersebut, penelitian ini dilakukan menjawab beberapa pertanyaan penelitian *(research Questions)*, antara lain:

1. Bagaimana penerapan DFR dan ISMS secara bersamaan di organisasi pemerintahan baik di indonesia maupun di luar negri ?
2. Apa dampak penerapan DFR dan ISMS secara bersamaan di organisasi pemerintahan baik di indonesia maupun di luar negri ?
3. Bagaimana merancang *Framework Model* penerapan DFR dan ISMS secara bersamaan di organisasi pemerintahan ?

1.3 Batasan Masalah

Berdasarkan rumusan masalah tersebut diatas, maka batasan masalah agar penelitian lebih fokus dan tepat sasaran antara lain:

1. Lingkup Sistem yang Diteliti

   Penelitian ini dibatasi pada integrasi antara *Digital Forensic Readiness* (DFR) dan Sistem Manajemen Keamanan Informasi (SMKI) dalam konteks Sistem Pemerintahan Berbasis Elektronik (SPBE). Fokus penelitiannya adalah pada bagaimana organisasi dapat mempersiapkan keamanan siber di lingkungan pemerintahan berbasis elektronik berdasarkan standar DFR dan ISMS.

2. Objek Penelitian

   Penelitian hanya mencakup institusi pemerintah yang menggunakan SPBE, dengan fokus pada aspek penerapan DFR yang diintegrasikan ke dalam ISMS/SMKI untuk meningkatkan efektivitas penanganan keamanan informasi.

3. Aspek Penelitian

   Penelitian ini tidak mencakup implementasi teknis dari *Framework* yang diusulkan, tetapi lebih pada usulan pengembangan *model* konseptual yang didasarkan pada analisis literatur menggunakan pendekatan *Systematic Literature Review* (SLR).

4. Pendekatan Metodologi

   Penelitian menggunakan pendekatan Bibliometrik dan SLR untuk mengidentifikasi, memfilter, dan mensintesis studi-studi yang relevan sebagai acuan dalam menjawab *research Question*. Metode lain yang digunakan dalam penelitian yang berhubungan

dengan pe*model*an/pembangunan/pembuatan *Framework* yang sesuai dengan standar DFR dan ISMS/SMKI untuk digunakan di lingkungan pemerintahan.

5. Keterbatasan Data

   Penelitian dibatasi pada literatur yang terpublikasi dalam jurnal bereputasi dan artikel ilmiah yang relevan dengan kriteria tertentu (sumber data, kata kunci pencarian, rentang waktu, dan lokasi publikasi). Tidak ada pengumpulan data primer melalui survei atau wawancara. Seluruh data yang digunakan dalam analisa SLR merupakan data sekunder dengan menerapkan protokol yang sistematis dan terukur.

6. Konteks Geografis

   Meskipun proses dan hasil penelitian ini akan digunakan dalam konteks sistem pemerintahan berbasis elektronik di Indonesia, penelitian ini juga mempertimbangkan temuan global sebagai perbandingan untuk membangun *Framework* yang aplikatif secara luas dari data sekunder yang dianalisa menggunakan metode SLR.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk mengidentifikasi dan menganalisa penerapan integrasi DFR dan ISMS secara bersamaan di organisasi pemerintahan berdasarkan data yang diperoleh dari beragam artikel jurnal publikasi yang terkait pada tahun 2018-2025. Selain itu, hasil analisa SLR pada penelitian ini tidak hanya dapat memetakan trend dan validasi mengenai urgensi penerapan DFR kedalam ISMS, namun juga memberikan *Framework Model* Integrasi DFR bagi organisasi.

1.5 Manfaat Penelitian

Penelitian ini memiliki manfaat baik secara teoritis maupun praktis. Secara teoritis, penelitian ini diharapkan dapat memperkaya wawasan dan literatur ilmiah mengenai tren dan urgensi penerapan *Digital Forensic Readiness* (DFR) ke dalam *Information Security Management System* (ISMS) khususnya dalam konteks pemerintahan berbasis elektronik *(e-Government)* berdasarkan hasil analisa dari berbagai artikel ilmiah bereputasi yang terpublikasi secara global dalam kurun waktu tertentu. Hasil penelitian ini juga dapat digunakan sebagai referensi untuk studi-studi lanjutan yang membahas peningkatan

keamanan informasi dan kesiapan forensik dalam lingkungan organisasi pemerintah dengan situasi, kondisi, karakteristik dan urgensi yang berbeda.

Secara praktis, hasil penelitian ini yang berupa *Framework model* penerapan DFR kedalam ISMS dapat memberikan panduan kepada instansi pemerintah dalam meningkatkan kesiapan keamanan siber organisasi. Usulan *Framework model* integrasi DFR dan ISMS yang dapat diterapkan pada organisasi pemerintahan diharapkan mampu menghadapi ancaman siber secara lebih efektif, terukur dan sistematis yang diwujudkan dalam pembuatan regulasi, kebijakan, prosedur, maupun pedoman yang relevan untuk memperkuat sistem keamanan informasi di sektor pemerintahan.

1.6 Review Penelitian

Berdasarkan latar belakang dan pertanyaan penelitian yang harus dipecahkan diatas, penelitian ini merujuk ke beberapa artikel ilmiah terpublikasi sebagai bahan rujukan dalam melanjutkan proses penelitian. Penelitian pertama yang dikaji oleh peneliti adalah penelitian dari Gusman (Gusman, S. W. 2024), latar belakang yang melandasi penelitian tersebut adalah Indonesia berpotensi menjadi kekuatan ekonomi dunia pada 2045 dengan penguasaan teknologi *Digital* dengan GDP diperkirakan meningkat menjadi Rp 22.500 triliun jika Indonesia mampu memanfaatkan *Digital*isasi serta pemerintahan *Digital* (*e-Government*) menjadi salah satu pilar utama pendukung visi *Digital* Indonesia 2045. Dari latar belakang tersebut muncul pertanyaan penelitian *(research Questions)* antara lain:

1. Bagaimana perkembangan transformasi *Digital* pemerintah Indonesia?
2. Apa hasil evaluasi dan audit implementasi SPBE?
3. Apa tantangan dalam implementasi SPBE?
4. Apa peluang perbaikan ke depan?

Berdasarkan *research Question* diatas, tujuan penelitian tersebut

1. Menganalisis perkembangan transformasi *Digital* pemerintah Indonesia
2. Menganalisis hasil evaluasi dan audit implementasi SPBE (Sistem Pemerintahan Berbasis Elektronik)
3. Mengidentifikasi tantangan dalam implementasi SPBE
4. Menganalisis peluang perbaikan ke depan

Penelitian Gusman ini menggunakan metode penelitian kualitatif dengan mengumpulkan data dari berbagai sumber sekunder yang dianalisis menggunakan teknik analisis data kualitatif. Adapun temuan penelitian Gusman tersebut antara lain:

Masih banyak kendala dalam penerapan SPBE (dari 451 instansi yang dimonitor, hanya 15 instansi atau 3% yang mendapat predikat Sangat Baik

Tantangan utama dalam penerapan SPBE antara lain infrastruktur teknologi yang terbatas, kapabilitas SDM belum memadai, aplikasi pemerintah belum terintegrasi, dan Manajemen keamanan siber masih rentan.

Adapun hasil kesimpulan dari penelitian Gusman tersebut antara lain:

1. SPBE memiliki potensi besar untuk meningkatkan efisiensi dan kualitas layanan
2. Keberhasilan ditentukan oleh kebijakan yang tepat, kepemimpinan *Digital*, kolaborasi antar sektor
3. Diperlukan pendekatan *whole-of-Government* untuk mewujudkan sistem pemerintahan berbasis *Digital*

Berdasarkan penjelasan tersebut, penelitian dari Gusman berbeda dengan penelitian yang diusulkan peneliti pada dokumen penelitian ini karena peneliti dan Gusman melakukan *research area* yang berbeda, namun peneliti menjadikan cakupan penelitian Gusman sebagai latar belakang pentingnya pengelolaan sistem manajemen berbasis elektronik di lingkungan pemerintahan. Dengan kata lain, penelitian terdahulu ini jika dibandingkan dengan penelitian yang kami lakukan memiliki *gap* sehingga *novelty* penelitian ini dapat terdefinisi.

Penelitian kedua yang dijadikan referensi adalah penelitian dari Mangindaan (Mangindaan, D., Adib, A., Febrianta, H., & Hutabarat, D. J. C. (2022), mengangkat tema tentang tren penelitian terkait bahaya bencana alam, pengurangan risiko dan perubahan iklim di Indonesia dengan menggunakan pendekatan *systematic literature Review* (SLR) dan Analisis bibliometrik berdasarkan data yang diambil dari *database* Scopus sebagai layanan pengindeksan untuk publikasi *peer-Reviewed*. Latar belakang permasalahan penelitian ini adalah belum adanya kajian sistematis (SLR) untuk menentukan kemajuan, topik kunci dan pola kepenulisan terkait manajemen bencana di Indonesia untuk mendapatkan *state of the art* dari penelitian di bidang ini. Adapun pertanyaan penelitiannya antara lain: Bagaimana tren penelitian terkait bahaya alam dan bencana di Indonesia? Apa saja topik utama yang dikaji? Bagaimana pola penulisan dan kolaborasi penelitian? Apa gap penelitian yang masih ada?

Penelitian ini menghasilkan temuan antara lain : Limbah medis dan penanganannya, perkembangan penanganan COVID-19 di indonesia, dan manajemen limbah sebagai efek dari penanganan COVID-19. Sedangkan hasil penelitiannya adalah terbentuknya *cluster*

merah (terkait limbah) *cluster* hijau (terkait COVID-19), serta *cluster* biru dan kuning yang merupakan turunan dari data *cluster* merah dan hijau.

Analisis gap penelitian ditemukan yang menjadi keunikan penelitian ini adalah identifikasi dan *Review* dari pirolisis, dampak lingkungan, dan manajemen limbah medis yang menjadi efek dari penanganan COVID-19. Peneliti mampu mencari celah penelitian ini yang belum diangkat peneliti lainnya sehingga menjadi kebaruan *(novelty)* dari artikel penelitian ini. Kesimpulan hasil penelitian ini adalah dengan menggunakan SLR, peneliti berhasil mengidentifikasi dan mengekstrak 24 publikasi inti dan membentuk 4 cluster utama pengembangan penanganan limbah di Indonesia selama pandemi COVID-19 sebagai acuan penanganan dimasa depan.

Berdasarkan penjabaran diatas, penelitian Mangindaan sangat berbeda area penelitian yang diajukan peneliti dalam penelitian ini, namun metode dan tahapan penelitian menggunakan SLR dan bibliografi menjadi acuan untuk dapat digunakan dalam penelitian ini DFR dan SMKI ini. Penelitian mangindaan jika dibanding penelitian yang dilakukan ini memiliki gap sehingga *novelty* penelitian ini dapat terdefinisi.

Penelitian ketiga yang dijadikan rujukan adalah penelitian dari Saputra, 2019 dengan judul penelitian *"Addressing Indonesia's Cyber Security through Public Private Partnership (PPP)"* ditemukan latar belakang:

1. Indonesia mengalami lebih dari 50 juta ancaman siber selama 2018, meningkat 240% dibanding 2017
2. 77.12% ancaman berasal dari pengguna pribadi, 22.88% dari pengguna bisnis
3. Indonesia menempati posisi ke-20 negara dengan serangan siber terbanyak di dunia
4. BSSN melaporkan dari 2018-Mei 2019 terjadi sekitar 232,447,974 percobaan serangan siber
5. Hanya 82 rumah sakit yang memiliki incinerator berlisensi dari total 2,899 rumah sakit

Berdasarkan latar belakang tersebut, ditentukanlah *research Questions* dalam penelitian tersebut yaitu "Bagaimana pendekatan PPP *(Public-Private Partnership)* dapat digunakan sebagai alternatif dalam membangun arsitektur keamanan siber Indonesia?" dan "Apa tantangan yang muncul dalam implementasi PPP terkait keamanan siber di Indonesia?". Tujuan Penelitian yang digunakan adalah "Menganalisis tantangan yang muncul dalam implementasi PPP khususnya terkait perjanjian dan kerangka kerja formal

serta kerja sama informal antara pemerintah dan sektor swasta dalam membangun arsitektur keamanan siber nasional". Pada penelitian ini digunakan metode penelitian kualitatif yang pengumpulan datanya melalui wawancara informal dengan perwakilan pemerintah dan sektor swasta selama 8 bulan, serta Studi literatur dari buku, jurnal, artikel, dan sumber *Internet*.

Temuan dalam penelitian ini adalah "Kebutuhan sinergi antara pemerintah dan sektor swasta dalam penanganan keamanan siber" dan "Tantangan dalam implementasi PPP", dimana tantangan tersebut berupa:

1. Belum ada koridor hukum yang memadai
2. Keengganan aktor kunci untuk berbicara terbuka
3. Kesulitan melihat detail kerja sama formal dan informal

Sedangkan Hasil Penelitian tersebut antara lain:

1. PPP dapat menjadi bagian dari strategi keamanan siber nasional
2. Identifikasi faktor-faktor yang mendukung pentingnya PPP yaitu profesionalisme pengelolaan *Digital* sektor swasta, kapabilitas perusahaan swasta dalam keamanan siber, dan Investasi sektor swasta dalam keamanan siber.

Penelitian ketiga ini memiliki perbedaan dengan usulan penelitian yang diangkat peneliti berdasarkan fokus penelitian yang diangkat oleh peneliti (DFR dan SMKI) sangat berbeda dengan latar belakang dan tujuan penelitian ini yang fokus pada peran PPP dalam membangun keamanan siber nasional. Pada penelitian ini, peneliti menggunakan data penelitian ketiga ini sebagai referensi urgensi manajemen sistem keamanan yang menjadi landasan penelitian pada dokumen ini. Penelitian Saputra ini jika dibandingkan dengan penelitian pada dokumen ini memiliki gap sehingga *novelty* penelitian ini dapat terdefinisi.

Penelitian ke-4 yang dijadikan referensi dalam dokumen ini adalah penelitian dari Hidayat, T., & Putri, R. A. (2023) yang mengangkat tema "*E-Government in Indonesia: Policy Review and Implementation of Jokowi's Government*" dengan mengangkat latar belakang *E-Government* Indonesia masih tertinggal dibanding negara lain di Asia Tenggara pada tahun 2014 kemudian Pemerintahan Jokowi memberikan perhatian besar pada pengembangan *e-Government* untuk meningkatkan efisiensi layanan publik. Pertanyaan penelitian yang terdapat pada artikel tersebut adalah "Bagaimana kebijakan dan implementasi *e-Government* di Indonesia selama pemerintahan Jokowi?" dan "Apa tantangan dan hambatan dalam upaya peningkatan pelayanan publik melalui teknologi informasi?" sehingga kedua *research Questions* ini menjadikan tujuan penelitiannya

"Bagaimana gambaran yang mendalam tentang kebijakan dan implementasi *E-Government* selama pemerintahan Jokowi". Penelitian ini menganalisis langkah-langkah kebijakan dalam memajukan *E-Government* sekaligus menganalisis tingkat keberhasilan implementasinya.

Metode penelitian yang digunakan adalah Kualitatif yaitu dengan menganalisis dokumen terkait (peraturan, laporan pemerintah, publikasi akademik), analisis dan interpretasi data, serta verifikasi dan validasi. Penelitian ini menghasilkan temuan kesimpulan penelitian: "Implementasi *e-Government* era Jokowi lebih baik dari periode sebelumnya" dengan interpretasi dan validasi data sampling "Pengembangan aplikasi dan layanan *e-Government* seperti e-Tax dan SIM online" dan "Program pengembangan infrastruktur TIK termasuk program Palapa Ring".

Penelitian Hidayat ini tidak cukup signifikan untuk dijadikan urgensi penelitian yang melandasi penelitian ini karena kedalaman penelitian dan *research area* yang tidak sama dengan yang diajukan dalam penelitian ini. Namun penelitian yang cukup *general* (tidak mendalam) ini menjadi tambahan referensi dalam menjawab tata kelola sistem pemerintahan yang diangkat pada penelitian kali ini. Dengan kata lain, penelitian hidayat ini jika dibandingkan dengan penelitian yang dilakukan penliti dalam dokumen ini memiliki gap sehingga *novelty* penelitian ini dapat terdefinisi.

Penelitian ke-5 yang dijadikan referensi adalah penelitian dari Suryono, R. R., Budi, I., & Purwandari, B. (2020) yang mengangkat tema *"Challenges and trends of financial technology (Fintech): A systematic literature Review"* mengangkat latar belakang Transformasi *Digital* menciptakan tantangan di semua industri dan sektor bisnis dan inisiatif fintech yang diakui sebagai inovasi penting dalam industri keuangan yang terdorong oleh adanya *sharing economy*, regulasi, dan teknologi informasi. Latar belakang ini memunculkan pertanyaan penelitian "Apa tantangan dan tren penelitian fintech?" sehingga mengerucut menjadi tujuan penelitian "Menentukan *state of the art* penelitian teknologi finansial dengan mengidentifikasi tantangan dan tren fintech untuk potensi penelitian masa depan".

Penelitian ini dilakukan dengan menggunakan metode *Systematic Literature Review* (SLR) dengan pendekatan *Kitchenham*, analisis tematik dan meta-analisis, serta observasi untuk memvalidasi kualitas literatur. Sumber data yang digunakan dalam analisis adalah SCOPUS, ACM, ScienceDirect, dan IEEE Xplore dalam periode penelitian: 2014-2019. Temuan dalam penelitian ini terbagi menjadi dua kategori, yaitu:

1. Klasifikasi artikel berdasarkan *model* bisnis *fintech*, yaitu antara lain: klasterisasi tentang jenis analisa *fintech*, analisa sistem pembayaran, analisa manajemen risiko dan investasi, analisa *aggregator* pasar, analisa sistem *crowdfunding*, analisa *P2P lending*, serta analisa *cryptocurrency* dan *blockchain.*
2. Klasifikasi artikel berdasarkan analisa tantangan utama penerapan *fintech*, yaitu: aspek kerangka kerja dan *model*, aspek regulasi dan kebijakan, aspek infrastruktur, aspek teknologi aspek perlindungan data pribadi, aspek keamanan, serta aspek pengawasan.

Penelitian ini menghasilkan Kesimpulan penelitian yaitu:

1. *Fintech* masih membutuhkan pengembangan kebijakan dan strategi di domain siber
2. Kolaborasi dengan sektor swasta sangat penting sebagai penyedia layanan *Internet*
3. Diperlukan pendekatan *whole-of-Government* untuk keberhasilan implementasi
4. Masih banyak peluang penelitian terkait kebijakan, keamanan, monitoring, dan pengembangan teknologi

Penelitian Suryono ini cukup dekat dengan area penelitian yang dilakukan dalam dokumen ini yaitu dalam hal urgensi penerapan SMKI dalam organisasi *(fintech)* serta metode penelitian yang menggunakan SLR. Namun penelitian ini lebih mendalam karena menambahkan urgensi DFR kedalam peran SMKI sehingga *novelty* penelitian ini terdefinisi.

Penelitian ke-6 yang dijadikan referensi adalah penelitian dari Bhatia, S., & Malhotra, J. (2018), mengangkat tema *CSPCR: Cloud Security, Privacy and Compliance Readiness - A Trustworthy Framework*. Penelitian ini menganalisa *research Question* sekaligus Mengusulkan *Framework model* CSPCR untuk mengevaluasi kesiapan organisasi dalam menangani ancaman dan bahaya di lingkungan *cloud computing*, serta membahas aturan dan regulasi yang dianggap sebagai prasyarat dalam migrasi ke layanan komputasi awan *(cloud services)*. Mereka membuat semacam *assesment tools* berdasarkan data dari *BSA Global Cloud Computing Scorecard 2016* yang digunakan untuk menganalisa kondisi di organisasi penelitian mereka sehingga menghasilkan beberapa temuan, atara lain:

1. Terdapat perubahan penting dalam kebijakan keamanan dan privasi komputasi awan di ekonomi global
2. Studi mencakup 24 negara utama yang mewakili lebih dari 80% pasar IT global

3. Sebagian besar negara telah memiliki kerangka kerja perlindungan data dan komisioner privasi yang independen
4. Beberapa negara menerapkan registrasi wajib untuk pengontrol data dan transfer data lintas batas
5. Infrastruktur setiap negara mengalami peningkatan dari waktu ke waktu

Berdasarkan data tersebut, penelitian mereka arahkan ke pe*model*an *Framework* yang menghasilkan beberapa temuan terkait *Model* CSPCR yang mereka usulkan, antar alain:

1. *Model* CSPCR ini membantu organisasi mengevaluasi kesiapan keamanan informasi, privasi dan kepatuhan yang ada
2. *Model* dapat digunakan sebagai alat optimasi bagi organisasi yang telah menerapkan layanan *cloud*
3. *Model* menciptakan lingkungan yang sadar akan bahaya serta mendukung operasi proaktif
4. *Model* membantu organisasi dalam penyebaran teknik dan metode di antara personel teknis; dalam hal evaluasi kesiapan organisasi terhadap ancaman *cloud*, serta dalam hal validasi dan pembaruan informasi untuk memastikan pemanfaatan yang optimal
5. Implementasi *Model* CSPCR bersifat multi-dimensi, multi domain dan multi-layer yang memungkinkan untuk dikaji dan dikembangkan lebih lanjut

Penelitian Bhatia ini cukup dekat dengan area penelitian yang diajukan dalam dokumen penelitian ini yaitu dalam hal pengembangan *model Framework* baru untuk organisasi, namun fokus area penelitian mereka di *Cloud computing* berbeda dengan yang dilakukan peneliti, yaitu di SPBE. Penelitian ini mempertimbangkan utnuk mengadopsi CSPCR *Framework* yang dikaji pada penelitian ini.

Penelitian ke-7 yang dijadikan referensi adalah penelitian dari Simou, S., & Kalloniatis, C. (2018) yang mengangkat tema *A Framework for Designing cloud Forensic-enabled services (CFeS)*. Kedua peneliti ini mengembangkan *Framework model* yang dapat membantu perancangan perangkat lunak dalam layanan *cloud* suatu organisasi yang dapat mendukung investigasi forensik? Serta usulan *Framework* tersebut dibuktikan dengan menjawab pertanyaan penelitian apakah usulan tersebut mampu menjembatani kesenjangan antara pemangku kepentingan dan analisis forensik dalam perancangan layanan *cloud* organisasi. Penelitian mereka menggunakan Analisis Studi Literatur & Pengembangan *Model* Konseptual *(Framework model CFeS)*. Untuk membangun *Framework CFeS*,

peneliti menerapkan *Design Science Research Methodology (DSRM). Framework* ini digunakan untuk menjawab temuan penelitian yang mereka definisikan antara lain:

1. Teridentifikasi 7 batasan penerapan *Framework* yang mereka usulkan, yaitu:
    a. Akuntabilitas
    b. Transparansi
    c. Prosedur disiplin internal
    d. Hak akses
    e. Isolasi
    f. Masalah hukum
    g. Kemampuan pelacakan
2. Kerangka kerja yang diusulkan berhasil membantu proses perancangan perangkat lunak untuk digunakan pada layanan *cloud* yang mendukung investigasi forensik, serta menjembatani kesenjangan antara pemangku kepentingan dan analis forensik.
3. *Model* konseptual yang dihasilkan dapat diterapkan dalam hal tahap persiapan pembuatan sistem yang *Digital Forensic enabled*, dapat digunakanpada tahap investigasi jika terjadi insiden keamanan tertentu, serta dapat digunakan dalam membantu membuat keputusan yang baru terkait rancangan layanan *cloud* yang lebih siap terhadap keamanan dan *Forensic-enable*.
4. Metodologi ini memberikan pendekatan terstruktur untuk *stakeholder* dan *software engineer* untuk menciptakan sistem layanan *cloud* yang lebih siap terhadap keamanan dan *Forensic-enable*.

Penelitian Simou ini cukup dekat dengan area penelitian yang diajukan dalam dokumen penelitian ini yaitu dalam hal pengembangan *model Framework* baru untuk organisasi, namun fokus area penelitian ini di *Cloud computing* yang berbeda dengan yang dilakukan peneliti pada dokumen ini, yaitu di SPBE. Pada penelitian ini, peneliti mempertimbangkan untuk menggunakan *Design Science Research Methodology (DSRM)* untuk membangun *Framework model* pada penelitiannya.

Penelitian ke-8 yang dijadikan referensi adalah penelitian dari Hakim, M. F., & Alamsyah. (2024) dengan tajuk *Development of Digital Forensic Framework for Anti-Forensic and Profiling Using Open Source Intelligence in Cyber Crime Investigation*. Penelitian Hakim & Alamsyah menjawa tentang *research Question* "Bagaimana mengembangkan proses atau kerangka kerja yang dapat digunakan sebagai referensi dalam menangani kasus kejahatan siber dalam proses forensik? dan Bagaimana memodifikasi

proses investigasi forensik *Digital* untuk menangani anti-forensik dan menambahkan informasi dari bukti *Digital*".

Pada penelitian ini disebutkan bahwa dalam proses investigasi forensik *Digital*, ditemukan 3 jenis temuan baru dalam bentuk data string, dimana salah satunya adalah link, dan 7 jenis baru dalam bentuk *user*name yang tidak ditemukan saat menggunakan *tools forensik Digital* biasa. Dari total 408 data awal dan temuan baru dengan total 10 temuan, persentase temuan meningkat sebesar 2,45%. Hal ini menunjukkan bahwa penambahan penggunaan *Open Source Intelligence (OSINT)* dan sentralisasi *tools*et pada tahap analisis dapat membantu menangani anti-forensik dan menambahkan informasi dari bukti *Digital* yang telah diperoleh. Temuan penelitian ini memang tidak signifikan terhadap penlitian pada dokumen ini, namun proses dan hasil penelitian yang dilakukan Hakim dalam penelitian ini mengungkapkan bahwa *Framework* yang dihasilkan berhasil mengembangkan tahapan identifikasi anti-forensik pada file media dan memanfaatkan OSINT untuk melakukan profiling tersangka kejahatan berdasarkan bukti yang dikumpulkan dalam tahap investigasi forensik *Digital*. Metodologi yang digunakan berhasil memodifikasi proses investigasi forensik *Digital* yang terdiri dari tahap persiapan, preservasi, akuisisi, pemeriksaan, analisis, pelaporan, dan presentasi dengan menambahkan penggunaan OSINT dan sentralisasi *tools*et pada tahap analisis.

Penelitian Hakim ini cukup dekat dengan area penelitian yang diajukan dalam proposal ini yaitu dalam hal pengembangan *model Framework* baru untuk organisasi, namun fokus area dan hasil penelitian Hakim yang melakukan pengidentifikasian Anti Forensik kedalam *frame work* yang dibuat berbeda aspek dengan yang diteliti pada dokumen penelitian ini. Namun penelitian Hakim menjadi referensi tambahan bagi peneliti mempertimbangkan untuk menggunakan referensi tersebut untuk membangun *Framework* DFR yang diusulkan..

Berdasarkan penjelasan beragam literatur tersebut diatas, maka rangkuman terhadap penelitian-penelitian yang telah dilakukan sebelumnya yang menjadi kontribusi sekaligus *research gap* dan *novelty* terhadap penelitian yang dilakukan dapat dilihat pada tabel perbandingan penelitian pada tabel 1.1 berikut ini.

Tabel 1.1 Tabel Perbandingan Penelitian Terdahulu

No	Nama	Tujuan	Pendekatan	*Research Gap*
1	Gusman, S. W. (2024)	1. Menganalisis perkembangan transformasi *Digital* pemerintah Indonesia 2. Menganalisis hasil evaluasi dan audit implementasi SPBE (Sistem Pemerintahan Berbasis Elektronik) 3. Mengidentifikasi tantangan dalam implementasi SPBE 4. Menganalisis peluang perbaikan ke depan	Analisis data kualitatif	Penelitian Gusman berbeda dengan penelitian yang diusulkan dalam hal *research area* yang berbeda. Gusman meneliti perkembangan dan evaluasi penerapan SPBE, sedangkan proposal penelitian ini menjadikan hasil penelitian Gusman sebagai latar belakang pentingnya pengelolaan sistem manajemen berbasis elektronik di lingkungan pemerintahan

2	Mangindaan, D., Adib, A., Febrianta, H., & Hutabarat, D. J. C. (2022)	Menjawab pertanyaan tentang Bagaimana penelitian terkait bahaya yang ditimbulkan dalam penanganan bencana COVID di Indonesia Menggunakan metode SLR	*Systematic Literature Review (SLR)*	Penelitian Mangindaan dan proposal penelitian ini berbeda area penelitian (area kesehatan dan teknologi) namuan penelitian tersebut dijadikan rujukan dalam menganalisis data penelitian berdasarkan metode SLR.
3	Saputra, (2019)	"Menganalisis tantangan yang muncul dalam implementasi PPP khususnya terkait perjanjian dan kerangka kerja formal serta kerja sama informal antara pemerintah dan sektor swasta dalam membangun arsitektur keamanan siber nasional".	Kualitatif: wawancara dan studi literatur	Penelitian Saputra berfokus pada urgensi penerapan PPP khususnya perjanjian pemerintah dengan pihak luar negeri untuk membangun arsitektur keamanan siber nasional dijadikan landasan penelitian yang diajukan peneliti namun dengan tambahan penekanan pada urgensi DFR dan SMKI untuk membangun arsitektur keamanan siber nasional.

4	Hidayat, T., & Putri, R. A. (2023).	Penelitian ini dilakukan untuk menjawab "Bagaimana kebijakan dan implementasi *e-Government* di Indonesia selama pemerintahan Jokowi?" dan "Apa tantangan dan hambatan dalam upaya peningkatan pelayanan publik melalui teknologi informasi?" sehingga kedua *research Questions* ini menjadikan tujuan penelitiannya "Bagaimana gambaran yang mendalam tentang kebijakan dan implementasi *E-Government* selama pemerintahan Jokowi".	Kualitatif: wawancara dan studi literatur	Penelitian ini tidak cukup signifikan untuk dijadikan urgensi penelitian yang melandasi proposal penelitian ini karena kedalaman penelitian dan *specific research area* yang tidak sama dengan yang diajukan dalam proposal ini. Namun penelitian ini menjadi tambahan referensi dalam menjawab pentingnya dan perkembangan tata kelola sistem pemerintahan yang diangkat pada penelitian kali ini.

5	Suryono, R. R., Budi, I., & Purwandari, B. (2020)	"Apa tantangan dan tren penelitian fintech?" sehingga mengerucut menjadi tujuan penelitian "Menentukan state of the art penelitian teknologi finansial dengan mengidentifikasi tantangan dan tren fintech untuk potensi penelitian masa depan".	*Systematic Literature Review (SLR)*	Penelitian ini cukup dekat dengan area penelitian yang diajukan dalam proposal ini yaitu dalam hal urgensi penerapan SMKI dalam organisasi *(fintech)* serta metode penelitian yang menggunakan SLR. Namun proposal penelitian ini lebih mendalam karena menambahkan urgensi DFR kedalam peran SMKI sehingga novelty proposal ini terdefinisi
6	Bhatia, S., & Malhotra, J. (2018)	Penelitian ini menganalisa *research Question* sekaligus Mengusulkan *Framework model* CSPCR untuk mengevaluasi kesiapan organisasi dalam menangani ancaman dan bahaya di lingkungan *cloud* computing, serta	Analisis Studi Literatur & Pengembangan *Model* Konseptual *(CSPCR Framework model)*	Penelitian Bhatia ini cukup dekat dengan area penelitian yang diajukan dalam proposal ini yaitu dalam hal pengembangan *model Framework* baru untuk organisasi, namun fokus area penelitian ini di *Cloud*

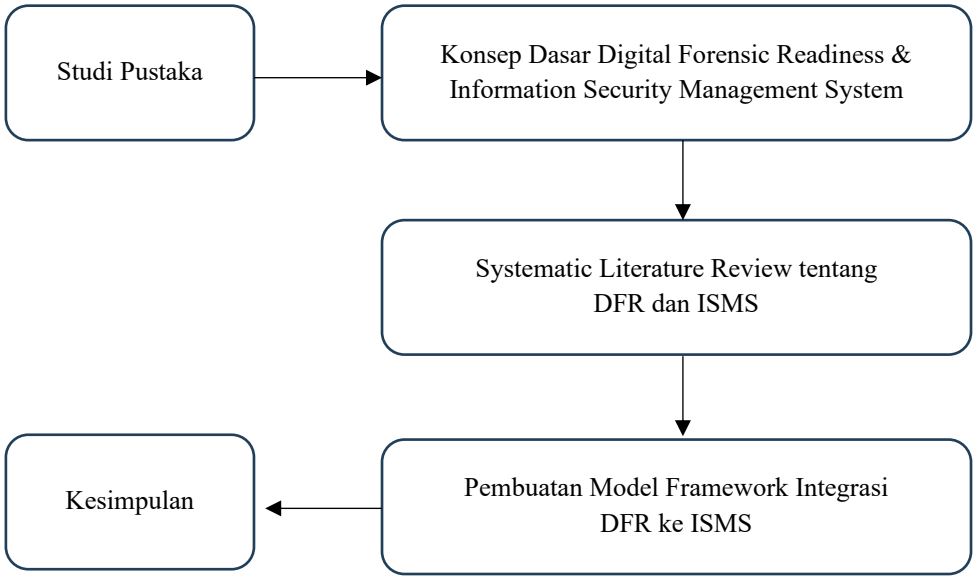
		membahas aturan dan regulasi yang dianggap sebagai prasyarat dalam migrasi ke layanan komputasi awan		*computing* berbeda dengan yang diusulkan peneliti, yaitu di SPBE. Proposal penelitian ini mempertimbangkan utnuk mengadopsi CSPCR *Framework* yang dikaji pada penelitian ini.
7	Simou, S., & Kalloniatis, C. (2018).	Kedua peneliti ini mengembangkan *Framework model* yang dapat membantu perancangan perangkat lunak dalam layanan *cloud* suatu organisasi yang dapat mendukung investigasi forensik? Serta usulan *Framework* tersebut dibuktikan dengan menjawab pertanyaan penelitian apakah usulan tersebut mampu menjembatani kesenjangan antara pemangku kepentingan dan analisis forensik dalam perancangan layanan *cloud* organisasi?	Analisis Studi Literatur & Pengembangan *Model* Konseptual *(Framework model CFeS).* Untuk membangun *Framework CFeS,* peneliti menerapkan *Design Science Research Methodology (DSRM).*	Penelitian Simou ini cukup dekat dengan area penelitian yang diajukan dalam proposal ini yaitu dalam hal pengembangan *model Framework* baru untuk organisasi, namun fokus area penelitian ini di *Cloud computing* berbeda dengan yang diusulkan peneliti, yaitu di SPBE. Pada Proposal penelitian ini, peneliti mempertimbangkan untuk menggunakan *Design Science Research*

				Methodology (DSRM) untuk membangun *Framework model* pada penelitiannya.
8	Hakim, M. F., & Alamsyah. (2024).	Penelitian Hakim & Alamsyah menjawa tentang *research Question* "Bagaimana mengembangkan proses atau kerangka kerja yang dapat digunakan sebagai referensi dalam menangani kasus kejahatan siber dalam proses forensik? dan Bagaimana memodifikasi proses investigasi forensik *Digital* untuk menangani anti-forensik dan menambahkan informasi dari bukti *Digital*".	Analisis Studi Literatur & Pengembangan *Model* Konseptual	Penelitian Hakim ini cukup dekat dengan area penelitian yang diajukan dalam proposal ini yaitu dalam hal pengembangan *model Framework* baru untuk organisasi, namun fokus area penelitian ini di fitur pengidentifikasian Anti Forensik kedalam frame work yang dibuat. Hal ini menjadi referensi tambahan bagi Proposal penelitian ini, peneliti mempertimbangkan untuk menggunakan referensi tersebut untuk membangun *Framework* DFR yang diusulkan.

9	**Usulan Penelitian**	1. Analisa urgensi penerapan *Digital* Forensik *Readiness* dan SMKI dalam pemerintahan berbasis elektronik dengan menganalisa berbagai sumber data artikel publikasi di Indonesia maupun didunia dengan menggunakan metode SLR. 2. Pembuatan *Framework Model* Integrasi DFR dan ISMS di lingkungan pemerintahan	*Systematic Literature Review (SLR)*	Kebaruan *(novelty)* pada proposal penelitian ini adalah mengisi kekosongan penelitian terhadap peran DFR yang diintegrasikan kedalam ISMS dilingkungan sistem pemerintahan berbasis elektronik. *Research Gap* dan *Novelty* secara visual ditunjukkan dalam tampilan *Heatmap* penelitian yang terdapat di bawah tabel ini.

1.7 Metodologi Penelitian

Agar penelitian ini tetap fokus dan terarah serta mendapatkan hasil yang maksimal, maka penelitian ini menggunakan beberapa tahapan metodologi penelitian yang dapat dilihat pada Gambar 1.3. Metodologi penelitian yang dibuat terdapat 4 tahapan utama, yaitu tahapan (1) Studi Pustaka; (2) Konsep Dasar Digital Forensic Readiness (DFR) dan Information Security Management System; (3) Systematic Literature Review tentang DFR dan ISMS; (4) Pembuatan Model Framework Integrasi DFR ke ISMS; (5) Kesimpulan.



Gambar 1.5. Metodologi Penelitian

1.8 Sistematikan Penulisan

Laporan penelitian ini disusun dengan sistematika penulisan yang dapat mempermudah proses pembahasan penelitian. Adapun sistematika penulisan yang dimaksud adalah sebagai berikut :

BAB 1 PENDAHULUAN

Pada bagian pendahuluan ini berisi latar belakang penelitian, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, review penelitian, metodologi penelitian dan sistematika penelitian.

BAB 2 LANDASAN TEORI

Pada bagian landasan teori ini berisi tentang teori-teori yang terkait dengan digital forensic, digital forensic readiness, information security management system, systematic literature review serta beberapa framework yang berhubungan dengan digital forensic readiness dan information security management system.

BAB 3 METODOLOGI PENELITIAN

Pada bagian metodologi penelitian ini berisi tentang langkah-langkah penelitian dan gambaran umum langkah penyelesaian.

BAB 4 HASIL DAN PEMBAHASAN

Pada bagian hasil dan pembahasan ini berisi tentang hasil proses dan analisa topik digital forensic readiness, information security management system, berdasarkan protokol prisma pada metode systematic literature review. Data hasil pemrosesan SLR digunakan sebagai landasan pembuatan model framework integrasi digital forensic readiness kedalam information security management system.

BAB 5 KESIMPULAN DAN SARAN

Pada bagian kesimpulan dan saran ini berisi tentang kesimpulan dari hasil penelitian yang telah dilakukan serta saran dan rekomendasi untuk penelitian selanjutnya.

BAB 2
Tinjauan Pustaka

2.1 *Digital* Forensik

Digital forensik adalah cabang ilmu yang berfokus pada pemeriksaan dan analisis barang bukti *Digital* dengan tujuan agar bukti tersebut dapat diterima dan dipertanggungjawabkan secara hukum di pengadilan. Barang bukti ini mencakup berbagai perangkat teknologi seperti ponsel, laptop, *server*, dan perangkat lain yang memiliki media penyimpanan yang dapat dianalisis (Alamsyah, 2009). Sebagai proses ilmiah, *Digital Forensic* melibatkan pemeliharaan, identifikasi, ekstraksi, serta dokumentasi barang bukti *Digital*, khususnya dalam konteks kejahatan komputer (Marcella & Greenfield, 2002). Selain itu, Palmer (2001) mendefinisikan *Digital* forensik sebagai penerapan metode ilmiah yang mencakup pelestarian, validasi, identifikasi, analisis, interpretasi, dokumentasi, dan presentasi barang bukti *Digital*. Proses ini bertujuan untuk membantu rekonstruksi peristiwa kriminal atau mencegah tindakan ilegal yang dapat mengganggu operasional sistem tertentu. Secara umum, *Digital Forensic* dapat dipahami sebagai metode sistematis untuk mengelola barang bukti *Digital* agar dapat digunakan dalam penyelesaian kasus kejahatan, baik di dalam maupun di luar pengadilan.

Digital forensik memiliki peran yang sangat penting dalam organisasi, terutama dalam menghadapi ancaman keamanan siber yang semakin kompleks. Dalam era *Digital*, banyak aktivitas organisasi yang bergantung pada teknologi informasi, sehingga risiko terhadap kejahatan siber seperti pencurian data, peretasan, serangan *malware,* serta insiden keamanan siber lainnya meningkat pesat. *Digital* forensik memungkinkan organisasi untuk mengidentifikasi, menganalisis, dan merespons insiden-insiden tersebut secara efektif. Melalui proses yang sistematis, *Digital* forensik dapat membantu mengumpulkan barang bukti *Digital* yang valid dan dapat dipertanggungjawabkan di pengadilan, sehingga memungkinkan organisasi untuk menuntut pelaku kejahatan secara hukum. Selain itu, *Digital* forensik juga membantu organisasi memahami bagaimana serangan terjadi, sehingga dapat memperkuat sistem keamanan untuk mencegah insiden serupa di masa depan.

Selain untuk mitigasi insiden, *Digital* forensik juga mendukung kepatuhan terhadap regulasi dan kebijakan hukum yang berlaku. Banyak negara dan industri memiliki standar dan regulasi yang mengharuskan organisasi melaporkan dan menangani pelanggaran data secara transparan. Dengan menggunakan *Digital* forensik, organisasi dapat memastikan bahwa proses investigasi dilakukan sesuai dengan aturan hukum, sehingga menghindari

potensi sanksi atau penalti. Di sisi lain, *Digital* forensik juga membantu organisasi membangun kepercayaan dengan pelanggan dan mitra bisnis. Kepercayaan ini terbentuk dari hal strategis maupun teknikal yang diterapkan organisasi untuk memastikan data dan informasi teridentifikasi, terbackup, serta mampu dilakukan restorasi jika terjadi insiden keamanan tertentu. Dengan menunjukkan komitmen dalam menangani insiden keamanan secara profesional dan bertanggung jawab seperti tersebut diatas, organisasi dapat memperkuat reputasi mereka sebagai entitas yang mengutamakan perlindungan data dan privasi. Secara keseluruhan, *Digital* forensik bukan hanya alat untuk menangani insiden, tetapi juga komponen penting dalam strategi manajemen risiko dan keberlanjutan operasional organisasi.

Digital forensik dalam organisasi dapat dikategorikan menjadi beberapa jenis berdasarkan area penerapannya, yaitu forensik komputer, forensik jaringan, forensik perangkat *mobile,* dan forensik *cloud*. Forensik komputer berfokus pada analisis data yang tersimpan di perangkat keras seperti hard disk, SSD, atau *server*, untuk mengungkap bukti terkait insiden keamanan atau aktivitas ilegal. Forensik jaringan berkaitan dengan pemantauan dan analisis data lalu lintas jaringan, log aktivitas, dan serangan siber untuk mendeteksi serta merespons ancaman seperti peretasan atau penyebaran *malware*. Forensik perangkat *mobile* mencakup investigasi pada ponsel pintar, tablet, dan perangkat IoT untuk memulihkan data seperti pesan, log panggilan, atau lokasi yang relevan dalam penyelidikan internal atau eksternal. Sementara itu, forensik *cloud* berfokus pada penyelidikan data yang tersimpan di lingkungan komputasi awan, termasuk penelusuran akses tidak sah atau pencurian data. Dengan membagi *Digital* forensik ke dalam kategori ini, organisasi dapat menerapkan strategi yang spesifik sesuai dengan kebutuhan investigasi mereka, memastikan efisiensi, dan memaksimalkan penggunaan teknologi yang relevan.

Secara umum, terdapat tahapan dalam *Digital* forensik meliputi identifikasi, pengambilan, analisis, dokumentasi, dan presentasi. Proses identifikasi dilakukan untuk menentukan lokasi dan jenis barang bukti *Digital* yang relevan dengan kasus. Tahap ini diikuti dengan pengambilan data menggunakan teknik tertentu dengan menggunakan *tool* yang spesifik *bitstream imaging* untuk memastikan data tidak berubah, atau validasi *hash function* seperti MD5 atau SHA-256 yang tertera pada file yang dianalisa, dan sebagainya. Pada tahap analisis, untuk mayoritas kasus maupun kasus yang spesifik tertentu, kadang kala dibutuhkan perangkat lunak khusus seperti EnCase atau FTK (*Forensic Tool*kit) digunakan untuk menggali data tersembunyi, dihapus, atau terenkripsi. Piranti hardware ini pun ada banyak jenisnya disesuaikan dengan tujuan, situasi kondisi kasus yang ditangani, serta

metode yang digunakan. Langkah langkah tersebut diproses dan didokumentasikan dengan baik untuk disusun sebagai laporan yang berisi bukti otentik *(evidence)* serta narasi penjelasan tentang apa, mengapa, kapan dan bagaimana bukti tersebut didapatkan. Bukti ini harus dapat dipertanggungjawabkan secara *scientific* atau keilmuan dan terkonfirmasi dari berbagai pihak yang berhubungan dengan kasus dan temuan tersebut. Temuan ini kemudian dipresentasikan dalam format yang mudah dipahami oleh pihak non-teknis, seperti hakim atau juri, maupun untuk publik tanpa mengurangi validitas ilmiah..

2.2 *Digital* Forensik *Readiness*

Digital Forensic Readiness (kesiapan forensik *Digital*) merupakan pendekatan proaktif yang bertujuan untuk memastikan organisasi dapat dengan cepat dan efisien merespons insiden keamanan siber. Dalam era *Digital* saat ini, banyak organisasi menghadapi ancaman yang semakin kompleks, mulai dari serangan malware, peretasan, hingga pelanggaran data. DFR memainkan peran penting dalam membantu organisasi mempersiapkan diri sebelum insiden terjadi dengan memastikan alat, prosedur, dan kebijakan terkait forensik *Digital* telah tersedia dan terintegrasi. Dengan kesiapan ini, organisasi tidak hanya dapat mengurangi waktu respons terhadap insiden tetapi juga meningkatkan kualitas investigasi dengan memastikan data relevan dapat segera diakses dan diolah. Hal ini memberikan keuntungan kompetitif bagi organisasi dalam menangani ancaman keamanan secara cepat dan efektif.

Menurut para ahli, *Digital Forensic Readiness* (DFR) adalah pendekatan yang dirancang sebelum insiden terjadi dalam siklus investigasi *Digital* forensik. Pendekatan ini mencakup aktivitas identifikasi, pelestarian, penyimpanan, analisis, dan pengelolaan bukti *Digital* dengan tujuan mengurangi biaya yang diperlukan untuk proses penyelidikan (Mouhtaropoulos & Li, 2014). DFR menekankan pentingnya mempersiapkan infrastruktur dan prosedur yang memungkinkan organisasi untuk memaksimalkan pemanfaatan bukti *Digital* secara efektif ketika insiden terjadi. Dengan kesiapan ini, organisasi dapat meningkatkan efisiensi investigasi dan memastikan bukti yang diperoleh tetap valid serta dapat digunakan dalam proses hukum.

Menurut Rowlingson (2004), *Digital Forensic Readiness* mencerminkan kemampuan suatu organisasi untuk mengoptimalkan potensi penggunaan bukti *Digital* dan secara bersamaan meminimalkan biaya yang dikeluarkan selama investigasi. Hal ini mencakup penerapan prosedur pengamanan data dan penerapan teknologi yang memungkinkan data *Digital* dapat diakses dengan cepat tanpa mengurangi keasliannya. Tan

(2001) juga menyoroti bahwa DFR bertujuan untuk memastikan data yang relevan dengan insiden dapat dimanfaatkan secara maksimal sebagai barang bukti, sambil mengurangi pengeluaran yang terkait dengan respons investigasi.

Salah satu peran utama DFR adalah mengoptimalkan proses pengumpulan barang bukti *Digital*. Ketika insiden terjadi, organisasi yang memiliki kesiapan forensik dapat dengan cepat mengidentifikasi, mengamankan, dan menganalisis data yang diperlukan tanpa mengganggu operasional sistem. Dengan prosedur yang terstandar, pengumpulan barang bukti dilakukan secara sistematis dan mematuhi prinsip-prinsip hukum, sehingga bukti tersebut dapat dipertanggungjawabkan di pengadilan jika diperlukan. Kesiapan ini juga membantu mengurangi risiko kehilangan atau kerusakan data selama proses investigasi, yang seringkali menjadi tantangan dalam penanganan insiden keamanan. Dalam konteks regulasi, kemampuan organisasi untuk mematuhi standar hukum dan menunjukkan bukti *Digital* yang valid dapat memperkuat kredibilitas dan menghindari potensi sanksi hukum.

DFR juga mendukung peningkatan keamanan sistem informasi melalui pencegahan dan deteksi dini terhadap potensi ancaman. Dengan memantau aktivitas jaringan, log sistem, dan data operasional secara berkelanjutan, organisasi dapat mengenali pola-pola yang mencurigakan sebelum menjadi ancaman yang serius. Proses ini melibatkan penggunaan alat forensik modern yang mampu menganalisis data secara real-time untuk memberikan wawasan tentang potensi serangan. Selain itu, kesiapan forensik memungkinkan tim keamanan untuk memperbaiki celah keamanan dan menyusun strategi mitigasi berdasarkan data empiris dari insiden sebelumnya. Dengan pendekatan ini, organisasi tidak hanya bersifat reaktif tetapi juga proaktif dalam melindungi aset *Digital*nya.

Dari perspektif manajemen risiko, DFR membantu organisasi dalam memitigasi dampak insiden keamanan. Ketika insiden terjadi, dampaknya tidak hanya terbatas pada kerugian finansial tetapi juga reputasi organisasi. Dengan memiliki sistem kesiapan forensik, organisasi dapat dengan cepat merespons insiden dan mengkomunikasikan langkah-langkah yang diambil kepada pemangku kepentingan, termasuk pelanggan, mitra bisnis, dan regulator. Respon yang cepat dan terukur ini menunjukkan komitmen organisasi dalam menjaga integritas data dan transparansi, yang pada akhirnya dapat meningkatkan kepercayaan publik terhadap organisasi. Selain itu, kesiapan forensik juga dapat mengurangi biaya yang terkait dengan investigasi dan pemulihan pasca-insiden.

Dalam konteks regulasi, DFR memungkinkan organisasi untuk memenuhi persyaratan hukum yang mengatur pengelolaan bukti *Digital*, seperti yang tercantum dalam *General* Data Protection Regulation (GDPR) atau standar keamanan data lainnya. Dengan implementasi DFR yang efektif, organisasi tidak hanya mampu mengatasi insiden dengan lebih baik tetapi juga menjaga reputasi mereka di mata publik dan pemangku kepentingan lainnya. Hal ini menjadikan DFR sebagai elemen penting dalam strategi keamanan dan manajemen risiko organisasi modern. Implementasi DFR dalam organisasi memerlukan integrasi lintas fungsi dalam organisasi. Ini melibatkan kolaborasi antara departemen keamanan informasi, teknologi informasi, dan manajemen untuk merancang kebijakan dan prosedur yang relevan. Pelatihan bagi karyawan juga menjadi bagian penting untuk memastikan semua pihak memahami peran mereka dalam mendukung kesiapan forensik. Selain itu, investasi dalam perangkat lunak dan alat forensik yang sesuai harus diimbangi dengan pembaruan teknologi secara berkala untuk menghadapi ancaman yang terus berkembang. Organisasi yang berhasil mengintegrasikan *Digital Forensic Readiness* ke dalam budaya kerjanya akan memiliki kemampuan yang lebih baik untuk menghadapi tantangan keamanan informasi di masa depan.

Kesimpulan yang dapat diambil dari berbagai pendapat ahli adalah bahwa *Digital Forensic Readiness* merupakan langkah strategis yang dilakukan sebelum insiden terjadi, dengan fokus pada penggunaan barang bukti *Digital* untuk mendukung investigasi dan efisiensi biaya penyelidikan. Selain itu, DFR tidak hanya membantu organisasi mempersiapkan respons yang cepat, tetapi juga memperkuat posisi mereka dalam menghadapi tuntutan hukum dan regulasi. DFR memainkan peran krusial dalam membantu organisasi mengelola risiko keamanan informasi. Dengan mempersiapkan alat, prosedur, dan kebijakan yang relevan, organisasi dapat merespons insiden dengan cepat dan efektif. Selain itu, kesiapan ini juga mendukung kepatuhan terhadap regulasi, perlindungan reputasi, dan peningkatan keamanan sistem secara keseluruhan. Dalam dunia yang semakin tergantung pada teknologi, *Digital Forensic Readiness* bukan lagi pilihan tetapi kebutuhan strategis yang harus diimplementasikan oleh setiap organisasi yang ingin bertahan dan berkembang dalam lingkungan *Digital* yang penuh tantangan.

2.3 Tahapan dalam *Digital Forensik Readiness*

Dalam proses *Digital Forensic Readiness* dibutuhkan tahapan-tahapan untuk mencapai tujuan dari DFR itu sendiri. Tahapan-tahapan dari DFR (Robert Rowlingson Ph, 2004) adalah, sebagai berikut :

1. Menentukan Skenario bisnis yang membutuhkan barang bukti *Digital*.
2. Mengidentifikasi sumber-sumber yang tersedia dari barang bukti yang potensial.
3. Menentukan barang bukti yang perlu dikumpulkan.
4. Menetapkan kemampuan dalam organisasi untuk mengumpulkan barang bukti secara aman agar dapat dijadikan barang bukti yang memenuhi persyaratan atau sah secara hukum.
5. Menetapkan kebijakan-kebijakan untuk mengamankan media penyimpanan dan menangani barang bukti yang potensial.
6. Memastikan sumber-sumber sistem informasi terawasi untuk mendeteksi dan mencegah insiden besar.
7. Mengidentifikasi keadaan ketika investigasi normal dilakukan pada saat kejadian.
8. Melatih anggota organisasi/institusi dalam kesadaran terhadap insiden sehingga semua pihak yang terlibat memahami peran dan tanggungjawab mereka dalam proses barang bukti *Digital* dan kepekaan terhadap hukum atas barang bukti tersebut.
9. Mendokumentasikan kasus-kasus yang berbasis barang bukti yang menjelaskan insiden dan dampaknya terhadap organisasi/institusi.
10. Memastikan telah dilakukannya *Review* hukum untuk memfasilitasi berbagai tindakan dalam merespon insiden yang terjadi.

Untuk mendukung proses DFR yang akan diterapkan pada organisasi, selain menggunakan rujukan yang dijelaskan sebelumnya, tahapan DFR juga perlu dilakukan pemetaan dan sinkronisasi berdasarkan standar yang berlaku agar kualitas tahapan DFR yang dilakukan masih berada pada standar yang berlaku dan memastikan kualitas yang dilakukan pada proses dan yang dihasilkan memiliki standar yang terukur.

Berikut adalah pemetaan tahapan DFR berdasarkan kerangka kerja dan standar ISO yang menjadi acuan global yang berlaku:

1. Identifikasi Bukti *Digital* (ISO/IEC 27037:2012)
   - ✓ Menentukan sumber-sumber potensial dari bukti *Digital* yang mungkin relevan dengan insiden keamanan.
   - ✓ Mengidentifikasi perangkat keras, perangkat lunak, atau sistem lain yang berisi data penting.

- ✓ Menganalisis jenis data yang harus dipertahankan dan strategi untuk mengaksesnya tanpa memengaruhi integritas data.

2. Pengumpulan dan Akuisisi Data (ISO/IEC 27037:2012)
   - ✓ Mengembangkan prosedur standar untuk pengumpulan data secara legal dan aman.
   - ✓ Menggunakan alat seperti *write blockers* untuk memastikan bukti tidak termodifikasi selama proses akuisisi.
   - ✓ Memastikan semua aktivitas pengumpulan bukti didokumentasikan dengan rinci untuk menjaga rantai pengawasan *(chain of custody).*
3. Pelestarian Bukti *Digital* (ISO/IEC 27037:2012; ISO/IEC 27043:2015)
   - ✓ Menyimpan bukti *Digital* dalam lingkungan yang aman untuk mencegah kerusakan, kehilangan, atau manipulasi data.
   - ✓ Menerapkan hashing untuk memastikan integritas data.
   - ✓ Menyediakan akses terbatas ke bukti *Digital* untuk menjaga kerahasiaan dan otentikasi.
4. Analisis dan Interpretasi Bukti *Digital* (ISO/IEC 27042:2015)
   - ✓ Melakukan analisis mendalam terhadap data yang telah dikumpulkan menggunakan alat forensik *Digital* seperti EnCase atau FTK.
   - ✓ Menginterpretasikan hasil analisis untuk mengidentifikasi pola, hubungan, atau bukti yang mendukung penyelidikan.
   - ✓ Menyusun laporan analisis yang dapat dimengerti oleh pemangku kepentingan, termasuk yang tidak memiliki latar belakang teknis.
5. Pemantauan dan Deteksi Insiden (ISO/IEC 27043:2015)
   - ✓ Mengintegrasikan sistem pemantauan yang memungkinkan deteksi dini terhadap aktivitas mencurigakan.
   - ✓ Mengembangkan indikator kinerja utama (*key performance indicators*) untuk mengukur efektivitas sistem deteksi.
   - ✓ Meningkatkan respons insiden melalui pengumpulan data waktu nyata selama insiden terjadi.
6. Eskalasi dan Investigasi Formal (ISO/IEC 27043:2015)
   - ✓ Menentukan kapan insiden harus ditingkatkan menjadi investigasi formal berdasarkan tingkat keparahan atau potensi dampaknya.
   - ✓ Mengaktifkan prosedur investigasi yang lebih mendalam sesuai dengan prinsip-prinsip hukum.

- ✓ Melibatkan tim internal atau eksternal untuk memverifikasi temuan investigasi.

7. Dokumentasi Kasus dan Penyimpanan Data (ISO/IEC 30121:2015)
   - ✓ Menyusun dokumentasi lengkap dari seluruh tahapan proses investigasi, termasuk bukti *Digital*, analisis, dan tindakan yang diambil.
   - ✓ Memastikan semua dokumentasi disimpan dengan aman untuk mematuhi kebijakan hukum atau regulasi yang relevan.
   - ✓ Menyiapkan dokumen yang dapat digunakan dalam persidangan jika diperlukan.
8. Evaluasi dan Tinjauan Hukum (ISO/IEC 27043:2015)
   - ✓ Melakukan evaluasi akhir untuk menilai efektivitas proses kesiapan forensik.
   - ✓ Meninjau kebijakan dan prosedur yang diterapkan untuk memastikan kesesuaiannya dengan perubahan ancaman keamanan.
   - ✓ Memperbarui dan meningkatkan kebijakan kesiapan berdasarkan hasil evaluasi.

Tahapan-tahapan ini membantu organisasi membangun kerangka kerja yang memungkinkan mereka untuk merespons insiden keamanan secara efektif, efisien, dan sesuai dengan hukum serta standar yang berlaku.

2.4 *Model Digital* Forensik *Readiness*

Berdasarkan studi pustaka dan *Review* beberapa penelitian-penelitian sebelumnya, pada penelitian ini penulis membagi kedua *model Digital Forensic Readiness* yang menjadi rujukan dalam implementasi DFR dalam organisasi. Rujukan pertama bersumber dari Rowlingson (2004), dan Bates (2011) dimana mereka mendefinikan enam komponen utama dalam menerapkan DFR dalam organisasi. Sedangkan *model* DFR yang kedua peneliti ambil rujukan dari (Elyas et al., 2015) yang lebih terperinci dalam menyajikan komponen FDR yang dapat berpengaruh terhadap implementasinya di organisasi.

DFR *Model* yang bersumber dari Rowlingson (2004), dan Bates (2011), memiliki enam komponen kunci, antara lain:

1. *Strategy*.

   Kesiapan organisasi dalam *Digital* forensik terlihat dari strategi dan perencanaan sebuah organisasi, tanpa rencana dan strategi yang matang, organisasi akan kesulitan menangani kejahatan siber dan aktivitas *Digital* forensik lainya. Pentingnya komponen strategi ini dikemukakan oleh Rowlingson (2004), dan Bates (2011). Komponen ini meliputi diantaranya seperti Program-program DFR yang berlaku dalam organisasi, aturan kebijakan dan dan kewajiban menyimpan dokumen/file/rekaman, serta kebijakan ketika terjadi peristiwa yang membutuhkan barang bukti *Digital*.selain itu, strategi terhadap ketersediaan teknologi dan dana yang akan digunakan dalam program menjadi hal yang harus diidentifikasi dalam aspek strategis ini.

2. *Policy & Procedure*.

   Setiap aktivitas organisasi harus dilandaskan pada kebijakan dan prosedur tertentu yang telah ditetapkan. Prosedur ini akan menjadi dasar dan petunjuk bagi anggota organisasi untuk menjalankan aktivitas dan kegiatan. Untuk menjamin kesiapan organisasi dalam *Digital* forensi, harus ada prosedur yang ditetapkan. Pentingnya komponen *Policy* & *Procedure* ini dikemukakan oleh Tan (2001), Bates (2011), Barske et al. (2010), dan Sommer (2012). Terdapat setidaknya tiga komponen utama yang menjadi landasan komponen *Policy & Procedure* ini, yaitu:

   - Kebijakan organisasi dan Pembagian tugas, wewenang dan tanggungjawab.
   - Kebijakan & SOP pemanfaatan TIK organisasi beserta pendukungnya.
   - Kebijakan & SOP terkait pengumpulan, perawatan, dan pengamanan barang bukti *Digital* sesuai standar tertentu.

3. *Technology & security*, infrastruktur dan keamanan TIK.

   Untuk mengimplementasikan *Digital* forensik, organisasi harus didukung oleh *hardware* maupun software yang digunakan untuk mencari, mengambil, dan melindungi barang bukti *Digital*. Pentingnya komponen technology & *security* ini dikemukakan oleh Grobbler & Lowrens (2007) dan Barske et al. (2010). Terdapat setidaknya tiga komponen utama yang menjadi landasan komponen *Technology & security* ini, yaitu:

   - Ketersediaan perangkat penyimpanan/pencatat setiap aktivitas TIK.
   - Ketersediaan perangkat akuisisi, pengamanan dan analisa barang bukti *Digital*.

- Ketersediaan perangkat pengamanan sistem dan TIK.

4. *Digital Forensic response*.

   Dalam menjalankan tugas maupun aktivitas *Digital Forensic*, dibutuhkan tenaga-tenaga ahli dan memiliki ketrampilan di bidang *Digital* forensik. Pentingnya Aspek *DigitalForensic response* ini dikemukakan oleh Barske et al. (2010). Terdapat setidaknya dua komponen utama yang menjadi landasan komponen *Digital Forensic response* ini, yaitu:

   - SOP penanganan insiden, pelaporan, pencegahan dan tindakan *Digital* forensik.
   - Ketersediaan SDM dan komponen pendukung (tempat dan alat).

5. *Control*.

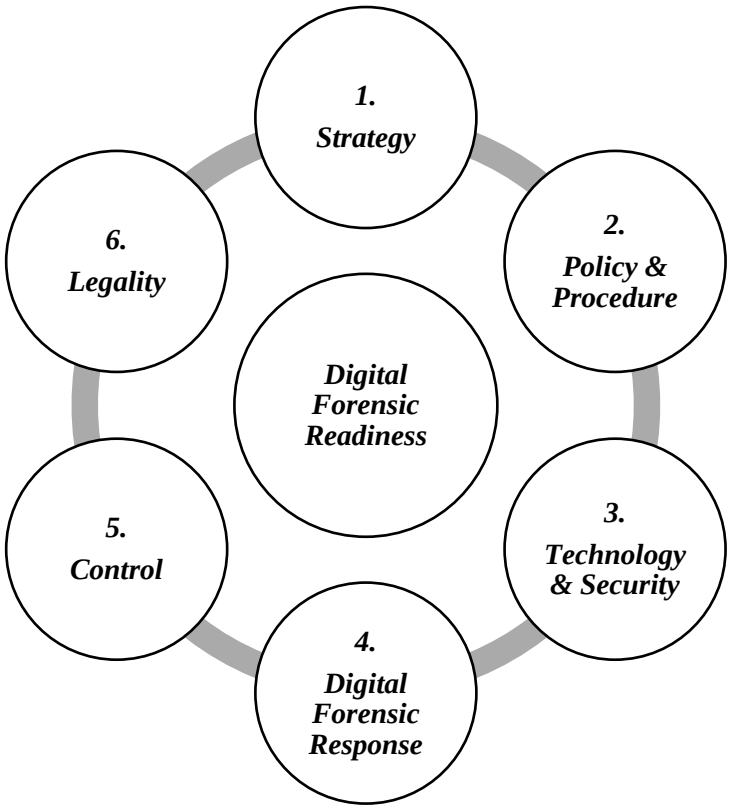
   Ketika program dan aktivitas pendukung maupun penanganan *Digital* forensik, dibutuhkan pengawasan dan kendali akan resiko-resiko yang ditimbulkan, agar program-program DFR dilaksanakan oleh setiap anggota organisasi. Pentingnya komponen *Control* ini dikemukakan oleh Rowlingson (2004), dan Barske et al. (2010). Terdapat setidaknya enam indikator utama yang menjadi pemilaian komponen *Digital Forensic response* ini, yaitu:

   - Pengawasan program DFR.
   - Evaluasi secara berkala program DFR.
   - Sosialisasi program DFR kepada anggota organisasi.
   - Pemahaman pada anggota setiap proses *Digital Forensic* dan resiko kegagalan setiap proses.
   - Pembaharuan perangkat, *tool*, dan sistem secara berkala.
   - Pembahasan hasil investigasi maupun publikasi hasil investigasi kepada kepala-kepala departemen/sub bagian.

6. *Legality,*

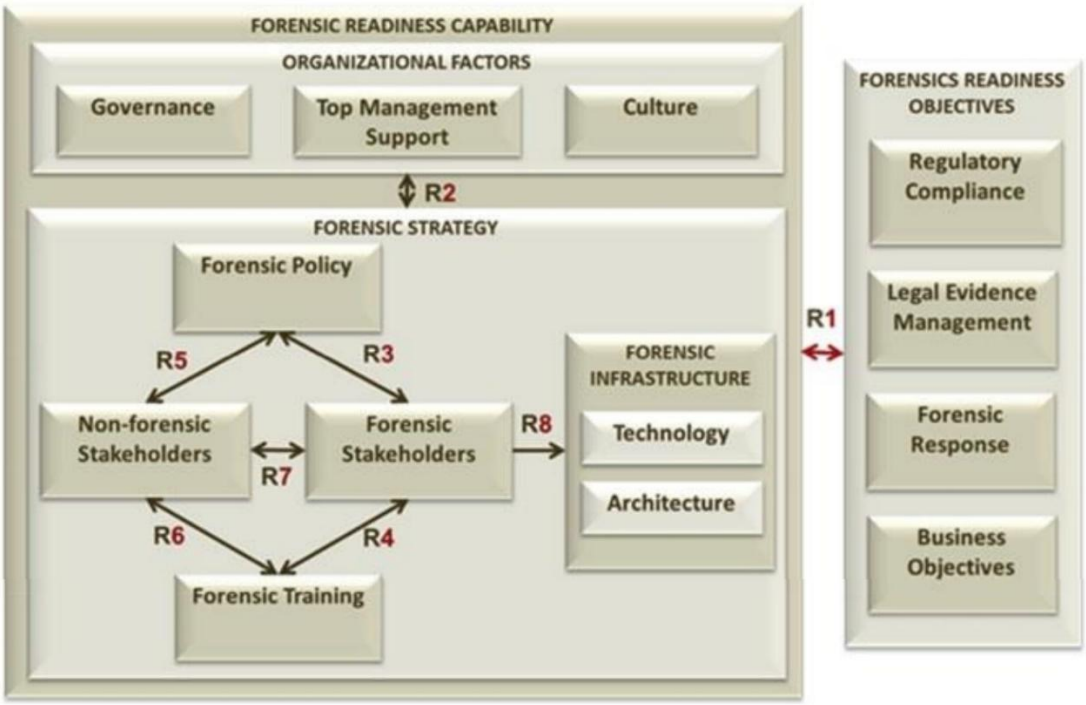
   Merupakan aspek kesesuaian setiap aktivitas/penanganan data *Digital* yang sesuai dengan undang-undang transaksi elektronik. Agar setiap data dapat digunakan secara sah sebagai barang bukti. Pentingnya komponen legality ini dikemukakan oleh Tan (2001), dan Rowlingson (2004)

Keenam kriteria tersebut akan mempengaruhi tingkat keberhasilan implementasi DFR disuatu institusi, seperti terlihat pada gambar berikut.



Gambar 2.1. Komponen utama *Digital Forensic Readiness*

Sedangkan *model Digital Forensic Readiness* yang cukup terperinci dan spesifik, seperti yang dikemukakan oleh Elyas et al. (2015), ditunjukkan pada Gambar berikut.



Gambar 2.2. *Model Digital Forensic Readiness* (Elyas et al., 2015)

Model ini terdiri dari dua komponen utama, yaitu *Forensic Readiness Capability*, *Forensic Strategy* dan *Forensic Readiness Objectives*. Setiap komponen dari ketiga komponen utama tersebut kemudian terbagi lagi menjadi sub-komponen yang saling mendukung dalam membentuk keseluruhan *model*. Pada *Forensic Readiness Capability*, terdapat dua sb komponen yaitu *Organizational Factors* dan *Forensic Strategy Factors. Organizational Factors yang* didalamnya terdapat komponen *Governance* (tata kelola), *Top Management Support* dan *Culture*. Sementara itu, pada komponen *Forensic Strategy Factors* terdapat sub komponen antara lain:

a. *Forensic Policy,*
b. *Non-Forensic Stakeholders*
c. *Forensic Stakeholders*
d. *Forensic Training*
e. *Forensic Infrastructure (didalmnya terdapat Technology dan Architecture)*

Sedangkan pada *Forensic Readiness Objectives*, terdapat empat sub-komponen utama, yakni *Regulatory Compliance, Legal Evidence Management, Forensic Response,* dan *Business Objectives*. *Model* ini memberikan kerangka kerja yang komprehensif untuk implementasi kesiapan forensik *Digital* dalam organisasi.

Model DFR yang dikemukakan oleh Elyas et al. (2015) memberikan kerangka kerja yang terstruktur untuk mempersiapkan organisasi dalam menghadapi tantangan keamanan *Digital*. Komponen *Forensic Readiness Capability* yang terdiri dari *Organizational Factors*, *Forensic Strategy*, dan *Forensic Infrastructure*, berfokus pada penguatan kemampuan internal organisasi. *Organizational Factors* mencakup aspek budaya, kebijakan, dan pelatihan yang memastikan semua pihak di dalam organisasi memahami pentingnya kesiapan forensik. *Forensic Strategy* merujuk pada pendekatan strategis yang diterapkan organisasi untuk mengelola bukti *Digital* secara efektif, termasuk proses pengumpulan, pelestarian, dan analisis data. Sementara itu, *Forensic Infrastructure* menekankan pentingnya infrastruktur teknologi yang mendukung, seperti perangkat lunak dan perangkat keras forensik, untuk memfasilitasi investigasi yang efisien dan aman.

Disisi lain, komponen *Forensic Readiness Objectives* mencakup *Regulatory Compliance, Legal Evidence Management, Forensic Response,* dan *Business Objectives*. *Regulatory Compliance* memastikan bahwa semua aktivitas forensik organisasi sesuai dengan hukum dan regulasi yang berlaku, sehingga menghindari potensi sanksi hukum. *Legal Evidence Management* berfokus pada pengelolaan bukti *Digital* agar dapat diterima

di pengadilan, termasuk menjaga integritas dan otentikasi data. *Forensic Response* mengacu pada kemampuan organisasi untuk merespons insiden secara cepat dan terukur melalui prosedur yang telah ditetapkan sebelumnya. Terakhir, *Business Objectives* menekankan bahwa kesiapan forensik tidak hanya mendukung keamanan, tetapi juga melindungi kepentingan bisnis, seperti reputasi perusahaan dan keberlanjutan operasional. Dengan kerangka ini, organisasi dapat mengintegrasikan kesiapan forensik ke dalam strategi keseluruhan, meningkatkan efektivitas dalam menghadapi ancaman *Digital*.

2.5 *Digital Forensik Readiness Framework*

Kerangka Kesiapan Forensik *Digital (Digital Forensic Readiness Framework)* adalah pendekatan proaktif yang dirancang untuk mempersiapkan organisasi dalam mengumpulkan, menyimpan, dan menganalisis bukti *Digital* sebelum terjadinya insiden keamanan siber. Tujuan utamanya adalah meminimalkan biaya dan gangguan operasional saat investigasi forensik diperlukan, serta memastikan bahwa bukti yang dikumpulkan memenuhi standar hukum dan etika. Kesiapan forensik *Digital* membantu organisasi dalam memenuhi kepatuhan regulasi, klaim asuransi, dan deteksi ancaman.

Implementasi kerangka ini melibatkan beberapa langkah kunci. Pertama, organisasi harus mengidentifikasi aset *Digital* kritis dan potensi sumber bukti yang relevan. Kedua, menetapkan kebijakan dan prosedur yang mendukung pengumpulan dan penyimpanan data secara aman. Ketiga, memastikan bahwa infrastruktur teknologi informasi mendukung aktivitas forensik, termasuk penggunaan alat dan teknik yang sesuai. Terakhir, melatih personel terkait untuk meningkatkan kesadaran dan keterampilan dalam menangani bukti *Digital*.

Penerapan Kerangka Kesiapan Forensik *Digital* memberikan berbagai manfaat bagi organisasi. Dengan kesiapan yang baik, organisasi dapat merespons insiden keamanan dengan lebih efisien, mengurangi dampak finansial dan reputasi. Selain itu, bukti *Digital* yang dikumpulkan secara proaktif dapat digunakan untuk mendukung klaim asuransi, proses litigasi, atau investigasi internal. Menurut SISA Infosec (2023), kesiapan forensik merupakan elemen krusial dalam keamanan siber yang memastikan organisasi siap menghadapi dan merespons insiden dengan efektif. SISA dalam publikasinya menjelaskan beberapa jenis DFRF yang dapat digunakan organisasi untuk mendukung proses tata kelola dan manajemen DF, antara lain seperti disajikan pada tabel berikut.

Tabel 2.1. Jenis-jenis *Digital Forensic Readiness Framework* yang digunakan di dunia Global

Framework Name	***Applicable Cybersecurity Environments***	***Issuing Body/Organization***
*Digital Forensic*s and *Incident Response* (DFIR)	*General* IT, OT, hybrid environments (*cyber Incident response*, *Forensic* analysis)	National Institute of Standards and Technology (NIST), SANS Institute
NIST *Cybersecurity Framework* (CSF)	*General* IT, OT, and Critical Infrastructure (*cybersecurity* risk *Management* and *Forensic Readiness*)	National Institute of Standards and Technology (NIST)
Cloud Forensic Readiness Framework	*Cloud* environments (IaaS, PaaS, SaaS) for *cloud security* and *Incident response*	Various academic and industry bodies (e.g., Journal of *Cloud* Computing)
ETHI*Core Framework*	*General* IT *Cybersecurity* environments (with *Ethical* concerns like *Privacy* and bias)	Developed through collaborative *research* (ETHI*Core* group)
ISO/IEC 27037	*General* IT environments (guidelines on *identification*, *collection*, and preservation of *Digital* evidence)	*International Organization* for Standardization (ISO)
*Digital Forensic*s *Readiness Index* (DFRI) *Model*	*General* IT environments (guidelines, *identification* and *assessment* for maturity *index*)	*Research* and publications

2.6 Sistem Manajemen Keamanan Informasi

Informasi merupakan entitas hasil pemrosesan data yang memberikan nilai atau value tertentu. Data dan informasi pada era sekarang ini menjadi sesuatu yang bernilai. Semakin kompleksnya penggunaan pemrosesan data menjadi informasi disertai dengan interkoneksi yang dapat menghubungkan berbagai layanan selain memberikan dampak positif bagi peradaban dan perkembangan zaman, tentu memiliki dampak negatif yang perlu diwaspadai, dikontrol, dimanajemen dengan baik untuk mendapatkan manfaatnya.

Informasi dapat memiliki nilai manfaat *(value)* bagi pemiliknya jika setidaknya memiliki aspek empat dimensi utama dasar informasi, yaitu relevansi informasi, akurasi informasi, ketepatan waktu dan kelengkapan informasi.

1. **Relevansi**. Suatu informasi tidak akan ada gunanya, apabila tingkat relevansinya dengan keadaan yang sedang dianalisis sangat tipis. Relevansi suatu informasi akan menjadi penting karena hal itu bisa menjadi variabel-variabel yang menentukan pengambilan keputusan oleh organisasi. Informasi memiliki relevansi jika informasi tersebut memiliki hubungan dengan masalah yang dihadapi. Pengguna haruslah

dapat memilih data yang diperlukan tanpa harus melewati dahulu sejumlah fakta-fakta yang tidak berhubungan.

2. **Akurasi**. Informasi yang diterima organisasi harusnya dapat dipercaya adanya. Dengan demikian penting kiranya kita mengetahui sumber pertama pembawa informasi tersebut. Apabila kita tidak mengetahui siapa pembawa pertama informasi tersebut, maka ini akan berbahaya karena tidak ada yang bertanggung jawab sehubungan dengan akibat yang ditimbulkan oleh adanya informasi tersebut. Informasi yang akurat juga akan menjadi tolok ukur ketepatan dan keberhasilan pengambilan keputusan.
3. **Ketepatan waktu**. Informasi harus tersedia pada saat pengambilan keputusan sebelum situasi yang genting atau hilangnya peluang yang ada. Informasi yang datang setelah suatu keputusan diambil tidak akan memiliki nilai. Ketepatan waktu juga amat penting artinya bagi datangnya informasi yang dibutuhkan oleh keadaan tertentu. Semakin *up to date* suatu informasi yang ada, maka akan semakin berguna informasi tersebut. Sebaliknya, semakin kadaluwarsa suatu informasi, maka akan semakin tidak ada artinya.
4. **Kelengkapan**. Para pengguna harus memperoleh informasi yang menyajikan suatu gambaran lengkap atas suatu masalah tertentu atau solusinya. Pengguna hendaknya dapat menentukan jumlah rincian yang dibutuhkan. Informasi dikatakan lengkap apabila memiliki jumlah rincian agregasi yang tepat dan mendukung semua area di mana keputusan akan diambil.

Sedangkan Keamanan informasi adalah sekumpulan metodo*log*i, praktik, ataupun proses yang dirancang dan diterapkan untuk melindungi informasi atau data pribadi dari akses, penggunaan, penyalahgunaan, gangguan, atau modifikasi yang tidak sah. Keamanan informasi bertujuan untuk melindungi data pada berbagai tahap, baik saat terjadi tahapan proses menyimpan, mentransfer, atau menggunakannya. Adapun aspek Keamanan informasi terdiri dari tiga hal yang sering dikenal dengan istilah **CIA Triad**, yaitu ***Confidentiality, Availability,*** dan ***Integrity*** di mana jika ketiganya diterapkan maka akan menghasilkan ***non-Repudiation*** atau kenirsangkalan pada aspek keamanan informasi.

Aspek dalam Keamanan Informasi *(CIA Triad)* adalah *model* standar dalam keamanan informasi yang dirancang untuk mengatur dan mengevaluasi bagaimana sebuah organisasi atau perusahaan ketika data disimpan, dikirim, atau diproses. Setiap aspek yang ada di dalam

CIA Triad (Confidentiality – Integrity – Availability) akan menjadi komponen penting dari keamanan informasi.

Gambar 2.3. Konsep dasar *Information Security, CIA Triad*

1. ***Confidentiality*** **(Kerahasiaan)**

   Aspek *confidentiality* atau kerahasiaan informasi adalah serangkaian upaya perlindungan agar informasi untuk memastikan pengguna yang melakukan akses terhadap informasi tersebut dalam melakukan aktivitasnya dapat terdeteksi, teridentifikasi, terkontrol, termonitor, serta memang memiliki otorisasi. Poin intinya pada aspek ini adalah memastikan bahwa informasi **hanya** dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

2. ***Integrity*** **(integritas / keaslian)**

   Integrity atau integritas mengacu pada suatu metode atau langkah-langkah untuk menjaga agar data atau informasi tidak dapat dimanipulasi, diubah atau diedit oleh pihak yang tidak punya wewenang baik pada piranti pemrosesan maupun pada pengiriman informasinya (telekomunikasi). Aspek ini merupakan kelanjutan dari aspek pertama yaitu Confidentiality (kerahasiaan) informasi yang hanya dapat diakses oleh orang yang berhak namun juga memastikan data/informasi tersebut memiliki keaslian atau integritas yang baik.

3. ***Availability*** **(ketersediaan)**

   Aspek *Availability* atau ketersediaan informasi memiliki arti dalam konteks keamanan informasi bahwa serangkaian upaya untuk memastikan agar sebuah sistem tetap bisa digunakan, diakses oleh penggunanya pada saat dibutuhkan.

Ketiga aspek keamanan informasi ini digunakan oleh dua golongan pengguna sistem, yaitu golongan pengelola sistem layanan pengolah data/informasi maupun digunakan oleh golongan penyerang keamanan sistem. Pengelola menerapkan serangkaian manajemen pengendalian keamanan informasi berdasarkan ketiga aspek di atas dengan berbagai metode, tahapan, *tools* dan sumber daya lainnya. Namun disisi sebaliknya, para penyerang *(attacker, intruder)* juga menggunakan ketiga aspek tersebut untuk melakukan targeting terhadap penggunaan informasi yang mereka inginkan dengan berbagai cara, metode, tahapan dengan menggunakan berbagai sarana. Maka dari itulah pemahaman mendasar terhadap pemenuhan kenirsangkalan *(nonrepudiation)* perlu dipahami dengan seksama dalam mengelola keamanan informasi bagi organisasi.

Beberapa aspek yang terkait dengan keamanan informasi yang mempengaruhi CIA Triad keamanan informasi antara lain *Privacy, identification, Authorization, authentication,* dan *accountability*.

1. ***Privacy*** merupakan Informasi yang dikumpulkan, digunakan, dan disimpan oleh pengguna maupun organisasi yang dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik informasi dari pengguna lain.
2. ***Identification*** merupakan serangkaian proses mengidentifikasi data/informasi berdasarkan aset informasi, risiko, serta berdasarkan penggunaannya dan pemrosesannya. Identifikasi adalah langkah pertama dalam memitigasi risiko keamanan informasi sebelum serangan dilakukan lebih jauh oleh penyerang. Tahap ini pun menjadi tahap awal dalam melakukan proteksi dan monitoring aset dan keamanan informasi yang dikelola.
3. ***Authentication*** merupakan proses yang dilakukan sistem untuk memastikan atau membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas dan hak akses yang di klaim.
4. ***Authorization*** dibutuhkan pada saat setelah identitas pengguna diotentikasi, yakni sebuah proses yang memberikan jaminan bahwa pengguna (manusia dan komputer) telah mendapatkan otorisasi secara spesifik dan jelas untuk mengakses, mengubah, atau menghapus isi dari data dan informasi.
5. ***Accountability*** merupakan proses perhitungan pada manajemen keamanan informasi untuk memastikan data semua aktivitas terhadap informasi yang telah

dilakukan, siapa yang melakukan aktivitas itu serta berapa level risiko yang akan didapatkan atau berdampak terhadapnya.

Terwujudnya pelayanan publik yang berkualitas dan terpercaya dalam mengelola data dan informasi perlu didukung dengan metode, standar, tahapan, strategi, *tools* dan sumber daya lainnya yang berkontribusi secara holistik (utuh) dalam satu kesatuan skema manajemen informasi. Ada beberapa standar manajemen keamanan informasi berdasarkan *level, scope area* serta spesifik penggunaannya. *ISO 27000 family* merupakan salah satu dari sekian jenis standar manajemen keamanan informasi yang mencakup banyak sektor. Pemerintah Indonesia sendiri telah mengesahkan ISO/SNI 270001 (berbahasa Indonesia) sebagai materi adopsi murni dari ISO/IEC 27001 yang dapat diterapkan untuk standarisasi global keamanan informasi. Standar SMKI berbasis ISO/IEC 27001 tidak mewajibkan suatu kontrol keamanan informasi secara spesifik, karena kontrol keamanan yang diperlukan dapat beragam sesuai dengan keperluan organisasi yang akan menerapkannya. Perusahaan atau organisasi diperbolehkan untuk mengadopsi ISO/IEC 27001 dengan memilih kontrol keamanan informasi tertentu untuk penerapan SMKI. Secara umum implementasi Sistem Manajemen Keamanan Informasi berbasis ISO 27001:2022 dengan mereferensi pada konsep manajemen ***PLAN* – DO – CHECK – ACTION**.

Selain membutuhkan standar keamanan informasi, pengelola data/informasi perlu melakukan eksekusi standar tersebut ke dalam beberapa tahapan proses mulai dari menetapkan, menerapkan, memelihara, meningkatkan secara berkesinambungan terhadap SMKI. Penerapan/implementasi SMKI dilakukan dengan menyelaraskan kegiatan yang sedang berlangsung di instansi/Lembaga. Secara umum keuntungan yang didapat oleh organisasi yang menerapkan Sistem Manajemen Keamanan Informasi:

1. Meningkatkan reputasi organisasi
2. Meningkatkan kepercayaan stakeholder
3. Pengelolaan insiden menjadi lebih baik
4. Meningkatkan kualitas layanan
5. Perbaikan respons time
6. Perubahan proses reaktif menjadi proaktif
7. Peningkatan berkelanjutan
8. Mendukung proses bisnis

Lingkup dan Tujuan dari SNI ISO 27001:2022 meliputi:

1. Mendefinisikan persyaratan untuk menetapkan, menerapkan, memelihara, meningkatkan secara berkesinambungan terhadap sistem manajemen keamanan informasi
2. Persyaratan dalam standar ini bersifat umum dimaksudkan agar dapat diterapkan oleh organisasi tanpa membatasi jenis, ukuran, serta sifat organisasi
3. Persyaratan dalam standar ini dirancang untuk memastikan bahwa organisasi memiliki langkah-langkah yang tepat untuk melindungi aset informasi yang dimiliki organisasi
4. Merupakan standar dengan pendekatan berbasis risiko, artinya melibatkan asesmen serta manajemen risiko terkait keamanan informasi
5. Merupakan standar internasional dengan sasaran melindungi informasi dalam kontak CIA (*Confidentiality*, *Integrity*, dan *Availability*)

Data organisasi pada dasarnya adalah bagian dari sistem informasi yang harus terus ditingkatkan keamanannya. Akan berakibat fatal jika organisasi tidak mampu melindungi keamanan informasi baik dari sisi informasi organisasi dan informasi publik. Sehingga dibutuhkan standar yang digunakan untuk melakukan manajemen keamanan informasi tersebut, ISO/IEC 27001:2022 adalah standar internasional yang digunakan untuk manajemen keamanan informasi. Berikut adalah penguraian umum dari 11 Chapter pada ISO/IEC 27001:2022:

1. ***Chapter 1 - Scope:*** Bab ini memberikan penjelasan mengenai cakupan dan batasan dari standar ISO/IEC 27001:2022 yang memberikan pandangan umum tentang tujuan dan aplikasi standar ini.
2. ***Chapter 2 - Normative References****:* Bab ini mencantumkan referensi-normatif yang diperlukan untuk memahami dan menerapkan ISO/IEC 27001:2022.
3. ***Chapter 3 - Terms and Definitions:*** Bab ini menyajikan definisi dari termino*log*i yang digunakan dalam standar sehingga membantu dalam mengklarifikasi makna istilah yang digunakan di seluruh dokumen.
4. ***Chapter 4 - Context of the Organization:*** Bagian ini membahas langkah-langkah untuk menetapkan konteks organisasi, termasuk pihak-pihak yang terlibat dan persyaratan bisnis yang perlu diperhitungkan dalam manajemen keamanan informasi.

5. ***Chapter 5 - Leadership:*** Bab ini menekankan peran kepemimpinan dalam menentukan dan mendukung kebijakan keamanan informasi, serta memastikan keterlibatan dan dukungan manajemen tingkat atas.
6. ***Chapter 6 - Planning:*** Bagian ini mencakup rencana keamanan informasi, termasuk risiko dan peluang, serta bagaimana organisasi merencanakan tindakan untuk mengelola risiko tersebut.
7. ***Chapter 7 - Support:*** Bab ini membahas faktor pendukung, seperti sumber daya, kompetensi, dan kesadaran yang diperlukan untuk mendukung implementasi dan pemeliharaan sistem manajemen keamanan informasi.
8. ***Chapter 8 - Operation:*** Bagian ini mencakup langkah-langkah operasional untuk mengelola risiko dan menjalankan kontrol keamanan informasi.
9. ***Chapter 9 - Performance Evaluation:*** Bab ini membahas bagaimana organisasi dapat mengevaluasi kinerja sistem manajemen keamanan informasi, termasuk pemantauan dan pengukuran kinerja sistemnya.
10. ***Chapter 10 - Improvement:*** Bagian ini menyoroti pentingnya peningkatan berkelanjutan dalam manajemen keamanan informasi dan bagaimana organisasi dapat mengidentifikasi peluang perbaikan.
11. ***Chapter 11 - Annex A:*** *Annex*e ini berisi kontrol keamanan informasi dan panduan yang dijelaskan lebih lanjut, memungkinkan organisasi untuk memilih dan menerapkan kontrol yang sesuai dengan kebutuhan.

SNI ISO 27001:2022 mencakup total 93 kontrol yang kemudian dikonsolidasikan menjadi 4 grup kategori kontrol sebagai berikut:

1. Organisasi (*Organizational*) (37 pengendalian) – jika menyangkut organisasi, seperti kebijakan untuk informasi, pengembalian aset, keamanan informasi untuk penggunaan layanan *cloud*.
2. Orang (*People*) (8 pengendalian) – jika menyangkut orang individu, seperti kerja jarak jauh, penyaringan, kerahasiaan, atau perjanjian kerahasiaan.
3. Fisik (*Physical*) (14 pengendalian) – jika menyangkut objek fisik, seperti media penyimpanan, pemeliharaan peralatan, pemantauan keamanan fisik, atau pengamanan kantor, ruangan, dan fasilitas.
4. Teknologi (*Technological*) (34 pengendalian) – jika menyangkut tekno*log*i, seperti otentikasi yang aman, penghapusan informasi, pencegahan kebocoran data, atau pengembangan yang dialihdayakan.

Gambar 2.4. *Annex Control* ISO 27001:2022

Dalam Standar ISO/IEC 27001:2022 tidak secara eksplisit mencantumkan daftar kontrol dalam klausulnya. Namun, dalam *Annex* A dari standar ini berisi 93 kontrol keamanan informasi yang direkomendasikan untuk diterapkan dalam organisasi. Dijabarkan dari Gambar 2.4. Kontrol keamanan yang terdapat pada *Annex control* ISO 27001:2022 berhubungan dnengan proses *Digital Forensic*. *Digital Forensic Readiness* (DFR) memiliki posisi strategis dalam mendukung implementasi dan keberlanjutan ISO 27001:2022 *Information Security Management System* (ISMS), terutama dalam kerangka kerja *(Framework)* pengelolaan insiden keamanan informasi, investigasi, dan respons insiden. ISO 27001:2022 menetapkan standar untuk melindungi kerahasiaan, integritas, dan ketersediaan informasi, di mana DFR memainkan peran penting dalam memastikan bahwa bukti *Digital* dapat diidentifikasi, dikumpulkan, dan dilestarikan dengan cara yang memenuhi prinsip-prinsip hukum dan standar internasional. Urgensi DFR dalam konteks ISO 27001:2022 juga semakin meningkat karena banyak organisasi menghadapi ancaman siber yang terus berkembang, sehingga kesiapan forensik menjadi elemen penting dalam manajemen risiko keamanan informasi. Dengan mengintegrasikan DFR ke dalam ISMS, organisasi dapat meningkatkan kemampuan deteksi, respons, dan mitigasi insiden, sekaligus memastikan kepatuhan terhadap regulasi dan persyaratan audit.

Secara umum, ISMS ISO/IEC 27001 merupakan bagian dari ISO/IEC 27000 *family* yang meliputi berbagai standar yang relevan dengan manajemen keamanan informasi, termasuk keamanan privasi, manajemen identitas, kolaborasi dan berbagi data yang aman, serta transaksi dan pembayaran online yang aman. Kumpulan standar ini memberikan panduan untuk membantu organisasi dalam mengelola dan melindungi data sensitif, serta memastikan bahwa sistem keamanan informasi dapat menangani ancaman dan insiden dengan cara yang sah dan efektif. Secara terperinci, ISO/IEC 27000 *family* memiliki daftar sebagai berikut.

Tabel 2.2. ISO/IEC 27000 *Family Standards*

Kode Standar	Judul Standar	Penjelasan Singkat
ISO/IEC 27000	*Information security Management systems – Overview and vocabulary*	Memberikan gambaran umum dan mendefinisikan istilah-istilah yang digunakan dalam keluarga ISO/IEC 27000.
ISO/IEC 27001	*Information security Management systems – Requirements*	Menyediakan persyaratan untuk membangun, mengimplementasikan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi (ISMS).
ISO/IEC 27002	*Information security controls: A catalog of controls*	Menyediakan katalog kontrol untuk mengelola keamanan informasi dalam ISMS, sebagai pedoman untuk melaksanakan kontrol yang relevan.
ISO/IEC 27003	*Information security Management system - Guidance*	Memberikan pedoman untuk mengimplementasikan ISO/IEC 27001, serta mendukung pembangunan ISMS di organisasi.
ISO/IEC 27004	*Information security Management – Monitoring, measurement, analysis and evaluation*	Memfokuskan pada pengukuran dan evaluasi untuk manajemen keamanan informasi, membantu organisasi dalam menentukan metrik keamanan yang efektif.
ISO/IEC 27005	*Guidance on managing information security risks*	Memberikan panduan dalam mengidentifikasi, menganalisis, mengevaluasi, dan menangani risiko terhadap keamanan informasi.
ISO/IEC 27006	*Requirements for bodies providing audit and certification of ISMS*	Menetapkan persyaratan untuk lembaga yang melakukan audit dan sertifikasi ISMS sesuai dengan ISO/IEC 27001.
ISO/IEC 27007	*Guidelines for ISMS auditing*	Menyediakan pedoman untuk audit sistem manajemen keamanan informasi (ISMS), termasuk prinsip dan prosedur audit yang efektif.
ISO/IEC 27008	*Guidance for the assessment of information security controls*	Menyediakan panduan untuk menilai kontrol keamanan informasi dalam ISMS.

ISO/IEC 27009	*Sector-specific applications of ISO/IEC 27001*	Menyesuaikan implementasi ISO/IEC 27001 untuk sektor-sektor tertentu dengan kebutuhan keamanan yang berbeda
ISO/IEC 27010	*Information security Management for inter-sector and inter-Organizational communications*	Memberikan panduan tentang manajemen keamanan informasi untuk komunikasi antar sektor dan antar organisasi, termasuk pengelolaan data dan berbagi informasi dalam kolaborasi antar organisasi.
ISO/IEC 27011	*Information security Management for telecommunications Organizations*	Menyediakan pedoman untuk organisasi telekomunikasi dalam mengelola keamanan informasi, melindungi data sensitif, dan memenuhi regulasi terkait keamanan jaringan telekomunikasi.
ISO/IEC 27013	*Integrated implementation of ISO/IEC 20000-1 and ISO/IEC 27001*	Panduan untuk mengintegrasikan penerapan ISO/IEC 20000-1 (manajemen layanan TI) dan ISO/IEC 27001 (manajemen keamanan informasi) agar kedua sistem manajemen dapat saling mendukung.
ISO/IEC 27014	*Governance of information security*	Memberikan panduan untuk tata kelola keamanan informasi di tingkat organisasi, termasuk bagaimana mengelola risiko dan menetapkan peran manajerial yang jelas untuk tujuan keamanan informasi.
ISO/IEC 27015	*Information security Management guidelines for financial services Organizations*	Panduan untuk organisasi jasa keuangan dalam mengelola keamanan informasi, dengan fokus pada pengelolaan data sensitif dan perlindungan terhadap ancaman yang mengarah pada kerugian finansial.
ISO/IEC 27016	*Information security Management - Organizational economics*	Membahas bagaimana ekonomi organisasi dapat diterapkan dalam manajemen keamanan informasi, termasuk analisis biaya dan manfaat dari kontrol yang diterapkan dalam pengelolaan keamanan informasi.
ISO/IEC 27017	*Code of practice for information security controls for cloud services*	Memberikan panduan tentang kontrol keamanan untuk penyedia layanan *cloud* dan pengguna *cloud*, untuk mengelola dan melindungi data yang ada di lingkungan *cloud*.
ISO/IEC 27018	*Protection of personal data in the cloud*	Berfokus pada perlindungan data pribadi dalam lingkungan *cloud*, serta pengelolaan data pribadi yang sesuai dengan regulasi perlindungan data pribadi (misalnya GDPR).
ISO/IEC 27019	*Information security Management for process control systems*	Memberikan panduan untuk organisasi yang menggunakan sistem kontrol proses, seperti industri manufaktur atau energi, untuk mengelola keamanan informasi dalam sistem ini.
ISO/IEC 27021	*Competence requirements for information security Management systems auditors*	Mengatur persyaratan kompetensi bagi auditor ISMS, termasuk keterampilan, pengetahuan, dan pengalaman yang diperlukan untuk melakukan audit ISMS secara efektif.

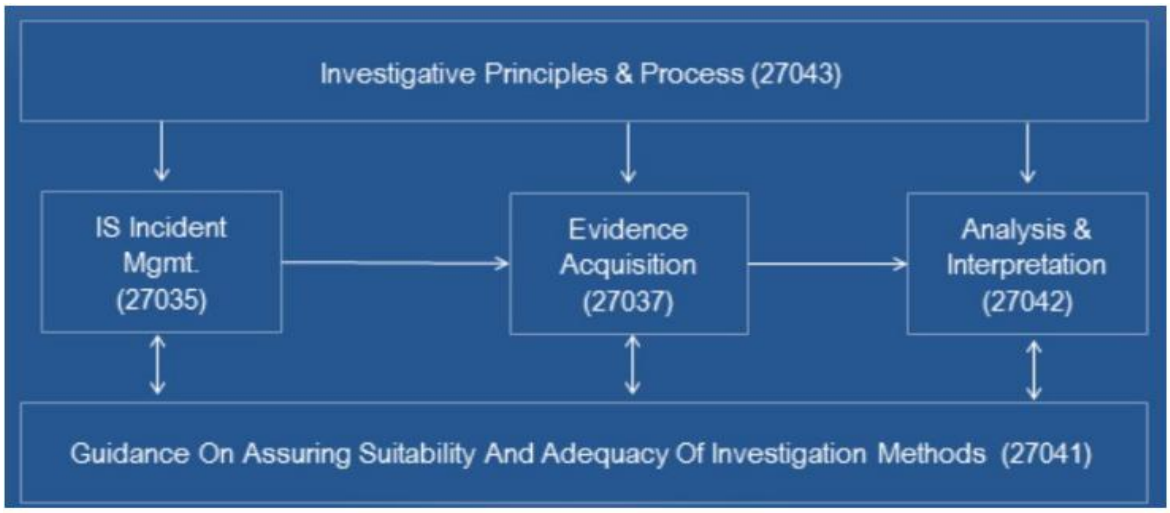
ISO/IEC 27022	*Information security Management guidelines for the healthcare sector*	Memberikan panduan untuk sektor kesehatan dalam mengelola keamanan informasi, dengan fokus pada perlindungan data pasien dan kepatuhan terhadap regulasi perlindungan data kesehatan.
ISO/IEC 27023	*Framework for information security Management system measurement and improvement*	Menyediakan kerangka untuk pengukuran dan peningkatan sistem manajemen keamanan informasi, dengan memberikan metode untuk menilai keberhasilan ISMS.
ISO/IEC 27024	*Information security Management - Measurement and reporting*	Memberikan panduan untuk mengukur kinerja ISMS dan melaporkan hasilnya, termasuk metrik yang relevan untuk penilaian keberhasilan implementasi kontrol keamanan.
ISO/IEC 27025	*Information security - Cloud computing security Management*	Panduan untuk pengelolaan keamanan informasi dalam komputasi awan, termasuk kontrol dan kebijakan yang diperlukan untuk menjaga keamanan data dan aplikasi yang disimpan di *cloud*.
ISO/IEC 27025	*Information security - Cloud computing security Management*	Menyediakan panduan untuk pengelolaan keamanan informasi dalam komputasi awan, termasuk kontrol dan kebijakan yang diperlukan untuk menjaga keamanan data dan aplikasi yang disimpan di *cloud*.
ISO/IEC 27026	*Information security Management - Information security controls for Digital payment systems*	Memberikan pedoman mengenai pengelolaan keamanan informasi untuk sistem pembayaran *Digital*, dengan fokus pada perlindungan data transaksi dan pembayaran elektronik yang sensitif.
ISO/IEC 27027	*Information security Management - Information security controls for mobile phone applications*	Menyediakan pedoman mengenai kontrol keamanan untuk aplikasi ponsel, termasuk pengelolaan data pengguna dan pengamanan aplikasi yang berjalan pada perangkat seluler.
ISO/IEC 27028	*Information security Management - Cyber security controls for critical infrastructure*	Menyediakan kontrol keamanan siber untuk infrastruktur kritis yang penting untuk melindungi data dan sistem operasional, seperti dalam sektor energi dan telekomunikasi, guna mengurangi kerentanannya terhadap serangan siber.
ISO/IEC 27029	*Information security Management - Cloud security controls*	Menyediakan pedoman untuk pengelolaan kontrol keamanan informasi di lingkungan komputasi awan, termasuk perlindungan data dan kontrol akses pada aplikasi *cloud*.
ISO/IEC 27030	*Information security Management - Information sharing and governance*	Panduan tentang cara organisasi dapat berbagi informasi secara aman dan mengelola aspek hukum serta kebijakan berbagi informasi dalam ekosistem yang lebih luas, dengan memperhatikan risiko dan kontrol yang diperlukan.
ISO/IEC 27031	*Information security Management - Business continuity Management and information security*	Memberikan panduan untuk melindungi keberlanjutan bisnis dengan memadukan pengelolaan keberlanjutan operasional dengan sistem manajemen keamanan informasi,

		memastikan bahwa informasi tetap tersedia meskipun terjadi gangguan operasional.
ISO/IEC 27032	*Information security Management - Cybersecurity guidelines*	Memberikan panduan untuk pengelolaan keamanan siber dengan fokus pada perlindungan data yang berada di dalam atau melalui jaringan *Internet*, serta pengamanan infrastruktur dan kebijakan terkait.
ISO/IEC 27033	*Information security Management - Network security*	Menyediakan panduan untuk mengelola keamanan jaringan, dengan fokus pada kontrol yang melindungi data dan komunikasi di dalam jaringan organisasi dari ancaman dan gangguan.
ISO/IEC 27034	*Information security Management - Application security*	Memberikan panduan untuk pengelolaan keamanan aplikasi, termasuk perlindungan terhadap perangkat lunak dan aplikasi dari kerentanannya terhadap ancaman yang dapat membahayakan data dan proses bisnis.
ISO/IEC 27035	*Information security Management - Incident Management*	Menyediakan panduan untuk pengelolaan insiden keamanan informasi, dengan fokus pada penanganan dan respons terhadap serangan atau insiden yang memengaruhi kerahasiaan, integritas, atau ketersediaan informasi.
ISO/IEC 27036	*Information security Management - Supplier relationships*	Menyediakan kontrol keamanan yang berkaitan dengan hubungan antara organisasi dan pemasok, untuk memastikan bahwa pemasok mengelola keamanan informasi dengan cara yang sesuai dan tidak menambah risiko bagi organisasi.
ISO/IEC 27037	*Information security Management - Guidelines for identification, collection, acquisition, and preservation of Digital evidence*	Menyediakan pedoman untuk pengumpulan, akuisisi, dan pelestarian bukti *Digital* yang dapat digunakan dalam investigasi, termasuk prosedur yang diperlukan untuk memastikan bukti yang diperoleh sah dan terverifikasi.
ISO/IEC 27038	*Information security Management - Guidelines for the use of encryption for information security Management*	Panduan untuk penggunaan teknik enkripsi dalam manajemen keamanan informasi, meliputi kontrol terkait enkripsi untuk melindungi data yang sensitif.
ISO/IEC 27039	*Information security Management - Selection, deployment and operations of intrusion detection systems*	Memberikan panduan mengenai pemilihan, penerapan, dan pengoperasian sistem deteksi intrusi untuk mengidentifikasi potensi ancaman terhadap informasi dan sistem.
ISO/IEC 27040	*Information security Management - Storage security*	Memberikan panduan untuk mengelola keamanan penyimpanan data, baik dalam bentuk *Digital* maupun fisik, termasuk kontrol untuk memastikan bahwa data disimpan secara aman dan terjaga integritasnya.
ISO/IEC 27041	*Information security Management - Guidance on auditing Digital Forensics*	Menyediakan pedoman tentang bagaimana melakukan audit terhadap prosedur dan teknik forensik *Digital* untuk memastikan bahwa bukti

		yang dikumpulkan dapat diterima di pengadilan dan sesuai dengan standar yang berlaku.
ISO/IEC 27042	*Information security Management - Guidelines for the analysis and interpretation of Digital evidence*	Memberikan pedoman untuk menganalisis dan menafsirkan bukti *Digital* yang dikumpulkan selama investigasi, memastikan bahwa bukti tersebut diproses dengan cara yang sah dan sesuai dengan prosedur yang diterima.
ISO/IEC 27043	*Information security Management - Incident investigation principles and processes*	Memberikan pedoman untuk investigasi insiden yang terkait dengan keamanan informasi, termasuk prosedur untuk memastikan bahwa bukti yang dikumpulkan dapat digunakan dalam penyelidikan dan tindakan hukum lebih lanjut.
ISO/IEC 27044	*Information security Management - Secure data destruction*	Menyediakan pedoman untuk penghapusan data dengan cara yang aman untuk mencegah kebocoran informasi dan menjaga kerahasiaan serta integritas data yang dihancurkan.
ISO/IEC 27045	*Information security Management - Protection of personal data*	Memberikan pedoman untuk melindungi data pribadi dalam manajemen keamanan informasi, memastikan perlindungan terhadap informasi pribadi sesuai dengan hukum dan peraturan yang berlaku.
ISO/IEC 27046	*Information security Management - Guidelines for data retention and disposal*	Memberikan panduan terkait dengan kebijakan dan prosedur untuk menyimpan dan membuang data dengan cara yang aman, sehingga informasi yang disimpan tetap terjaga selama masa simpan yang relevan.

Berdasarkan tabel diatas, standar ISO 27000 family yang memiliki keterkaitan antara *Digital Forensic* dan ISMS sesuai dengan tema penelitian ini antara lain:

1. ISO/IEC 27001: *Information Security Management Systems*
2. ISO/IEC 27037: *Information Security Management - Guidelines for identification, collection, acquisition, and preservation of Digital evidence*
3. ISO/IEC 27042 *Information Security Management - Guidelines for the analysis and interpretation of Digital evidence*
4. ISO/IEC 27043 *Information Security Management - Incident investigation principles and processes*



Gambar 2.5. *ISO/IEC 27000 Family (ISMS)* yang berhubungan dengan *Digital Forensic*

2.7 Sistem Pemerintahan Berbasis Elektronik

Sistem Pemerintahan Berbasis Elektronik (SPBE) atau *E-Government* didefinisikan sebagai penyelenggaraan pemerintah yang memanfaatkan teknologi informasi dan komunikasi (TIK) untuk memberikan layanan kepada Pengguna SPBE. Pengguna SPBE adalah instansi pusat, pemerintah daerah, pegawai Aparatur Sipil Negara, perorangan, masyarakat, pelaku usaha, dan pihak lain yang memanfaatkan Layanan SPBE. Definisi ini didasarkan pada Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik mencakup sistem-sistem yang dipergunakan untuk berinteraksi antara organisasi pemerintah dengan masyarakat (*Government-to-Citizen* atau G2C), organisasi pemerintah dengan kalangan bisnis (*Government-to-Business* atau G2B), organisasi pemerintah dengan staf internal organisasi pemerintah sendiri (*Government-to-Employee* atau G2E), dan organisasi pemerintah dengan organisasi pemerintah lainnya baik yang memiliki hubungan setara/horizontal maupun yang memiliki hubungan vertikal (*Government-toGovernment* atau G2G).

Untuk mewujudkan good governance berdasarkan konsep yang ditawarkan SPBE tersebut, instansi pemerintah pusat telah menetapkan Visi dari SPBE Nasional, adapun visi tersebut adalah “Terwujudnya Sistem Pemerintahan Berbasis Elektronik yang terpadu dan menyeluruh untuk mencapai birokrasi dan pelayanan yang berkinerja tinggi”. Untuk mencapai Visi tersebut, didefinisikanlah Visi SPBE yang telah ditetapkan tersebut menjadi acuan dalam mewujudkan pelaksanaan SPBE yang terpadu di Instansi Pemerintah Pusat dan Instansi Pemerintah Daerah untuk menghasilkan birokrasi pemerintah yang integratif, dinamis, transparan dan inovatif serta peningkatan kualitas pelayanan publik yang terpadu,

efektif, responsif dan adaptif. Dalam rangka mencapai visi SPBE tersebut, maka diturunkan dan dijelaskan dalam bentuk Misi SPBE, yang meliputi:

1. Melakukan penataan dan penguatan organisasi dan tata kelola Sistem Pemerintah Berbasis Elektronik yang terpadu;
2. Mengembangkan pelayanan publik berbasis elektronik yang terpadu, menyeluruh dan menjangkau masyarakat luas;
3. Membangun fondasi teknologi informasi dan komunikasi yang terintegrasi, aman dan andal; dan
4. Membangun Sumber Daya Manusia (SDM) yang kompeten dan inovatif berbasis teknologi informasi dan komunikasi.

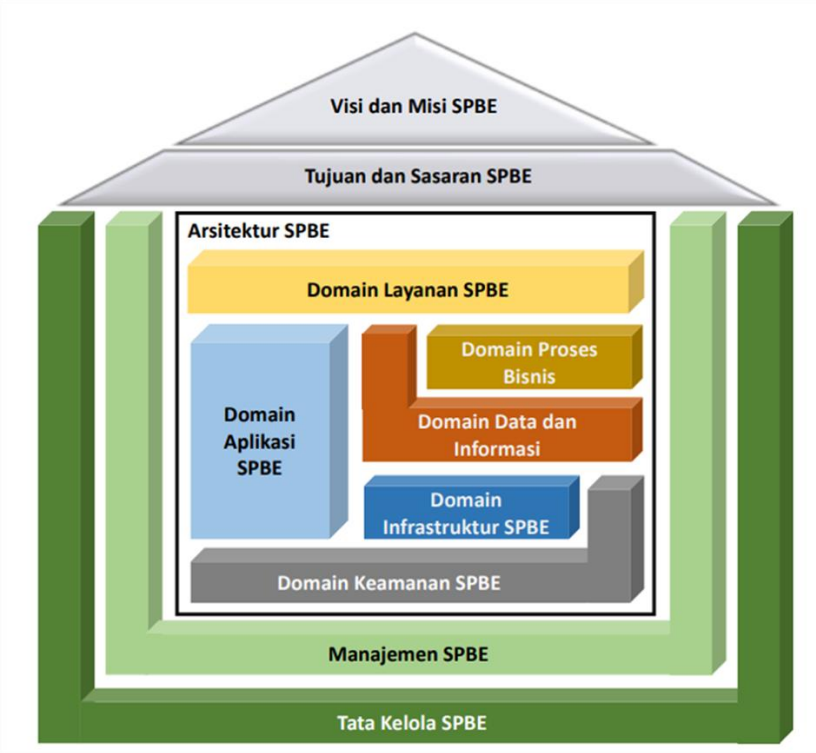
Berdasarkan Visi dan Misi SPBE yang telah disampaikan diatas, maka ditetapkan tujuan dari SPBE, sebagai berikut:

1. Mewujudkan tata kelola pemerintahan yang bersih, efektif, efisien, transparan dan akuntabel;
2. Mewujudkan pelayanan publik yang berkualitas dan terpercaya; dan
3. Mewujudkan Sistem Pemerintahan Berbasis Elektronik yang terpadu

Untuk mencapai tujuan SPBE maka ditetapkan sasaran SPBE, yaitu antara lain sebagai berikut:

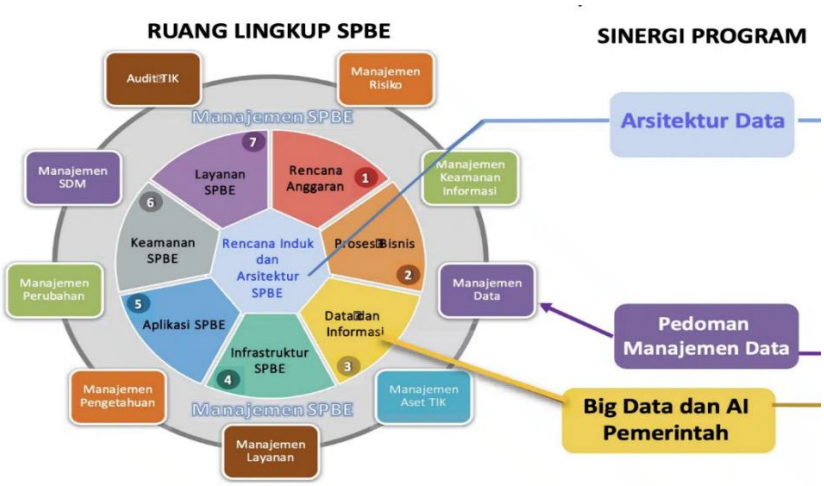
1. Terwujudnya tata kelola dan manajemen TIK yang efektif dan efisien;
2. Terwujudnya layanan SPBE yang terpadu dan berorientasi kepada pengguna;
3. Terselenggaranya infrastruktur SPBE yang terintegrasi; dan
4. Meningkatnya kapasitas SDM TIK.

Untuk mewujudkan cita-cita, visi, misi, tujuan, dan sasaran tersebut, dibuatlah Arsitektur SPBE yang komponennya dapat divualisasikan seperti pada gambar berikut.



Gambar 2.6. Komponen Arsitektur Sistem Pemerintahan Berbasis Elektronik (sumber: https://spbe.madina.go.id/category/arsitektur-spbe-nasional)

Berdasarkan gambar komponen Arsitektur SPBE diatas, sebuah organisasi pemerintahan mulai dari level Kementrian, Lembaga Tinggi Negara, dan :embaga Daerah wajib membuat, mendefinisikan Visi & Misi SPBE, Tujuan dan Sasaran SBPE beserta komponen pendukungnya. Secara terperinci, komponen SPBE dijabarkan kedalam Ruang lingkup SPBE seperti terlihat pada gmabar berikut, yaitu:



Gambar 2.7. Ruang Lingkup Sistem Pemerintahan Berbasis Elektronik (sumber: https://menpan.go.id/site/berita-terkini/wujudkan-birokrasi-berkelas-dunia-melalui-spbe)

Berdasarkan runaglingkup SPBE tersebut diatas, *Digital Forensic Readiness* (DFR) memiliki peran yang sangat penting dalam mendukung implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE). Salah satu bukti dibutuhkannya DFR dalam SPBE adalah terdapatnya komponen Domain Keamanan yang mengacu pada SMKI (sistem Manajemen Keamanan Informasi) dimana didalamnya terdapat unsur Penanganan Insiden Keamanan yang harus diterapkan baik secara tata kelola maupun manajemennya.

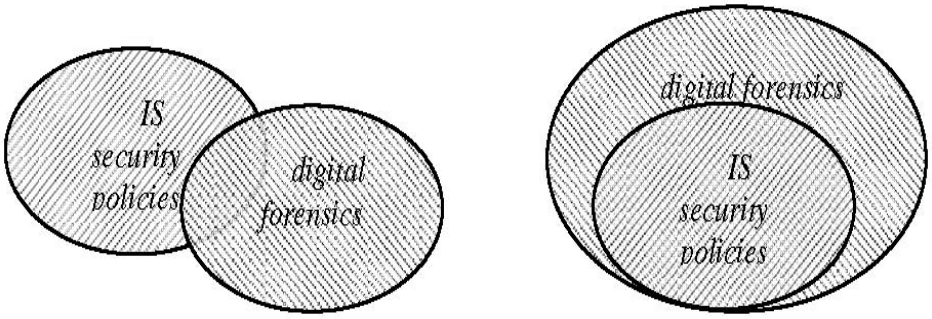
Dalam SPBE, data dan informasi menjadi aset utama yang harus dilindungi dari ancaman keamanan siber seperti peretasan, penyalahgunaan data, atau kebocoran informasi sensitif. DFR membantu memastikan bahwa bukti *Digital* yang relevan dapat diidentifikasi, dikumpulkan, dan dilestarikan secara efektif untuk mendukung investigasi insiden keamanan yang mungkin terjadi dalam sistem SPBE. Dengan kesiapan forensik, pemerintah dapat merespons insiden dengan cepat, mengurangi dampak negatif terhadap layanan publik, dan memastikan integritas data serta sistem elektronik tetap terjaga. Hal ini juga penting dalam memenuhi standar keamanan yang diatur oleh regulasi nasional, seperti Peraturan Presiden No. 95 Tahun 2018 tentang SPBE.

Selain itu, DFR memperkuat kepercayaan publik terhadap sistem elektronik pemerintah. Ketika insiden keamanan dapat ditangani secara profesional dan transparan, masyarakat akan merasa lebih yakin bahwa data pribadi mereka aman dalam sistem SPBE. DFR juga mendukung transparansi dan akuntabilitas dalam pengelolaan data pemerintah, terutama dalam menghadapi audit atau perselisihan hukum. Dengan memanfaatkan kerangka kerja DFR, pemerintah dapat memastikan bahwa sistem SPBE tidak hanya berfungsi sebagai alat pelayanan publik, tetapi juga sebagai *model* tata kelola data yang baik dan aman. Dalam jangka panjang, kesiapan forensik *Digital* menjadi bagian integral dari strategi pengelolaan risiko dalam SPBE, membantu pemerintah menjaga keberlanjutan layanan elektronik sekaligus mematuhi regulasi keamanan informasi.

2.8 Pentingnya DFR terhadap ISMS

Digital Forensic Readiness (DFR) merupakan komponen integral dari *Information Security Management System* (ISMS) yang tidak hanya memastikan kesiapan organisasi untuk menghadapi insiden keamanan secara reaktif, tetapi juga secara proaktif dengan mengumpulkan bukti *Digital* yang sah tanpa mengganggu proses bisnis organisasi. Dengan mengintegrasikan DFR ke dalam ISMS, organisasi dapat memperkuat kebijakan, prosedur, dan kontrol keamanan yang ada, serta memastikan bahwa setiap insiden dapat diinvestigasi

dengan efektif sambil mematuhi regulasi hukum. Keterkaitan antara DFR dan ISMS berada pada area irisan *(overlaping)* yang didalamnya mencakup perencanaan, kesiapan infrastruktur, kontrol keamanan, kesiapan insiden serta penilaian dan evaluasi ISMS, sebagaimana disajikan pada gambar berikut.



Gambar 2.8 *The overlapping scopes between IS security and Forensics* (Pangalos, G., Ilioudis, C., et, al. 2010)

Memasukkan aspek kesiapan forensik *Digital* dalam arsitektur keamanan informasi memudahkan untuk menghubungkan sumber serangan dengan insiden dan memungkinkan manajemen untuk menilai kontrol keamanan yang ada sekaligus membuktikan apakah kontrol tersebut efisien dan efektif. Kesiapan forensik *Digital* (DFR) berfokus pada antisipasi insiden dan pemanfaatan bukti *Digital*, sementara keamanan informasi memastikan kelangsungan manfaat bisnis dari informasi tanpa memperhitungkan bukti *Digital* merupakan bagian yang utuh dan saling berhubungan (T. Grobler, et.al, 2007). Sebagai contoh, dalam kasus Kebijakan Retensi Rekaman Elektronik, pertimbangan kesiapan forensik menyarankan untuk memasukkan persyaratan keamanan tambahan yang meningkatkan keamanan informasi secara keseluruhan, seperti: "Rekaman yang disimpan harus dapat diakses", "Versi elektronik harus mewakili format asli secara akurat", "Meta-data seperti penulis dan tanggal harus disertakan dengan rekaman", dan sebagainya. Oleh karena itu, kesiapan forensik dapat dilihat sebagai komponen dari Best Practice ISMS.

2.9 *Systematic Literature Review*

Systematic Literature Review (SLR) adalah suatu metode penelitian yang terstruktur, sistematis, dan transparan untuk mengidentifikasi, memilih, dan melakukan penilaian kritis terhadap studi-studi yang relevan guna menjawab pertanyaan penelitian tertentu. Tidak seperti ulasan literatur tradisional yang cenderung bersifat naratif dan subjektif, SLR menggunakan kriteria yang telah ditetapkan sebelumnya untuk menentukan kelayakan suatu

studi, menilai kualitasnya, serta mensintesis temuannya untuk ditarik kesimpulan tertentu. Metode ini bertujuan untuk meminimalkan bias serta memberikan gambaran menyeluruh mengenai penelitian yang telah dilakukan pada topik tertentu. Dengan pendekatan yang sistematis, SLR memastikan bahwa proses peninjauan literatur dapat direplikasi dan hasil yang diperoleh memiliki tingkat keandalan yang tinggi (Kumar, 2020).

Menurut Kitchenham dan *Chart*ers (2007), SLR adalah "cara untuk mengevaluasi dan menginterpretasi semua penelitian yang tersedia yang relevan dengan pertanyaan penelitian tertentu, area topik, atau fenomena yang menarik". SLR bertujuan untuk memberikan ringkasan yang objektif dan tidak bias dari penelitian yang ada, mengidentifikasi kesenjangan dalam penelitian saat ini, dan memberikan latar belakang untuk penelitian baru (Petticrew & Roberts, 2006). Tujuan utama dari SLR adalah untuk menyediakan rangkuman yang mendalam dan komprehensif terhadap literatur yang relevan dengan pertanyaan penelitian. SLR merupakan alat yang penting bagi peneliti dan praktisi karena mampu memberikan pemahaman yang lebih mendalam tentang perkembangan penelitian pada suatu isu tertentu. Selain itu, SLR membantu mengidentifikasi kesenjangan penelitian, memberikan dasar bagi pengambilan keputusan berbasis bukti, serta menawarkan panduan bagi penelitian masa depan. Melalui sintesis temuan dari berbagai studi, SLR dapat menghasilkan kesimpulan berbasis bukti yang lebih kuat dibandingkan dengan studi individual, sehingga memperkuat validitas hasil penelitian secara keseluruhan (Snyder, 2019).

SLR banyak digunakan oleh para peneliti, profesional di bidang kesehatan, pembuat kebijakan, dan pendidik untuk mendukung praktik berbasis bukti dan pengambilan keputusan yang informasional. Misalnya, dalam sektor kesehatan, SLR sering digunakan untuk mengevaluasi efektivitas suatu intervensi, yang selanjutnya menjadi dasar pengembangan pedoman klinis dan keputusan kebijakan. Proses pelaksanaan SLR melibatkan beberapa tahapan utama, seperti merumuskan pertanyaan penelitian yang jelas, mengembangkan protokol, melakukan pencarian literatur secara menyeluruh, memilih studi yang relevan berdasarkan kriteria yang telah ditetapkan, mengekstraksi dan menganalisis data, serta menyajikan temuan secara sistematis dan tidak bias. Pendekatan yang ketat ini memastikan bahwa kesimpulan yang dihasilkan didasarkan pada penilaian yang menyeluruh dan objektif terhadap bukti yang tersedia (Tranfield et al., 2020).

Terdapat banyak pendekatan dalam melakukan SLR berdasarkan tujuan penelitian, metodologi, serta jumlah data yang akan dianalisa. Pendekatan-pendekatan ini dapat bersifat kualitatif, kuantitatif, atau menggunakan desain campuran tergantung pada fase kajian.

Berikut ini, tiga jenis utama metode yang umum digunakan akan dijelaskan, sebagaimana dirangkum dalam tabel berikut (Snyder, 2019).

Tabel 2.3. Pendekatan yang digunakan dalam SLR (Snyder, 2019).

Approach	Systematic	Semi-systematic	Integrative
Typical purpose	Synthesize and compare evidence	Overview research area and track development over time	Critique and synthesize
Research questions	Specific	Broad	Narrow or broad
Search strategy	Systematic	May or may not be systematic	Usually not systematic
Sample characteristics	Quantitative articles	Research articles	Research articles, books, and other published texts
Analysis and evaluation	Quantitative	Qualitative/quantitative	Qualitative
Examples of contribution	Evidence of effect Inform policy and practice	State of knowledge Themes in literature Historical overview Research agenda Theoretical model	Taxonomy or classification Theoretical model or framework

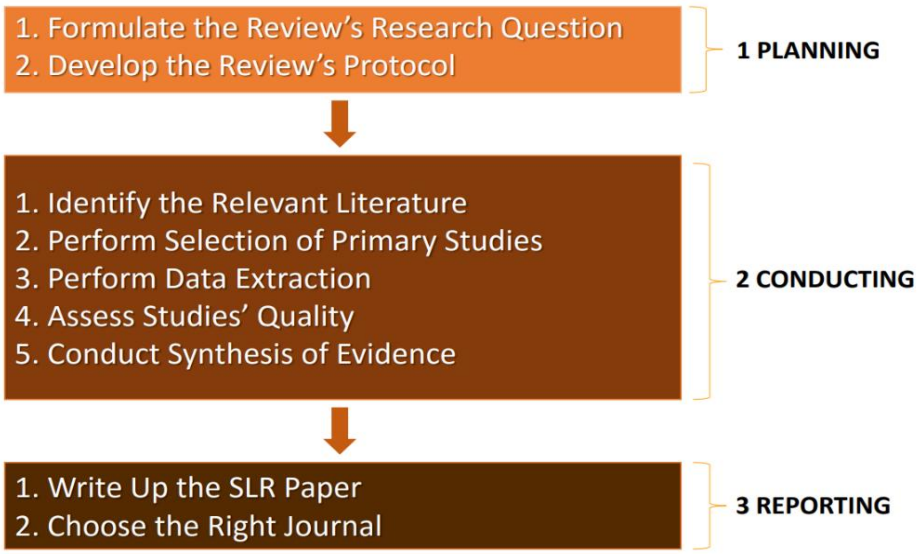
2.10 Tahapan *Systematic Literature Review*

Berdasarkan studi sebelumnya terhadap pendapat berbagai ahli yang mendefinisikan SLR, dapat disimpulkan bahwa *Systematic Literature Review* (SLR) merupakan metode penelitian yang terstruktur untuk mengidentifikasi, mengevaluasi, dan mensintesis literatur yang relevan dengan pertanyaan penelitian tertentu. Proses SLR terdiri dari beberapa tahapan yang harus dilalui secara sistematis. Menurut Okoli (2015), tahapan-tahapan tersebut meliputi:

1. Perencanaan *(Planning):* Tahap ini mencakup perumusan pertanyaan penelitian yang spesifik dan relevan, serta pengembangan protokol penelitian yang akan menjadi panduan dalam pelaksanaan SLR. Protokol ini berisi metode dan kriteria yang akan digunakan dalam proses *Review*.
2. Pelaksanaan *(Conducting):* Pada tahap ini, peneliti melakukan pencarian literatur secara komprehensif menggunakan database yang relevan, kemudian melakukan seleksi studi berdasarkan kriteria inklusi dan eksklusi yang telah ditetapkan. Selanjutnya, dilakukan penilaian kualitas studi dan ekstraksi data dari studi yang terpilih.

3. Pelaporan *(Reporting):* Tahap akhir ini melibatkan sintesis data yang telah diekstraksi dan penyusunan laporan hasil SLR. Laporan harus disusun secara transparan dan komprehensif, mencakup temuan utama, interpretasi, serta implikasi dari hasil *Review*.

Ketiga tahapan tersebut divisualisasikan kedalam gambar berikut



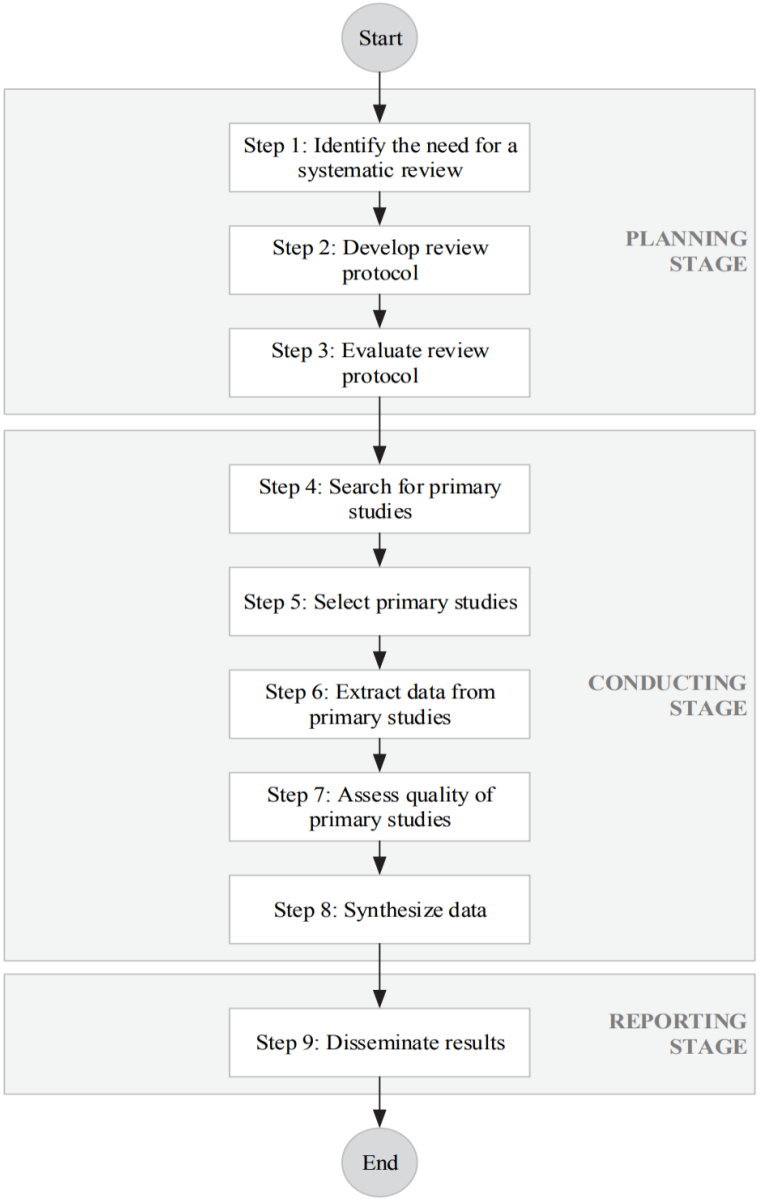
Gambar 2.9. Tahapan *Systematic Literature Review*

Berdasarkan gambar tahapan SLR diatas, Tahap pertama dalam proses SLR adalah *Plan*ning. Pada tahap ini, peneliti harus merumuskan pertanyaan penelitian secara spesifik untuk memberikan arah yang jelas pada kajian yang akan dilakukan. Setelah itu, peneliti harus mengembangkan protokol SLR, yaitu dokumen terstruktur yang mencakup metodologi pencarian, kriteria seleksi, serta langkah-langkah evaluasi studi. Protokol ini berfungsi sebagai panduan untuk memastikan bahwa proses SLR dilaksanakan secara konsisten dan bebas bias.

Tahap kedua adalah *Conducting*, yang mencakup lima langkah utama. Langkah pertama adalah mengidentifikasi literatur yang relevan melalui pencarian menyeluruh di berbagai database akademik. Setelah itu, peneliti melakukan seleksi studi primer berdasarkan kriteria inklusi dan eksklusi yang telah ditentukan sebelumnya. Langkah berikutnya adalah ekstraksi data dari studi yang terpilih, diikuti oleh penilaian kualitas studi untuk memastikan keandalan temuan. Tahap terakhir dalam fase ini adalah melakukan sintesis bukti, yang bertujuan untuk menggabungkan informasi dari berbagai studi menjadi kesimpulan yang bermakna dan informatif.

Tahap terakhir adalah *Reporting*, di mana hasil dari proses SLR disusun dalam bentuk laporan atau artikel ilmiah. Peneliti harus menuliskan temuan utama secara terstruktur dan transparan sehingga dapat dipahami dan direplikasi oleh peneliti lain. Selain itu, peneliti juga perlu memilih jurnal yang tepat untuk mempublikasikan hasil SLR agar dapat menjangkau audiens yang relevan. Dengan mengikuti tiga tahapan utama ini, proses SLR dapat memberikan kontribusi yang signifikan dalam memperkaya literatur dan membantu menjawab pertanyaan penelitian dengan bukti yang kuat.

Nmun dedikit berbeda dengan Okoli (2015), Wahono,R.S, et.all (2015) dan Kitchenham, *Chart*ers (2007), yang membuat tahapan SLR lebih sistematis seperti terlihat pada gambar berikut ini.



Gambar 2.10. Tahapan SLR (Kitchenham, et.all, 2009 & Wahono, 2015)

Berdasarkan gambar tahapan SLR diatas, tahapan ini akan memdefinisikan *Research Question* dengan lebih terstruktur/berurutan. Namun sebelum mendefinisikan *RQ*, terdapat tabel PICOC (*Population, Intervention, Comparison, Outcomes dan Context*) yang dapat membantu proses identifikasi sehingga pendefinisian RQ dapat tetap fokus dan konsisten terhadap beragam variabel yang dianalisa, Contoh penerapan PICOC dan RQ disajikan pada tabel dibawah ini.

Tabel 2.4. Contoh penerapan PICOC dan *Research Question* dalam penelitian SLR

Population	Software, software application, software system, information system
Intervention	Software defect prediction, fault prediction, error-prone, detection, classification, estimation, models, methods, techniques, datasets
Comparison	n/a
Outcomes	Prediction accuracy of software defect, successful defect prediction methods
Context	Studies in industry and academia, small and large data sets

ID	Research Question	Motivation
RQ1	Which journal is the most significant software defect prediction journal?	Identify the most significant journals in the software defect prediction field
RQ2	Who are the most active and influential researchers in the software defect prediction field?	Identify the most active and influential researchers who contributed so much on a research area of software defect prediction
RQ3	What kind of research topics are selected by researchers in the software defect prediction field?	Identify research topics and trends in software defect prediction
RQ4	What kind of datasets are the most used for software defect prediction?	Identify datasets commonly used in software fault prediction
RQ5	What kind of methods are used for software defect prediction?	Identify opportunities and trends for software defect prediction method
RQ6	What kind of methods are used most often for software defect prediction?	Identify the most used methods for software defect prediction
RQ7	Which method performs best when used for software defect prediction?	Identify the best method in software defect prediction
RQ8	What kind of method improvements are proposed for software defect prediction?	Identify the proposed method improvements for predicting the software defect
RQ9	What kind of frameworks are proposed for software defect prediction?	Identify the most used frameworks in software defect prediction

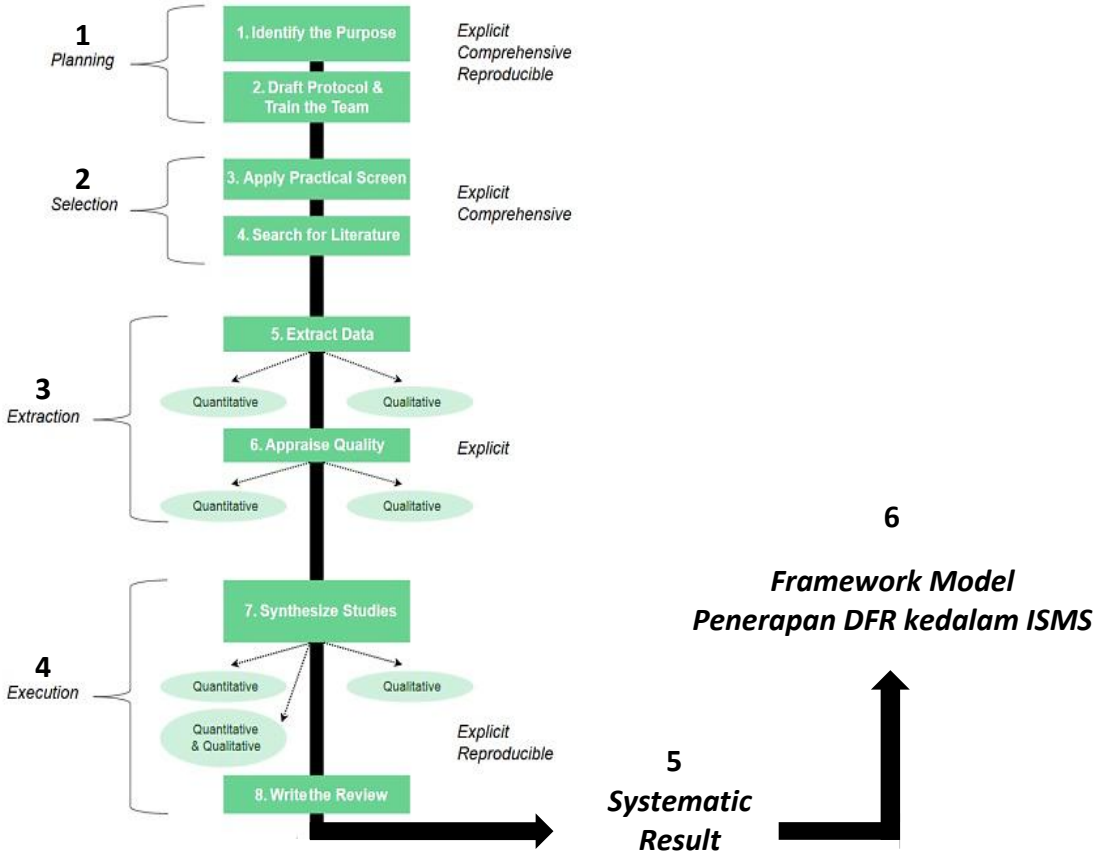
Dengan mengikuti tahapan-tahapan tersebut diatas, SLR dapat memberikan gambaran yang komprehensif dan objektif mengenai topik penelitian, serta membantu dalam pengambilan keputusan berbasis bukti. Penerapan SLR yang tepat juga dapat mengidentifikasi kesenjangan dalam literatur dan memberikan arah bagi penelitian selanjutnya.

BAB 3
Metodologi

Bab ini menjelaskan tentang metode-metode yang dilakukan pada penelitian sehingga diketahui dengan jelas dan terperinci tentang apa yang akan dilakukan, urutan langkah-langkah yang dibuat sistematis dan dapat dijadikan pedoman menyelesaikan penelitian ini. Peneliti membagi dua kategori metodologi yang dijabarkan pada bab ini, yaitu metodologi untuk melakukan *Review* dan analisis data tren penerapan *Digital Forensic Readiness* (DFR) dan *Information Security Management System* (ISMS) dengan menggunakan *Systematic Literature Review (SLR)*, dan metodologi untuk membuat *model Framework* yang dapat diterapkan pada organisasi pemerintahan.

3.1 Metodologi *Systematic Literature Review*

Berdasarkan judul dan latar belakang penelitian yang dijabarkan pada bab sebelumnya, untuk mendapatkan *Framework model* integrasi DFR terhadap ISMS yang akan diterapkan pada organisasi pemerintahan, penelitian ini menggunakan Metodologi *Systematic Literature Review* (SLR) sebagai landasan untuk menganalisa urgensi penerapan integrasi *Digital Forensic Readiness (DFR)* dan Sistem Manajemen Keamanan Informasi (SMKI) pada organisasi pemerintahan berdasarkan barbagai artikel penelitian yang sudah terpublikasi dan memiliki reputasi sesuai dengan *research area* yang relevan dengan tema penelitian. Sumber data pencarian artikel tersebut antara lain *database* Scopus *(sciencedirect)* sebagai sumber data primer, serta *Google Scholar*, dan repository terindeks Sinta sebagai sumber data sekunder yang sifatnya opsional atau tambahan. Untuk menjalankan SLR, perlu dilakukan beberapa tahapan *(fase)* agar menghasilkan output yang baik, pemrosesan data yang akurat, serta sintesis laporan SLR yang berkualitas. Tahapan tersebut antara lain dijabarkan pada gambar dan penjelasan berikut.



Gambar 3.1. Tahapan *Systematic Literature Review* (SLR) yang digunakan dalam penelitian

1. Tahap Perencanaan *(Planning)*

   Tahap ini dimulai dengan mengidentifikasi tujuan penelitian dan menyusun protokol penelitian. Tim peneliti perlu dilatih untuk memahami protokol yang telah disusun agar dapat melaksanakan penelitian dengan baik. Tahap ini harus dilakukan secara eksplisit, komprehensif dan dapat direproduksi. Pada proposal penelitian ini, peneliti menggunakan tiga poin utama dari tema yang diangkat yaitu "*Digital Forensic Readiness*", "ISMS", E-Gov" dan "SLR". Seperti dijabarkan pada bab awal, tujuan penelitian ini adalah untuk menganalisa urgensi implementasi DFR dan ISMS dalam organisasi pemerintahan dengan menggunakan metode SLR.

2. Tahap Seleksi *(Selection)*

   Pada tahap ini dilakukan penyaringan praktis terhadap literatur yang akan digunakan dalam penelitian. Pencarian literatur dilakukan secara sistematis menggunakan kriteria inklusi dan eksklusi yang telah ditentukan. Tahap ini juga harus dilakukan secara eksplisit dan komprehensif. Pada tahap ini dilakukan pencarian artikel sebagai data masukan (data sekunder) dalam proses SLR. Pencarian ini

dilakukan dengan cara mencari secara langsung pada data base sumber *(Scopus, ProQuest, IEEE Xplore, Open Journal)* dan melakukan pencarian dengan menggunakan *tools Publish or Perish* dengan mendefinisikan kata kunci target pencarian, sumber data, jenis artikel yang akan dicari, dan rentang waktu tahun pencarian tertentu (2018-2025). Terdapat beberapa kata kunci yang digunakan sebagai pencarian artikel awal berdasarkan data base sumber artikel ilmiah, seperti diantaranya: "*Digital Forensic*" OR "*Digital* investigation" AND "*cyber security*" OR "*cyber attack*" OR "ISMS" OR "*information security Management system*" OR "keamanan informasi" OR "SMKI" OR "sistem manajemen keamanan informasi" AND "*Government*" OR "governance" OR "*Management*" AND "SLR" OR "*systematic literature Review*" OR "*systematic literature*" OR "*systematic Review*".

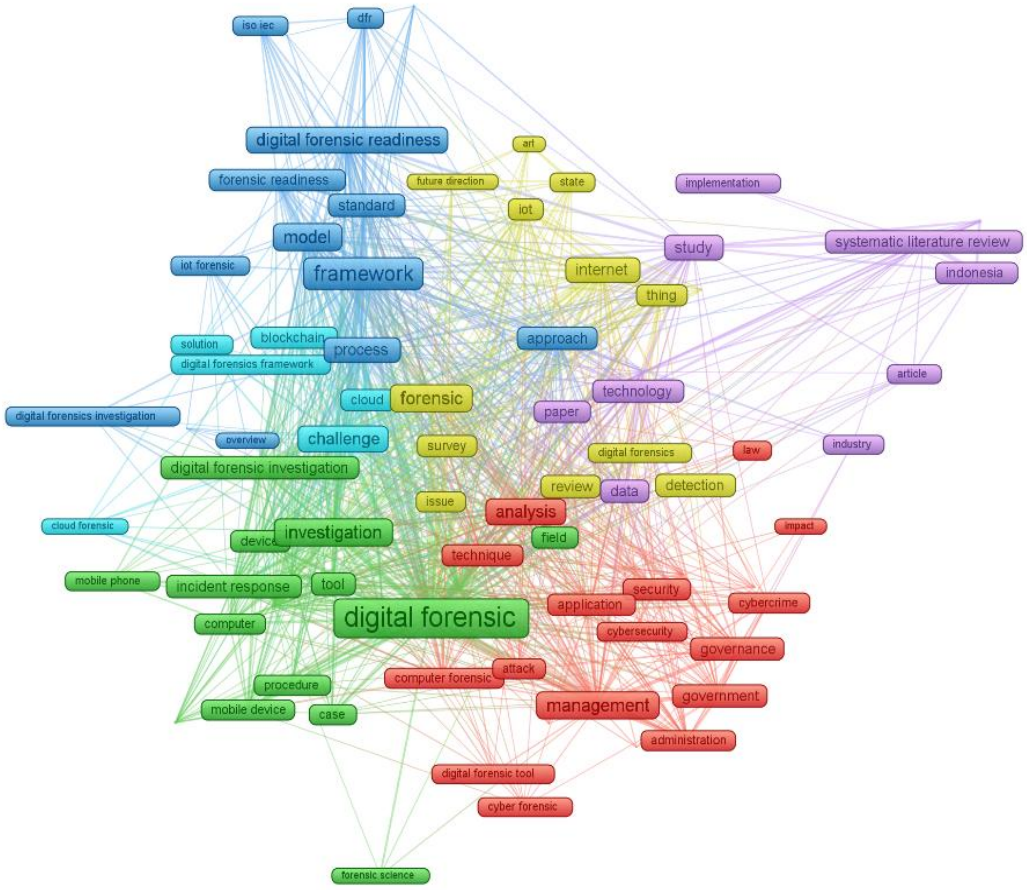
3. Tahap Ekstraksi *(Extraction)*

Tahap ekstraksi melibatkan pengambilan data baik kuantitatif maupun kualitatif dari literatur yang telah diseleksi. Dalam tahap ini juga dilakukan penilaian kualitas data yang diekstrak untuk memastikan validitas dan reliabilitasnya. Proses ini harus dilakukan secara eksplisit. Proses ini dilakukan dengan menganalisis data pencarian ke dalam *reference manager* (Mendeley atau Zotero, peneliti menggunakan *Mendeley Desktop* dan *Web Importer*) sehingga didapatkan metadata setiap artikel yang dicari dan diunduh. Ekstraksi terhadap metadata artikel setidaknya bertujuan untuk mengambil data penulis *(Author)*, judul artikel, tahun penelitian, lokasi penelitian, *url* artikel (DOI atau *full url* jurnal terpublikasi), nama jurnal/konferensi/prosiding, *volume*/edisi cetakan publikasi, institusi tempat penulis bekerja, kategori bidang ilmu/area penelitian, kata kunci yang digunakan, abstrak, tujuan penelitian, pendekatan metodologi yang digunakan, temuan penelitian, hasil daan/atau kesimpulan penelitian, serta daftar referensi dan sitasi penelitian.

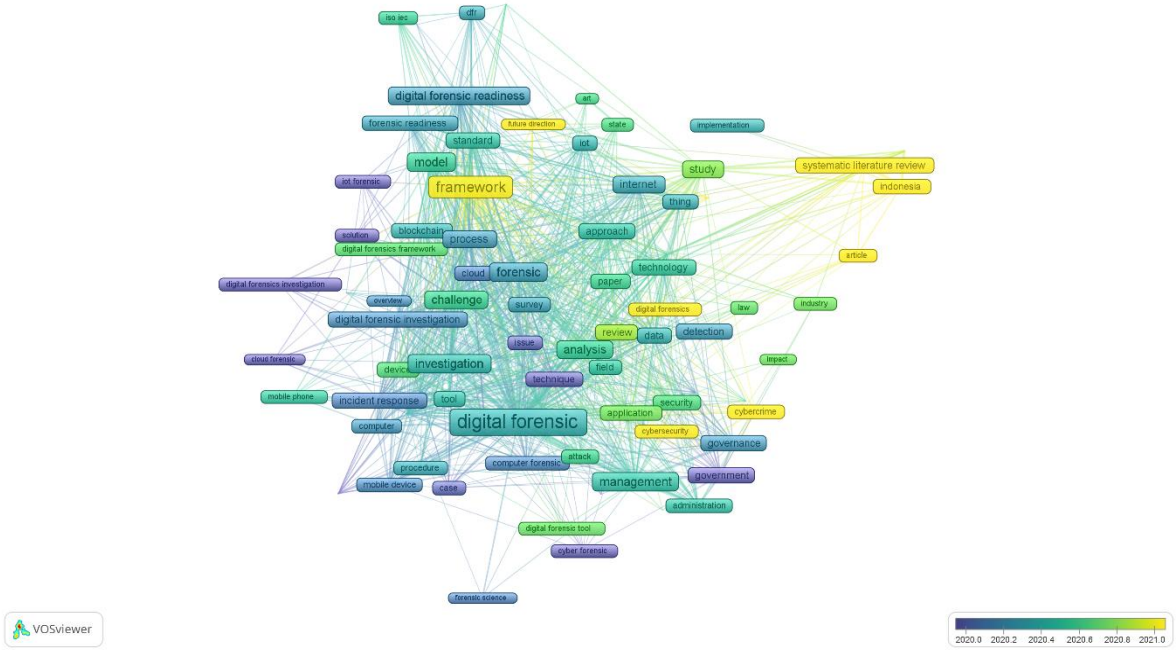
Pada tahap ini dilakukan juga proses *filtering and refining* kata kunci dan beberapa variabel lainnya yang dianggap perlu untuk dilakukan perbaikan, validasi, seleksi dan kasterisasi/pengelompokan. Filtrasi, seleksi dan klasterisasi akan berpengaruh pada efektifitas dan akurasi analisa pada tahap SLR. Penulis menggunakan *tool Openrefine* untuk memproses data filtrasi dan *clearance* beragam variabel penelitian sehingga didapatkan tabel bibliografi yang baik dan berkualitas.

Pada tahap ini juga dilakukan proses konversi data bibliografi yang sudah terfilter dan terklaster/terkelompokkan pada tahapan sebelumnya untuk diubah menjadi visualisasi kata kunci berdasarkan *volume, density/Threshold*, serta

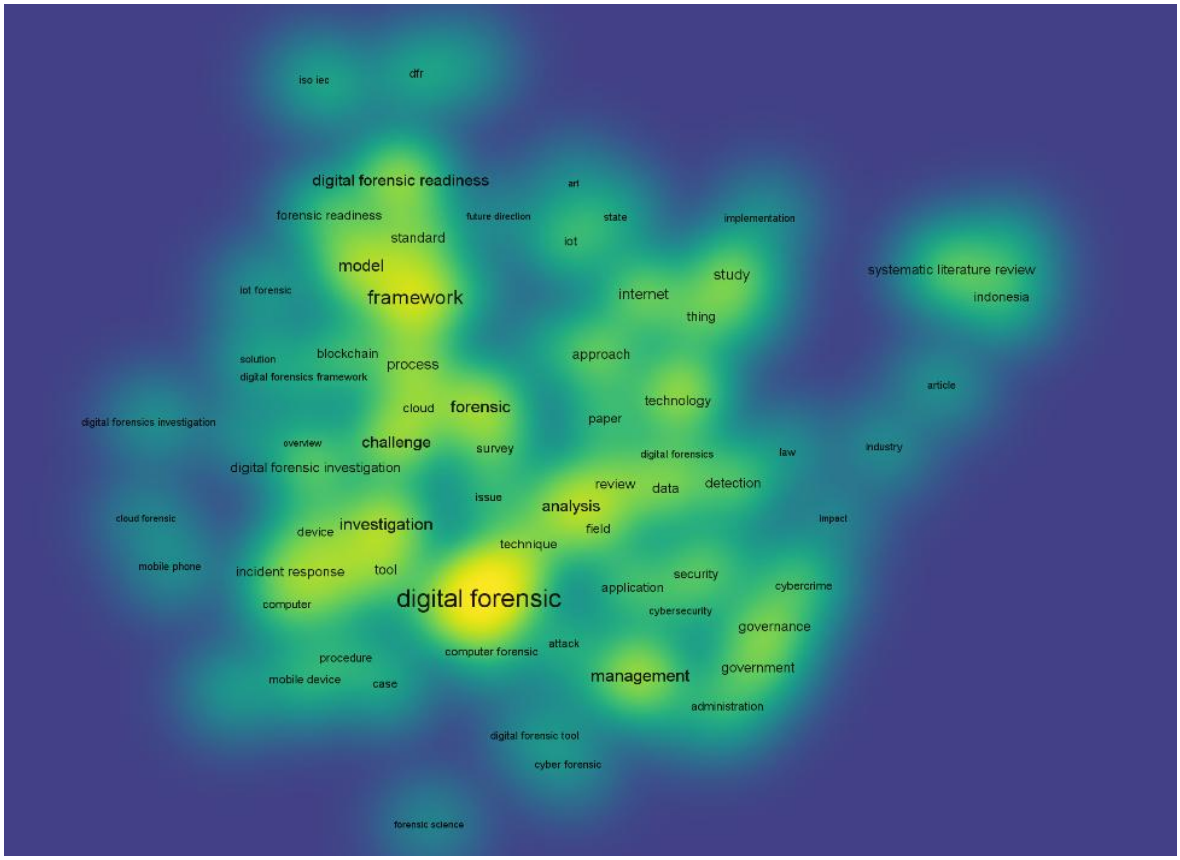
interconnected key word yang berhasil dijaring. Tahap ini sangat penting untuk mengetahui posisi penelitian kita apakah memiliki *tren* dan *novelty* yang layak diangkat dalam penelitian. Para proposal kali ini, peneliti menyajikan tiga buah gambar yang merupakan hasil pencarian artikel, ekstraksi metadata, dan filtrasi kata kunci dari sekitar 300+ artikel dari sumber *Scopus* dan *Google Scholar* dengan kata kunci seperti yang dijabarkan pada tahap satu diatas yang disajikan dalam beberapa gambar berikut.



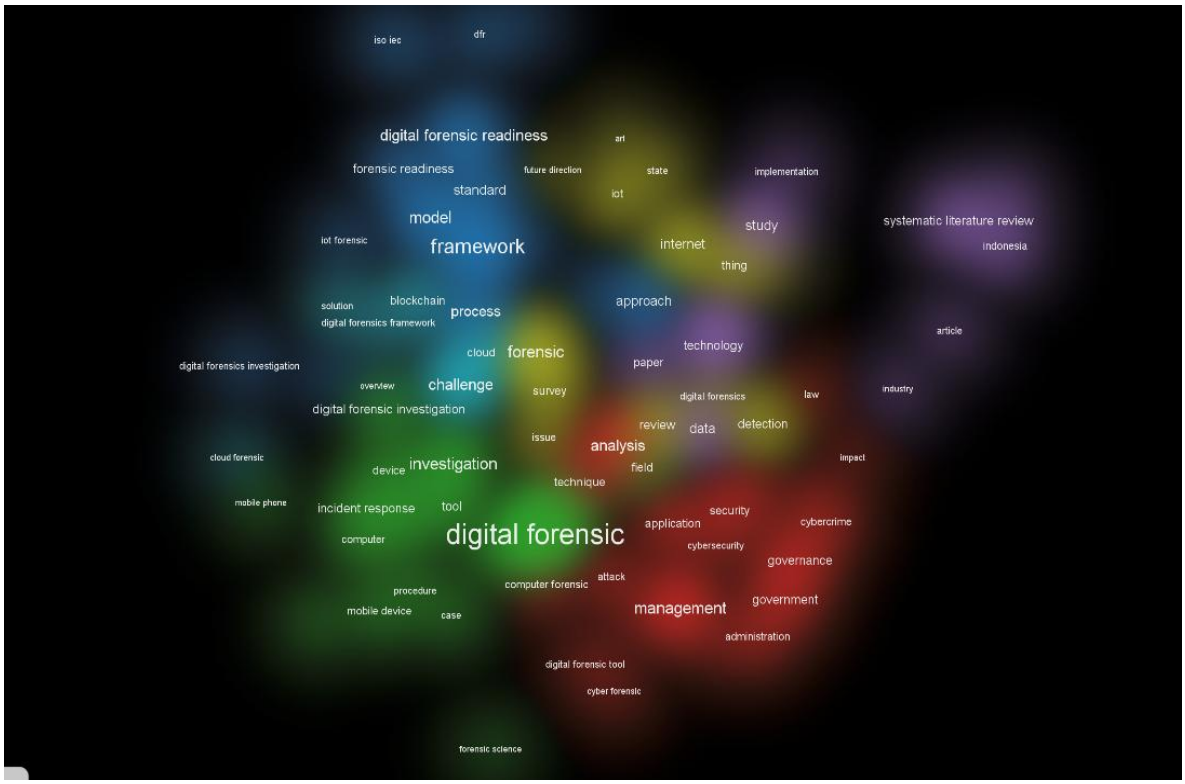
Gambar 3.2. Network Visualisasi kata kunci artikel penelitian berdasarkan interkoneksi antar cluster kata kunci dengan menggunakan VOS *Viewer*



Gambar 3.3.Overlay Visualisasi kata kunci artikel penelitian berdasarkan tahun penelitian dengan menggunakan VOS *Viewer*



Gambar 3.4.Density Visualisasi kata kunci artikel penelitian berdasarkan *Threshold* penggunaan kata kunci dengan menggunakan VOS *Viewer*



Gambar 3.5.Density Visualisasi kata kunci artikel penelitian berdasarkan Cluster *Threshold* penggunaan kata kunci dengan menggunakan VOS *Viewer*

4. Tahap Eksekusi *(Execution)*

   Tahap ini merupakan tahapan dimana analisis dan sintesis studi yang menggabungkan hasil analisis kuantitatif maupun kualitatif dari data yang telah diekstrak disimpulkan. Hasil sintesis ini kemudian ditulis kedalam bentuk dokumen *Review* yang sistematis dan dapat digunakan sebagai informasi ataupun pengambilan keputusan pada tahap selanjutnya (pe*model*an *Framework*).

5. Tahap Pelaporan

   Tahap terakhir dari proses SLR adalah melakukan pelaporan, penyajian dokumen hasil proses SLR secara keseluruhan yang disajikan dengan menggunakan data tabel, data visual, ataupun penjelasan simpulan yang menjadi hasil pemroesan SLR yand dihasilkan. Selain berfungsi sebagai simpulan, tahap ini juga berfungsi sebagai penentuan keputusan yang sesuai dengan tujuan penelitian. Selain itu, pada penelitian ini, hasil SLR juga berfungsi sebagai klaim, validasi sekaligus landasan dalam pengembangan *Framework model* integrasi DFR kedalam ISMS pada organisasi pemerintahan.

6. Pengembangan *Framework Model*

   Tahap terakhir ini merupakan tahap pembuatan *model Framework* yang sesuai untuk menerapkan DFR kedalam ISMS pada ruang lingkup organisasi pemerintahan.

Agar lebih terperinci, terstruktur dan mampu menjawab rumusan permasalahan yang diangkat pada penelititian ini, maka sebelum memulai proses SLR, perlu dilakukan pemetaan atau pendefinisian pertanyaan penelitian atau *Research Question* (RQ) berdasarkan rumusan permasalahan yang diangkat dalam penelitian agar tahapan analisa yang dilakukan pada proses SLR berikutnya dapat terstruktur, terukur, spesifik dan mampu menunjukkan arah penelitian. RQ ini berupa rangkaian pertanyaan yang akan dijawab dalam penelitian melalui metode SLR diterapkan. Berikut ini tabel pemetaan rumusan masalah dan pertanyaan penelitian yang menjadi dasar proses penelusuran dan analisis SLR.

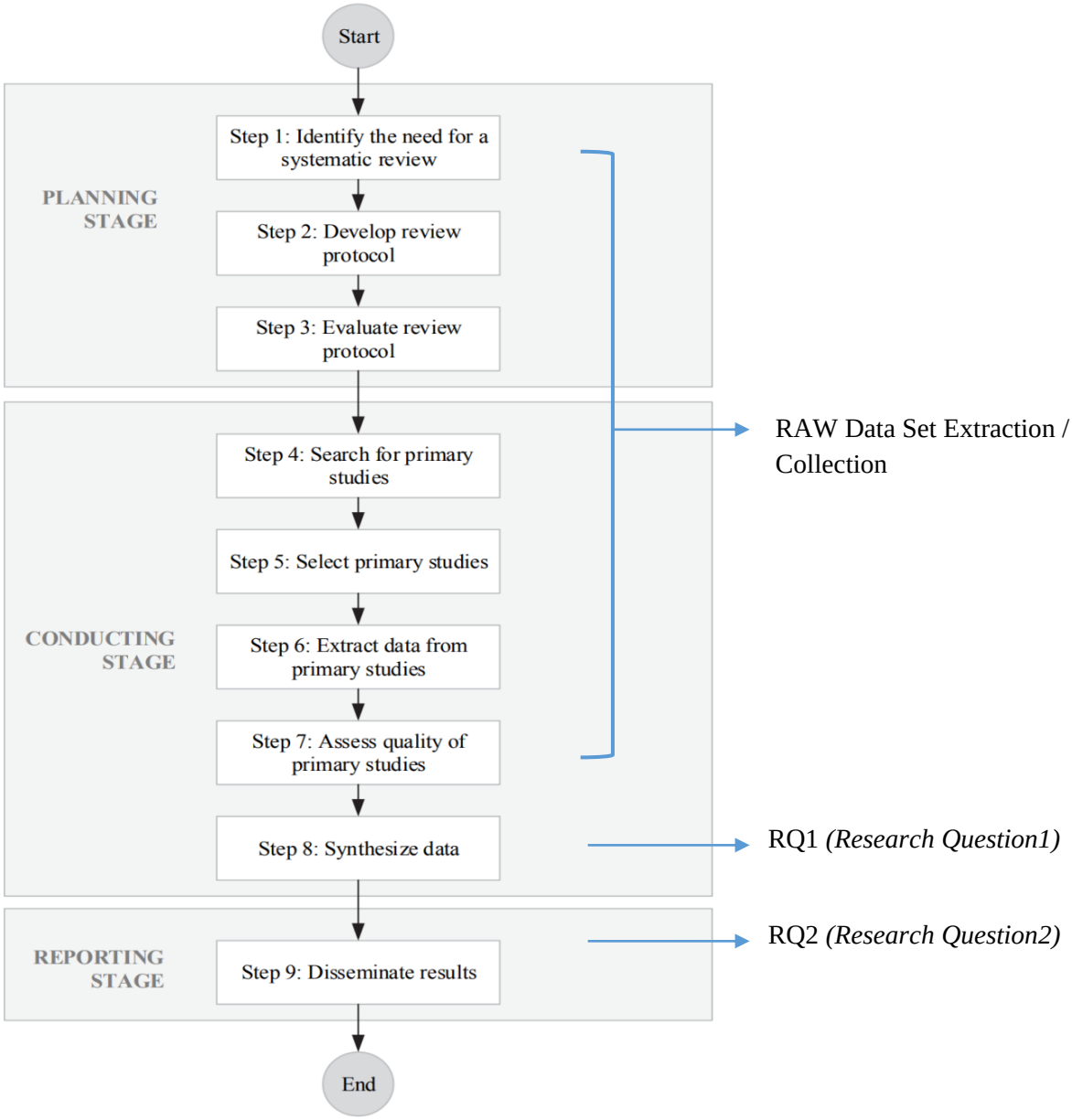
Tabel 3.1. Pemetaan pertanyaan penelitian (Q) berdasarkan rumusan masalah penelitian

Rumusan Masalah (RM)	**Pertanyaan Penelitian (RQ)**	**Analisis Kesesuaian antara RM-RQ**
RM1. Bagaimana penerapan DFR dan ISMS secara bersamaan di organisasi pemerintahan?	RQ1. Bagaimana penerapan integrasi *Digital Forensic Readiness* (DFR) dan *Information Security Management System* (ISMS) ISO 27001 secara bersamaan di organisasi pemerintahan, baik di Indonesia maupun di luar negeri, berdasarkan data yang diperoleh dari artikel jurnal yang dipublikasikan antara 2018-2025 ?	RQ1 secara langsung menjawab RM1, karena RQ1 berfokus pada penerapan integrasi DFR dan ISMS di organisasi pemerintahan dengan batasan geografis (Indonesia dan internasional) serta batasan waktu (2018-2025). RQ1 lebih terfokus dan spesifik dalam hal pencarian literatur yang relevan mengenai penerapan kedua sistem tersebut dalam organisasi pemerintahan. Pernyataan RQ1 ini sejalan dengan penelitian berjudul "*Digital Forensic Readiness in Organizations: Issues and*

		Challenges" (Karie & Karume, 2017)yang menyatakan tantangan yang dihadapi oleh organisasi adalah kurangnya rencana dan kebijakan kesiapan forensik, proses pengumpulan bukti digital yang sah kurang efektif, keterbatasan personel yang terampil dan berpengetahuan, investasi teknologi yang tinggi, serta aspek penegakan hukum yang dinamis berdasarkan yurisdiksi suatu negara.
RM2. Apa dampak penerapan DFR dan ISMS di organisasi pemerintahan?	RQ2. Apa dampak penerapan integrasi DFR dan ISMS secara bersamaan di organisasi pemerintahan, baik di Indonesia maupun di luar negeri, berdasarkan analisis literatur yang tersedia antara 2018-2025?	RQ2 sinkron dan sangat relevan dengan RM2 karena keduanya bertujuan untuk menganalisis dampak yang ditimbulkan dalam penerapan DFR dan ISMS pada organisasi pemerintahan dalam konteks yang lebih luas (Indonesia dan internasional). Rumusan RQ ini sejalan dengan penelitian "Tinjauan Pustaka Sistematis: Tantangan Dan Faktor-Faktor Pengembangan Kesiapan Forensik Digital" (Rochmadi, et.al, 2024) dimana penelitian tersebut melandasi dan melanjutkan penelitian yang dijelaskan RQ2.

RM3. Bagaimana merancang *Framework* integrasi DFR dan ISMS di organisasi pemerintahan?	RQ3. Bagaimana merancang *Framework Model* Integrasi *Digital Forensic Readiness* (DFR) ke dalam ISMS ISO 27001 bagi organisasi pemerintahan, berdasarkan hasil analisis literatur yang ada?	RQ3 dengan jelas mengarah pada perancangan *Framework model* integrasi DFR dan ISMS dalam organisasi pemerintahan yang juga merupakan fokus dari RM3. RQ3 terstruktur dan terfokus pada kerangka teoretis atau *Framework model* yang dapat diterapkan pada DFR dan ISMS. RQ3 akan mencari literatur yang relevan untuk membangun *Framework model* integrasi keduanya. Perumusan RQ3 ini sejalan dengan beberapa penelitian yang mengajukan model framework DFR baru untuk kebutuhan ataupun situasi tertentu, seperti contohnya penelitian Collie, M. (2018) "*A Strategic Model for Forensic Readiness*" yang menjabarkan framework model berdasarkan aspek strategis.

Setelah pendefinisian pertanyaan penelitian atau *Research Question* (RQ) berdasarkan rumusan permasalahan yang terdapat pada tabel diatas, langkah selanjutnya adalah inisiasi tahapan SLR berdasarkan protokol PRISMA. Beberapa tahapan SLR harus dapat menjawab beberapa atau keseluruhan poin RQ. Maka dari itu peneliti membuat visualisasi tahapan SLR yang memiliki luaran untuk menjawab RQ, seperti terlihat pada gambar berikut ini.



Gambar 3.6. Tahapan SLR untuk menjawab *Research Question* (RQ)

Pada diagram diatas, tahap 1 sampai 7 SLR merupakan proses pencarian dan analisis artikel berdasarkan PRISMA sehingga didapatkan RAW Data yang akan dijadikan bahan untuk menjawab RQ1, yaitu antara lain berupa:

1. Data artikel hasil pencarian berdasarkan kata kunci
2. Meta data artikel setelah proses filtering berdasarkan PRISMA, antara lain: judul artikel, *Author*, nama jurnal, tahun publikasi, doi, url paper, lokasi peneltian
3. Data ekstraksi isi artikel, antara lain : abstrak, masalah yang diangkat dalam penelitian, *research Question*, metode penelitian, teori yang digunakan,

pendekatan penelitian (kualitatif/kuantitatif), *Framework*, temuan penelitian, kesimpulan penelitian, dan usulan penelitian.

Untuk mendapatkan Raw Data tersebut, penentuan PICOC yang relevan untuk memulai tahapan pemrosesan SLR berdasarkan PRISMA perlu didefinisikan dengan baik, seperti tersaji pada tabel berikut ini.

Tabel 3.2. PICOC pada penelitian urgensi integrasi DFR kedalam ISMS

Item PICOC	Aktualisasi PICOC dalam Penelitian
Population	Organisasi pemerintahan dalam dan luar negeri, menerapkan IT Governance, memiliki IT Asset
Intervention	*Digital Forensic*, *Incident Response*, SMKI, ISMS, ISO 27001, Indeks Keamanan Informasi
Comparison	Organisasi non pemerintahan, organisasi tanpa penerapan IT Governance, organisasi tanpa pengelolaan IT Asset
Outcomes	Penguatan keamanan data, Peningkatan respon insiden, Kepatuhan terhadap regulasi, Efisiensi operasional, Pengurangan biaya dan waktu yang diperlukan untuk investigasi forensik *Digital*
Context	Organisasi Pemerintahan di Era Transformasi *Digital* yang memiliki tantangan pengelolaan keamanan data dan informasi

3.1.1. Identifikasi Kebutuhan SLR

Langkah pertama dalam *Systematic Literature Review* (SLR) adalah mengidentifikasi kebutuhan untuk melakukan tinjauan sistematis. Langkah ini mencakup proses awal untuk menentukan relevansi dan tujuan utama dari penelitian. Menurut Kitchenham et al. (2009), identifikasi kebutuhan ini penting untuk memastikan bahwa tinjauan sistematis dapat memberikan kontribusi yang signifikan terhadap pengembangan ilmu pengetahuan, dengan menjawab pertanyaan penelitian yang belum terjawab sebelumnya. Dalam tahapan ini, peneliti harus mengevaluasi literatur yang sudah ada untuk mengidentifikasi kesenjangan penelitian atau area yang memerlukan eksplorasi lebih lanjut. Sebagai contoh, dalam konteks rekayasa perangkat lunak, Wahono (2015) menekankan pentingnya mengidentifikasi tren penelitian, metode, dan dataset yang relevan untuk

memastikan bahwa studi yang diusulkan memiliki dasar yang kuat dalam literatur yang sudah ada.

Proses identifikasi ini melibatkan berbagai aktivitas, seperti eksplorasi literatur awal untuk memahami konteks penelitian, diskusi dengan ahli di bidang terkait, dan analisis kebutuhan praktis di industri atau bidang akademik. Pada tahap ini, peneliti juga harus merumuskan tujuan penelitian yang spesifik, relevan, dan dapat dicapai. Tujuan ini harus mencerminkan kontribusi yang diharapkan dari SLR, baik dalam menjawab pertanyaan teoretis maupun memberikan solusi praktis. Dengan identifikasi yang jelas, langkah selanjutnya dalam SLR dapat dilakukan secara sistematis dan terarah, sehingga menghasilkan hasil yang valid dan dapat dipercaya (Kitchenham et al., 2009; Wahono, 2015).

Tahap identifikasi SLR pada penelitian ini adalah aktivitas eksplorasi terhadap topik penelitian, penentuan pertanyaan penelitian *(Research Questions),* dataset pencarian penelitian termasuk parameter untuk pencarian literatur dan kriteria seleksi studi primer poin penting yang akan menjadi dasar untuk mengembangkan protokol SLR ditahap berikutnya. Output ini berfungsi sebagai panduan yang memastikan bahwa langkah-langkah selanjutnya dalam SLR dilakukan dengan fokus dan tujuan yang jelassebagai dasar. Secara sistematis, implementasi tahap ini dalam penelitian ini tersaji pada tabel berikut ini.

Tabel 3.3. Identifikasi Kebutuhan SLR dalam Penelitian

Item Identifikasi	**Penjelasan**
Topik Penelitian	Pe*model*an Integrasi *Framework Digital Forensic Readiness* kedalam Sistem Manajeman Keamanan Informasi pada Sistem Pemerintahan Berbasis elektronik
Poin utama landasan SLR	Analisa penerapan *Digital Forensic Readiness* kedalam Sistem Manajeman Keamanan Informasi di organisasi
PICOC	Terdefinisi pada tabel 3.2
Research Question	Terdefinisi pada tabel 3.4
Articel Databases	Scopus (primer), Google Scholar (opsional tambahan)
Key word pencarian	"*Digital Forensic*" OR "*Digital* investigation" OR "computer *Forensic*" OR "*Incident response*" OR "mobile *Forensic*" OR "IT *Forensic*" OR "memory *Forensic*" OR "live *Forensic*" OR "network *Forensic*" OR "Video

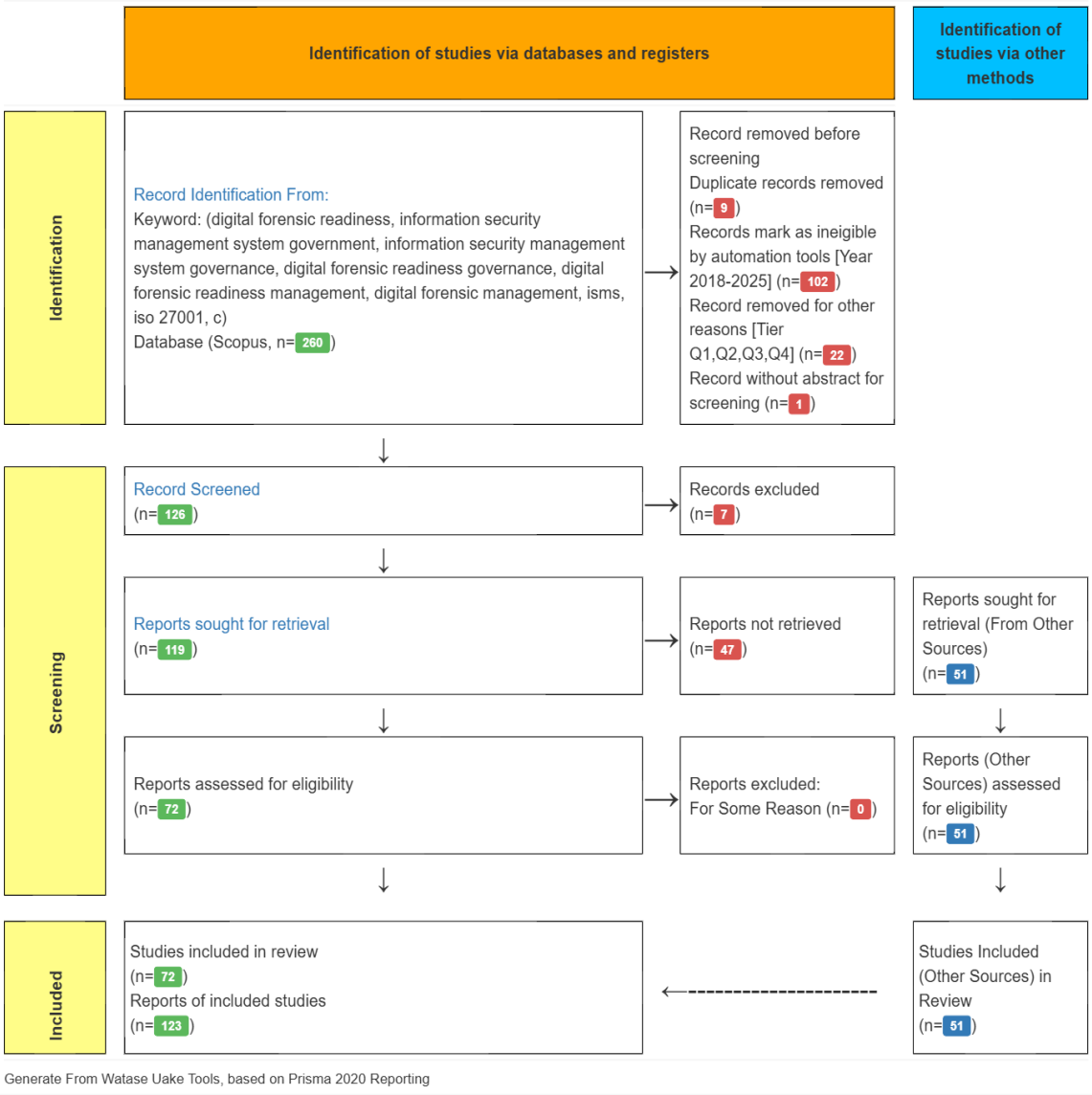
	Forensic" OR "file *Forensic*" OR "file *Forensic*" OR "*Digital Forensic Framework*" OR "IT *Forensic Framework*" AND "*Cyber Security*" OR "ISMS" OR "ISO 27000" OR "*Incident response*" OR "*Incident respond*" AND "governance" OR "*Government*" OR "*Management*"
Year	2018-2024
Tier	Q1, Q2, Q3, Q4, Sinta1, Sinta2, Sinta3, Sinta4, Sinta5, Sinta6

Tabel 3.4. Identifikasi *Research Question* dalam Penelitian SLR

ID	Pertanyaan Penelitian	Keterangan/Motivativasi RQ
RQ1	Bagaimana penerapan integrasi *Digital Forensic Readiness* (DFR) dan *Information Security Management System* (ISMS) ISO 27001 secara bersamaan di organisasi pemerintahan, baik di Indonesia maupun di luar negeri, berdasarkan data yang diperoleh dari artikel jurnal yang dipublikasikan antara 2018-2025 ?	Mengidentifikasi, mendefinisikan dan memahami penerapan integrasi DFR dan ISMS di berbagai organisasi pemerintahan secara global dan terkini.
RQ2	Apa dampak penerapan integrasi DFR dan ISMS secara bersamaan di organisasi pemerintahan, baik di Indonesia maupun di luar negeri, berdasarkan analisis literatur yang tersedia antara 2018-2025?	Mengidentifikasi, mendefinisikan dan memahami urgensi serta dampak integrasi ini dalam konteks pemerintahan baik di Indonesia maupun di luar negeri
RQ3	RQ1. Bagaimana merancang *Framework Model* Integrasi *Digital Forensic Readiness* (DFR) ke dalam ISMS ISO 27001 bagi organisasi pemerintahan, berdasarkan hasil analisis literatur yang ada?	Mengidentifikasi, mendefinisikan dan merancang *model* praktis yang dapat diimplementasikan oleh organisasi pemerintahan dalam mengintegrasikan DFR ke dalam ISMS ISO 27001

Pendefinisian RQ dan PICOC seperti dijelaskan pada dalam diatas, tahap *planning* SLR sebagaimana dijelaskan dalam artikel Kitchenham et al. (2009), adalah salah satu langkah yang fundamental dan sangat penting dalam menyiapkan protokol SLR. Peneliti menggunakan *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA) sebagai kerangka kerja untuk menjaga sekaligus meningkatkan transparansi dan kualitas luaran SLR. PRISMA menyediakan panduan sistematis dalam melaporkan setiap tahapan tinjauan, mulai dari perencanaan, pemilihan studi, ekstraksi data, hingga sintesis hasil. Salah satu komponen utama PRISMA adalah diagram alur yang menjelaskan proses penyaringan literatur, termasuk jumlah literatur yang diidentifikasi, dievaluasi, dan dikeluarkan pada setiap tahap berdasarkan kriteria inklusi dan eksklusi. PRISMA membantu memastikan bahwa SLR dilakukan secara transparan dan dapat direproduksi, sehingga memberikan kejelasan kepada pembaca tentang metodologi yang digunakan dan bagaimana hasil akhir diperoleh.

Terdapat beberapa *Framework* lain yang dapat digunakan sebagai alternatif PRISMA seperti beberapa diantaranya yang cukup dikenal secara global yaitu SPAR-4 SLR *Framework* dan Roses *Framework*. Beberapa *Framework* ini memiliki karakteristik, kelebihan dan kekurangan masing-masing, namun menghasilkan luaran SLR yang setara dengan PRISMA. Pada penelitian ini, peneliti menggunakan PRISMA *Framework* seperti terlihat pada gambar berikut ini.



Gambar 3.7. PRISMA protokol analisis Integrasi DFR kedalam ISMS SLR

Berdasarkan gambar PRISMA diatas, peneliti melakukan pencarian dengan kata kunci seperti terdefinisi pada tabel 3.3 pada sub bab sebelumnya dengan sumber data dari Scopus, didapatkan 260 artikel. Kemudian dilakukan *screening* atau filter hasil pencarian beberapa kriteria, antara lain pengecekan duplikasi menghasilkan 9 temuan, pengecekan selain tahun publikasi 2018-2025 menghasilkan 102 temuan, pengecualian terhadap kualitas Q1-Q4 menghasilkan 22 temuan, serta pengecekan tanpa abstrak menghasilkan 1 temuan. Total temuan dari proses *screening* adalah 134 artikel. Hasil artikel pencarian yang melalui proses *screening* adalah 128 artikel. Pada tahap selanjutnya, artikel yang telah dilakukan *screening*, masih dilakukan filtering artikel berdasarkan tiga kategori yaitu *exclude* filtering, artikel tidak dapat diakses, serta alasan lainnya yang membuat artikel tidak dapat dimasukkan kedalam proses SLR berikutnya.

Penelitian ini memasukkan parameter *Exclude* filtering berdasarkan beberapa kata kunci yang kurang relevan terhadap topik penelitian, seperti terdapatnya kata kunci tertentu baik yang terdapat di judul, abstrak, maupun isi artikel yang diperoleh. Tabel 3.7 dan Tabel 3.8 pada sub bab berikutnya mendefinisikan contoh beberapa kata kunci yang termasuk dalam *include & exclude configuration* pada proses SLR artikel yang kami teliti.

3.1.2. Evaluasi dan *Review* Protokol SLR

Tahap Evaluasi dan *Review* Protokol dalam *Systematic Literature Review* (SLR) adalah langkah penting untuk memastikan protokol penelitian yang dirancang mampu mendukung proses pengumpulan dan analisis data secara valid dan dapat diandalkan. Dalam konteks penelitian yang berfokus pada implementasi *Digital Forensic Readiness* (DFR) dan *Information Security Management System*s (ISMS) pada organisasi pemerintahan, evaluasi protokol mencakup penilaian terhadap kejelasan tujuan penelitian, relevansi pertanyaan penelitian, serta kelengkapan metodologi yang digunakan. Protokol harus dirancang untuk mencakup kerangka kerja yang relevan, seperti standar ISO/IEC 27043 untuk kesiapan forensik *Digital* dan ISO/IEC 27001 untuk sistem manajemen keamanan informasi, guna memastikan bahwa literatur yang dipilih dapat memberikan wawasan yang tepat tentang kesiapan forensik dan keamanan informasi di sektor pemerintahan.

Tahap ini juga melibatkan *Review* terhadap kriteria inklusi dan eksklusi literatur untuk memastikan hanya penelitian yang relevan dengan topik yang dianalisis. Misalnya, dalam topik implementasi DFR dan ISMS pada organisasi pemerintahan, literatur yang difokuskan adalah yang membahas implementasi standar, tantangan khusus dalam sektor pemerintahan, dan interaksi antara strategi forensik *Digital* dengan kebijakan keamanan informasi. Tim peneliti dapat melibatkan ahli di bidang DFR dan ISMS untuk memberikan masukan guna memastikan protokol ini sesuai dengan standar metodologis dan kebutuhan penelitian. Protokol yang telah di*Review* memungkinkan peneliti untuk melaksanakan SLR secara transparan, konsisten, dan sistematis, menghasilkan temuan yang dapat mendukung organisasi pemerintahan dalam meningkatkan kesiapan mereka terhadap insiden keamanan *Digital*. Untuk menunjang proses SLR pada tahap ini, peneliti mendefinisikan beragam kata kunci yang tersaji pada tabel berikut ini.

Tabel 3.5. Tabel *Exclude keywords* pada PRISMA SLR

Kategori	***Exclude Key Words***
Health	*Public Health, Healthcare Technology, Mental Health, Chronic Diseases, Telemedicine, Preventive Medicine, Health Policy, Vaccination Programs, Patient Safety, Epidemiology, Health Informatics, Nutrition and Dietetics, Physical Activity, Health Equity, Global Health, Personalized Medicine, Medical Devices, Clinical Trials, Health Literacy, Disease Surveillance*
Power Plant	*Renewable Energy, Nuclear Power, Thermal Power Plants, Hydroelectric Power, Power Generation Efficiency, Carbon Emissions, Smart Grid Technology, Coal-Fired Plants, Power Plant Maintenance, Combined Cycle Power, Turbine Optimization, Distributed Energy Systems, Energy Storage, Green Energy Transition, Solar Power Plants, Fossil Fuels, Biomass Energy, Emission Control Systems, Hydrogen Power, Microgrid Integration*
Transportation	*Sustainable Transport, Electric Vehicles, Urban Mobility, Smart Transportation Systems, Autonomous Vehicles, Public Transit Systems, Freight Logistics, Road Safety, Transport Infrastructure, Mobility as a Service (MaaS), Air Transportation, Rail Transport, Maritime Logistics, Traffic Management, Fuel Efficiency, Multimodal Transport, Shared Mobility, Intelligent Transportation Systems, Hyperloop Technology, Sustainable Aviation*
Flood, Water, Ocean	*Flood Risk Management, Hydrology, Coastal Erosion, Tsunami Monitoring, Ocean Currents, Climate Change Impact on Water, Water Quality, Aquatic Ecosystems, Marine Biodiversity, Rainwater Harvesting, Drought Management, Desalination Technologies, Sea Level Rise, Flood Forecasting, Groundwater Management, Oceanography, Wetland Conservation, Watershed Management, Waterborne Diseases, Urban Flooding*
Finance, Bank	*Financial Technology (FinTech), Blockchain in Banking, Digital Payments, Risk Management, Investment Strategies, Central*

	Bank Policies, Cryptocurrencies, Banking Regulations, Credit Scoring, Microfinance, Sustainable Finance, Machine Learning in Finance, Stock Market Analysis, Wealth Management, Peer-to-Peer Lending, Bank Customer Behavior, Financial Inclusion, Corporate Finance, Venture Capital, Financial Fraud Detection
Nature	*Biodiversity Conservation, Wildlife Habitat, Ecological Restoration, Sustainable Forestry, Endangered Species, Nature-Based Solutions, Ecosystem Services, Urban Green Spaces, Natural Disaster Mitigation, Environmental Degradation, Wetland Preservation, Carbon Sequestration, Rewilding, Marine Conservation, Renewable Natural Resources, Climate Change Mitigation, Soil Health, Agroforestry, Landscape Ecology, Biophilia*
Social, Culture	*Cultural Heritage, Social Inclusion, Multiculturalism, Identity and Diversity, Community Development, Intercultural Communication, Migration and Diaspora, Social Justice, Gender Equality, Civic Engagement, Urban Sociology, Social Innovation, Digital Culture, Family Structures, Indigenous Knowledge, Cross-Cultural Psychology, Social Media Influence, Cultural Anthropology, Ethnic Studies, Community Resilience*
Religion	*Religious Tolerance, Comparative Religion, Faith and Spirituality, Interfaith Dialogue, Religious Rituals, Theology, Sacred Texts, Pilgrimage Studies, Religion and Ethics, Secularism, Religious Fundamentalism, Religion in Politics, Religious History, Philosophy of Religion, Mysticism, Religious Art, Religion and Science, Religious Education, New Religious Movements, World Religions*
Parenting	*Child Development, Parenting Styles, Parental Involvement in Education, Attachment Theory, Positive Parenting, Parenting Challenges, Discipline Strategies, Work-Life Balance, Early Childhood Education, Parental Stress, Adolescent Behavior, Single Parenting, Co-Parenting Dynamics, Child Safety, Digital Parenting, Foster Parenting, Parenting in Multicultural*

	Families, Role of Fathers, Parenting Support Programs, Parenting and Technology
Space, Atmosphere, Universe	*Space Exploration, Astrobiology, Exoplanets, Atmospheric Sciences, Space Weather, Black Holes, Cosmic Rays, Satellite Technology, Planetary Science, Space Debris, Lunar Research, Interstellar Travel, Mars Colonization, Earth Observation, Dark Matter, Gravitational Waves, Rocket Propulsion, Space Sustainability, Big Bang Theory, Space Law*
Law	*Criminal Justice, International Law, Human Rights, Constitutional Law, Environmental Law, Corporate Law, Intellectual Property Law, Tax Law, Family Law, Maritime Law, Forensic Law, Contract Law, Employment Law, Immigration Law, Arbitration, Tort Law, Civil Law, Public Policy, Legislative Studies*
Arts	*Visual Arts, Performing Arts, Contemporary Art, Art History, Digital Art, Sculpture, Photography, Painting, Graphic Design, Art Therapy, Music Composition, Theater Production, Literary Arts, Film Studies, Art Criticism, Calligraphy, Cultural Preservation, Dance Choreography, Media Arts, Art Education*
Entertainment	*Film Production, Television Shows, Streaming Media, Video Games, Pop Culture, Music Industry, Animation, Celebrities, Entertainment Law, Reality TV, Event Management, Concert Organization, Online Content Creation, Podcasting, Esports, Talent Management, Stand-Up Comedy, Social Media Entertainment, Festivals, Theme Parks*
Sports	*Sports Analytics, Physical Fitness, Professional Sports, Youth Sports, Sports Psychology, Athletic Training, Sports Nutrition, Injury Prevention, Team Sports, Individual Sports, Outdoor Activities, Extreme Sports, Paralympic Sports, E-Sports, Sports Management, Sports Marketing, Performance Enhancement, Coaching Strategies, Sports Physiology*

Tabel 3.6. Key words *Include* dalam proses *Screening* SLR Artikel

Kategori	***Include Key Words***
General Keywords	*Digital Forensic Readiness, information security Management system Government, information security Management system governance, Digital Forensic Readiness governance, Digital Forensic Readiness Management, Digital Forensic Management, isms, iso 27001*
Digital Forensic	*Evidence Acquisition, Chain of Custody, Digital Investigation, Forensic Imaging, Incident Response, Cybercrime Analysis, Data Recovery, Anti-Forensics, Mobile Forensics, Network Forensics, Cloud Forensics, Memory Forensics, IoT Forensics, Digital Evidence Preservation, Forensic Soundness, Legal Admissibility, Live Forensics, Timeline Analysis, Malware Forensics, Forensics Tools Development*
Digital Forensic Readiness	*Proactive Evidence Collection, Incident Preparedness, Forensic Policy Development, Forensic Readiness Metrics, Digital Evidence Planning, Security Incident Logging, Forensic Capabilities, Evidence Preservation Protocols, Readiness Assessment, Threat Intelligence Integration, Forensic Data Management, Pre-Incident Analysis, Policy Compliance, Real-Time Evidence Monitoring, Digital Forensic Training, Forensic Risk Analysis, Evidence Storage Standards, Preparedness Planning, Organizational Forensic Culture, Forensics Readiness Strategy*
Digital Forensic Framework	*Forensic Process Models, Evidence Handling Standards, Investigation Workflow, Case Management Systems, ISO/IEC 27043, NIST Guidelines for Digital Forensics, Forensic Tools Integration, Forensics-by-Design, Cloud Forensic Framework, Cyber Forensics Lifecycle, Incident Analysis Framework, Digital Evidence Standards, Case Documentation Templates, Standardized Forensic Procedures, Network Forensics Framework, IoT Forensics Framework, Forensic Framework*

	Validation, Proactive Forensics, Reactive Forensics, AI in Forensic Frameworks
ISMS	*Information Security Policy, Risk Assessment, Security Controls, ISO/IEC 27001, Security Awareness Training, Access Control Management, Compliance Audit, Incident Management, Data Classification, Encryption Standards, Security Metrics, Vulnerability Assessment, Business Continuity Planning, Third-Party Risk Management, Security Documentation, Security Monitoring, Asset Management, Identity Management, ISMS Framework, Organizational Security Culture*
IT Governance	*IT Strategy Alignment, Risk Management, Compliance Management, IT Service Management, Enterprise Architecture, COBIT Framework, IT Audit, IT Portfolio Management, IT Resource Allocation, Business-IT Alignment, Governance Metrics, IT Policy Development, Strategic Planning, IT Risk Assessment, Change Management, IT Performance Measurement, Stakeholder Engagement, IT Governance Models, Technology Oversight, IT Governance Maturity Models*

Berdasarkan hasil konfigurasi *screening* pada tahap ini, artikel yang terfilter kedalam *exclude screening* berjumlah 7 artikel, sehingga total artikel yang terfilter untuk dapat dilanjutkan ke tahap selanjutnya sejumlah 119 artikel.

3.1.3. Pencarian Studi Primer SLR

Tahap pencarian studi primer SLR ini merupakan tahap dimana semua data yang terjaring pada tahap sebelumnya yang telah mengalami filtering, dilakukan pencarian terhadap sumber aslinya. Tahap ini merupakan proses dimana peneliti mencari, mengunduh artikel sumber tersebut. Peneliti menggunakan beberapa *tools* dan metode untuk mendapatkan artikel yang diharapkan dapat dilanutkan ke tahap berikutnya, seperti dengan cara :

1. Mengakses dan mengunduh database artikel sumber secara langsung, yaitu mengakses laman *scopus, science direct* dengan menggunakan akun tertentu.

2. Mengakses dan mengunduh menggunakan *tools Publish or Perish* dan *Refference Manager* (Zotero dan Mendeley).
3. Mengakses dan mengunduh artikel dari *tools* Watase uake secara langsung.
4. Melakukan pencarian manual melalui web engine.

Dengan menggunakan beberapa teknik pencarian sumber tersebut diatas, ada kalanya artikel yang dicari tidak dapat diakses karena beberapa hal, seperti contohnya terdapat limitasi tertentu seperti hak akses ke full paper artikel yang tidak mengijinkan diunduh. Pada penelitian ini didapatkan data artikel yang tidak dapat diunduh karena beragam limitasi dan dinamika para pengelola artikel tersebut adalah sejumlah 47 artikel. Total artikel yang dapat diakses dan diunduh sejumlah 72 artikel yang siap diproses ke tahap selanjutnya. Artikel yang dapat diunduh, kemudian disimpan dalam repositori tertentu untuk digunakan sebagai bahan pemrosesan SLR selanjutnya.

3.1.4. Pemilihan Studi Primer SLR

Artikel yang telah melalui tahap pencarian, *screening* dan dapat diunduh oleh peneliti, selanjutnya dilakukan pemilihan artikel yang sesuai dengan topik yang diangkat. Pemilihan ini dilakukan dengan proses manual dengan menganalisa judul artikel, abstrak, isi artikel, serta hasil dan kesimpulan penelitian yang didapat. Artikel dengan konteks isinya yang sesuai dengan topik penelitian akan tetap dilanjutkan ke tahap berikutnya, yaitu ekstraksi data artikel. Artikel yang memiliki memiliki judul, abstrak dan kata kunci penelitian yang sesuai dengan topik namun substansi isi artikelnya tidak sesuai dengan topik penelitian yang diangkat, akan terfilter (tidak akan dilanjutkan ke proses berikutnya). Total jumlah artikel yang berhasil dilakukan analisa *Article Selection* pada proses ini adalah sejumlah 72 artikel dengna sumber primer *(scopus, science direct).*

Setelah proses SLR yang telah menargetkan artikel yang akan dianalisa (sebanyak 72 artikel), pada tahap ini juga dilakukan validasi dan konfirmasi substansi artikel yang dilakukan secara manual oleh peneliti untuk mengurangi kesalahan proses selanjutnya. Peneliti melakukan analisa substansi terhadap judul, abstrak, full paper dokumen apakah masih relevan terhadap topik penelitian. Peneliti mendapatkan 5 artikel yang tidak dapat dilanjutkan ketahap berikutnya karena alasan penarikan dokumen *(retraction),* koreksi *(correction),* duplikasi *(duplicate),* maupun ketidak sesuaian lainnya. Total dokumen yang dapat dilanjutkan ketahap SLR selanjutnya adalah 67 dokumen artikel.

Tabel berikut merupakan rancangan meta data untuk analisa substansi artikel yang telah didapatkan guna proses ekstraksi dan proses analisis maupun sintesis pada tahap SLR selanjutnya.

Tabel 3.7. Contoh rancangan meta data ekstraksi filtering artikel SLR

No	DOI	*Author*	Judul	Sitasi	Rating
1	....	....	....	....	....
2	....	....	....	....	....
n	....	....	....	....	....

3.1.5. Ekstraksi Data dari Studi Primer SLR

Setelah proses identifikasi dan retrieval (pencarian full paper/pdf artikel) telah terkumpul, tahap selanjutnya adalah tahap ekstraksi data dari dokumen artikel yang dimiliki. Ekstraksi data merupakan bagian yang sangat penting untuk memetakan analisa SLR dengan akurat, komprehensif dan sistematis. Beberapa variabel yang diabil datanya dari artikel tersebut antara lain (namun tidak terbatas pada): *Abstract, Publication Year, Theory, Methodology, Findings, Result, Conclusion, Recomendation dan Future Works*. Variabel ini ditentukan berdasarkan *Research Question* yang telah didefinisi dan perlu dicari jawabannya.

Tabel 3.8. Contoh rancangan meta data ekstraksi substansi artikel SLR

No	DOI	*Author*	Judul	Abstract	*Methodology*	Conclusion
1	....	....	....	....	....	
2	....	....	....	....	....	
n	....	....	....	....	....	

3.1.6. Akses terhadap Kualitas Data Studi Primer SLR

Tahap akses terhadap kualitas data studi primer dalam *Systematic Literature Review (SLR)* adalah langkah penting untuk memastikan bahwa studi-studi yang digunakan dalam penelitian memiliki kredibilitas, relevansi, dan validitas yang memadai. Dalam konteks penelitian tentang implementasi *Digital Forensic Readiness (DFR) dan Information Security Management Systems (ISMS)* pada organisasi pemerintahan, tahap ini melibatkan evaluasi kualitas setiap studi primer berdasarkan kriteria yang telah ditentukan. Kriteria tersebut

meliputi validitas metodologi, relevansi konteks penelitian terhadap sektor pemerintahan, dan keandalan hasil penelitian yang dilaporkan. Sebagai contoh, literatur yang membahas penerapan standar seperti ISO/IEC 27043 untuk kesiapan forensik *Digital* atau ISO/IEC 27001 untuk keamanan informasi dalam konteks pemerintahan akan memiliki nilai yang lebih tinggi dibandingkan studi yang hanya membahas teori umum tanpa penerapan praktis.

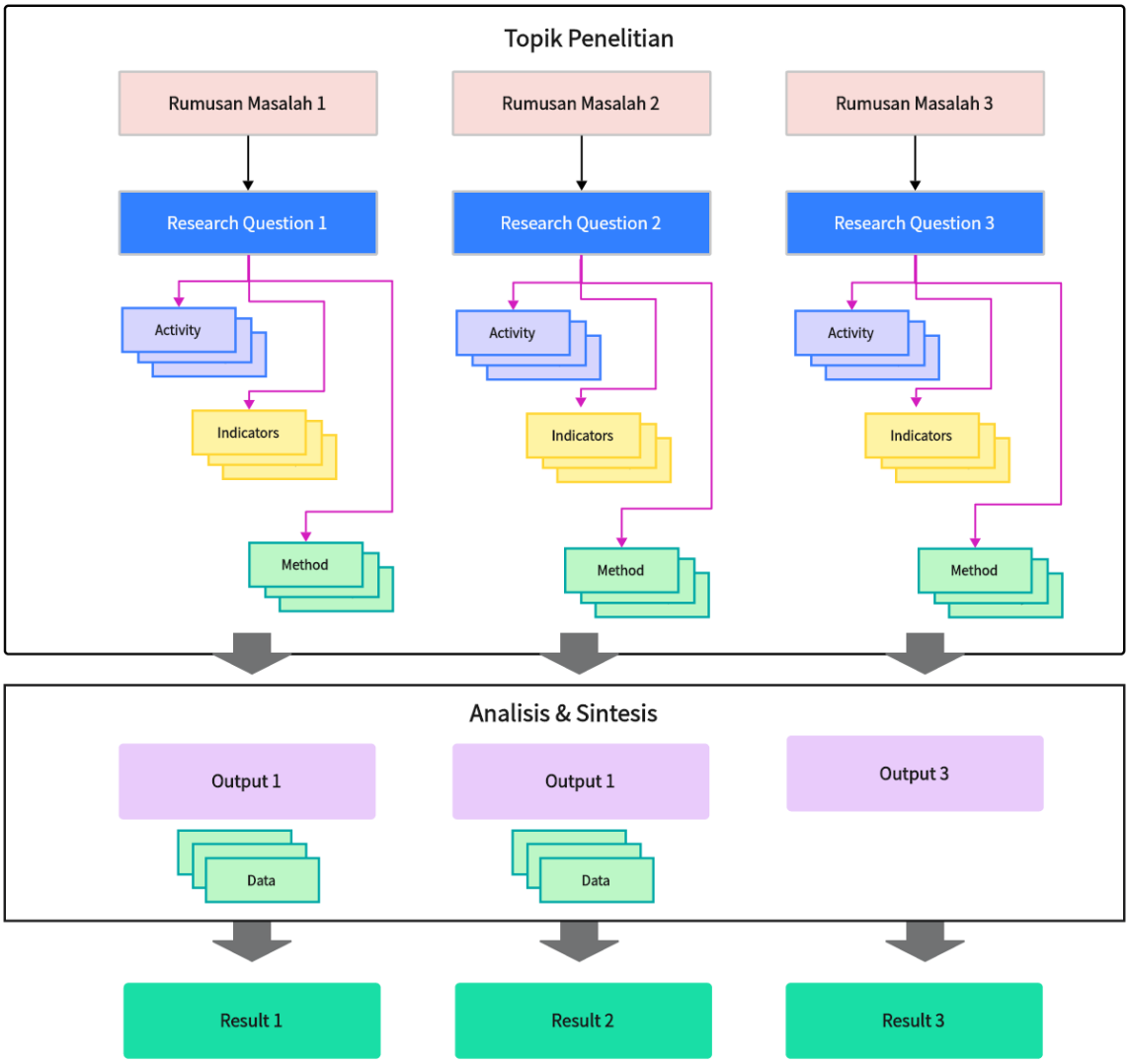
Proses evaluasi kualitas ini biasanya dilakukan menggunakan kerangka kerja atau alat penilaian seperti pedoman *Critical Appraisal Skills Programme (CASP)* atau *Quality Assessment Tools* yang disesuaikan dengan fokus penelitian. Penilaian mencakup aspek metodologi penelitian, seperti apakah desain studi sesuai untuk menjawab pertanyaan penelitian, kejelasan dalam pengumpulan dan analisis data, serta apakah hasil penelitian dapat diterapkan dalam konteks yang sesuai dengan tema penelitian yang diangkat. Namun peneliti tidak menggunakan *Framework* maupun assesment *tools* yang dapat menilai kualitas data yang diekstraksi. Peneliti hanya menggunakan analisis manual yang berbasis relevansi dengan topik penelitian yang diangkat disertai dengan terdapatnya penerapan standar yang berlaku (seperti iso dan semacamnya) yang ada dalam pembahasan artikel tersebut.

Peneliti mempertimbangkan artikel dengan rating yang tinggi (secara berurutan prioritasnya mulai dari Q1, Q1, Q3, Q4) serta artikel yang memiliki sitasi terbanyak, atau *Author* dengan jumlah publikasi dan sitasi terbanyak sebagai prioritas. Peneliti mebuat 16 artikel dengan Q-rating tertinggi dan jumlah sitasi terbanyak sebagai acuan untuk mencari interkoneksi, hubungan antara satu artikel dengan artikel lainnya dalam populasi artikel yang dimiliki untuk kemudian dipetakan hubungan antar artikelnya menggunakan *article's network map*. Penjelasan interkoneksi beberapa artikel divisualisasikan pada bab pembahasan.

3.1.7. Sintesis Data SLR

Tahapan "*Synthesize Data*" dalam proses *systematic literature Review* (SLR) merupakan langkah penting di mana peneliti harus mengintegrasikan dan menganalisis data yang telah diekstraksi dari studi-studi primer yang dimiliki pada tahap sebelumnya Tujuannya adalah untuk mengidentifikasi pola, hubungan, atau temuan signifikan yang relevan dengan pertanyaan penelitian. Proses sintesis ini tidak hanya mencakup pengorganisasian data secara sistematis, tetapi juga penginterpretasian hasil untuk menghasilkan kesimpulan yang bermakna. Teknik sintesis dapat bervariasi tergantung pada sifat penelitian, misalnya seperti pada penelitian kuantitatif, metode meta-analisis sering digunakan untuk menggabungkan hasil statistik, sedangkan dalam penelitian kualitatif,

pendekatan seperti analisis tematik digunakan untuk mengidentifikasi tema utama dari data. Selama proses sintesis, peneliti mempertimbangkan heterogenitas studi yang dianalisis, baik dari segi metodologi maupun konteks penelitian yang diangkat yang telah dirumuskan pada *research Question*. Hasil akhir dari proses ini adalah ringkasan terintegrasi yang memberikan wawasan mendalam, menjawab pertanyaan penelitian, dan mengarahkan pada implikasi teoretis maupun praktis yang dapat digunakan dalam konteks penelitian lanjutan. Penjelasan teknis terperinci mengenai proses sintesis SLR dijelaskan pada bab 4 berdasarkan data tabel berdasarkan *flow* diagram yang disajikan pada gambar berikut.



Gambar 3.8. *Flow* diagram sintesis SLR berdasarkan topik penelitian dan RQ

3.1.8. Pelaporan Hasil SLR

Tahapan deseminasi atau pelaporan hasil dalam *systematic literature Review (SLR)* merupakan langkah akhir yang berisi hasil analisa dari beberapa tahapan sebelumnya yang diproses secara sistematis. Tahapan ini sangat penting untuk memastikan bahwa temuan penelitian dapat diakses oleh pembacanya seperti komunitas ilmiah untuk dilakukan studi lanjutan, pembuat kebijakan untuk mendefinisikan keputusan terbaik dilingkungannya, praktisi yang mengimplementasikan aktivitas tertentu yang relevan, atau siapapun yang memanfaatkan data serta hasil analisa SLR ini. Laporan hasil SLR juga dapat digunakan sebagai landasan pekerjaan selanjutnya yang memiliki relevansi. Hasil analisis dan sintesis SLR pada penelitian ini disajikan pada bab 4.

3.2 *Framerok Model Digital Forensic Readiness* dan *Information System Management System*

Seperti dijelaskan pada Gambar 2.1. Komponen utama *Digital Forensic Readiness* dan Gambar 3.8 *Model Digital Forensic Readiness* bahwa beberapa *model Framework Digital Forensic Readiness* yang ada dan digunakan secara umum saat ini harus memiliki komponen yang sama meskipun setiap *Framework* memiliki alur dan karakteristik masing-masing. Secara umum komponen DFR tersebut antara lain "*Organizational Factor", "Forensic Strategy", dan "Forensic Readiness Objective"*. Tabel 3.9 juga menjelaskan jenis-jenis *model Digital Forensic Readiness Framework* yang digunakan di dunia dari berbagai aspek kebutuhan organisasi. Tabel tersebut selain menjadi acuan penelitian, juga berfungsi sebagai alternatif *model* DFR yang bagaimana yang paling tepat untuk diterapkan ke ISMS organisasi pemerintahan. Beberapa *model Digital Forensic Readiness* yang dapat digunakan antara lain :

1. *Digital Forensics and Incident Response* (DFIR)
2. ISO/IEC 27037
3. ETHI*Core Framework*
4. *Cloud Forensic Readiness Framework*
5. *Digital Forensics Readiness Index* (DFRI)

3.2.1 *Digital Forensic*s and *Incident Response* (DFIR)

Digital Forensics and Incident Response (DFIR) adalah bidang dalam keamanan siber yang berfokus pada penanganan insiden *Digital*, seperti pelanggaran data dan serangan

siber. Disiplin ini melibatkan identifikasi, investigasi, dan respons terhadap ancaman yang dapat membahayakan aset *Digital* organisasi. Salfati dan Pease (2022) menjelaskan bahwa DFIR memiliki peran penting dalam menangani insiden yang melibatkan Teknologi Operasional (OT), yang membutuhkan pendekatan berbeda dibandingkan Teknologi Informasi (IT). Pentingnya DFIR terletak pada kemampuannya untuk membantu organisasi mendeteksi ancaman dengan cepat, memberikan respons efektif, serta mengurangi dampak negatif terhadap operasional dan keberlanjutan bisnis.

Proses DFIR mencakup beberapa tahap utama, yaitu persiapan, deteksi ancaman, analisis insiden, penahanan, eradikasi, pemulihan, dan evaluasi pasca-insiden. Dalam konteks OT, Salfati dan Pease (2022) menyatakan bahwa setiap tahap perlu disesuaikan agar dapat menangani karakteristik unik dari sistem OT. DFIR sangat relevan untuk digunakan oleh organisasi yang bergantung pada infrastruktur kritis, seperti sektor energi, transportasi, dan industri, di mana stabilitas dan ketersediaan sistem menjadi prioritas utama. Keunggulan utama dari DFIR adalah kemampuannya untuk memberikan respons cepat terhadap insiden keamanan, mengurangi waktu henti operasional, dan mengumpulkan bukti *Digital* yang berguna untuk proses penegakan hukum. Namun, seperti yang disebutkan oleh Salfati dan Pease (2022), penerapan DFIR di lingkungan OT menghadapi berbagai tantangan, termasuk keterbatasan sumber daya, kompleksitas infrastruktur, serta kebutuhan akan keahlian teknis yang memahami integrasi antara komponen IT dan OT. Hal ini menuntut pendekatan yang lebih spesifik untuk memastikan bahwa DFIR dapat diimplementasikan dengan efektif.

Respon terhadap insiden berfokus pada mendeteksi dan merespons pelanggaran keamanan. Tujuan utama dari respon insiden adalah mencegah serangan sebelum terjadi dan meminimalkan biaya serta gangguan bisnis akibat serangan yang sudah terjadi. Upaya dalam respon insiden dipandu oleh rencana respon insiden *(Incident Response Plan/IRP),* yang menjelaskan bagaimana tim respon insiden harus menangani ancaman siber. Penerapan DFIR dalam organisasi dilakukan dengan menentukan ruang lingkup, situasi dan kondisi, serta beberapa komponen yang menunjang proses DFIR dapat dilakukan, yaitu antara lain seperti terlihat pada gambar berikut.

Gambar 3.9. Komponen Implementasi DFIR pada Organisasi berdasarkan NIST

Untuk menerapkannya, terdapat bebeapa proses *Digital Forensic* yang menjadi landasan utama pemrosesan DFIR, yaitu sebagai berikut:

1. *Koleksi (Collection)*

   Data yang relevan diidentifikasi, diberi label, direkam, dan dikumpulkan. Tahap ini memastikan bahwa semua bukti yang diperlukan diamankan tanpa merusak integritasnya, sehingga dapat digunakan dalam analisis lebih lanjut atau proses hukum.

2. *Eksaminasi (Examination)*

   Teknik dan alat forensik diterapkan untuk mengidentifikasi dan mengekstrak informasi yang relevan dari data yang telah dikumpulkan. Proses ini bertujuan menyaring data mentah agar hanya informasi penting yang diperoleh untuk langkah analisis berikutnya.

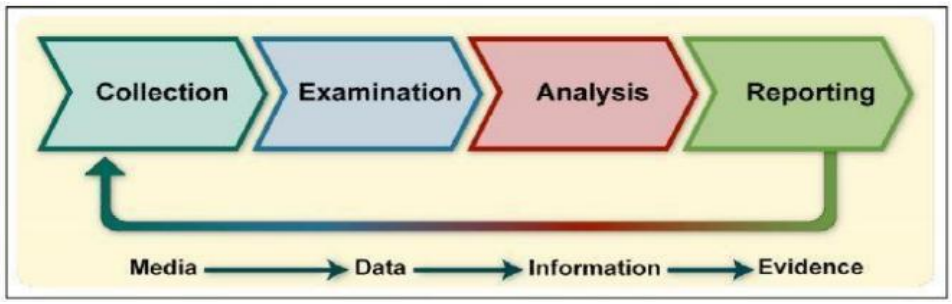
3. *Analisis (Analysis)*

   Informasi dianalisis untuk mendapatkan bukti yang dapat menjelaskan akar penyebab insiden. Tahap ini menghubungkan berbagai potongan bukti untuk membuat gambaran menyeluruh tentang insiden, seperti siapa pelaku atau bagaimana insiden terjadi.

4. Pelaporan *(Reporting)*

   Hasil dari analisis dirangkum bersama rekomendasi untuk langkah perbaikan atau pencegahan di masa depan. Laporan ini memberikan dokumentasi resmi

yang dapat digunakan untuk pengambilan keputusan strategis atau sebagai referensi dalam penanganan insiden serupa.



Gambar 3.10. NIST SP 800-86 *Framework*

Empat poin utama DF proses tersebut kemudian dimasukkan kedalam *Framework* seperti gambar berikut.

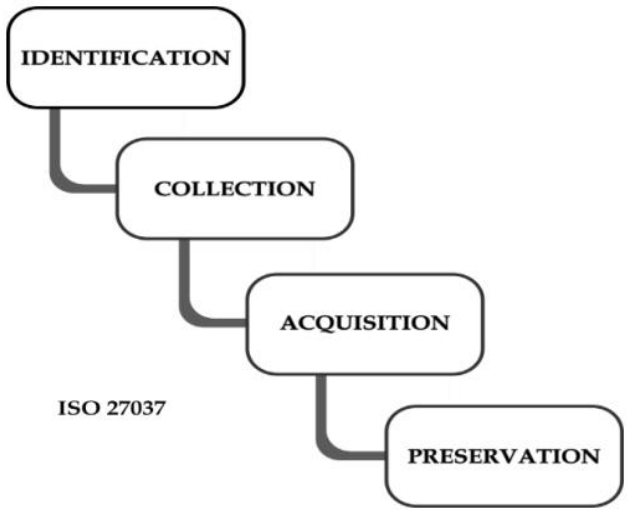
Gambar 3.11. NIST DFIR *Framework, general perspective*

Framework ini dapat digunakan untuk organisasi dengan kriteria:

1. Organisasi umum *(general Organization)* maupun pemerintahan
2. IT/OT Infrastructure
3. Menerapkan IT Risk *Management* atau ISMS
4. Memiliki atau berencana menerapkan *Security Operation Centre (SOC)*

3.2.2 ISO/IEC 27037

NIST SP 800-86 dan ISO/IEC 27037 merupakan dua standar utama dalam investigasi forensik *Digital* yang memberikan panduan sistematis pada pengelolaan bukti *Digital*. NIST SP 800-86 menekankan pendekatan langkah demi langkah dari identifikasi, pengumpulan, pemeriksaan, analisis, hingga pelaporan, sedangkan ISO/IEC 27037 lebih berfokus pada identifikasi, pengumpulan, akuisisi, dan pelestarian bukti *Digital* (Arif & Luthfi, 2024; Sudyana et al., 2019). Kerangka kerja ini penting untuk menjaga integritas dan keabsahan bukti dalam investigasi, yang menjadi kunci untuk proses hukum yang adil dan dapat dipertanggungjawabkan. Implementasi yang disiplin pada tahapan ini memastikan investigasi forensik berjalan secara efisien dan efektif. Penjelasan tentang ISO/IEC 27037 *Framework* terdapat pada gambar berikut.

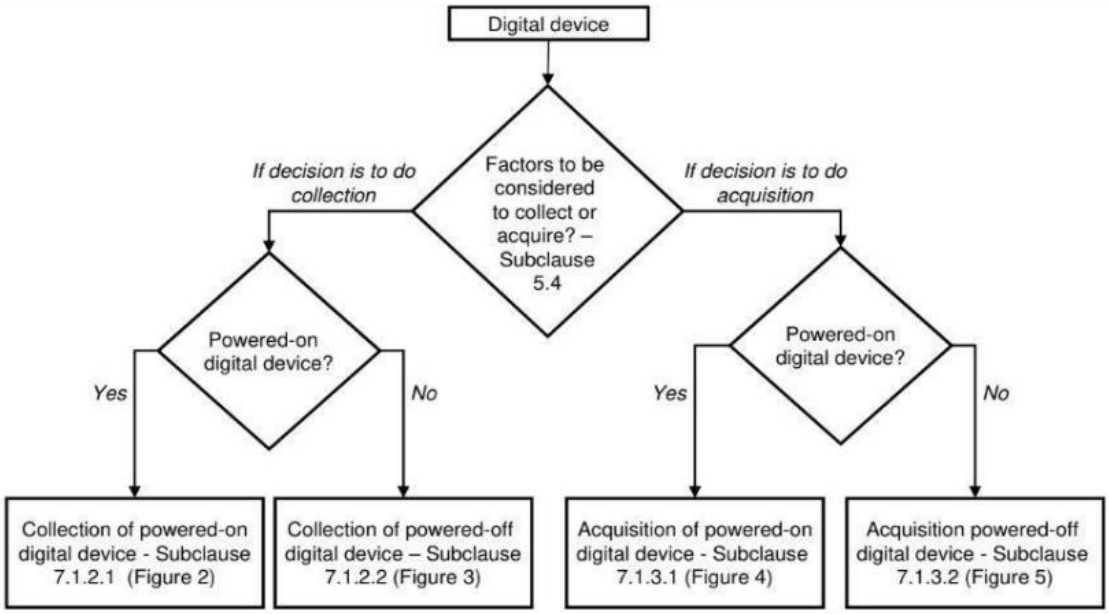


Gambar 3.12. ISO/IEC 27037 *Framework*

Framework NIST SP 800-86 cocok untuk tim forensik *Digital*, insiden respons, dan penegak hukum yang membutuhkan panduan menyeluruh untuk investigasi, sedangkan ISO/IEC 27037 lebih relevan untuk organisasi yang ingin meningkatkan pengelolaan bukti *Digital* mereka secara strategis. Kelebihan utama *Framework* ini adalah kemampuannya untuk menjamin konsistensi dan keandalan bukti *Digital*, memperkuat proses hukum, dan memfasilitasi kerja sama antar tim investigasi. Sebagai contoh, ISO/IEC 27037 memberikan fleksibilitas dalam penanganan bukti yang tersebar di berbagai yurisdiksi, sedangkan NIST SP 800-86 menawarkan pendekatan yang lebih komprehensif untuk analisis bukti *Digital* (Arif & Luthfi, 2024; Sudyana et al., 2019).

Meskipun memiliki banyak kelebihan, *Framework* ini memiliki beberapa kekurangan. NIST SP 800-86 terkadang dianggap terlalu kaku dan membutuhkan sumber daya besar untuk implementasi penuh, terutama pada tahap analisis dan pelaporan yang memerlukan waktu dan tenaga ahli. Sebaliknya, ISO/IEC 27037 cenderung kurang mendalam dalam membahas proses analisis dan pelaporan, sehingga membutuhkan panduan tambahan untuk investigasi yang kompleks (Arif & Luthfi, 2024; Sudyana et al., 2019). Untuk mengatasi kelemahan ini, integrasi kedua standar dapat memberikan pendekatan yang lebih holistik dan komprehensif dalam mengelola bukti *Digital*.

Menurut Arif & Luthfi (2024) dalam penelitiannya menjelaskan bahwa sebelum memilih atau membandingkan *Framework* mana yang akan digunakan (dalam penelitiannya membandingkan NIST SP 800-86 *Framework* dengan ISO ISO 27037), tahapan pertama yang harus dilalui adalah menentukan kerangka berfikir *Decision Making Framework,* seperti dijelaskan gambar berikut.



Gambar 3.13. *Decision Making Framework* (Arif & Luthfi, 2024; Sudyana et al., 2019).

Implementasi *Framework* mana yang terbaik yang akan digunakan dalam insiden respon organisasi antara NIST SP 800-86 atau ISO 270023 dijabarkan oleh peneliti (Arif, F., & Luthfi, A. (2024)) pada tabel berikut

Tabel 3.9. Perbandingan NIST SP 800-86 dan ISO 270023

No	Feature	NIST SP 800-86	ISO 27037
1	*Standardized Methodology*	*Promote a structured approach consisting of six stages: identification, preservation, collection, inspection, analysis, and reporting*	*Emphasizes risk Management and risk assessment, which can be applied in prioritizing Digital evidence checks*
2	*Chain of Custody*	*Recommend Approaches like keyword search and hashing to discover relevant Digital evidence*	*Encourages data classification based on sensitivity to help identify Digital evidence*
	Read-Only Acquisition	*Emphasizes the need of maintaining custody chains and employing read-only acquisition Procedures to ensure evidence integrity*	*It does not specifically address evidence collecting, but its principles can be used to assure good evidence processing*
3	*Forensic Tools and Techniques*	*Recognize the use of specialist Forensic instruments and techniques for thorough analysis*	*Instead, then directly discussing evidence analysis, emphasis is placed on correct documentation and reporting*
4	*Data Correlation*	*It necessitates extensive and well-documented reporting, including Methodology, instruments employed, analysis results, and chain of custody.*	*It does not directly address the reporting of Digital evidence, but the principles can be used to ensure accurate and concise reporting*

Tabel 3.10. Perbandingan NIST SP 800-86 dan ISO 27037 berdasarkan proses

No	Comparison	NIST SP 800-86	ISO 27037
1	Investigation	N/A	Available
2	Collection	Available	Available
3	Examination	Available	N/A
4	Analysis	Available	N/A
5	Acquisition	N/A	Available
6	Preservation	N/A	Available
7	Reporting	Available	N/A

Tabel 3.11. Perbandingan NIST SP 800-86 dan ISO 27037 berdasarkan *Framework* Focus

No	Feature	NIST SP 800-86	ISO 27037
1	Main focus	Guide to computer forensic investigation and incident response	Standard for information security management systems (ISMS)
2	Objective	Provides a structured framework for digital forensic investigations, from identification to reporting	Establish requirements for effective implementation and maintenance of ISMS
3	Target User	Digital forensic investigators, incident response team	Organizations that want to improve their information security posture

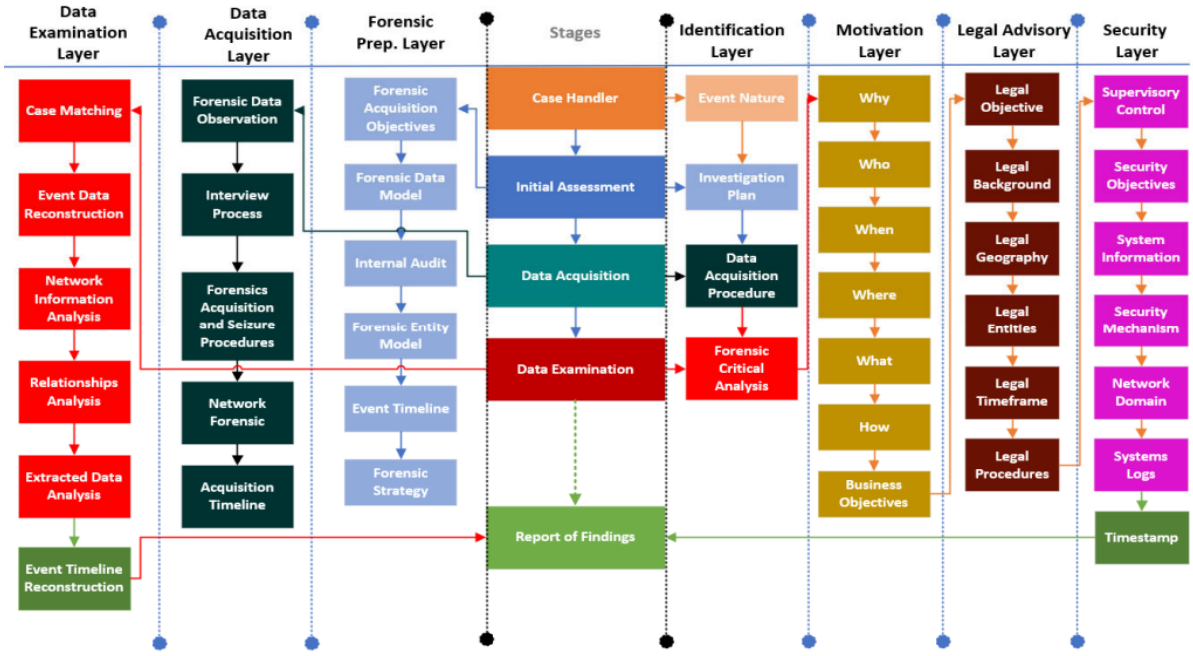
Penelitian Arif & Luthfi ini menghasilkan kesimpulan bahwa ISO/IEC 27037 menawarkan pendekatan holistik yang berkesinambungan, filosofi perbaikan dan manfaat sertifikasi, namun rumit dan membutuhkan banyak sumber daya, lebih fokus pada pencegahan dari pada respon terhadap insiden. Sebaliknya, NIST SP 800-86 memberikan prosedur khusus untuk penyelidikan forensik *Digital*, pembuatan hal ini dapat diakses dan praktis, namun tidak memiliki kerangka komprehensif ISO/IEC 27037. Pilihan antara standar-standar ini bergantung pada kebutuhan organisasi, dan penelitian di masa depan harus bertujuan untuk mengembangkan kerangka terpadu yang mengintegrasikan penelitian mereka kekuatan untuk meningkatkan praktik forensik *Digital*.

3.2.3 ETHI*Core Framework*

Dokumen membahas dua pendekatan utama dalam *Digital* forensik: ISO/IEC 27037 dan ETHI*Core Framework*. ISO/IEC 27037 berfokus pada pedoman identifikasi, pengumpulan, akuisisi, dan pelestarian bukti *Digital* dengan tujuan menjaga integritas dan keabsahan bukti untuk kepentingan hukum (Sudyana et al., 2019). Di sisi lain, ETHI*Core* menawarkan pendekatan yang lebih komprehensif dengan tujuh lapisan yang mencakup identifikasi, persiapan forensik, akuisisi data, dan pemeriksaan, sambil mengintegrasikan aspek teknis dan etika untuk memastikan kepatuhan hukum dan integritas proses (Adel et al., 2024). Kedua *Framework* memberikan dasar kuat untuk investigasi yang sistematis dan kredibel.

Framework ini dirancang untuk digunakan oleh berbagai pihak seperti tim respons insiden, penegak hukum, dan organisasi yang menghadapi ancaman siber. ISO/IEC 27037 sangat cocok untuk organisasi yang berfokus pada pengelolaan bukti *Digital* dengan presisi tinggi, sementara ETHI*Core* lebih relevan untuk mereka yang membutuhkan pendekatan holistik, termasuk panduan etika dalam investigasi. Manfaat utama dari *Framework* ini adalah meningkatkan efisiensi investigasi, memastikan bukti *Digital* dapat diterima di pengadilan, dan meminimalkan risiko pelanggaran etika selama proses investigasi (Adel et al., 2024; Sudyana et al., 2019).

Kelebihan ISO/IEC 27037 adalah struktur yang sederhana dan spesifik untuk pengelolaan bukti, namun *Framework* ini kurang membahas aspek analisis dan pelaporan secara mendalam (Sudyana et al., 2019). ETHI*Core*, dengan pendekatan tematiknya, memperluas cakupan hingga mencakup privasi, keamanan, dan integrasi etika, tetapi implementasinya lebih kompleks dan membutuhkan sumber daya lebih besar (Adel et al., 2024). Integrasi kedua *Framework* ini dapat memberikan pendekatan yang lebih seimbang antara teknis dan etika, menciptakan investigasi forensik yang lebih efektif dan terpercaya. Berikut ini gambar yang menjelaskan ETHI*Core Framework*



Gambar 3.14. ETHI*Core*: *Ethical Compliance and Oversight Framework (thematic roadmap).*

3.2.4 *Cloud Forensic Readiness Framework*

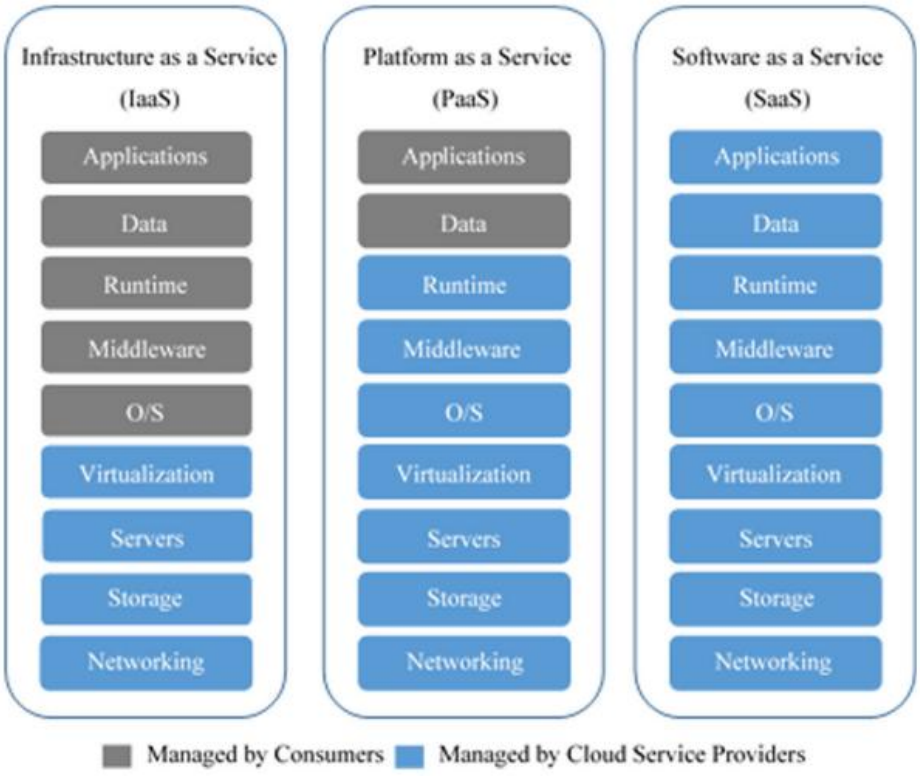
Digital Forensic Readiness (DFR) dalam lingkungan *cloud* menjadi fokus utama dalam dokumen-dokumen ini, dengan pendekatan yang berbeda. Dokumen pertama oleh Kebande dan Venter (2019) membahas desain *arsitektur Cloud Forensic Readiness as-a-Service (CFRaaS)* yang menggunakan botnet non-malicious (NMB) sebagai agen forensik. *Model* ini dirancang untuk membuat *cloud* siap secara forensik dengan pendekatan proaktif yang berfokus pada perencanaan, pelaksanaan, dan pelestarian bukti *Digital* (Kebande & Venter, 2019). Dokumen kedua oleh Alenezi et al. (2019) memberikan kerangka kerja berbasis faktor untuk kesiapan forensik di organisasi *cloud*, mencakup dimensi teknologi, hukum, dan organisasi yang berperan penting dalam memastikan bahwa bukti *Digital* dapat dikumpulkan dan digunakan secara efektif selama investigasi forensik *Digital* (Alenezi et al., 2019).

Framework CFRaaS cocok untuk organisasi dengan infrastruktur *cloud* yang kompleks yang memerlukan mekanisme pengumpulan bukti otomatis tanpa mengganggu operasi bisnis. Sementara itu, kerangka kerja yang diusulkan Alenezi et al. dirancang untuk organisasi yang menggunakan *model Cloud Infrastructure-as-a-Service (IaaS)*, dengan fokus pada peningkatan pengawasan manajemen, pelatihan staf, dan kepatuhan hukum.

Kedua pendekatan ini menyoroti pentingnya perencanaan pre-insiden, pelacakan bukti *Digital*, serta pelaporan hasil untuk menjaga keamanan data dan efisiensi proses investigasi.

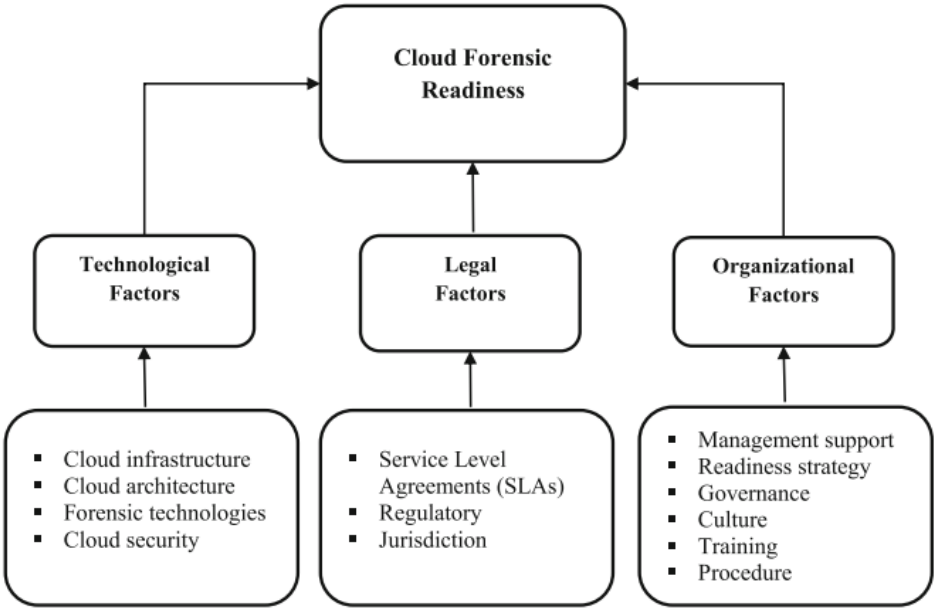
Meskipun memiliki keunggulan seperti proaktif dalam pengumpulan bukti dan kompatibilitas dengan standar internasional seperti ISO/IEC 27043, kedua *Framework* menghadapi tantangan seperti biaya implementasi yang tinggi dan kebutuhan akan pelatihan khusus untuk pengguna. Kerangka CFRaaS mungkin memerlukan integrasi yang rumit dengan sistem *cloud* yang ada, sementara *Framework* Alenezi menghadapi tantangan pada koordinasi lintas yurisdiksi dan kepatuhan hukum. Kedua pendekatan ini memberikan dasar penting untuk meningkatkan kesiapan forensik di era *cloud* computing yang semakin kompleks.

Implementasi *cloud Forensic* memerlukan tahap identifikasi kebutuhan berdasarkan perspektif pengguna agar pengelolaan DF dapat optimal sesuai dengan kebutuhan. Perspektif pengguna layanan *cloud* yang disajikan gambar berikut menjadi landasan untuk mendefinisikan kebutuhan DF.



Gambar 3.15. *Consumers' control over various models of cloud services*

Berdasarkan peta identifikasi kebutuhan layanan penggunanya, DFR pada layanan *cloud* dijabarkan pada gambar berikut.



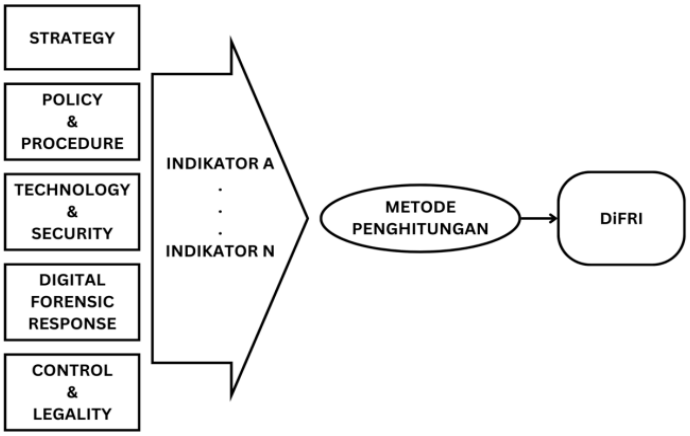
Gambar 3.16. *Cloud Forensic Readiness Framework* (Alenezi, et.al, 2019)

3.2.5 *Digital Forensics Readiness Index* (DFRI)

Digital Forensic Readiness Index (DiFRI) adalah sebuah alat ukur yang digunakan untuk menilai sejauh mana suatu organisasi siap dalam menangani dan merespons insiden yang melibatkan kejahatan dunia maya, terutama yang terkait dengan bukti *Digital*. Tujuan utama DiFRI adalah untuk memastikan bahwa institusi memiliki prosedur yang tepat dalam mengumpulkan, melindungi, dan menganalisis bukti *Digital* yang sah secara hukum. Salah satu keuntungan utama dari penggunaan DiFRI adalah memberikan gambaran yang jelas mengenai kesiapan organisasi dalam menghadapi ancaman *Digital*, yang memungkinkan pengurangan biaya investigasi serta peningkatan efektivitas dalam merespons insiden tersebut (Widodo & Prayudi, 2013). DiFRI sangat berguna bagi organisasi yang memiliki aktivitas *Digital* tinggi, seperti lembaga pemerintahan, perusahaan teknologi, atau institusi yang menangani data sensitif, yang sering menjadi target serangan dunia maya.

Metode kerja DiFRI melibatkan pengumpulan data melalui berbagai indikator yang ada pada komponen-komponen utama, yang selanjutnya dihitung dengan metode penilaian untuk menentukan tingkat kesiapan organisasi. Komponen-komponen yang ada dalam DiFRI mencakup *Strategy, Policy & Procedure, Technology & Security, Digital Forensic Response, Control & Risk*, serta *Legality*, yang masing-masing memiliki indikator untuk mengukur kesiapan pada bidang tersebut. Hasil dari perhitungan ini adalah skor yang mencerminkan sejauh mana suatu organisasi siap menghadapi ancaman dunia maya, dengan

skala kesiapan yang bervariasi dari "Siap" hingga "Tidak siap" (Widodo & Prayudi, 2013). *Model Digital Forensic Readiness Index* terdapat pada gambar berikut.



Gambar 3.17. *Model Digital Forensic Readiness Index* (Pratama, Y., et.al, 2024)

Beberapa detail komponen dan indikator pada DiFRI antara lain sebagai berikut.

1. Komponen *Strategy*
    a. Program *Digital Forensic Readiness*
    b. Aturan, regulasi dan kewajiban menyimpan dokumen dan rekaman (log, dokumen)
    c. Ketentuan ketika terjadi peristiwa yang membutuhkan barang bukti *Digital*
    d. Identifikasi sumber yang berbeda dari barang bukti *Digital*
    e. Identifikasi teknologi dan sumber daya manusia untuk menjamin *Digital Forensic Readiness*
2. Komponen *Policy & Procedure*
    a. Petunjuk atau prosedur aktivitas pegawai instansi dalam menggunakan TIK
    b. Mengetahui sanksi jika melanggar aturan dan prosedur dari *Digital Forensic Readiness*
3. Komponen *Technology & Security*
    a. Jaminan manajemen log
    b. Manajemen media penyimpanan dari perangkat komputer
    c. Ketersediaan perangkat akuisisi analisis barang bukti *Digital*, baik berupa hardware maupun software
    d. Jaminan keamanan barang bukti, baik secara online maupun offline
    e. Perangkat pendukung *Digital Forensic*
    f. Ketersediaan perangkat pengamanan sistem

g. Ketersediaan perangkat pendukung keamanan

4. Komponen *Digital Forensic Response*
   a. SOP dalam penanganan insiden atau tindakan *Digital Forensic*
   b. Pegawai instansi yang memiliki sertifikasi/keahlian di bidang *Digital Forensic*
   c. Pelatihan-pelatihan bagi pegawai instansi mengenai penanganan serangan malware dan *Digital Forensic*
   d. Tim penanganan malware dan *Digital Forensic*
   e. Petunjuk teknis pengaduan maupun pelaporan insiden
   f. Pegawai instansi memiliki pengetahuan tentang bahaya malware
   g. Alat peraga, petunjuk dan arahan mengenai malware berupa poster, banner dan alat peraga lainnya
5. Komponen *Control & Legality*
   a. Sosialisasi tentang *Digital Forensic* kepada pegawai instansi
   b. Sosialisasi tentang bahaya malware kepada pegawai instansi
   c. Pengawasan program *Digital Forensic Readiness*
   d. Pemahaman kepada setiap pegawai mengenai setiap proses *Digital Forensic* dan risiko kegagalan setiap prosesnya
   e. Pembaharuan perangkat, *tool* dan sistem secara berkala
   f. Kebijakan aspek hukum setiap proses investigasi *Digital Forensic*
   g. Pemahaman setiap pegawai instansi akan undang-undang ITE
   h. Sosialisasi peraturan dan undang-undang ITE
   i. Pelatihan penanganan terhadap serangan malware dan proses hukumnya

Setelah semua komponen dan indikator dianalisa dan dinilai dengan formula tertentu, hasilnya disajikan dalam bentuk skala dan indeks sebagai rekomendasi kepada organisasi sebagai gambaran pengelolaan sekaligus perbaikan dimasa depan. Contoh skala penilaian indeks penilaian DiFRI disajikan pada tabel berikut.

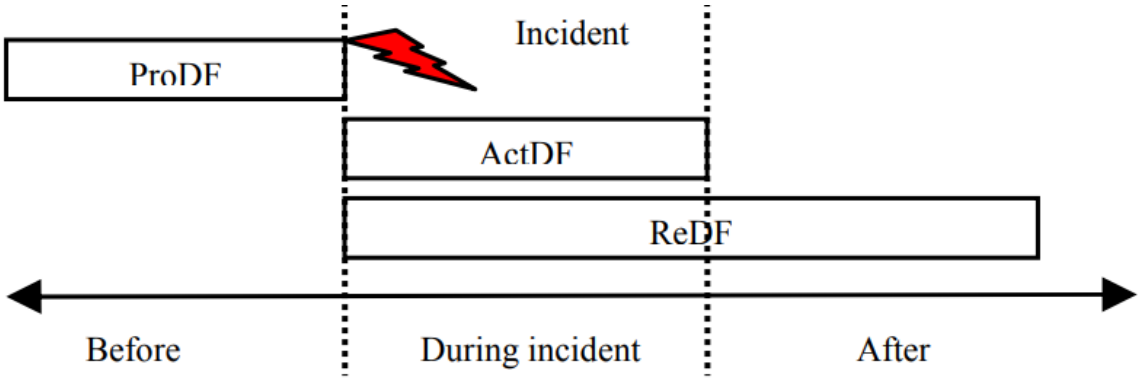
Tabel 3.12. Contoh Skala Penilaian dan Indeks DiFRI

No	Range/Skala	Status
1	$8<i \leq 10$	Sangat Siap
2	$6<i \leq 8$	Siap
3	$4<i \leq 6$	Cukup Siap
4	$2<i \leq 4$	Kurang Siap
5	$0 \leq i \leq 2$	Tidak Siap

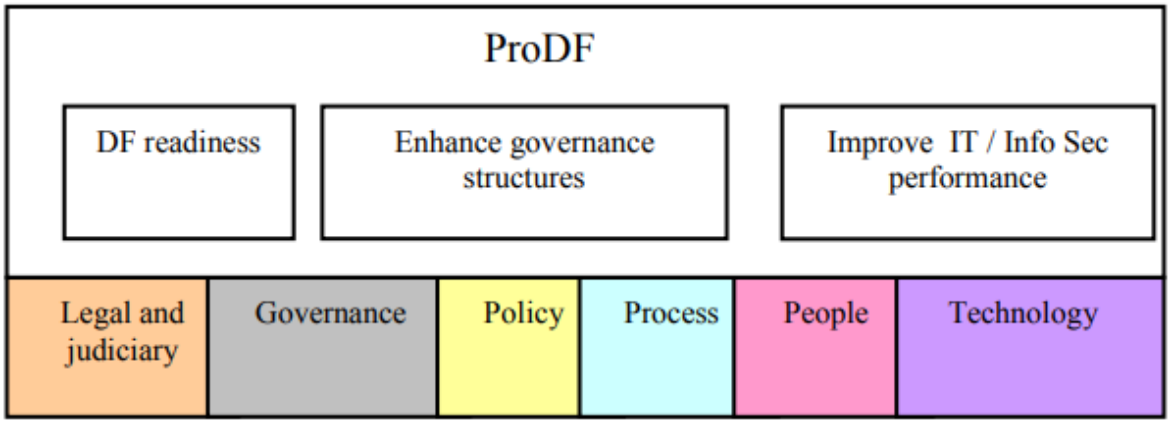
No	Komponen	Indeks
1	Strategy	6,25
2	Policy & Procedure	5,29
3	Technology & Security	6,93
4	Digital Forensic Response	4,86
5	Control & Risk	4,75
6	Legality	5,33
DiFRI		5,57

3.2.6 Proactive *Digital Forensics Framework*

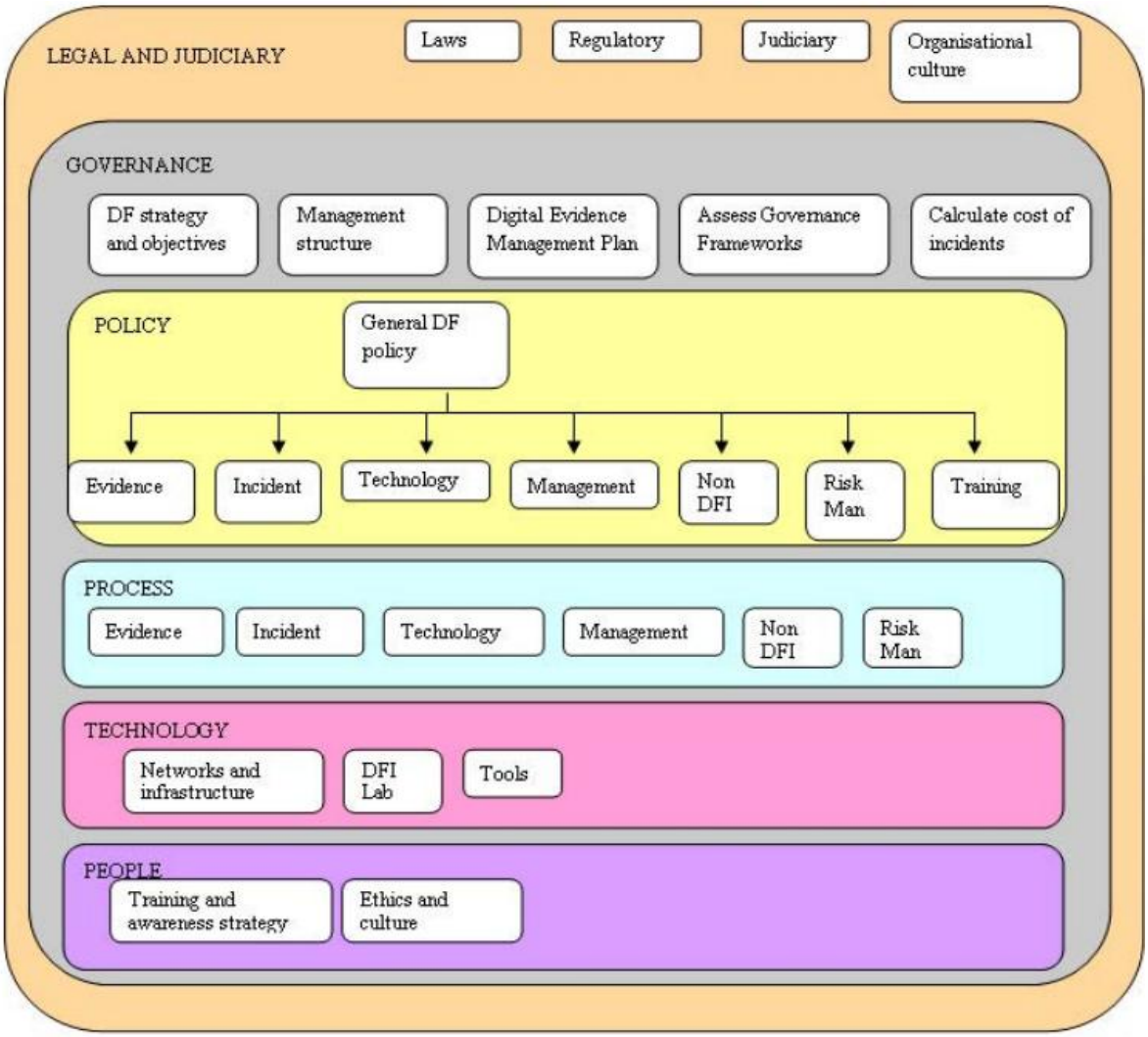
Berdasarkan penelitian (CP. Grobler, et, al. 2010) yang disajikan dalam artikel dengan judul *"A Framework to guide the implementation of Proactive Digital Forensics in Organizations"* memulai penelitian dari permasalahan yang muncul ketika sebagian besar organisasi meremehkan kebutuhan akan bukti *Digital*. Seringkali, ketika bukti diperlukan untuk membuktikan transaksi penipuan, tidak cukup atau bukti yang dapat dipercaya tersedia untuk menghubungkan pelaku dengan insiden tersebut. Organisasi perlu mempersiapkan diri untuk investigasi Forensik *Digital* (DF) dan memastikan seluruh lingkungan operasional organisasi siap, misalnya untuk investigasi (kriminal atau internal) atau uji kepatuhan. Mayoritas literatur yang ada mengenai kesiapan DF lebih fokus pada identifikasi bukti, penanganan dan penyimpanan, respons insiden, dan kebutuhan pelatihan. Namun, hal ini tidak mempertimbangkan penerapan proaktif pada DF untuk meningkatkan struktur tata kelola perusahaan (khususnya tata kelola TI & IS). Proactive *Digital Forensic* (ProDF) memungkinkan organisasi untuk mengambil inisiatif dengan menerapkan langkah-langkah yang memadai untuk siap DF, menunjukkan kewaspadaan untuk tata kelola perusahaan yang baik, khususnya Tata Kelola TI, dan memberikan mekanisme untuk menilai dan meningkatkan kerangka kerja Tata Kelola TI. Makalah ini mendefinisikan, mengidentifikasi tujuan, langkah-langkah, dan hasil dari ProDF, mengidentifikasi dimensi DF, dan mengusulkan kerangka manajemen DF teoretis untuk memandu implementasi ProDF di organisasi.



Gambar 3.18. Hubungan *Incident*, ProDF, ActDF dan ReDF (CP. Grobler, et, al. 2010)



Gambar 3.19. Hubungan ProDF dengan ISMS (CP. Grobler, et, al. 2010)



Gambar 3.20. Komponen ProDF (CP. Grobler, et, al. 2010)

Penelitian ini menekankan *Framework model* yang diusulkan (ProDF) harus terdistribusi pada beberapa layer komponen organisasi, yaitu people, Process, Technology,

Policy, Governance, dan Legal Judiciary. ProDF *Framework* memetakan elemen kunci dari DF untuk diterapkan pada masing-masing layer tersebut sehingga kesiapan organisasi dalam menghadapi insiden sifatnya preventve proaktif.

3.2.7 Pemilihan *Digital Forensic Readiness* (DFR) terhadap implementasi *Information Security Management System* (ISMS) Organisasi Pemerintah

Berdasarkan penjelasan beberapa *model Digital Forensic Framework* yang dijabarkan pada bab-bab sebelumnya, terdapat keterkaitan peran *Digital Forensic Readiness* dalam proses ISMS, yaitu pada aspek berikut ini.

1. Aspek Ruang Lingkup dan Fokus.

   Ruanglingkup dan fokus perlu didefinisikan berdasarkan regulasi, proses bisnis organisasi, serta tujuan/capaian yang diinginkan. Sebagai landasan utama pengelolaan keamanan data dan informasi di organisai, ISO 27001 adalah standar internasional untuk yang menyediakan kerangka kerja untuk mengelola keamanan informasi dengan pendekatan berbasis risiko, termasuk pengelolaan kerahasiaan, integritas, dan ketersediaan informasi. Sedangkan standar yangmelandasi *Digital Forensic process* maupun kesiapannya *(Digital Forensic Readiness)* menggunakan landasan ISO 27037, di sisi lain, adalah standar yang lebih khusus yang berfokus pada kesiapan forensik *Digital* dan pengelolaan bukti *Digital*. ISO 27037 memberikan panduan dalam identifikasi, pengumpulan, akuisisi, dan pelestarian bukti *Digital*, yang sangat penting untuk mendukung investigasi insiden keamanan. Sebagai landasan utama proses DF yang dilakukan, perlu ada penjabaran serta penekanan atau standar turunan yang lebih spesifik dapat menjelaskan *guidance* tentang pemrosesan DF berdasarkan ISO 27000 *family standard*. Penjabaran tersebut diantaranya adalah:

   a. ISO/IEC 27041, merupakan standar yang menawarkan panduan tentang penjaminan kualitas dan pengelolaan proses investigasi *Digital*, termasuk evaluasi metode dan alat yang digunakan dalam investigasi forensik *Digital*.
   b. ISO/IEC 27042, merupakan standar yang berfokus pada analisis bukti *Digital*, memberikan panduan tentang bagaimana menganalisis dan menginterpretasikan bukti yang telah dikumpulkan untuk memastikan integritas dan validitas temuan.

c. ISO/IEC 27043, merupakan standar yang menyediakan kerangka kerja untuk kesiapan dan respons insiden forensik *Digital*, membantu organisasi mempersiapkan dan merespons insiden dengan cara yang memastikan bukti *Digital* ditangani dengan benar.

2. Keterkaitan DF dalam Sistem Manajemen Keamanan Informasi (SMKI/ISMS).
   ISO 27001 mengharuskan organisasi untuk menerapkan kontrol keamanan, termasuk proses untuk menangani insiden keamanan informasi. Dalam konteks ini, ISO 27037 yang masih merupakan turunan dari 27000 family standard, berfungsi melengkapi ISO 27001 dengan memberikan panduan teknis dan prosedural untuk mengelola bukti *Digital* selama atau setelah insiden keamanan terjadi. Proses-proses dalam ISO 27037, seperti identifikasi dan pengumpulan bukti *Digital*, dapat diintegrasikan ke dalam kontrol keamanan yang diatur dalam *Annex* A dari ISO 27001, khususnya dalam area A.16 (*Information Security Incident Management*) dan A.12 (Operations *Security*). Keterkaitan ini perlu dipilih beberapa elemen kunci dari DF yang mendukung ISMS.
3. Kesiapan dan Respons Insiden
   ISO 27001 mengharuskan organisasi untuk memiliki rencana respons insiden *(Incident Response Plan)*. ISO 27037 sebagai basis pemrosesan *Digital Forensic* terbukti mendukung kebutuhan pada aspek ini dengan menyediakan pedoman yang memastikan bukti *Digital* yang relevan dapat dikumpulkan dan dilindungi selama proses respons insiden. Dengan kata lain, ISO 27037 membantu organisasi yang menerapkan ISO 27001 untuk memastikan bahwa bukti insiden keamanan dapat diterima secara hukum dan memiliki integritas yang tinggi.
4. Komplementaritas dalam Investigasi Forensik *Digital*
   ISO 27037 menjadi komponen penting dalam organisasi yang ingin memastikan kesiapan forensik *Digital (Digital Forensic Readiness)* sebagai bagian dari ISMS. Kesiapan ini membantu organisasi yang menerapkan ISO 27001 untuk mengantisipasi kebutuhan investigasi bukti *Digital* dengan langkah-langkah proaktif. Sebagai contoh, organisasi yang memiliki ISO 27001 dapat menggunakan pedoman ISO 27037 untuk mengidentifikasi alat, teknik, dan prosedur yang sesuai untuk mendukung audit internal dan investigasi insidenaaa
5. Pengelolaan Risiko dan Bukti *Digital*
   ISO 27001 berbasis pada identifikasi dan mitigasi risiko dalam sistem informasi. ISO 27037 mendukung pendekatan ini dengan memastikan bahwa bukti *Digital*

yang berkaitan dengan insiden risiko dapat dikelola dengan cara yang dapat diterima di pengadilan atau dalam proses hukum lainnya. Dengan memastikan pengelolaan bukti *Digital* sesuai ISO 27037, organisasi dapat memenuhi persyaratan kepatuhan hukum (legal *Compliance*) yang sering menjadi bagian dari persyaratan ISO 27001

Selain beberapa aspek tersebut diatas, setiap *model Framework* tersebut memiliki karakteristik tersendiri seperti yang disajikan pada tabel perbandingan *model Framework* berikut ini.

Tabel 3.13. Perbandingan *model Framework*

Kriteria	**DFIR *Framework***	**ISO/IEC 27037**	**NIST SP800-86**	**ETHI*Core* *Framework***	***Cloud Forensic Readiness Framework***	**DFRI *Framework***
Fokus Utama	Forensik *Digital* dan respons insiden	Kesiapan forensik *Digital*, pelestarian bukti *Digital*	Proses forensik *Digital*: identifikasi, pengumpulan, analisis, pelaporan	Pendekatan komprehensif yang mengintegra-sikan aspek teknis dan etika dalam forensik *Digital*	Kesiapan forensik di lingkungan *cloud*, pendekatan proaktif	Mengukur dan meningkatkan kesiapan organisasi dalam menangani forensik *Digital*
Tujuan	Menanggapi insiden keamanan siber dengan cepat	Memastikan integritas dan pelestarian bukti *Digital*	Memberikan pendekatan sistematis untuk investigasi forensik *Digital*	Memberikan pendekatan holistik untuk forensik *Digital*, termasuk kepatuhan hukum	Memastikan kesiapan forensik dan pelestarian bukti di lingkungan *cloud*	Meningkat-kan kesiapan forensik *Digital* dan memberikan panduan implementasi
Target Pengguna	Tim respons insiden, penyelidik forensik, otoritas hukum	Organisasi yang mengelola bukti *Digital*	Tim forensik, tim respons insiden, penegak hukum	Tim respons insiden, penegak hukum, organisasi yang menghadapi ancaman siber	Penyedia layanan *cloud*, organisasi yang menggunakan infrastruktur *cloud*	Organisasi dengan aktivitas *Digital*, lembaga pemerintahan
Metodologi Standar	Pendekatan terstruktur dengan tahapan: persiapan,	Fokus pada identifikasi, pengumpulandan pelestarian	Pendekatan terstruktur: identifikasi, pengumpula	Pendekatan holistik dengan tujuh lapisan yang mencakup	Pendekatan proaktif dengan perencanaan dan pelestarian bukti *Digital*	Fokus pada kesiapan dengan indikator untuk

	deteksi, analisis, pemulihan	bukti *Digital*	n, analisis, pelaporan	identifikasi, akuisisi, etika		perbaikan dan penilaian
Rantai Keamanan (*Chain* of Custody)	Merekomendasikan metode seperti pencarian kata kunci dan hashing untuk pengumpulan bukti	Fokus pada menjaga integritas dan konsistensi bukti	Memastikan integritas melalui penanganan sistematis dan dokumentasi bukti	Menangani kepatuhan etika selama penanganan bukti dan memastikan integritasnya	Menekankan pelestarian rantai keamanan dalam lingkungan *cloud*	Memastikan pengelolaan dan dokumentasi penanganan bukti yang tepat
Akuisisi Hanya-Baca (Read-Only Acquisition)	Menekankan penggunaan metode akuisisi hanya-baca untuk menjaga integritas bukti	Tidak langsung dibahas tetapi prinsip-prinsipnya memandu pengumpulan bukti	Menekankan akuisisi hanya-baca untuk memastikan integritas bukti	Fokus pada dokumentasi penanganan bukti tanpa fokus khusus pada metode akuisisi	Merekomendasikan mekanisme pengumpulan bukti otomatis tanpa mengganggu operasi bisnis	Membantu organisasi memastikan integritas pengumpulan bukti
Alat dan Teknik Forensik	Menggunakan alat dan teknik forensik khusus untuk analisis mendalam	Tidak secara khusus membahas alat, tetapi memberikan panduan untuk penggunaannya	Mengakui penggunaan alat forensik khusus untuk analisis	Fokus pada dokumentasi dan pelaporan bukti, bukan pada alat spesifik	Mungkin memerlukan integrasi dengan sistem *cloud* yang ada dan alat forensik	Membantu institusi dalam menggunakan alat dan teknik forensik yang tepat
Korelasi Data	Memerlukan pelaporan yang terperinci dan terdokumentasi dengan baik, termasuk metodologi, alat, dan hasil analisis	Tidak langsung fokus pada korelasi data tetapi menyediakan prinsip-prinsip manajemen bukti	Memerlukan dokumentasi yang ekstensif, termasuk hasil dan metodologi	Tidak langsung membahas korelasi data tetapi fokus pada pelaporan yang akurat	Fokus pada pelacakan bukti *Digital* yang efektif dan pelaporan yang tepat	Menyediakan metode yang terstruktur untuk mengevaluasi kesiapan organisasi, termasuk korelasi data

Berdasarkan lima aspek tersebut diatas dan perbandingan karakteristik DF *Framework* pada tabel diatas, peneliti menyimpulkan bahwa ISO 27037 melengkapi ISO 27001 dengan menyediakan pedoman teknis untuk menangani bukti *Digital* selama manajemen insiden keamanan informasi. Kombinasi keduanya membantu organisasi tidak hanya untuk melindungi informasi secara proaktif, tetapi juga untuk memastikan bahwa bukti *Digital* dapat diandalkan dalam investigasi atau audit, sehingga memperkuat sistem

manajemen keamanan informasi secara keseluruhan. Standar turunan lainnya dari iso 27037 seperti ISO 27041, ISO 27042, dan ISO 27043 selain menjadi panduan penerapan DFR yang dapat melengkap pemrosesan DF dengan baik, namun juga menjadi komplemen terhadap ISMS ISO 27001. Dengan adanya asumsi tersebut diatas, peneliti akan mempertimbangkan aspek-aspek tersebut diatas untuk membangun *Digital Forensic Readines Framework* yang paling sesuai dengan ISMS dilingkungan organisasi pemerintahan.

BAB 4
Hasil dan Pembahasan

Bab ini berisi tentang hasil penelitian yang diperoleh dari pemrosesan penelitian berdasarkan penjelasan pada bab sebelmnya. Pada bab ini penjelasan dari kedua hal penting yang mendasari penelitian ini disajikan dengan data baik berupa tabel maupun visualisasi data yang dapat dijadikan sebagai interpretasi sekaligus sebagai alasan penentuan hasil dan kesimpulan penelitian. Kedua hal tersebut adalah data hasil pemrosesan SLR serta *Framework model* DFR yang diusulkan untuk digunakan bersamaan dengan SMKI bagi organisasi pemerintahan.

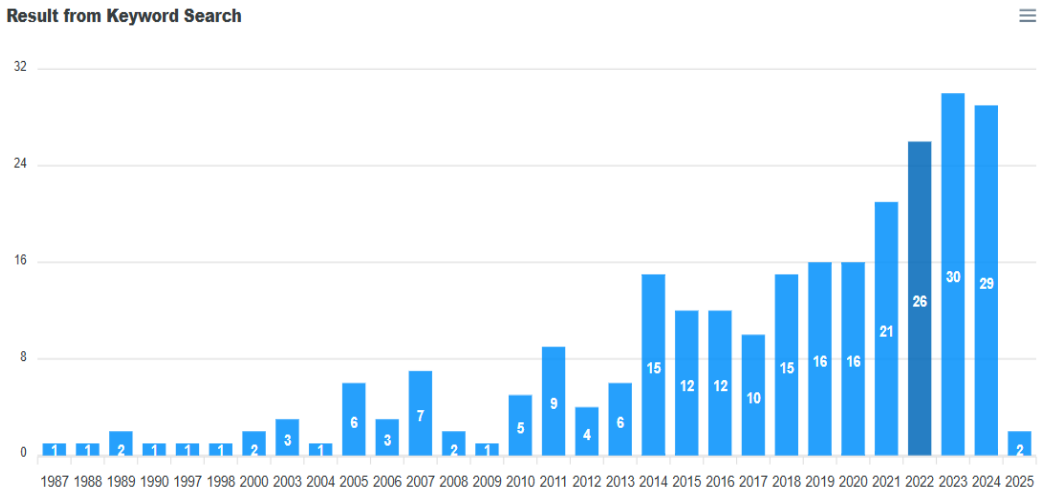
4.1 *Systematic Literature Review*

Bab 3 menjelaskan tahapan SLR dengan terperinci dengan mndefinisikan beberapa konfigurasi yang menjadi kriteria pemrosesan SLR. Tahapan SLR sangat bergantung pada variabel yang digunakan sebagai indentifikasi pencarian artikel untuk diproses dalam SLR. Tabel 3.3 dan 3.4 menjelaskan variabel apa yang dignakan peneliti untuk melakukan SLR sesuai dengan topik penelitian. Gambar 3.8 juga menjabarkan *flow* diagram analisa dan sistesis SLR berdasarkan RQ yang bersumber dari rumusan masalah dan topik penelitian. Berdasarkan proses identifikasi tersebut, data yang dihasilkan pada proses SLR untuk dilakukan sintesis agar dihasilkan result antara lain:

1. Data validasi penelitian berdasarkan tren pencarian kata kunci
2. Data validasi penelitian berdasarkan tren artikel terpublikasi
3. Data validasi penelitian berdasarkan *journal impact*
4. Data validasi penelitian berdasarkan *most Author* & *paper impact*
5. Data validasi penelitian berdasarkan sebaran lokasi penelitian
6. Data validasi penelitian berdasarkan pendekatan penelitian
7. Data validasi penelitian berdasarkan metode penelitian
8. Data validasi penelitian berdasarkan *Framework* penelitian
9. Data validasi penelitian berdasarkan temuan penelitian terhadap dampak diterapkannya DFR dalam organisasi
10. Data validasi penelitian berdasarkan temuan penelitian terhadap dampak diterapkannya ISMS dalam organisasi

11. Data validasi penelitian berdasarkan temuan penelitian terhadap dampak diterapkannya DFR dan ISMS dalam organisasi
12. Data validasi penelitian berdasarkan usulan penelitian lanjut

Data validasi tersebut diatas dihasilkan dari proses SLR tahap 1 hingga 8 dengan melakukan ekstraksi data dan menjadikannya RAW Data yang akan dilakukan analisis dan sistesis. Data tersebut disajikan dalam bentuk tabel maupun grafik berikut.



Gambar 4.1. Grafik Distribusi Artikel berdasarkan Key Word dan Parameter SLR

Berdasarkan data sebaran keyword dan grafik yang dianalisa peneliti yang divisualisasi pada grafik diatas, peneliti merumuskan "Simpulan-1" bahwa penelitian dengan topik integrasi DFR terhadap ISMS telah diteliti oleh berbagai peneilti dengan peningkatan jumlah publikasi disetiap tahunnya. Simpulan awal ini akan disimpan dan digabungkan dengan simpulan lainnya dan dirumuskan menjadi kesimpulan yang utuh di akhir dokumen.Trend penelitian ini sejalan dengan publikasi yang dilakukan oleh beberapa vendor pemegang merk platform keamanan seperti Tenable Security dalam laporannya (dimension report, 2018) dengan judul ”*Trends In Security Framework Adoption: A Survey of it and Security Professionals”* menyatakan bahwa serangan siber terhadap perusahaan enterprise meningkat 84% per tahunnya. Kemudian 70% perusahaan terkemuka didunia telah menerapkan DFR dan ISMS, meningkat sekitar 48% dari 2 tahun terahir dimana area survey penelitian ini melibatkan 388 IT Expert perusahaan terkemuka di dunia.

Tabel 4.1. Tabel Hasil Pencarian berdasarkan Key Word dan Parameter SLR

No	Title	Year	Count	Cit	Journal Rank	Int	Link
1	Enhanced Readiness Forensic Framework for the Complexity of Internet of Things (IoT) Investigation Based on Artificial Intelligence, *Journal of Advanced Research in Applied Sciences and Engineering Technology*	2025	1	0			View
2	SD-ABM-ISM: An integrated system dynamics and agent-based modeling framework for information security management in complex information systems with multi-actor threat dynamics, *Expert Systems with Applications*	2025	1	0	Q1		View
3	A High Abstract Digital Forensic Readiness Metamodel for Securing Smart Cities, *IEEE Access*	2024	1	0	Q1	✓	View
4	Analyzing Information Security Factors in Adoption of Intelligent Technologies for Medical Waste Management Systems, *IEEE Transactions on Consumer Electronics*	2024	1	1	Q1		View
5	AResNet Model Using Deep Learning Approach for Enhancing the Internet of Things (IoT) Forensic Readiness Framework, *International Journal of Intelligent Engineering and Systems*	2024	1	0	Q3		View
6	Assessing Indonesian MSMEs' Awareness of Personal Data Protection by PDP Law and ISO/IEC 27001:2013, *International Journal of Safety and Security Engineering*	2024	1	0	Q3		View
7	Construction information security management system based on data sharing algorithm, *Intelligent Decision Technologies*	2024	1	0	Q3		View
8	Correction to: Information security failures identified and measured – ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis (Information Security Journal: A Global Perspective, (2024), 33, 3, (285-306), 10.1080/19393555.2023.2270984), *Information Security Journal*	2024	1	0	Q2	✓	View
9	Design and implementation of marine information management network security system based on artificial intelligence embedded technology, *Journal of Intelligent and Fuzzy Systems*	2024	1	0	Q2		View
10	DEVELOPMENT OF A MECHANISM FOR INFORMATION SECURITY RISK MANAGEMENT OF TRANSPORT SERVICE PROVISION SYSTEMS, *Eastern-European Journal of Enterprise Technologies*	2024	1	0	Q2		View
11	DEVELOPMENT OF SECURITY POLICIES ASSESSMENT TOOLS FOR DATA COMMUNICATION IN ACCORDANCE WITH THE INTERNATIONAL STANDARD ON INFORMATION SECURITY MANAGEMENT ISO 27001:2013 USING ONTOLOGICAL CONCEPTS AND TEXT MINING METHODS, *ICIC Express Letters, Part B: Applications*	2024	1	0	Q3		View
12	Digital Forensics Readiness Framework (DFRF) to Secure Database Systems, *Engineering, Technology and Applied Science Research*	2024	1	1			View
13	Digital Forensics Readiness in Big Data Networks: A Novel Framework and Incident Response Script for Linux–Hadoop Environments, *Applied System Innovation*	2024	1	0	Q2	✓	View
14	ETHICore: Ethical Compliance and Oversight Framework for Digital Forensic Readiness, *Information (Switzerland)*	2024	1	0	Q2	✓	View
15	Forensic experts' view of forensic-ready software systems: A qualitative study, *Journal of software: Evolution and Process*	2024	1	0	Q2		View
16	ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management, *Information (Switzerland)*	2024	1	3	Q2	✓	View
17	Implementation plan of the information security management system based on the NTC-ISO-IEC 27001:2013 standard and security risk analysis. Case study: Higher education institution, *Transactions on Energy Systems and Engineering Applications*	2024	2	0			View
18	Information Security and Privacy Management in Intelligent Transportation Systems, *Complex Systems Informatics and Modeling Quarterly*	2024	1	1			View
19	Information security failures identified and measured–ISO/IEC 27001:2013 controls ranked based on GDPR penalty case analysis, *Information Security Journal*	2024	1	1	Q2	✓	View
20	INFORMATION SYSTEMS MANAGEMENT IN AGRITECH FOR FOOD SECURITY, *Proceedings on Engineering Sciences*	2024	1	0			View
21	IoT based Agriculture (Ag-IoT): A detailed study on Architecture, Security and Forensics, *Information Processing in Agriculture*	2024	1	24			View
22	IoT Forensics Readiness - influencing factors, *Forensic Science International: Digital Investigation*	2024	1	1	Q1	✓	View
23	Open Source Tools for Digital Forensic Investigation: Capability, Reliability, Transparency and Legal Requirements, *KSII Transactions on Internet and Information Systems*	2024	1	0	Q3	✓	View
24	Retraction Note: Application of embedded voice and digital forensics system in financial cost management (Soft Computing, (2023), 27, 14, (10081-10092), 10.1007/s00500-023-08214-9), *Soft Computing*	2024	1	0	Q2	✓	View
25	Retraction note: The design of network security protection trust management system based on an improved hidden Markov model (EURASIP Journal on Information Security, (2023), 2023, 1, (10), 10.1186/s13635-023-00146-z), *Eurasip Journal on Information Security*	2024	1	0	Q2	✓	View
26	RISK ASSESSMENT MATURITY LEVEL OF ACADEMIC INFORMATION SYSTEM USING ISO 27001 SYSTEM SECURITY ENGINEERING-CAPABILITY MATURITY MODEL, *Journal of Applied Engineering and Technological Science*	2024	1	0			View
27	The added value of an internet-based intervention for treatment of aggression in forensic psychiatric outpatients—study protocol for a multicentre, mixed-methods randomized controlled trial, *Digital Health*	2024	1	0	Q1		View
28	The Influence of Information Security Management System Implementation on the Financial Performance of Indian Companies: Examining the Moderating Effect of National Culture, *Sustainability*	2024	1	0	Q1	✓	View
29	Towards a Comprehensive Metaverse Forensic Framework Based on Technology Task Fit Model, *Future Internet*	2024	1	0	Q2	✓	View
30	Towards Digital Forensics Investigation of WordPress Applications Running Over Kubernetes, *IETE Journal of Research*	2024	1	0	Q3		View
31	A Survey on Industrial Control System Digital Forensics: Challenges, Advances and Future Directions, *IEEE Communications Surveys and Tutorials*	2023	1	16	Q1		View
32	Adaptive Observability for Forensic-Ready Microservice Systems, *IEEE Transactions on Services Computing*	2023	1	1	Q1	✓	View
33	Addressing insider attacks via forensic-ready risk management, *Journal of Information Security and Applications*	2023	1	16	Q1	✓	View
34	ADOPTION OF THE INFORMATION SECURITY MANAGEMENT SYSTEM STANDARD ISO/IEC 27001: A STUDY AMONG GERMAN ORGANIZATIONS, *International Journal for Quality Research*	2023	1	0	Q3		View
35	Application of embedded voice and digital forensics system in financial cost management, *Soft Computing*	2023	1	2	Q2		View
36	Assessing Information Security using COBIT 2019 and ISO 27001:2013 for Developing a Mitigation Plan, *SSRG International Journal of Engineering Trends and Technology*	2023	1	0	Q4		View
37	Bridging the gap: Assessing death certification competency in bulgarian healthcare education, *Russian Journal of Forensic Medicine*	2023	1	0			View
38	Converged Security and Information Management System as a Tool for Smart City Infrastructure Resilience Assessment, *Smart Cities*	2023	1	1			View
39	Cryptographic Techniques for Data Privacy in Digital Forensics, *IEEE Access*	2023	1	2	Q1	✓	View
40	Cyber Forensic Investigation Infrastructure of Pakistan: An Analysis of the Cyber Threat Landscape and Readiness, *IEEE Access*	2023	2	7	Q1	✓	View
41	Cyber supply chain risk management and performance in industry 4.0 era: information system security practices in Malaysia, *Journal of Industrial and Production Engineering*	2023	1	34	Q2		View
42	Erratum: Image Data Security Mechanism Based on the Internet of Things Cardiac Catheterization Laboratory Information Management System Research and Design (Journal of Healthcare Engineering (2021) 2021 (5592185) DOI: 10.1155/2021/5592185), *Journal of Healthcare Engineering*	2023	1	0	Q2		View
43	Forecasting the diffusion of ISO/IEC 27001: a Grey model approach, *TQM Journal*	2023	1	4	Q2	✓	View
44	Forensic investigation framework for cryptocurrency wallet in the end device, *Computers and Security*	2023	1	3	Q1		View
45	Forensic readiness of industrial control systems under stealthy attacks, *Computers and Security*	2023	1	10	Q1	✓	View

46	FRoMEPP: Digital forensic readiness framework for material extrusion based 3D printing process, *Forensic Science International: Digital Investigation*	2023	1	11	Q1	✓	View
47	Information management systems in the systematization of indicators for assessing the effectiveness of investment processes in the securities market, *Journal of Information Technology Management*	2023	1	0	Q4		View
48	Information Security Awareness Raising Strategy Using Fuzzy AHP Method with HAIS-Q and ISO/IEC 27001:2013: A Case Study of XYZ Financial Institution, *CommIT Journal*	2023	1	0			View
49	Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden, *Information Systems and e-Business Management*	2023	1	7	Q2	✓	View
50	Information Security on Learning Management System Platform from the Perspective of the User during the COVID-19 Pandemic, *Journal of Information and Communication Convergence Engineering*	2023	1	0	Q2		View
51	Innovative Integration of Embedded Voice and Digital Forensics Systems for Optimal Financial Cost Management: Commercialization and MarketingStrategies, *Journal of Commercial Biotechnology*	2023	1	2	Q4		View
52	ISO 27001 Information Security Survey of Medical Service Organizations †, *Engineering Proceedings*	2023	1	0			View
53	Laboratory Forensics for Open Science Readiness: an Investigative Approach to Research Data Management, *Information Systems Frontiers*	2023	1	4	Q1	✓	View
54	Network information security and legal management based on embedded real-time task processing and high-frequency acquisition system, *International Journal of Systems Assurance Engineering and Management*	2023	1	0	Q2		View
55	Ontology-based case study management towards bridging training and actual investigation gaps in digital forensics, *Forensic Science International: Digital Investigation*	2023	1	0	Q1	✓	View
56	Retraction Note to: A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud (Journal of Ambient Intelligence and Humanized Computing, (2021), 12, 5, (4911-4924), 10.1007/s12652-020-01931-1), *Journal of Ambient Intelligence and Humanized Computing*	2023	1	0	Q1	✓	View
57	The Information Security Management Systems in E-Business, *Journal of Global Information Management*	2023	1	12	Q2	✓	View
58	The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector, *Sustainability*	2023	1	24	Q1	✓	View
59	Unmanned Aerial Vehicle (UAV) Forensics: The Good, The Bad, and the Unaddressed, *Computers and Security*	2023	1	19	Q1		View
60	A case study on major cloud platforms digital forensics readiness – are we there yet?, *International Journal of Cloud Computing*	2022	1	1	Q3		View
61	A Conceptual Framework to Improve Cyber Forensic Administration in Industry 5.0: Qualitative Study Approach, *Forensic Sciences*	2022	1	10			View
62	A Novel Forensic Readiness Framework Applicable to the Drone Forensics Field, *Computational Intelligence and Neuroscience*	2022	1	19	Q1	✓	View
63	A Study of the iSchools Compound Talents Cultivation on Information Management and Digital Forensics in North America, *Documentation, Information and Knowledge*	2022	1	0			View
64	A systematic analysis on the readiness of Blockchain integration in IoT forensics, *Forensic Science International: Digital Investigation*	2022	1	12	Q1	✓	View
65	An extended digital forensic readiness and maturity model, *Forensic Science International: Digital Investigation*	2022	1	13	Q1	✓	View
66	An improved forensic-by-design framework for cloud computing with systems engineering standard compliance, *Forensic Science International: Digital Investigation*	2022	1	10	Q1		View
67	An insight into cloud forensic readiness by leading cloud service providers: a survey, *Computing (Vienna/New York)*	2022	1	3	Q2		View
68	Compliance with Saudi NCA-ECC based on ISO/IEC 27001, *Tehnicki Vjesnik*	2022	1	4	Q3		View
69	Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry, *Sustainability*	2022	1	19	Q1	✓	View
70	Digital forensics evidence management based on proxy re-encryption, *International Journal of Computer Applications in Technology*	2022	1	3	Q3		View
71	Information security and value creation: The performance implications of ISO/IEC 27001, *Computers in Industry*	2022	1	15	Q1		View
72	Modelling of Fuzzy Expert System for an Assessment of Security Information Management System UIS (University Information System), *Tehnicki Vjesnik*	2022	1	6	Q3		View
73	Process-Driven Modelling of Media Forensic Investigations-Considerations on the Example of DeepFake Detection, *Sensors*	2022	1	7	Q1	✓	View
74	Research on 3D Oil Pipeline Information Management and Security Warning System, *Journal of Geomatics*	2022	1	1	Q4		View
75	Research on Machine Learning Algorithm for Internet of Things Information Security Management System Research and Implementation, *Wireless Communications and Mobile Computing*	2022	1	2	Q2		View
76	Research Trends, Challenges, and Emerging Topics in Digital Forensics: A Review of Reviews, *IEEE Access*	2022	1	83	Q1	✓	View
77	Retraction: Design of Enterprise Financial Information Management System Based on Blockchain Technology (Security and Communication Networks (2022) 2022:8 (2566615) DOI: 10.1155/2022/2566615), *Security and Communication Networks*	2022	1	0	Q2	✓	View
78	Retraction: The security of student information management system based upon blockchain (Journal of Electrical and Computer Engineering (2022) 2022 (8186189) DOI: 10.1155/2022/8186189), *Journal of Electrical and Computer Engineering*	2022	1	0	Q2	✓	View
79	Risk Management; Risk Assessment of Information Technology Security System at Bank Using ISO 27001, *Journal of System and Management Sciences*	2022	2	5	Q3		View
80	Secure Mechanism Applied to Big Data for IIoT by Using Security Event and Information Management System (SIEM), *International Journal of Intelligent Engineering and Systems*	2022	1	14	Q3		View
81	Secure Storage Model for Digital Forensic Readiness, *IEEE Access*	2022	1	11	Q1	✓	View
82	Smart Digital Forensic Readiness Model for Shadow IoT Devices, *Applied Sciences (Switzerland)*	2022	1	16	Q2	✓	View
83	The effect of ISO/IEC 27001 standard over open-source intelligence, *PeerJ Computer Science*	2022	1	2	Q2	✓	View
84	The Security of Student Information Management System Based upon Blockchain, *Journal of Electrical and Computer Engineering*	2022	1	3	Q2		View
85	A Comprehensive Risk Management Approach to Information Security in Intelligent Transport Systems, *SAE International Journal of Transportation Cybersecurity and Privacy*	2021	1	5	Q4	✓	View
86	A novel privacy preserving digital forensic readiness provable data possession technique for health care data in cloud, *Journal of Ambient Intelligence and Humanized Computing*	2021	2	24	Q1		View
87	A Survey on Blockchain for Information Systems Management and Security, *Information Processing and Management*	2021	1	436	Q1	✓	View
88	Assessment of Information Security Risk Management System based on ISO/IEC27005 in the Independent High Electoral Commission: A Case Study, *Review of International Geographical Education Online*	2021	1	0			View
89	Avoiding Burnout at the Digital Forensics Coalface: Targeted strategies for forensic agencies in the management of job-related stress, *Forensic Science International: Digital Investigation*	2021	1	6	Q1		View
90	Digital forensics for skulls classification in physical anthropology collection management, *Computers, Materials and Continua*	2021	1	2	Q2		View
91	Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis, *IEEE Transactions on Engineering Management*	2021	2	48	Q1	✓	View
92	Fuzzy Expert System of Information Security Risk Assessment on the Example of Analysis Learning Management Systems, *IEEE Access*	2021	1	23	Q1	✓	View
93	Image Data Security Mechanism Based on the Internet of Things Cardiac Catheterization Laboratory Information Management System Research and Design, *Journal of Healthcare Engineering*	2021	1	5	Q2		View
94	Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0, *Computers and Security*	2021	1	44	Q1	✓	View
95	Information Management and IoT Technology for Safety and Security of Smart Home and Farm Systems, *Journal of Global Information Management*	2021	1	40	Q2		View

96	Inter-regional digital forensic knowledge management: needs, challenges, and solutions, *Journal of Forensic Sciences*	2021	1	5	Q2	✓	View
97	K-FFRaaS: A Generic Model for Financial Forensic Readiness as a Service in Korea, *IEEE Access*	2021	1	2	Q1	✓	View
98	LEChain: A blockchain-based lawful evidence management scheme for digital forensics, *Future Generation Computer Systems*	2021	1	88	Q1	✓	View
99	Next-generation digital forensic readiness BYoD framework, *Security and Communication Networks*	2021	1	7	Q2	✓	View
100	Role of information security-based tourism management system in the intelligent recommendation of tourism resources, *Mathematical Biosciences and Engineering*	2021	1	2	Q2	✓	View
101	Secured Access Control in Security Information and Event Management Systems, *Journal of Information Systems and Telecommunication*	2021	1	8	Q4		View
102	SPEAR SIEM: A Security Information and Event Management system for the Smart Grid, *Computer Networks*	2021	1	55	Q1	✓	View
103	The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda, *TQM Journal*	2021	1	51	Q2	✓	View
104	A natural human language framework for digital forensic readiness in the public cloud, *Australian Journal of Forensic Sciences*	2020	1	14	Q3	✓	View
105	A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues, *IEEE Communications Surveys and Tutorials*	2020	1	596	Q1	✓	View
106	An Ontology-Based Security Risk Management Model for Information Systems, *Arabian Journal for Science and Engineering*	2020	1	30	Q1	✓	View
107	Deep learning based security management of information systems: A comparative study, *Journal of Advances in Information Technology*	2020	1	11	Q2		View
108	Development of secure blockchain system to strengthen distributed information security management, *JP Journal of Heat and Mass Transfer*	2020	1	0	Q4		View
109	Digital transformation risk management in forensic science laboratories, *Forensic Science International*	2020	1	19	Q1	✓	View
110	Effective resource management in digital forensics: An exploratory analysis of triage practices in four English constabularies, *Policing*	2020	1	24	Q1	✓	View
111	ISM application tool, a contribution to address the barrier of information security management system implementation, *Journal of Information and Communication Convergence Engineering*	2020	1	1	Q2		View
112	New Approach for Information Security Evaluation and Management of IT Systems in Educational Institutions, *Journal of Shanghai Jiaotong University (Science)*	2020	1	3	Q3	✓	View
113	Orbit to Orbit Intersatellite Optical Wireless Communications with Customized Information Security Management System, *Menoufia Journal of Electronic Engineering Research*	2020	1	0			View
114	Organizational information security management for sustainable information systems: An unethical employee information security behavior perspective, *Sustainability*	2020	1	16	Q1	✓	View
115	Present a management information system deployment model for improving food security in agricultural sector of Khuzestan Province, *International Journal of Nonlinear Analysis and Applications*	2020	1	0			View
116	Prototype System of Information Security Management of Cereal and Oil Food Whole Supply Chain Based on Blockchain, *Nongye Jixie Xuebao/Transactions of the Chinese Society of Agricultural Machinery*	2020	1	25	Q2		View
117	SWOT analysis of information security management system ISO 27001, *International Journal of Services Operations and Informatics*	2020	2	2	Q4		View
118	Towards a capability maturity model for digital forensic readiness, *Wireless Networks*	2020	1	20	Q2	✓	View
119	A checklist based evaluation framework to measure risk of information security management systems, *International Journal of Information Technology (Singapore)*	2019	1	10	Q2	✓	View
120	Actionable threat intelligence for digital forensics readiness, *Information and Computer Security*	2019	1	13	Q2	✓	View
121	An integrated conceptual model for information system security risk management supported by enterprise architecture management, *Software and Systems Modeling*	2019	1	46	Q1	✓	View
122	Applying heuristics to the selection and prioritisation of security assessment items in software assessment: The case of ISO/IEC 27001, *Acta IMEKO*	2019	1	1	Q3		View
123	Best practices of auditing in an organization using ISO 27001 standard, *International Journal of Recent Technology and Engineering*	2019	1	3			View
124	CFRaaS: Architectural design of a Cloud Forensic Readiness as-a-Service Model using NMB solution as a forensic agent, *African Journal of Science, Technology, Innovation and Development*	2019	1	7	Q3	✓	View
125	Digital behavioral-fingerprint for user attribution in digital forensics: Are we there yet?, *Digital Investigation*	2019	1	24			View
126	Experts reviews of a cloud forensic readiness framework for organizations, *Journal of Cloud Computing*	2019	1	33	Q1	✓	View
127	FReadyPass: a digital forensic ready passport to control access to data across jurisdictional boundaries, *Australian Journal of Forensic Sciences*	2019	1	4	Q3	✓	View
128	Healthcare Data Breaches: Implications for Digital Forensic Readiness, *Journal of Medical Systems*	2019	1	79	Q1	✓	View
129	Implementation of ISO 27001 Standards as GDPR Compliance Facilitator, *Journal of Information Systems Engineering and Management*	2019	1	12			View
130	Improving forensic triage efficiency through Cyber Threat Intelligence, *Future Internet*	2019	1	20	Q2	✓	View
131	LiveBox: A Self-Adaptive Forensic-Ready Service for Drones, *IEEE Access*	2019	1	15	Q1	✓	View
132	Modeling Big Data Management Systems in Information Security, *Automatic Control and Computer Sciences*	2019	1	8	Q3	✓	View
133	SNAPS: Towards building snapshot based provenance system for virtual machines in the cloud environment, *Computers and Security*	2019	1	12	Q1	✓	View
134	The system of systems paradigm to reduce the complexity of data lifecycle management. Case of the security information and event management, *International Journal of System of Systems Engineering*	2019	1	6	Q4	✓	View
135	A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement, *Digital Investigation*	2018	1	15		✓	View
136	A digital forensic readiness architecture for online examinations, *South African Computer Journal*	2018	1	11	Q4		View
137	Adding Digital Forensic Readiness as a security component to the IoT domain, *International Journal on Advanced Science, Engineering and Information Technology*	2018	1	24	Q3		View
138	Advanced approach to information security management system utilizing maturity models in critical infrastructure, *KSII Transactions on Internet and Information Systems*	2018	1	8	Q3		View
139	An analytical analysis of Turkish digital forensics, *Digital Investigation*	2018	1	2			View
140	Functional requirements for adding digital forensic readiness as a security component in IoT environments, *International Journal on Advanced Science, Engineering and Information Technology*	2018	1	6	Q3		View
141	Information security: Self-diagnosis according to ISO/IEC 27001, *IRBM News*	2018	1	0	Q4		View
142	ISO/IEC 27001 implementation in SMEs: Investigation on management of information assets, *Indian Journal of Public Health Research and Development*	2018	1	2			View
143	Monitoring Data Management Information System for Securities Market, *Wireless Personal Communications*	2018	1	6	Q2	✓	View
144	Novel digital forensic readiness technique in the cloud environment, *Australian Journal of Forensic Sciences*	2018	1	43	Q3	✓	View
145	On digital forensic readiness in the cloud using a distributed agent-based solution: issues and challenges, *Australian Journal of Forensic Sciences*	2018	1	31	Q3	✓	View
146	Planning the selection and assignment of security forensics countermeasures, *Journal of Nuclear Engineering and Radiation Science*	2018	1	1	Q3	✓	View
147	Research on digital forensic readiness design in a cloud computing-based smart work environment, *Sustainability*	2018	1	20	Q1	✓	View
148	The need for integrated cybersecurity and safety training, *Journal of Nuclear Engineering and Radiation Science*	2018	1	5	Q3	✓	View

148	The need for integrated cybersecurity and safety training, *Journal of Nuclear Engineering and Radiation Science*	2018	1	5	Q3	✓	View
149	Weighing benefits and risks in aspects of security, privacy and adoption of technology in a value-based healthcare system 15 Commerce, Management, Tourism and Services 1503 Business and Management 08 Information and Computing Sciences 0806 Information Sys, *BMC Medical Informatics and Decision Making*	2018	1	15	Q1		View
150	A methodology for implementing an information security management system based on the family of ISO/IEC 27000 standards, *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*	2017	1	9	Q4		View
151	A Student Information Management System Based on Fingerprint Identification and Data Security Transmission, *Journal of Electrical and Computer Engineering*	2017	1	5	Q2		View
152	Big forensic data management in heterogeneous distributed systems: quick analysis of multimedia forensic data, *Software - Practice and Experience*	2017	1	28	Q2		View
153	Design architecture of digital evidence case management (DECMa): A proposed model for virtual environment digital forensics examination, *Advanced Science Letters*	2017	1	2			View
154	Development of information and management system for laboratory based on open source licensed software with security logs extension, *Journal of Intelligent and Fuzzy Systems*	2017	1	3	Q2		View
155	Forensically ready digital identity management systems, issues of digital identity life cycle and context of usage, *International Journal of Electronic Security and Digital Forensics*	2017	1	2	Q2		View
156	Information security management systems (ISMS) and computer security self-efficacy (CSSE) model comparison, *Advanced Science Letters*	2017	1	0			View
157	Methodology for management of information security in industrial control systems: A proof of concept aligned with enterprise objectives., *Advances in Science, Technology and Engineering Systems*	2017	1	5	Q3		View
158	Tablet Computers and Forensic and Correctional Psychological Assessment: A Randomized Controlled Study, *Law and Human Behavior*	2017	1	7	Q1		View
159	The impact of information system risk management on the frequency and intensity of security incidents, *International Journal of Electrical and Computer Engineering Systems*	2017	1	2	Q4		View
160	A novel security information and event management system for enhancing cyber security in a hydroelectric dam, *International Journal of Critical Infrastructure Protection*	2016	1	19	Q2		View
161	Adaptive evidence collection in the cloud using attack scenarios, *Computers and Security*	2016	1	27	Q1		View
162	An integrated system for information security management with the unified framework, *Journal of Risk Research*	2016	1	8	Q1		View
163	Applying the action-research method to develop a methodology to reduce the installation and maintenance times of Information Security Management Systems, *Future Internet*	2016	1	8	Q2		View
164	Information security in future air traffic management systems, *Journal of Aerospace Information Systems*	2016	1	4	Q2		View
165	Information security management system implementation success factors: A review, *Advanced Science Letters*	2016	1	6			View
166	Information security risk management for computerized health information systems in hospitals: A case study of Iran, *Risk Management and Healthcare Policy*	2016	1	9	Q2		View
167	Information system security commitment: A study of external influences on senior management, *Computers and Security*	2016	1	52	Q1		View
168	Integrated management model of the corporate digital forensic investigation, *Tehnicki Vjesnik*	2016	1	1	Q3		View
169	Security of data and information in vessel traffic management information systems, *Nase More*	2016	1	1	Q3		View

170	Towards an Integrated Management System (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2 standards, *International Journal of Software Engineering and its Applications*	2016	1	7			View
171	Using a standard approach to the design of next generation e-supply chain digital forensic readiness systems, *Transactions of the South African Institute of Electrical Engineers*	2016	1	4	Q4		View
172	A Comprehensive and Harmonized Digital Forensic Investigation Process Model, *Journal of Forensic Sciences*	2015	1	37	Q2		View
173	A novel Dr.KSM approach for information security and risk management in health care systems, *International Journal of Bio-Science and Bio-Technology*	2015	1	4			View
174	A structured approach to integrating audits to create organisational efficiencies: ISO 9001 and ISO 27001 audits, *Total Quality Management and Business Excellence*	2015	1	28	Q1		View
175	A system dynamics model for information security management, *Information and Management*	2015	1	93	Q1		View
176	A Weighted monte carlo simulation approach to risk assessment of information security management system, *International Journal of Enterprise Information Systems*	2015	1	21	Q3		View
177	Analysis of the legal framework for the information security management system of the nsmep, *Eastern-European Journal of Enterprise Technologies*	2015	1	5	Q2		View
178	Digital forensic readiness: Expert perspectives on a theoretical framework, *Computers and Security*	2015	1	50	Q1		View
179	Forensic readiness: Emerging discipline for creating reliable and secure digital evidence, *Journal of Harbin Institute of Technology (New Series)*	2015	1	8	Q4		View
180	Identifying management factors for digital incident responses on Machine-to-Machine services, *Digital Investigation*	2015	1	2			View
181	Information security management as a bridge in cloud systems from private to public organizations, *Sustainability*	2015	1	14	Q1		View
182	Major accident prevention and management of information systems security in technology-based work processes, *Journal of Loss Prevention in the Process Industries*	2015	1	7	Q1		View
183	Software for document management, a modular component of the Information Security Management System (ISMS), *Informacion Tecnologica*	2015	1	5			View
184	A method for forensic artefact collection, analysis and incident response in environments running session initiation protocol and session description protocol, *International Journal of Electronic Security and Digital Forensics*	2014	1	4	Q2		View
185	A study on the improvements of information security management system for environment education institutes, *International Journal of Security and its Applications*	2014	1	1			View
186	Adopting an information security management system in a co-opetition strategy context, *International Journal of Applied Systemic Studies*	2014	1	5	Q4		View
187	Advanced approach to information security management system model for industrial control system, *Scientific World Journal, The*	2014	1	16	Q2		View
188	An enhanced smartphone security model based on information security management system (ISMS), *Electronic Commerce Research*	2014	1	8	Q1		View
189	An information security management database system (ISMDS) for engineering environment supporting organizations with ISMSs, *IEICE Transactions on Information and Systems*	2014	1	5	Q3		View
190	Design and application research on management information system security architecture in digital campus, *Tongxin Xuebao/Journal on Communications*	2014	1	0	Q4		View
191	Effects of implementing information security management systems on the performance of marketing and sales departments, *International Journal of Business Information Systems*	2014	1	9	Q2		View
192	Influencing factors and control of management information system security in furniture enterprises, *Information Technology Journal*	2014	1	0			View
193	Land information management and landed property ownership security: Evidence from state-sponsored court system, *Habitat International*	2014	1	17	Q1		View
194	Secure and reliable electronic record management system using digital forensic technologies, *Journal of Supercomputing*	2014	1	6	Q2		View
195	The design and application of computer security management information system in coal mine, *Open Electrical and Electronic Engineering Journal*	2014	1	0			View

195	The design and application of computer security management information system in coal mine, *Open Electrical and Electronic Engineering Journal*	2014	1	0			View
196	The operational role of security information and event management systems, *IEEE Security and Privacy*	2014	1	141	Q1		View
197	Towards a forensic-aware database solution: Using a secured database replication protocol and transaction management for digital investigations, *Digital Investigation*	2014	1	25			View
198	Towards a systemic framework for digital forensic readiness, *Journal of Computer Information Systems*	2014	1	39	Q1		View
199	A pattern-based method for establishing a cloud-specific information security management system: Establishing information security management systems for clouds considering security, privacy, and legal compliance, *Requirements Engineering*	2013	1	33	Q1		View
200	Erratum to: A pattern-based method for establishing a cloud-specific information security management system (Requirements Eng, 10.1007/s00766-013-0174-7), *Requirements Engineering*	2013	1	1	Q1		View
201	Holistic and law compatible IT security evaluation: Integration of common criteria, ISO 27001/IT-grundschutz and KORA, *International Journal of Information Security and Privacy*	2013	1	14	Q3		View
202	The architecture of a digital forensic readiness management system, *Computers and Security*	2013	3	30	Q1		View
203	A data-driven assessment model for information systems security risk management, *Journal of Computers (Finland)*	2012	1	7			View
204	LOPD Compliance and ISO 27001 legal requirements in the Health Sector, *IEEE Latin America Transactions*	2012	1	3	Q3		View
205	Toward a target and coupling function of three different Information Security Management Systems, *Concurrency Computation Practice and Experience*	2012	1	1	Q2		View
206	Using time-driven activity-based costing to manage digital forensic readiness in large organisations, *Information Systems Frontiers*	2012	1	15	Q1		View
207	A novel security mechanism for hybrid encryption in mineral management information system, *Intelligent Automation and Soft Computing*	2011	1	0	Q3		View
208	Advanced information security management evaluation system, *KSII Transactions on Internet and Information Systems*	2011	1	13	Q3		View
209	An investigation on compliance with ISO 27001 in Cypriot private and public organisations, *International Journal of Services and Standards*	2011	1	3	Q4		View
210	Building foundations for Digital Records Forensics: A comparative study of the concept of reproduction in digital records management and digital forensics, *American Archivist*	2011	1	10	Q2		View
211	Differentiated security levels for personal identifiable information in identity management system, *Expert Systems with Applications*	2011	1	24	Q1		View
212	Evaluating the ISO/IEC 27001 with experts` knowledge for Taiwanese medical center, *Journal of Convergence Information Technology*	2011	1	1			View
213	Improving the quality of information security management systems with ISO27000, *TQM Journal*	2011	1	41	Q2		View
214	Is ISO 27001 worth it?, *Computer Fraud and Security*	2011	1	5	Q2		View
215	[Information security management for remote maintenance service of medical information systems]., *Nihon Hoshasen Gijutsu Gakkai zasshi*	2011	1	0			View
216	Advanced framework for digital forensic technologies and procedures, *Journal of Forensic Sciences*	2010	1	18	Q2		View
217	An audit framework to support information system security management, *International Journal of Electronic Security and Digital Forensics*	2010	1	2	Q2		View
218	Analysis of information security management systems at 5 domestic hospitals with more than 500 beds, *Healthcare Informatics Research*	2010	1	17	Q2		View
219	User participation in information systems security risk management, *MIS Quarterly: Management Information Systems*	2010	1	341	Q1		View
220	[Information security management for health information systems]., *Nippon Hoshasen Gijutsu Gakkai zasshi*	2010	1	0			View
221	Information Systems Security Assurance Management at Municipal Software Solutions, Inc., *International Journal of Information Security and Privacy*	2009	1	0	Q3		View
222	Reaching escape velocity: A practiced approach to information security management system implementation, *Information Management and Computer Security*	2008	1	5			View
223	The role of organizational cultures in information-systems security management: A goal-setting perspective, *Journal of Leadership Studies*	2008	1	3	Q3		View

234	A roadmap for quantifying the efficacy of risk management of information security and interdependent SCADA systems, *Journal of Homeland Security and Emergency Management*	2005	1	40	Q2		View
235	Examining the state of preparedness of Information Technology management in New Zealand for events that may require forensic analysis, *Digital Investigation*	2005	1	3			View
236	Including technical and security risks in the management of information systems: A programmatic risk management model, *Systems Engineering*	2005	1	15	Q2		View
237	Information systems security from a knowledge management perspective, *Information Management and Computer Security*	2005	1	46			View
238	The significance of the Serial Copy Management System (SCMS) in the forensic analysis of digital audio recordings, *International Journal of Speech, Language and the Law*	2005	1	14	Q2		View
239	A study on information security management system evaluation - Assets, threat and vulnerability, *Computer Standards and Interfaces*	2004	1	29	Q1		View
240	An integral framework for information systems security management, *Computers and Security*	2003	1	55	Q1		View
241	An integrated system theory of information security management, *Information Management and Computer Security*	2003	1	119			View
242	Paper: A study on the certification of the information security management systems, *Computer Standards and Interfaces*	2003	1	22	Q1		View
243	Health care management and information systems security: Awareness, training or education?, *International Journal of Medical Informatics*	2000	1	59	Q1		View
244	Information system security management in the new millennium, *Communications of the ACM*	2000	1	296	Q1		View
245	Security in the Management of Information Systems, *Health Care Manager*	1998	1	3	Q3		View
246	Information systems security metrics management, *Computers and Security*	1997	1	5	Q1		View
247	Computers II: Security of data and the management of integrated museum information systems, *Museum Management and Curatorship*	1990	1	1	Q1		View
248	Identity-Based Information Security Management System for Personal Computer Networks, *IEEE Journal on Selected Areas in Communications*	1989	1	36	Q1		View
249	Risk analysis and risk management models for information systems security applications, *Reliability Engineering and System Safety*	1989	1	3	Q1		View
250	Measuring information systems performance: Experience with the management by results system at security pacific bank, *MIS Quarterly: Management Information Systems*	1988	1	44	Q1		View
251	Information systems security: Management success factors, *Computers and Security*	1987	1	13	Q1		View

Gambar grafik dan data tabel diatas menjelaskan bahwa pencarian artikel dengan kata kunci dan parameter yang ditentukan dalam proses identifikasi SLR dapat menjangkau artikel dengan tahun publikasi mulai dari 1987 hingga 2025. *Database scopus* memberikan hasil pencarian yang berhubungan dengan kata kunci tersebut sejumlah 1054 artikel dengan

keterangan hasil pencarian tersebut berdasarkan kata kunci yang terjaring di judul artikel, abstrak, kata kunci yang didefinisikan, isi artikel, serta artikel yang terhubung secara sitasi maupun referensi. Namun dengan mendefinisikan penghubung kata kunci berupa ”OR” dan ”AND” menjadikan hasil pencarian lebih spesifik dan lebih relevan, Total artikel yang terjaring dari pencarian kata kunci yang relevan pada tahap identifikasi ini adalah sejumlah 273 artikel. Hasil tersebut dimasukkan kedalam tahap *screening (filtering)* dengan beberapa kriteria yang dijabarkan pada protokol PRISMA yang menghasilkan luaran seperti terlihat pada visual gambar 3.7. Ringkasan hasil pemrosesan PRISMA dijabarkan pada tabel berikut.

Tabel 4.2. Data pemrosesan protokol PRISMA SLR

Tahapan SLR	**Hasil Awal**	**Pengurangan / *Filtering***	**Hasil Akhir**
Identifikasi Kata Kunci	1054 artikel	Filtering kata kunci dengan operand AND/OR	260
Screening Kata Kunci	260	Duplicate (9), Tahun publikasi (102), Kualitas Q1-Q4 (22), Abstrak tidak ada (1)	126
Creening Exclude	126	*Exclude (7)*	119
Access Retrival	119	Not Retrived, Limitation (47)	72
Retrieval Artikel	72	Ketidak tersediaan artikel karena alasan lain (5)	67
Proses analisa konten artikel	-	-	67
Opsi penambahan artikel dari Data base lokal selain Scopus (jika relevansi artikel yang dianalisa <5%)	51	Opsi penambahan kedalam SLR tahap analisa konten (0)	0
Total artikel yang diproses			**67**

Tabel 4.3. Data Artikel yang diproses analisa dalam SLR

No	**DOI**	**Authos**	**Judul Artikel**	**Tahun**
1.	10.1080/00450618.2016.1194473	Kebande Victor R., Venter H.S.	On *Digital Forensic Readiness* in the *cloud* using a distributed agent-based solution: issues and *Challenges*	2016
2.	10.1080/00450618.2016.1267797	Kebande Victor R., Venter H.S.	Novel *Digital Forensic Readiness* technique in the *cloud* environment	2017

3.	10.1080/00450618.2018.1444090	Trenwith P.M., Venter H.S.	FReadyPass: a *Digital Forensic* ready passport to *control* access to data across jurisdictional boundaries	2018
4.	10.1115/1.4040372	Gupta D., Bajramović E., Hoppe H., Ciriello A.	The Need for Integrated *Cybersecurity* and Safety Training	2018
5.	10.1115/1.4040650	Bajramovic E.	*Plan*ning the Selection and Assignment of *Security Forensic*s Countermeasures	2018
6.	10.3390/su10041203	Kim H.J., Chang H.B.	*Research* on *Digital Forensic Readiness Design* in a *Cloud* Computing Environment	2018
7.	10.1007/s11277-018-5444-8	Zhang L., Zhang X.	Monitoring Data *Management Information System* for Securities Market	2018
8.	10.1007/s11276-018-01920-6	Ludwig Englbrecht, Stefan Meier, Gnther Pernul	Towards a capability maturity *model* for *Digital Forensic Readiness*	2019
9.	10.1016/j.cose.2019.05.021	BKSP Kumar Raju, G Geethakumari	SNAPS: Towards building snapshot-based provenance *system* for virtual machines in the *cloud* environment	2019
10.	10.1080/20421338.2019.1585675	Victor R. Kebande, H.S. Venter	CFRaaS: Architectural *Design* of a *Cloud Forensic Readiness* as-a-Service *Model* using NMB solution as a *Forensic* agent	2019
11.	10.1108/ICS-09-2018-0110	Serketzis N., Katos V., Ilioudis C., Baltatzis D., Pangalos G.J.	Actionable threat intelligence for *Digital Forensic*s *Readiness*	2019
12.	10.1109/ACCESS.2019.2942033	Yijun Yu, Danny Barthaud, Bashar Nuseibeh	LiveBox: A Self-Adaptive *Forensic*-Ready Service for Drones	2019
13.	10.1186/s13677-019-0133-z	Kebande V.R., Karie N.M., Venter H.S.	Experts *Review*s of a *cloud Forensic Readiness Framework* for *Organization*s	2019
14.	10.3390/fi11070162	Serketzis N., Katos V., Ilioudis C., Baltatzis D., Pangalos G.	Improving *Forensic* Triage Efficiency through *Cyber* Threat Intelligence	2019
15.	10.1007/s10270-018-0661-x	Mayer N., Aubert J., Grandry E., Feltus C., Goettelmann E., Wieringa R.	An integrated conceptual *model* for *information system security* risk *Management* supported by enterprise architecture *Management*	2019
16.	10.1007/s41870-019-00302-0	Mortazavi R., Safi-Esfahani F.	A checklist-based evaluation *Framework* to measure risk of *information security Management system*s	2019

17.	10.1504/IJSSE.2019.104173	Assaad M.A., et al.	The *system* of *system*s paradigm to reduce the complexity of data lifecycle *Management*	2019
18.	10.1108/PIJPSM-07-2019-0126	[*Author*s not shown in results]	Effective resource *Management* in *Digital Forensic*s	2019
19.	10.1080/00450618.2020.1789742	Stacey O. Baror, Hein S. Venter, Richard Adeyemi	A natural human language *Framework* for *Digital Forensic Readiness* in the public *cloud*	2020
20.	10.1109/COMST.2019.2962586	Stoyanova M., Nikoloudakis Y., Panagiotakis S., Pallis E., Markakis E.K.	A Survey on the *Internet of thing*s (IoT) *Forensic*s: *Challenges*, *Approaches*, and Open Issues	2020
21.	10.1007/s12204-020-2231-y	Chen M.	New Approach for *Information Security* Evaluation and *Management* of IT *System*s in Educational Institutions	2020
22.	10.1007/s13369-020-04524-4	Arogundade O.T., Abayomi-Alli A.	An Ontology-Based *Security* Risk *Management Model* for *Information System*s	2020
23.	10.1016/j.ipm.2020.102397	Listiawan I., et al.	WALLET-BASED AUTHENTICATION ON COLLEGE *INFORMATION SYSTEM*	2020
24.	10.1109/TEM.2020.2977815	Susanto H., et al.	Exploring the Adoption of the *International Information Security Management* Standard ISO/IEC 27001	2020
25.	10.3390/SU12083163	Chu A.M.Y., So K.P.	An Un*Ethical* Employee *Information Security* Behavior Perspective	2020
26.	10.1016/j.forsciint.2020.110486	Casey E., Souvignet T.R.	*Digital* transformation risk *Management* in *Forensic* science laboratories	2020
27.	10.1007/s10796-021-10165-2	Armel Lefebvre, Marco Spruit	Laboratory *Forensic*s for Open Science *Readiness*: an Investigative Approach to *Research* Data *Management*	2021
28.	10.1016/j.cose.2021.102238	Khairul Akram Zainol Ariffin, Faris Hanif Ahmad	Indicators for maturity and *Readiness* for *Digital Forensic* investigation in era of industrial revolution 4.0	2021
29.	10.1109/ACCESS.2021.3114233	Sung Jin Lee, Gi Bum Kim	K-FFRaaS: A Generic *Model* for Financial *Forensic Readiness* as a Service in Korea	2021

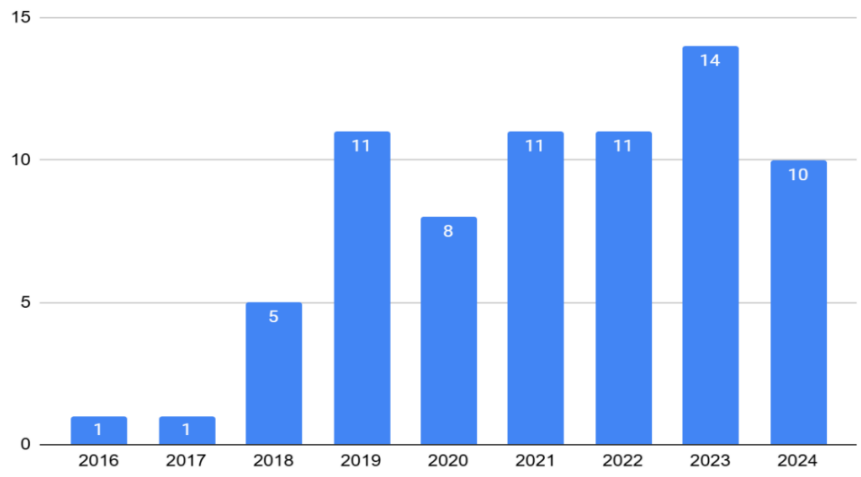
30.	10.1155/2021/6664426	Ali M.I., Kaur S.	Next-Generation *Digital Forensic Readiness* BYOD *Framework*	2021
31.	10.1016/j.comnet.2021.108008	Radoglou-Grammatikis P., Sarigiannidis P., et al.	SPEAR SIEM: A *Security Information* and Event *Management system* for the Smart Grid	2021
32.	10.1109/ACCESS.2021.3129488	Kalinin M., et al.	Fuzzy Expert *System* of *Information Security* Risk *Assessment* on the Example of Analysis Learning *Management System*s	2021
33.	10.3934/mbe.2021394	Nan X., Kanato K.	Role of *information security*-based tourism *Management system* in the intelligent recommendation of tourism resources	2021
34.	10.4271/11-04-01-0003	Vogt T., et al.	A Comprehensive Risk *Management* Approach to *Information Security* in Intelligent Transport *System*s	2021
35.	10.1108/TQM-09-2020-0202	Culot G., Nassimbeni G., Podrecca M., Sartor M.	The ISO/IEC 27001 *information security Management* standard: *literature Review* and theory-based *research* agenda	2021
36.	10.1016/j.future.2020.09.038	Li M., Lal C., Conti M., Hu D.	LE*Chain*: A *blockchain*-based lawful evidence *Management* scheme for *Digital Forensic*s	2021
37.	10.1111/1556-4029.14613	Casey E., Zehnder A.	Inter-regional *Digital Forensic* knowledge *Management*: needs, *Challenges*, and solutions	2021
38.	10.1016/j.fsidi.2022.301349	Felix Bankole, Ayankunle Taiwo, Ivan Claims	An extended *Digital Forensic Readiness* and maturity *model*	2022
39.	10.1016/j.fsidi.2022.301472	Khanji Salam, Alfandi Omar, Ahmad Liza, Kakkengal Lubna, Al-kfairy Mousa	A *systematic* analysis on the *Readiness* of *Blockchain* integration in IoT *Forensic*s	2022
40.	10.1109/ACCESS.2022.3151403	Avinash Singh, Richard Adeyemi Ikuesan, Hein Venter	Secure Storage *Model* for *Digital Forensic Readiness*	2022
41.	10.1109/ACCESS.2022.3154059	Casino Fran, Dasaklis Thomas K., Spathoulas George	*Research* Trends, *Challenges*, and Emerging Topics in *Digital Forensic*s: A *Review* of *Review*s	2022
42.	10.1155/2022/8002963	Alotaibi F.M., Al-Dhaqm A., Al-Otaibi Y.D.	A Novel *Forensic Readiness Framework* Applicable to the Drone *Forensic*s Field	2022

43.	10.3390/app12020730	Friedl S., Pernul G.	Smart *Digital Forensic Readiness Model* for Shadow IoT Devices	2022
44.	10.3390/s22093137	Riess C., Bestagini P., Rössler A., Stamm M.	Process-Driven *Model*ling of Media *Forensic* Investigations-Considerations on the Example of DeepFake Detection	2022
45.	10.3390/su14031269	Di Bona G., et al.	Developing a Risk Analysis Strategy *Framework* for *Impact Assessment* in *Information Security Management System*s	2022
46.	10.7717/PEERJ-CS.810	Qusef A., Alkilani H.	The effect of ISO/IEC 27001 standard over open-source intelligence	2022
47.	10.1016/j.cose.2022.103011	Mazen Azzam, Liliana Pasquale, Gregory Provan, Bashar Nuseibeh	*Forensic Readiness* of industrial *control system*s under stealthy *attack*s	2023
48.	10.1016/j.fsidi.2023.301510	Rais Muhammad Haris, Ahsan Muhammad, Ahmed Irfan	*Digital Forensic Readiness Framework* for material extrusion based 3D printing process	2023
49.	10.1016/j.jisa.2023.103433	Daubner Lukas, Macak Martin, Matulevičius Raimundas, Buhnova Barbora, Maksović Sofija, Pitner Tomas	Addressing insider *attack*s via *Forensic*-ready risk *Management*	2023
50.	10.1109/ACCESS.2023.3268529	Ehtisham Ul Haque, Waseem Abbasi, Sathishkumar Murugesan, Muhammad Shahid	*Cyber Forensic* Investigation Infrastructure of Pakistan: An Analysis of *Cyber* Threat Landscape and *Readiness*	2023
51.	10.1109/ACCESS.2023.3343360	Taiwo Blessing Ogunseyi, Oluwasola Mary Adedayo	Cryptographic Techniques for Data *Privacy* in *Digital Forensic*s	2023
52.	10.1109/TSC.2023.3290474	Monteiro D., Yu Y., Zisman A., Nuseibeh B.	Adaptive Observability for *Forensic*-Ready Microservice *System*s	2023
53.	10.3390/su16209058	Duggal K., Myeong S.	The Influence of *Information Security Management System* Implementation on Financial Performance	2023
54.	10.4018/JGIM.316833	Bolek V., Romana A., Korcek F.	The *Information Security Management System*s in E-Business	2023
55.	10.1007/s10257-023-00646-y	Kamil Y., Lund S., Islam M.S.	*Information security* objectives and the output legitimacy of ISO/IEC 27001	2023

56.	10.1080/19393555.2023.2270984	Hirvonen M., et al.	ISO/IEC 27001:2013 *control*s ranked based on GDPR penalty case analysis	2023
57.	10.1080/19393555.2023.2270984	Suorsa M., Helo P.	ISO/IEC 27001:2013 *control*s ranked based on GDPR penalty case analysis	2023
58.	10.1108/TQM-07-2022-0220	Podrecca M., Sartor M.	Forecasting the diffusion of ISO/IEC 27001: a Grey *model* approach	2023
59.	10.3390/su15075828	Kitsios F., Chatzidimitriou E., Kamariotou M.	The ISO/IEC 27001 *Information Security Management* Standard: How to Extract Value from Data in the IT Sector	2023
60.	10.1016/j.fsidi.2023.301621	Ngo T.H., Le-Khac N.A.	Ontology-based case study *Management* towards bridging training and actual investigation gaps in *Digital Forensic*s	2023
61.	10.1016/j.fsidi.2024.301768	Sabrina Friedl, Günther Pernul	IoT *Forensic*s *Readiness* - influencing factors	2024
62.	10.1109/ACCESS.2024.3483173	Alotibi Gaseb	A High Abstract *Digital Forensic Readiness* Meta*model* for Securing Smart Cities	2024
63.	10.3390/asi7050090	Mpungu C., George C., Mapp G.	*Digital Forensic*s *Readiness* in Big Data Networks: A Novel *Framework* and *Incident Response* Script for Linux-Hadoop Environments	2024
64.	10.3390/fi16120437	AlMutawa A., Ikuesan R., Said H.	Towards a Comprehensive Metaverse *Forensic Framework* Based on Technology Task Fit *Model*	2024
65.	10.3390/info15060363	Daubner L., Buhnova B., Matulevicius R.	ETHI*Core*: *Ethical Compliance* and Oversight *Framework* for *Digital Forensic Readiness*	2024
66.	10.3837/tiis.2024.09.012	Isa I., Ariffin K.A.Z.	Open Source *Tools* for *Digital Forensic* Investigation: Capability, Reliability, Transparency and Legal Requirements	2024
67.	10.3390/info15020109	Alqahtany, S. S., & Syed, T. A.	*Forensic*TransMonitor: A Comprehensive *Blockchain* Approach to Reinvent *Digital Forensic*s and Evidence *Management*	2024
68.	10.1186/s13635-024-00167-2	Chen S.	Retraction Note: The *Design* of network *security* protection trust *Management system*	2024

69.	10.1155/2022/9781939	[Retracted]	The *Security* of Student *Information Management System* Based upon *Blockchain*	2022
70.	10.1155/2022/9803298	[Retracted]	*Design* of Enterprise Financial *Information Management System* Based on *Blockchain* Technology	2022
71.	10.1080/19393555.2024.2305508	[Correction Notice]	Correction	2024
72.	10.1007/s00500-024-10152-z	[Retraction Notice]	Retraction Note: Application of embedded voice and *Digital Forensics system* in financial cost *Management*	2024

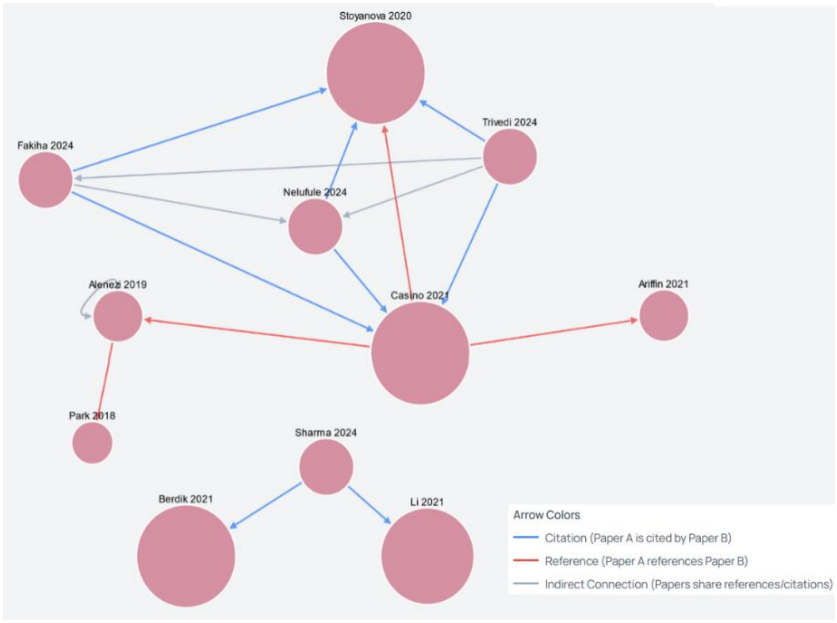
Peneliti mendapatkan 5 artikel yang tidak dapat dilanjutkan ketahap berikutnya karena alasan penarikan dokumen *(retraction)*, dan koreksi *(correction)*, maupun ketidak sesuaian lainnya (5 artikel terahir pada tabel 4.3), sehingga total dokumen yang dapat dilanjutkan ketahap SLR selanjutnya adalah 67 dokumen artikel. Data hasil pencarian dan analisa artikel ini kami eksplorasi lebih lanjut untuk menjawab *research trends* dan korelasinya dengan topik penelitian seperti yang disajikan pada gambar berikut.



Gambar 4.2. Distribusi Artikel berdasarkan tahun publikasi untuk *research trends*

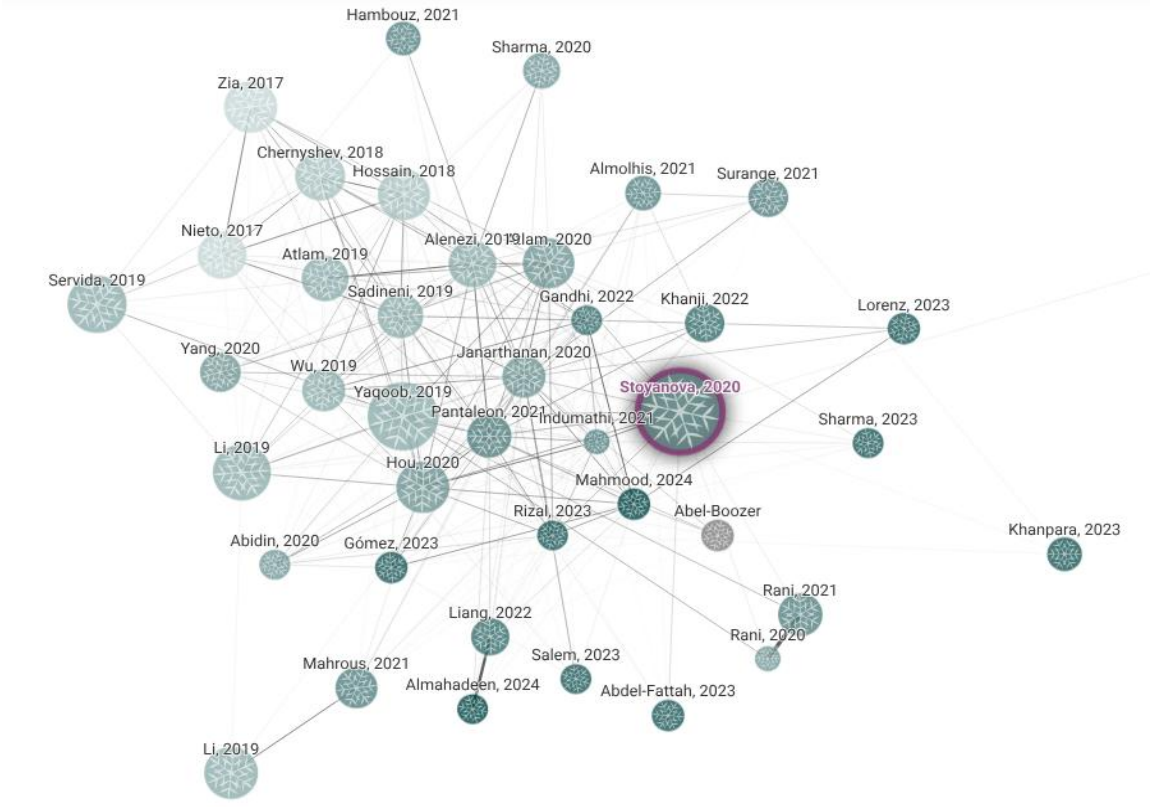
Peneliti melakukan melanjutkan analisa untuk menjawab *most journal impact, most Author, dan most papers* yang berhubungan dengan *research Question*s sebagai bagian dari proses SLR dengan menggunakan *connected papers network analysis* terhadap 16 top artikel untuk mengetahui signifikansi *paper* tersebut terhadap populasi artikel yang dilakukan analisa SLR. berdasarkan 67 artikel yang diproses analisa berdsarkan 16 *top cited articles*,

menghasilkan Total *connected papers* sebanyak 741 *connected papers* dalam populasi seperti disajikan pada gambar berikutseperti yang disajikan pada tabel dan gambar berikut.

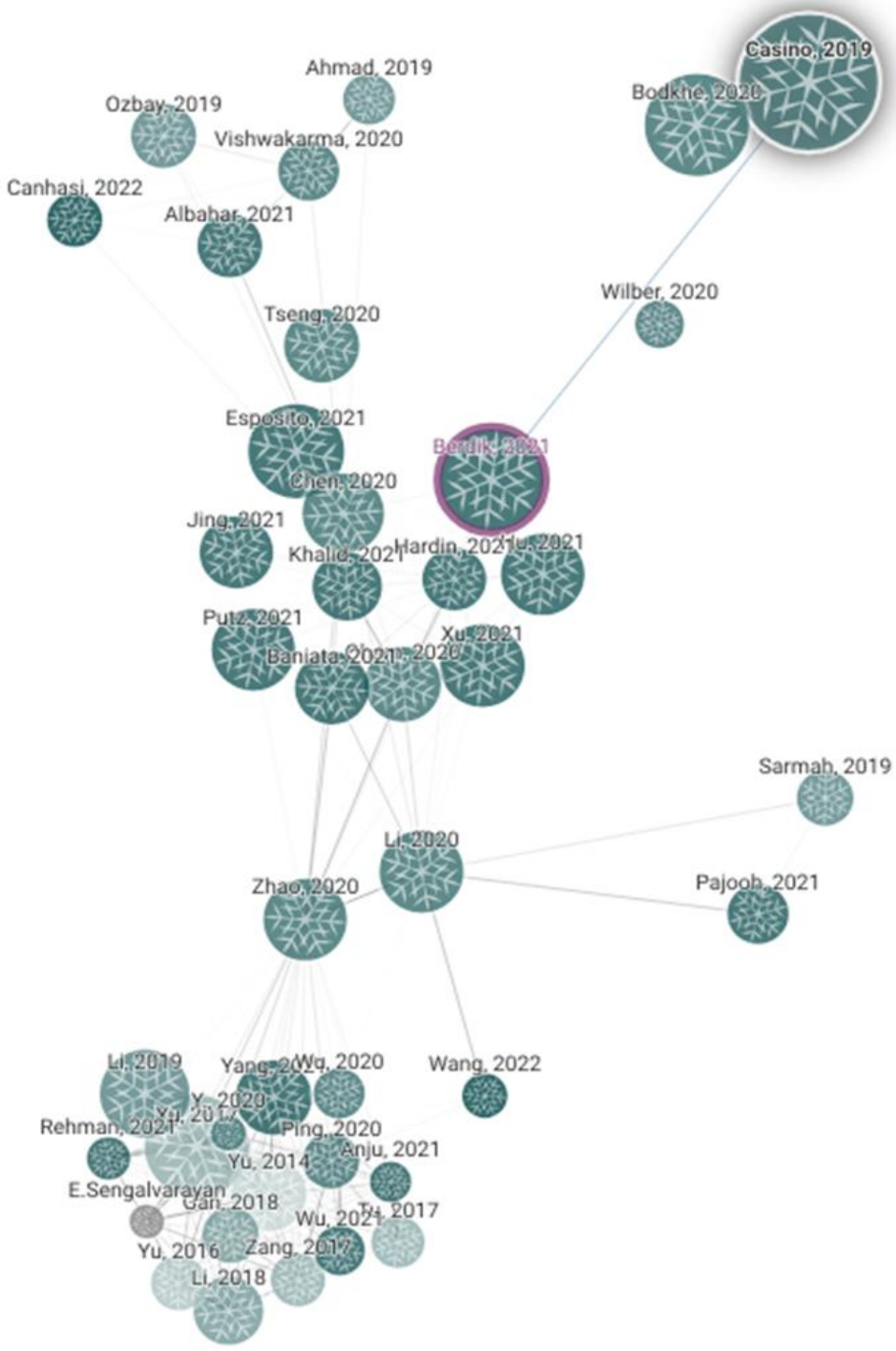


.

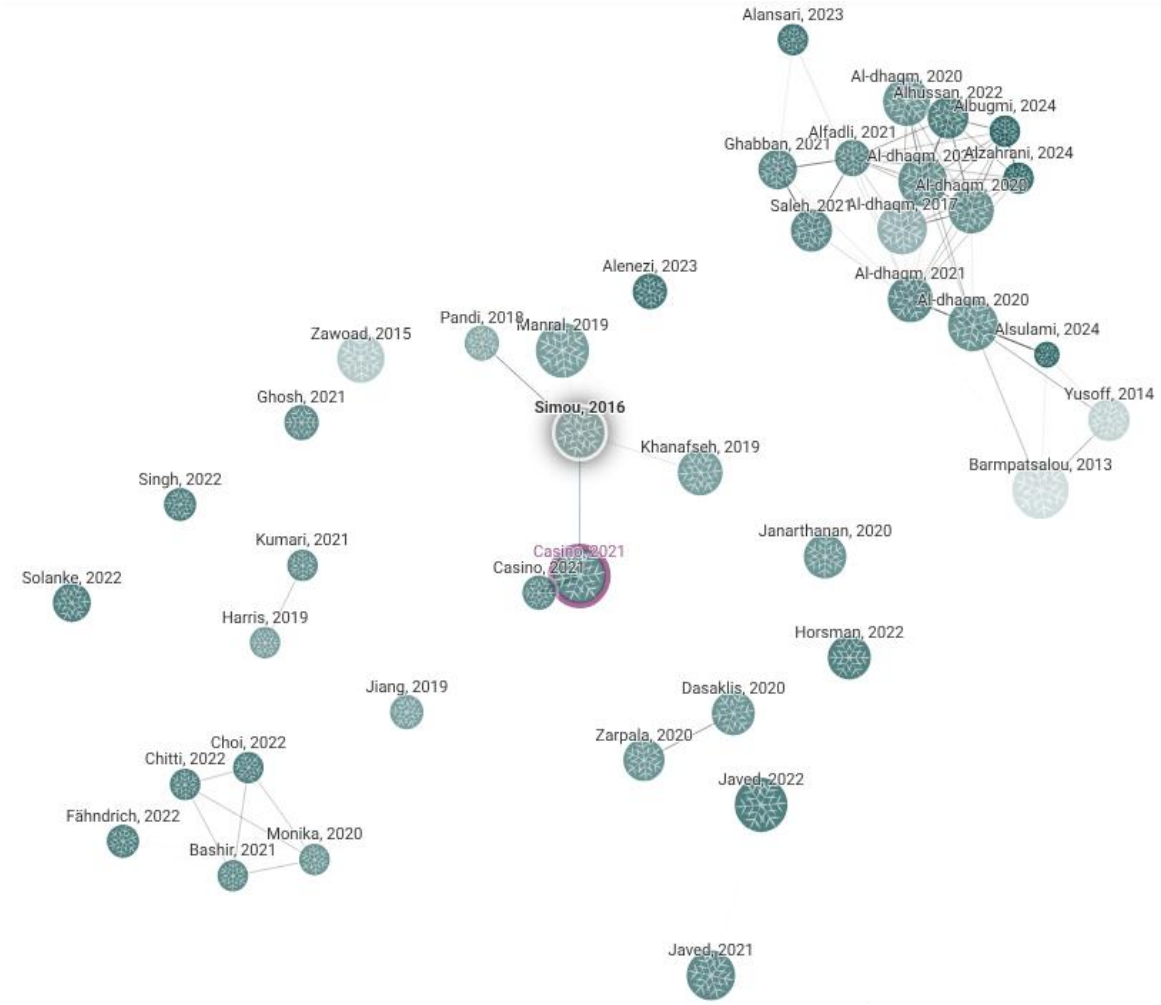
Gambar 4.3. Posisi *Author* yang paling banyak dirujuk (M. Conti 15 refference papers, 596 citations, A Survey on the *Internet of things* (IoT) *Forensics*: *Challenges*, *Approaches*, and Open Issues, 2020) berdasarkan interkoneksi ke top 16 paper SLR yang dianalisa



Gambar 4.4. Visualisasi *connected paper "A Survey on the Internet of things (IoT) Forensics: Challenges, Approaches, and Open Issues"*, terhadap semua paper (global), 597 *citations*.



Gambar 4.5. visualisasi *Connected paper "A Survey on Blockchain for Information Systems Management and Security",* terhadap semua paper (global), 372 *citations*.

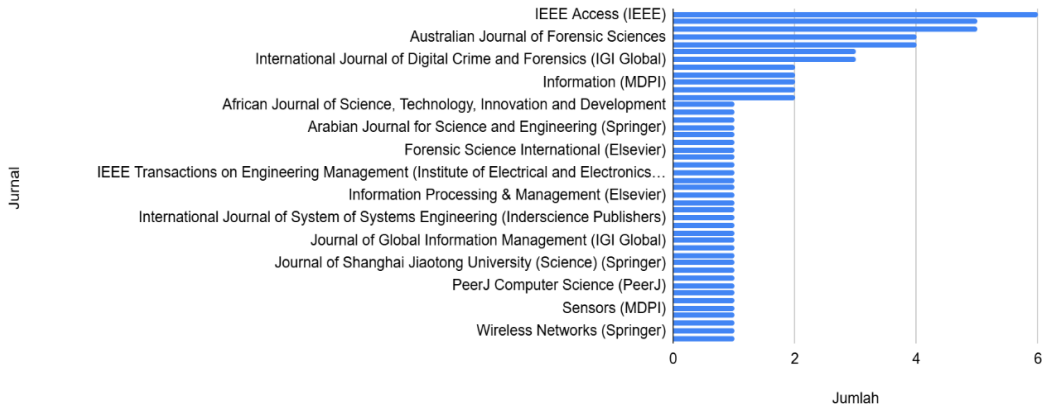


Gambar 4.6. *Connected paper "Research Trends, Challenges, and Emerging Topics in Digital Forensics A Review of Reviews",* terhadap semua paper (global), 83 *citations*.

Tabel 4.4. Data Jumlah Jurnal Publikasi Artikel SLR

No	Jurnal	Jumlah
1.	IEEE Access (IEEE)	6
2.	*Forensic* Science *International*: *Digital* Investigation (Elsevier)	5
3.	Sustainability (MDPI)	5
4.	Australian Journal of *Forensic* Sciences	4
5.	*Security* and Communication Networks (Hindawi)	4
6.	Computers & *Security* (Elsevier)	3
7.	*International* Journal of *Digital* Crime and *Forensic*s (IGI Global)	3
8.	Future *Internet* (MDPI)	2
9.	IEEE Access (Institute of Electrical and Electronics Engineers - IEEE)	2
10.	*Information* (MDPI)	2
11.	Journal of Manufacturing Science and Engineering (American Society of Mechanical Engineers - ASME)	2

12.	The TQM Journal (Emerald Publishing)	2
13.	African Journal of Science, Technology, Innovation and Development	1
14.	Applied Sciences (MDPI)	1
15.	Applied *System* Innovation (MDPI)	1
16.	Arabian Journal for Science and Engineering (Springer)	1
17.	Computer Networks (Elsevier)	1
18.	*Cybersecurity* (Springer)	1
19.	*Forensic* Science *International* (Elsevier)	1
20.	Future Generation Computer *System*s (Elsevier)	1
21.	IEEE Communications Surveys & Tutorials (Institute of Electrical and Electronics Engineers - IEEE)	1
22.	IEEE Transactions on Engineering *Management* (Institute of Electrical and Electronics Engineers - IEEE)	1
23.	IEEE Transactions on Services Computing (IEEE)	1
24.	*Information* and Computer *Security* (Emerald Publishing)	1
25.	*Information* Processing & *Management* (Elsevier)	1
26.	*Information System*s Frontiers (Springer)	1
27.	*Information* Technology and *Management* (Springer)	1
28.	*International* Journal of *System* of *System*s Engineering (Inderscience Publishers)	1
29.	Journal of *Cloud* Computing: Advances, *System*s and Applications (SpringerOpen)	1
30.	Journal of *Forensic* Sciences (Wiley)	1
31.	Journal of Global *Information Management* (IGI Global)	1
32.	Journal of *Information Security* and Applications (Elsevier)	1
33.	Journal of Reliable Intelligent Environments (Springer)	1
34.	Journal of Shanghai Jiaotong University (Science) (Springer)	1
35.	KSII Transactions on *Internet* and *Information System*s (Korea Society of *Internet Information*)	1
36.	Mathematical Biosciences and Engineering (American Institute of Mathematical Sciences)	1
37.	PeerJ Computer Science (PeerJ)	1
38.	Policing: An *International* Journal (Emerald Publishing)	1
39.	SAE *International* Journal of Electrified Vehicles (SAE *International*)	1
40.	Sensors (MDPI)	1
41.	Soft Computing (Springer)	1
42.	Software and *Systems Model*ing (Springer)	1
43.	Wireless Networks (Springer)	1
44.	Wireless Personal Communications (Springer)	1



Gambar 4.7. Grafik Distribusi Jumlah artikel berdasarkan Jurnal

Tabel 4.5. Data Distribusi Lokasi Penelitian

Lokasi	Jml
Jerman	6
Afrika Selatan	6
Inggris	5
Yunani	4
Cina	4
Malaysia	3
Belanda	2
USA	2
UEA	2
Swiss	2
Swedia	2
Rusia	2
Korsel	2
India	2

Lokasi	Jml
Arab Saudi	2
Ceko, Estonia	1
Jepang	1
Australia	1
Prancis	1
Hong Kong	1
Pakistan	1
Kazakhstan	1
Yordania	1
Italia	2
Irlandia	2
Spanyol	1
Pakistan	1
Ghana	1

Lokasi	Jml
Finlandia	1
Nigeria & Turki	2
Norwegia	1
Slovakia	1
Kanada	1
Prancis	1
Iran	1
Yordania	1
Spanyol	1
Slovakia	1
Global	1
Tidak disebutkan	4
TOTAL	**67**

Berdasarkan data sebaran artikel, jurnal publikasi dan tahun terbitnya artikel, serta sebaran lokasi penelitian yang disajikan pada beberapa tabel dan grafik diatas, peneliti merumuskan "Simpulan-2" bahwa penelitian dengan topik integrasi DFR terhadap ISMS telah terkonfirmasi secara global. Hal ini sesuai dengan laporan yang ditulis pada *Center* for *Strategic* and *International* Studies. (2020) yang menyebutkan bahwa Jerman, Afrika Selatan, Inggris, Yunani, dan Cina termasuk dalam negara dengan target serangan siber terbesar. Beberapa negara seperti Amerika Serikat, Rusia, Tiongkok, Iran, dan Korea Utara, yang memiliki infrastruktur kritis yang signifikan, sering menjadi pelaku serangan siber terhadap negara lain sekaligus target seragan dari negara lain terhadap mereka.

Selain itu, peneliti juga menganalisa substansi topik DFR dan ISMS didalam masing-masing artikel apakah memiliki kesesuaian dengan tema penelitian, menggunakan metodologi, *Framework*, standard maupun teori-teori yang terkait dengan DFR dan ISMS, serta menggunakan pendekatan penelitian (kualitatif/kuantitatif) seperti disajikan pada beberapa tabel dan gambar berikut ini.

Tabel 4.6. Data Topik Penelitian dari Artikel yang dianalisa

No	Judul Artikel	Klasifikasi Kesesuaian Topik	Apakah Artikel Menganalisa Dampak DFR/ISMS
1.	On *Digital Forensic Readiness* in the *cloud* using a distributed agent-based solution: issues and *Challenges*	DFR	Ya, DFR & ISMS
2.	Novel *Digital Forensic Readiness* technique in the *cloud* environment	DFR	Ya, DFR
3.	FReadyPass: a *Digital Forensic* ready passport to *control* access to data across jurisdictional boundaries	DFR	Ya, DFR & ISMS
4.	The Need for Integrated *Cybersecurity* and Safety Training	ISMS	Ya, DFR & ISMS
5.	*Plan*ning the Selection and Assignment of *Security Forensic*s Countermeasures	DF	Ya, DFR & ISMS
6.	*Research* on *Digital Forensic Readiness Design* in a *Cloud* Computing Environment	DFR	Ya, DFR
7.	Monitoring Data *Management Information System* for Securities Market	ISMS	Ya, DFR & ISMS
8.	Towards a capability maturity *model* for *Digital Forensic Readiness*	DFR	Ya, ISMS
9.	SNAPS: Towards building snapshot-based provenance *system* for virtual machines in the *cloud* environment	ISMS	Ya, DFR & ISMS
10.	CFRaaS: Architectural *Design* of a *Cloud Forensic Readiness* as-a-Service *Model* using NMB solution as a *Forensic* agent	DFR	Ya, DFR
11.	Actionable threat intelligence for *Digital Forensic*s *Readiness*	DFR	Ya, DFR
12.	LiveBox: A Self-Adaptive *Forensic*-Ready Service for Drones	DFR	Ya, DFR
13.	Experts *Review*s of a *cloud Forensic Readiness Framework* for *Organization*s	DFR	Ya, DFR
14.	Improving *Forensic* Triage Efficiency through *Cyber* Threat Intelligence	ISMS	Ya, DFR
15.	An integrated conceptual *model* for *information system security* risk *Management* supported by enterprise architecture *Management*	ISMS	Ya, DFR & ISMS

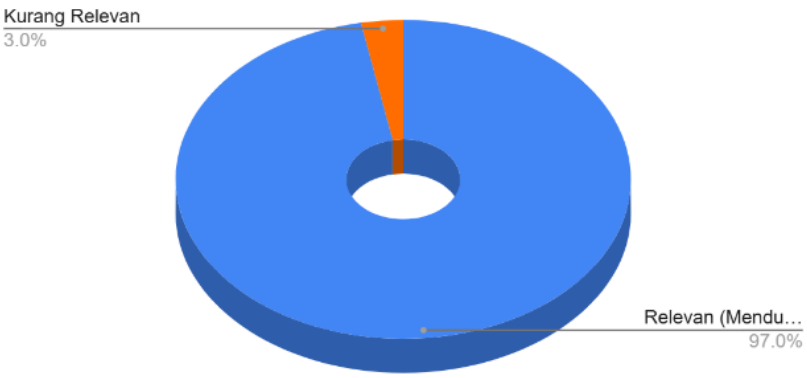
16.	A checklist-based evaluation *Framework* to measure risk of *information security Management systems*	ISMS	Ya, DFR & ISMS
17.	The *system* of *systems* paradigm to reduce the complexity of data lifecycle *Management*	ISMS	Ya, DFR
18.	Effective resource *Management* in *Digital Forensics*	DF	Ya, DFR
19.	A natural human language *Framework* for *Digital Forensic Readiness* in the public *cloud*	DFR	Ya, DFR
20.	A Survey on the *Internet of things* (IoT) *Forensics*: *Challenges*, *Approaches*, and Open Issues	DF	Tidak
21.	New Approach for *Information Security* Evaluation and *Management* of IT *Systems* in Educational Institutions	ISMS	Ya, DFR & ISMS
22.	An Ontology-Based *Security* Risk *Management Model* for *Information Systems*	ISMS	Ya, DFR
23.	WALLET-BASED AUTHENTICATION ON COLLEGE *INFORMATION SYSTEM*	ISMS	Ya, DFR & ISMS
24.	Exploring the Adoption of the *International Information Security Management* Standard ISO/IEC 27001	ISMS	Ya, DFR
25.	*Organizational Information Security Management* for Sustainable *Information Systems*: An Un*Ethical* Employee *Information Security* Behavior Perspective	ISMS	Ya, DFR & ISMS
26.	*Digital* transformation risk *Management* in *Forensic* science laboratories	ISMS	Ya, DFR & ISMS
27.	Laboratory *Forensics* for Open Science *Readiness*: an Investigative Approach to *Research* Data *Management*	DFR	Ya, DFR
28.	Indicators for maturity and *Readiness* for *Digital Forensic* investigation in era of industrial revolution 4.0	DFR	Ya, DFR
29.	K-FFRaaS: A Generic *Model* for Financial *Forensic Readiness* as a Service in Korea	DFR	Ya, DFR
30.	Next-Generation *Digital Forensic Readiness* BYOD *Framework*	DFR	Ya, DFR
31.	SPEAR SIEM: A *Security Information* and Event *Management system* for the Smart Grid	ISMS	Ya, DFR
32.	Fuzzy Expert *System* of *Information Security* Risk *Assessment* on the Example of Analysis Learning *Management Systems*	ISMS	Ya, DFR & ISMS
33.	Role of *information security*-based tourism *Management system* in the intelligent recommendation of tourism resources	ISMS	Ya, DFR & ISMS
34.	A Comprehensive Risk *Management* Approach to *Information Security* in Intelligent Transport *Systems*	ISMS	Ya, DFR & ISMS

35.	The ISO/IEC 27001 *information security Management* standard: *literature Review* and theory-based *research* agenda	ISMS	Ya, DFR & ISMS
36.	LE*Chain*: A *blockchain*-based lawful evidence *Management* scheme for *Digital Forensic*s	DF	Ya, DFR
37.	Inter-regional *Digital Forensic* knowledge *Management*: needs, *Challenges*, and solutions	DF	Ya, DFR
38.	An extended *Digital Forensic Readiness* and maturity *model*	DFR	Ya, DFR
39.	A *systematic* analysis on the *Readiness* of *Blockchain* integration in IoT *Forensic*s	DFR	Ya, DFR
40.	Secure Storage *Model* for *Digital Forensic Readiness*	DFR	Ya, DFR
41.	*Research* Trends, *Challenges*, and Emerging Topics in *Digital Forensic*s: A *Review* of *Review*s	DF	Ya, DFR
42.	A Novel *Forensic Readiness Framework* Applicable to the Drone *Forensic*s Field	DFR	Ya, DFR
43.	Smart *Digital Forensic Readiness Model* for Shadow IoT Devices	DFR	Ya, DFR
44.	Process-Driven *Model*ling of Media *Forensic* Investigations-Considerations on the Example of DeepFake Detection	DF	Ya, DFR
45.	Developing a Risk Analysis Strategy *Framework* for *Impact Assessment* in *Information Security Management System*s	ISMS	Ya, DFR & ISMS
46.	The effect of ISO/IEC 27001 standard over open-source intelligence	ISMS	Ya, DFR & ISMS
47.	*Forensic Readiness* of industrial *control system*s under stealthy *attack*s	DFR	Ya, DFR
48.	*Digital Forensic Readiness Framework* for material extrusion-based 3D printing process	DFR	Ya, DFR
49.	Addressing insider *attack*s via *Forensic*-ready risk *Management*	ISMS	Ya, DFR
50.	*Cyber Forensic* Investigation Infrastructure of Pakistan: An Analysis of *Cyber* Threat Landscape and *Readiness*	DFR	Ya, DFR
51.	Cryptographic Techniques for Data *Privacy* in *Digital Forensic*s	DF	Ya, DFR
52.	Adaptive Observability for *Forensic*-Ready Microservice *System*s	DF	Ya, DFR
53.	The Influence of *Information Security Management System* Implementation on Financial Performance	ISMS	Ya, DFR & ISMS
54.	The *Information Security Management System*s in E-Business	ISMS	Ya, DFR & ISMS
55.	*Information security* objectives and the output legitimacy of ISO/IEC 27001	ISMS	Ya, DFR & ISMS
56.	ISO/IEC 27001:2013 *control*s ranked based on GDPR penalty case analysis	ISMS	Ya, DFR & ISMS

57.	ISO/IEC 27001:2013 *control*s ranked based on GDPR penalty case analysis	ISMS	Ya, DFR & ISMS
58.	Forecasting the diffusion of ISO/IEC 27001: a Grey *model* approach	ISMS	Ya, DFR & ISMS
59.	The ISO/IEC 27001 *Information Security Management* Standard: How to Extract Value from Data in the IT Sector	ISMS	Ya, DFR & ISMS
60.	Ontology-based case study *Management* towards bridging training and actual investigation gaps in *Digital Forensic*s	DF	Ya, DFR
61.	IoT *Forensics Readiness* - influencing factors	DFR	Ya, DFR
62.	A High Abstract *Digital Forensic Readiness* Meta*model* for Securing Smart Cities	DFR	Ya, DFR & ISMS
63.	*Digital Forensic*s *Readiness* in Big Data Networks: A Novel *Framework* and *Incident Response* Script for Linux-Hadoop Environments	DFR	Ya, DFR & ISMS
64.	Towards a Comprehensive Metaverse *Forensic Framework* Based on Technology Task Fit *Model*	DF	Ya, DFR & ISMS
65.	ETHI*Core*: *Ethical Compliance* and Oversight *Framework* for *Digital Forensic Readiness*	DFR	Ya, DFR & ISMS
66.	Open Source *Tools* for *Digital Forensic* Investigation: Capability, Reliability, Transparency and Legal Requirements	DF	Ya, DFR
67.	The *Security* of Student *Information Management System* Based upon *Blockchain*	ISMS	Tidak
68.	*Design* of Enterprise Financial *Information Management System* Based on *Blockchain* Technology	ISMS	Ya, DFR
69.	Retraction Note: The *Design* of network *security* protection trust *Management system*	ISMS	Tidak
70.	Correction	ISMS	Tidak
71.	Retraction Note: Application of embedded voice and *Digital Forensic*s *system* in financial cost *Management*	DF	Tidak
72.	*Forensic*TransMonitor: A Comprehensive *Blockchain* Approach to Reinvent *Digital Forensic*s and Evidence *Management*	DF	Tidak

Tabel 4.7. Data Rekapitulasi Jumlah Topik Artikel

Topik	Jumlah	%
Digital Forensic	14	19,5
Digital Forensic Readiness	26	36,1
Information Security Management System	32	44,4

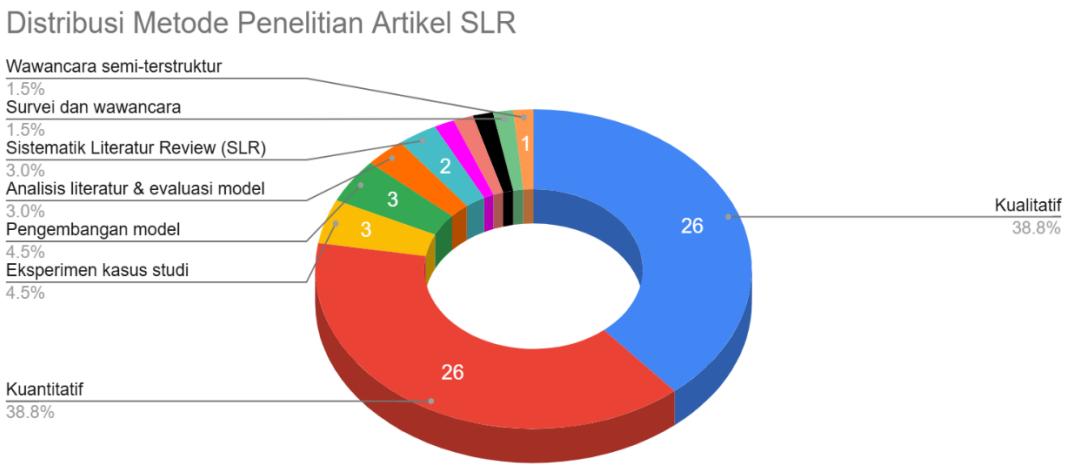


Gambar 4.8.Distribusi relevansi artikel penelitian dengan topik DF-ISMS

Berdasarkan data kesesuaian tema DFR-ISMS, ketersediaan analisa terkait DFR-ISMS yang dianalisa dan divisualisasi pada beberapa tabel dan grafik diatas, peneliti merumuskan "Simpulan-3" bahwa penelitian dengan topik integrasi DFR terhadap ISMS memiliki urgensi suatu organisasi terhadap penerapan DFR (56%) terhadap ISMS (44%). Artinya organisasi membutuhkan DFR dan ISMS untuk mengelola dan memastikan keamanan data dan informasi yang mereka miliki.Perumusan Simpulan-3 yang berbasis data yang dianalisa menggunakan SLR ini ternyata sejalan dengan hasil penelitian Wijatmoko, T. E. (2020) dengan judul Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Kantor Wilayah Kementerian Hukum dan HAM DIY. CyberSecurity dan Forensik Digital yang menghasilkan kesimpulan penelitian pentingnya evaluasi keamanan informasi yang dapat ditingkatkan melalui integrasi DFR dalam ISMS.

Tabel 4.8. Distribusi pendekatan metode penelitian yang digunakan

Metode Penelitian	**Jumlah**
Kualitatif	26
Kuantitatif	26
Eksperimen kasus studi	3
Pengembangan *model*	3
Analisis literatur & evaluasi *model*	2
Sistematik Literatur *Review* (SLR)	2
Kualitatif dg desain *Framework*	1
Kualitatif dg prototipe	1
Pendekatan konseptual	1
Survei dan wawancara	1
Wawancara semi-terstruktur	1



Gambar 4.9. Grafik Distribusi relevansi artikel penelitian dengan topik DF-ISMS

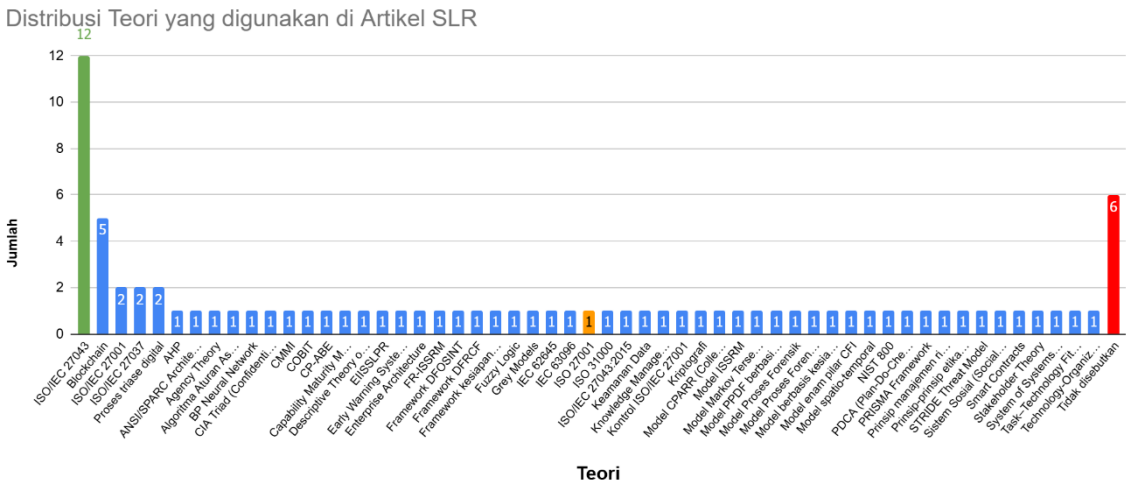
Tabel 4.9. Distribusi Analisa dampak penerapan DFR/ISMS Organisasi

Metode Penelitian	Ya	Tidak
DFR berdampak pada organisasi	16	0
ISMS berdampak pada organisasi	25	0
DFR & ISMS berdampak pada organisasi	13	0
Tidak disebutkan	13	

Berdasarkan data substanasi tema dampak DFR-ISMS yang dianalisa pada setiap artikel yang disajikan pada data maupun grafik diatas, peneliti merumuskan "Simpulan-4" bahwa DFR dan ISMS berdampak dalam peningkatan pengamanan data dan informasi organisasi. ISMS memiliki peranan lebih besar daripada DFR sebagai alat untuk penanggulangan dampak keamanan data dan informasi pada organisasi. Rumusan simpulan-4 ini juga terkonfirmasi ata sesuai dengan penelitian Wijatmoko, T. E. (2020) dengan judul Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Kantor Wilayah Kementerian Hukum dan HAM DIY. CyberSecurity dan Forensik Digital yang menghasilkan kesimpulan penelitian pentingnya evaluasi keamanan informasi yang dapat ditingkatkan melalui integrasi DFR dalam ISMS. Selain itu, penelitian Hayeri Khyavi, M. (2020). ISMS Role in the Improvement of Digital Forensics Related Process in SOC's yang menyimpulkan bahwa implementasi ISMS yang sesuai dengan ISO 27001:2013 dapat meningkatkan kredibilitas informasi yang dikumpulkan dalam penyelidikan forensik digital, sehingga memperkuat pengamanan data dan informasi.

Tabel 4.10. Distribusi teori yang digunakan pada artikel yang dianalisa

Teori	Jumlah	Teori	Jumlah
ISO/IEC 27043	13	IEC 62645	1
Blockchain	5	IEC 63096	1
ISO/IEC 27001	4	ISO 31000	1
ISO/IEC 27037	2	COBIT	1
Proses triase *Digital*	2	PRISMA *Framework*	1
AHP	1	Keamanan Data	1
ANSI/SPARC Architecture	1	Early Warning *System* (EWS)	1
Agency Theory	1	STRIDE Threat *Model*	1
Algoritma Aturan Asosiasi	1	Kriptografi	1
BP Neural Network	1	*Model* CPARR	1
CIA Triad	1	*Model* ISSRM	1
CMMI	1	*Model* Markov	1
Capability Maturity *Model* (CMM)		*Model* PPDF berbasis kriptografi	1
CP-ABE	1	*Model* berbasis DFR	1
Descriptive Theory of *Information*	1	*Model* Proses Forensik *Digital*	1
EIISSLPR	1	*Model* Proses Forensik	1
Knowledge *Management*	1	*Model* enam pilar CFI	1
Enterprise Architecture	1	*Model* spatio-temporal	1
FR-ISSRM	1	NIST 800	1
DFR untuk big data	1	IEC 62645	1
Framework DF-OSINT	1	Prinsip manajemen risiko *Digital*	1
Fuzzy Logic	1	Prinsip-prinsip etika *Digital*	1
DFRCF *Framework*	1	Smart Contracts	1
Technology-*Organization*-Environment (TOE)	1	Sistem Sosial (Social *System*s Thinking)	1
Stakeholder Theory	1	Grey *Model*s	1
Tidak disebutkan			6



Gambar 4.10. Grafik Distribusi teori yang digunakan pada artikel yang dianalisa

Tabel 4.11. Data rekap usulan *Framework* pada artikel yang dianalisa

Usulan *Framework*	**Jumlah**	**Usulan *Framework***	**Jumlah**
DFR - ISMS	18	LiveBox - ISMS	1
ISMS	9	SEMEIS - ISMS	1
Cloud Forensic-ISMS	4	Ontology *Model* ISMS	1
Blockchain Sec.*Framework*	3	SecureRS - ISMS	1
IoT *Forensic* - ISMS	2	ICS *Readiness* - ISMS	1
BYOD *Framework* - ISMS	2	*Ransomware Readiness* - ISMS	1
DF - ISMS	2	CFRaaS - ISMS	1
K-FFRaaS - ISMS	1	CPARR - ISMS	1
Digital Forensic Metaverse - ISMS	1	ISSRM - ISMS	1
DeepFake-ISMS	1	Evaluasi DFR - ISMS	1
Counter Measure *Framework*	1	Teknologi Baru di ISMS	1
DFR-ISMS: OSINT	1	SNAPS	1
DFR-ISMS: SIEM	1	Fuzzy *Model* - ISMS	1
OpenSource ISMS	1	SoS - ISMS	1
Treat Intel - ISMS	1	DFR-ISMS Awarenes	1
Forensic Lab - ISMS	1	LiveBox - ISMS	1
LE*Chain* - ISMS	1	SEMEIS - ISMS	1

Berdasarkan data substanasi tema DFR-ISMS yang dianalisa pada setiap artikel, ketersediaan standar apa saja yang perlu disiapkan organisasi dapat dijawab dengan mengambil data dan tabel diatas. Peneliti merumuskan "Simpulan-5" bahwa Organisasi memerlukan standar DFR dan ISMS berbasis ISO dibandingkan dengan standar lainnya (seperti NIST atau *best practice* lainnya yang lebih spesifik). Rumusan simpulan yang dianalisa dari data SLR ini sejalan dengan survey dari tim riset vendor platform dan aplikasi keamanan yaitu Tenable Security yang merilis laporan (dimension report, 2018) dengan

judul ”*Trends In Security Framework Adoption: A Survey of it and Security Professionals”* menyatakan bahwa dari 388 perusahaan enterprise diseluruh dunia yang disurvey, 47% diantaranya menggunakan PCI standard, 35% menggunakan ISO Standard, 32 menerapkan CIS standard, 29% menggunakan NIST Framework, dan sisanya 16% menerapkan *framework* lainnya (termasuk DFR) serta 3% tidak menerapkan standar/framework apapun.

Sampai pada tahap ini, beberapa pertanyaan penelitian telah dapat dijawab seperti tersaji pada tabel berikut ini.

Tabel 4.12. Pertanyaan dan Jawaban *Research Question* SLR RQ1-RQ3

ID	Pertanyaan Penelitian	Jawaban
RQ1	Bagaimana penerapan integrasi *Digital Forensic Readiness* (DFR) dan *Information Security Management System* (ISMS) ISO 27001 secara bersamaan di organisasi pemerintahan, baik di Indonesia maupun di luar negeri, berdasarkan data yang diperoleh dari artikel jurnal yang dipublikasikan antara 2018-2025 ?	DFR dan ISMS secara global dibutuhkan dalam pengelolaan keamanan. Mayoritas organisasi menggunakan salah satu dari keduanya. Namun DFR dan ISMS diterapkan secara terpisah (tidak terintegrasi) oleh beberapa organisasi. Hasil ini didapat dari data distribusi artikel berdasarkan raw data lokasi jurnal, analisis metode penerapan, dan beberapa data penunjang lainnya yang dirumuskan pada "Simpulan-1, 2, dan 3".
RQ2	Apa dampak penerapan integrasi DFR dan ISMS secara bersamaan di organisasi pemerintahan, baik di Indonesia maupun di luar negeri, berdasarkan analisis literatur yang tersedia antara 2018-2025?	Penerapan DFR dan ISMS memiliki dampak positif dalam peningkatan keamanan data dan informasi dalam organisasi pemerintah. Hal ini didapat dari data serta rumusan "Simpulan-4 & 5"
RQ3	Bagaimana merancang *Framework Model* Integrasi *Digital Forensic Readiness*	1. Menganalisa beberapa usulan *Framework* yang terdapat pada beberapa artikel yang dianalisa.

	(DFR) ke dalam ISMS ISO 27001 bagi organisasi pemerintahan, berdasarkan hasil analisis literatur yang ada?	2. Membandingkan kapabilitas dan karakteristik masing-masing *Framework model* maupun standar yang sudah eksiting. 3. Menerapkan rumusan kebutuhan pe*model*an (dijabarkan pada bab 4.2)

Berdasarkan proses SLR yang dijabarkan dengan data pada beberapa tabel dan grafik diatas, tema DFR untuk mendukung ISMS/SMKI telah diteliti oleh banyak peneliti didunia. DFR memiliki peran dalam melengkapi ISMS yang diterapkan di organisasi pemerintah, terbukti dari penelitian ini dengan menggunakan SLR, tema DFR, ISMS, dan Egov ditemukan pada 1054 publikasi internasional namun dengan tujuan yang beragam serta keterkaitan yang belum terdefinisi. SLR dengan protokol PRISMA menghasilkan 64 dokumen yang dianalisis dan menghasilkan beberapa poin kesimpulan, antara lain:

1. Tema *Digital Forensic Readiness* dan ISMS sekaligus pengaruhnya terhadap keamanan data/informasi memiliki trend positif yang dianalisa dan dilakukan penelitian dalam skala global, dibuktikan dengan grafik tren distribusi artikel penelitian selama setidaknya 8 tahun terahir. Selain itu artikel yang membahas topik DFR dan ada kaitannya dengan ISMS disitasi oleh banyak sekali peneliti dibuktikan dengan *connected papers* artikel penelitian yang bereputasi internasional
2. Tema DFR yang berhubugnan dengan ISMS diteliti oleh mayoritas peneliti yang memiliki reputasi tinggi, dibuktikan dengan tabel sebaran negara penelitian serta sumber data base artikel yang berkualitas (Scopus Q1,Q2,Q3,Q4)
3. Metode, Standar dan teori yang banyak digunakan peneliti untuk menjawab permasalahan dalam penelitian mereka berkisar pada ISO 27000 family standard, selain itu juga terdapat beberapa standar lain seperti NIST 800 serta standar lainnya yang disesuaikan dengan objektif dan area penelitian.
4. Setidaknya terdapat 23 usulan *Framework* dari 64 artikel yang diteliti mengusulkan tema integrasi DFR kedalam ISMS dengan menggunakan pendekatan kualitatif maupun kuantitatif yang disesuaikan dengan objektif dan area implementasi di organisasi.

5. Kesimpulan akhir dari proses SLR ini adalah konfirmasi bahwa topik DFR dibutuhkan dalam area ISMS untuk kematangan dan kesiapan organisasi dalam mengamanakan aset informasi melalui ISMS serta memastikan penanganan insiden melalui DFR.

4.2 *Framework Model*

Berdasarkan pembahasan sub bab 3.2 dijelaakan beberapa *DF Framework* yang telah dan masih diusulkan untuk dapat digunakan organisasi sebagai tindakan preventive maupun pro-active penanganan insiden pada *information technology* (IT) maupun *information system* (IS), antara lain:

1. *Digital Forensics and Incident Response* (DFIR)
   Framework: Collection, Examination, Analysis, dan Reporting
   DFIR menawarkan *Framework* yang secara praktis dapat langsung digunakan pada *wide range organisation tipe*, serta tujuan dan kondisi yang beragam (*general*).
2. *ISO/IEC 27037 dan NIST SP 800-86*
   Framework: Identification, Collection, Acquisition and Preservation
   ISO 27037 merupakan *Framework* sekaligus standar yang memiliki dukungan luas, dukungan terhadap sertifikasi kelayakan implementasinya dalam organisasi, serta strategi dan pemenuhan kebijakan dan regulasi serta kelayakan aspek hukum terhadap kasus tertentu. Sedangkan NIST memiliki kelebihan simpel, praktis, dan dapat langsung diterapkan pada organisasi yang memiliki keterbatasan maupun kedalaman kompleksitas tertentu.
3. *Ethicore Framework*
   Framework: DF Readiness Map berdasarkan Data Examination Layer, Forensic Preparation Layer, Stages layer, Identifitacion Layer, Motivation Layer, Legal Advisory Layer dan Security Layer
   Ethicore menawarkan pendekatan yang lebih kompleks, komprehensif untuk mengelola aktivitas DF pada organisasi yang memerlukan pemrosesan dan pembuktian dengan level kredibilitas tinggi seperti organisasi pemerintahan tinggi negara, lembaga penegak hukum dan organisasi lainnya yang menangani kasus dengan kompleksitas dan memerlukan pemrosesan presisi tinggi.

4. *Cloud Forensic Readiness Framework*

   Framework: implementasi Digital Fprensic berdasarkan IaaS, Paas, SaaS

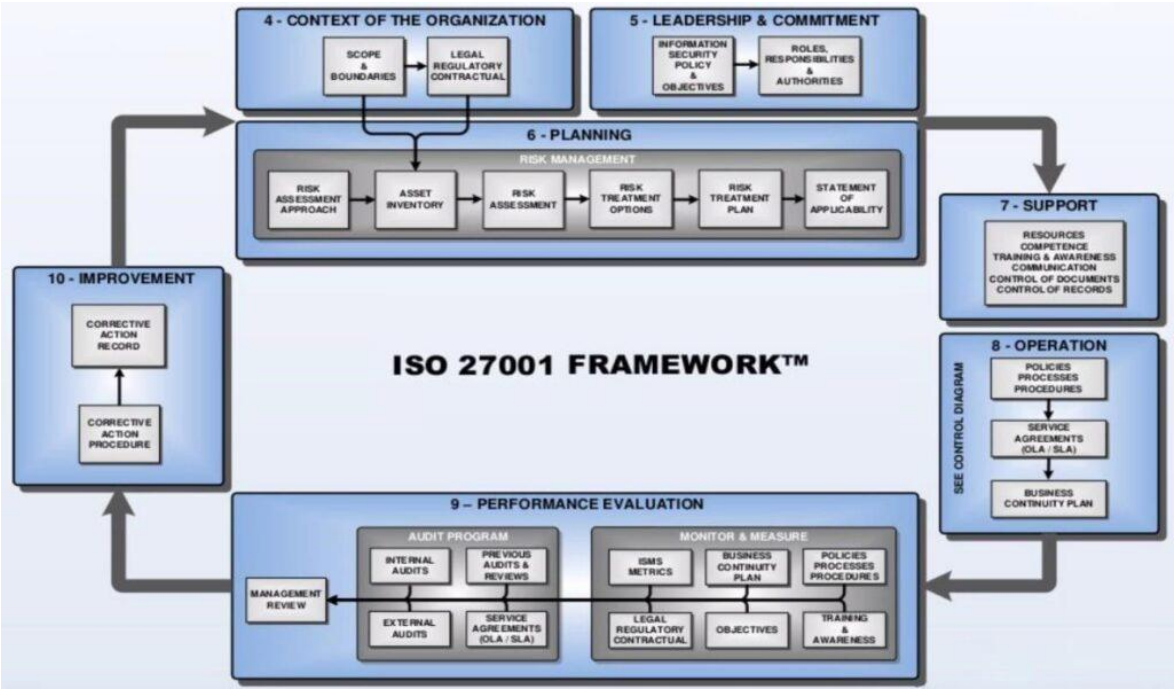
   Framework ini ditujukan untuk memastikan pemrosesan DF pada platform berbagi pakai (IaaS, PaaS, SaaS) dapat dimungkinkan.

5. *Proactive Digital Forensic* (ProDF)

   Framework: Maping DF Readiness, Enhanced Governance Structure & Infosec Performace melalui *Multi Layer Framework yaitu Legal and Judiciary Layer, Governance Layer, Policy Layer, Technology Layer, Process Layer, dan People Layer.*

   Framework ini cocok digunakan untuk mayoritas organisasi dengan skala medium enterprise corporate yang mau memastikan kesiapan pengamanan data dan informasi melalui proses preventif proaktif *Digital* forensik.

Beberapa *Framework* tersebut diatas memiliki karakteristik, keunggulan dan keterbatasan masing-masing, serta area implementasi/peruntukan penggunaan ppada situasi dan kondisi yang spesifik. Peneliti juga melakukan analisa terhadap ISMS Component dan kriteria kunci yang dapat diintegrasikan dengan DFR *Framework* yang akan diusulkan.



Gambar 4.11. *ISO 27001 ISMS Framework Components*

Komponen ISO 27001 ISMS sebagaimana divisualisasikan pada gambar diatas, antara lain:

1. *Context of Organisation* (kalusul 4)
2. *Leadership and Commitment* (kalusul 5)
3. *Planning* (kalusul 6)
4. *Support* (kalusul 7)
5. *Operation* (kalusul 8)
6. *Performance Evaluation* (kalusul 9)
7. *Improvement* (kalusul 10)
8. *Annex Control* (tambahan untuk mendukung klausul iso yang terdefinisi)

Komponen tersebut diatas perlu dipetakan dengan kebutuhan *Digital Forensic* Standard, sehingga terdapat aspek DF yang dapat diintegrasikan dengan klausul ISMS tersebut. Klausul ISMS ISO 27001 yang dapat diintegrasikan dengan *Digital Forensic Proses* antara lain:

1. *Planning* (kalusul 6)

   Pada klausul ini, organisasi harus menilai dan merencanakan kontrol untuk mengelola risiko yang teridentifikasi, termasuk risiko yang terkait dengan forensik *Digital*. Sedangkan ISO/IEC 27037 yang memberikan pedoman untuk identifikasi dan pengumpulan bukti *Digital*, dapat diintegrasikan dalam proses ini dengan menentukan kontrol forensik yang diperlukan untuk pengumpulan bukti yang sah dan terorganisir. Organisasi dapat merencanakan dan mengintegrasikan kesiapan forensik *Digital* ke dalam sistem manajemen keamanan informasi untuk memastikan bahwa mereka siap menangani insiden dan mengumpulkan bukti secara sah tanpa mengganggu operasi berdasarkan rekomendasi dari standar yang diacu.
2. *Support* (kalusul 7)

   Dukungan berdasarkan kemampuan dan kesdiaan sumberdaya organisasi yang sesuai dengan ISO/IEC 27001 bisa dihubungkan langsung dengan kesiapan sumberdaya berdasarkan standar ISO/IEC 27037, ISO/IEC 27042, ISO/IEC 27043 atau standar lainnya yang berhubugnan dengan DF, untuk memastikan bahwa organisasi sudah siap dalam mengelola sumberdaya keamanan dan siap dalam pemrosesan/pengelolaan DF.
3. *Operation* (kalusul 8)

Proses pengelolaan dan implementasi kontrol yang sesuai dengan ISO/IEC 27001 bisa dihubungkan langsung dengan ISO/IEC 27037 dan ISO/IEC 27043 untuk memastikan bahwa organisasi tidak hanya mengelola keamanan informasi secara proaktif, tetapi juga memiliki mekanisme yang memungkinkan pengumpulan bukti *Digital* yang diperlukan selama penanganan insiden keamanan. ISO/IEC 27043, yang memberikan panduan mengenai investigasi insiden, dapat diterapkan untuk mendefinisikan langkah-langkah proses investigasi dan pengelolaan bukti *Digital* secara tepat. Penggunaan standar, *Framework* maupun best practice DF lainnya juga sangat dimungkinkan diterapkan.

4. *Performance Evaluation* (kalusul 9)

   Organisasi harus memantau dan mengevaluasi efektivitas kontrol yang diterapkan dalam ISMS. Dalam konteks forensik *Digital*, ISO/IEC 27037 dan ISO/IEC 27042 dapat diterapkan untuk memastikan bahwa prosedur pengumpulan bukti dan teknik analisis forensik telah diterapkan dengan benar. ISO/IEC 27043 juga membantu organisasi untuk mengevaluasi apakah proses pengumpulan bukti selama insiden dijalankan sesuai dengan prosedur forensik yang diterima. Penggunaan standar maupun *Framework* DF lainnya juga sangat dimungkinkan diterapkan.

5. *Improvement* (kalusul 10)

   Organisasi harus mengambil tindakan korektif jika hasil evaluasi atau audit terhadap penerapan ISMS ditemukan kontrol terhadap pengelolaan bukti *Digital* atau investigasi insiden tidak efektif. Proses korektif ini bisa mengintegrasikan dengan ISO/IEC 27037 untuk meninjau dan memperbaiki prosedur pengumpulan bukti *Digital* yang spesifik. Tindakan perbaikan dapat mencakup peningkatan prosedur pengumpulan bukti, perbaikan dokumentasi, atau penambahan kontrol baru untuk mengatasi kekurangan yang ditemukan selama investigasi insiden.

Agar dapat mengintegrasikan DFR kedalam ISMS sebagaimana penjelasan keempat poin diatas, organisasi juga membutuhkan beberapa aspek untuk memastikan penerapannya sesuai dengan situasi, kondisi dan kemampuan sumberdaya organisasi yang dimiliki, yaitu antara lain:

1. Aspek Ruang Lingkup dan Fokus.

   Ruanglingkup dan fokus perlu didefinisikan berdasarkan regulasi, proses bisnis organisasi, serta tujuan/capaian yang diinginkan.

2. Kesiapan dan Respons Insiden

ISO 27001 mengharuskan organisasi untuk memiliki rencana respons insiden *(Incident Response Plan)*. ISO 27037 sebagai basis pemrosesan *Digital Forensic* terbukti mendukung kebutuhan pada aspek ini dengan menyediakan pedoman yang memastikan bukti *Digital* yang relevan dapat dikumpulkan dan dilindungi selama proses respons insiden.

3. Komplementaritas dalam Investigasi Forensik *Digital*

   Beberapa aspek pada ISO 27001 ISMS yang dapat dipetakan kedalam proses DF berdasarkan ISO 27037, ISO 27042, ISO 27043, NIST SP 800-86, atau lainnya, perlu disesuaikan dengan sumberdaya dan rencana penanganan yang telah ditetapkan, seperti diantaranya kesiapan alat, teknik, prosedur, tata kelola dan personil yang sesuai dan memadai untuk mendukung proses tersebut.

4. Pengelolaan Risiko dan Bukti *Digital*

   ISO 27001 berbasis pada identifikasi, analisis/perhitungan serta langkah mitigasi risiko berdasarkan kriteria tertentu untuk memastikan keamanan aset data dan informasi. ISO 27037, ISO 27042, ISO 27043, yang berbasis DF proses mendukung pendekatan ini dengan memastikan bahwa bukti *Digital* yang berkaitan dengan insiden risiko dapat dikelola dengan cara yang dapat diterima baik dalam aspek teknis maupun aspek hukum.

Berdasarkan data pemetaan ISMS maupun DFR, serta analisis dan usulan *model Framework* DFR yang ada, peneliti mengusulkan *Model* Integrasi *Digital Forensic Radiness* terhadap ISMS khusus untuk organisasi pemerintah dengan melakukan penggabungan antara beberapa standard dan *Framework* kedalam beberapa tahapan sebagai berikut.

1. Pemenuhan konteks organisasi yang sesuai dengan ISMS

   Pemenuhan ini terdapat penjelasan ruang lingkup organisasi, limitasi, tujuan/konteks pengamanan serta pemenuhan terhadap regulasi/legal tertentu.

2. Pemenuhan terhadap Leadership & Commitment

   Pada tahap ini organisasi harus mendefinisikan 2 hal, yaitu *Leadership & Commitment* (SK Tim dan Tupoksi) SMKI serta *Leadership & Commitment* untuk CSRIT *(Computer Security Incident Response Team)*. Kedua hal ini perlu didefinisikan, disahkan dan dijalankan secara terpisah.

3. Pemenuhan terhadap *Planning* (Perencanaan)

   Organisasi harus mendefinisikan beberapa komponen dari perencanaan dan strategi SMKI berdasarkan ISO 27001, dimana beberapa komponen yang berhubungan dengan *Digital Forensic* dapat diintegasikan seperti diantaranya:

a. Penambahan komponen strategi kesiapan DF pada strategi SMKI.
b. Penambahan komponen identifikasi, analisis/perhitungan maupun mitigasi risiko yang ada di SMKI berdasarkan standar penanganan bukti *Digital* tertentu.
c. Penambahan komponen kebijakan dalam preventif maupun penanganan insiden pada kebijakan mapun prosedur SMKI.
d. Penambahan komponen strategi, kebijakan dan prosedur pencadangan, pemulihan, serta strategi penanganan insiden terkait pihak eksternal.

4. Pemenuhan terhadap Dukungan (Support)

   Organisasi harus mendefinisikan beberapa komponen dari support berdasarkan klausul ISO 27001 ISMS, dan menambahkan beberapa komponen yang berhubungan dengan *Digital Forensic* dapat diintegasikan seperti diantaranya:

   a. Penambahan komponen pelatihan terhadap penanganan insiden.
   b. Penambahan komponen pelatihan terhadap penanganan bukti *Digital* yang mendukung *Management* DF untuk pemenuhan aspek hukum.
   c. Penambahan komponen kontrol terhadap akses data dan informasi baik secara langsung maupun tidak langsung berdasarkan standar tertentu yang diacu.
   d. Penambahan komponen tertentu untuk memastikan data rekaman terhadap kritikal sistem tertentu dapat dimanajemen dengan baik.

5. Pemenuhan terhadap Operasional

   Organisasi harus mendefinisikan beberapa komponen operasional berdasarkan ISO 27001 ISMS, dan menambahkan beberapa komponen yang berhubungan dengan pengelolaan insiden baik secara preventive, proaktif maupun penanangan insiden dan pasca insiden berdasarkan standar DF yang diacu.

6. Pemenuhan *Performance Evaluation*

   Organisasi harus mendefinisikan beberapa komponen operasional berdasarkan ISO 27001 ISMS, dan menambahkan beberapa komponen yang berhubungan dengan pengukuran/perhitungan kesiapan dan evektivitas penerapan DF dalam organisasi. Penambahan pemenuhan ini seperti diantaranya:

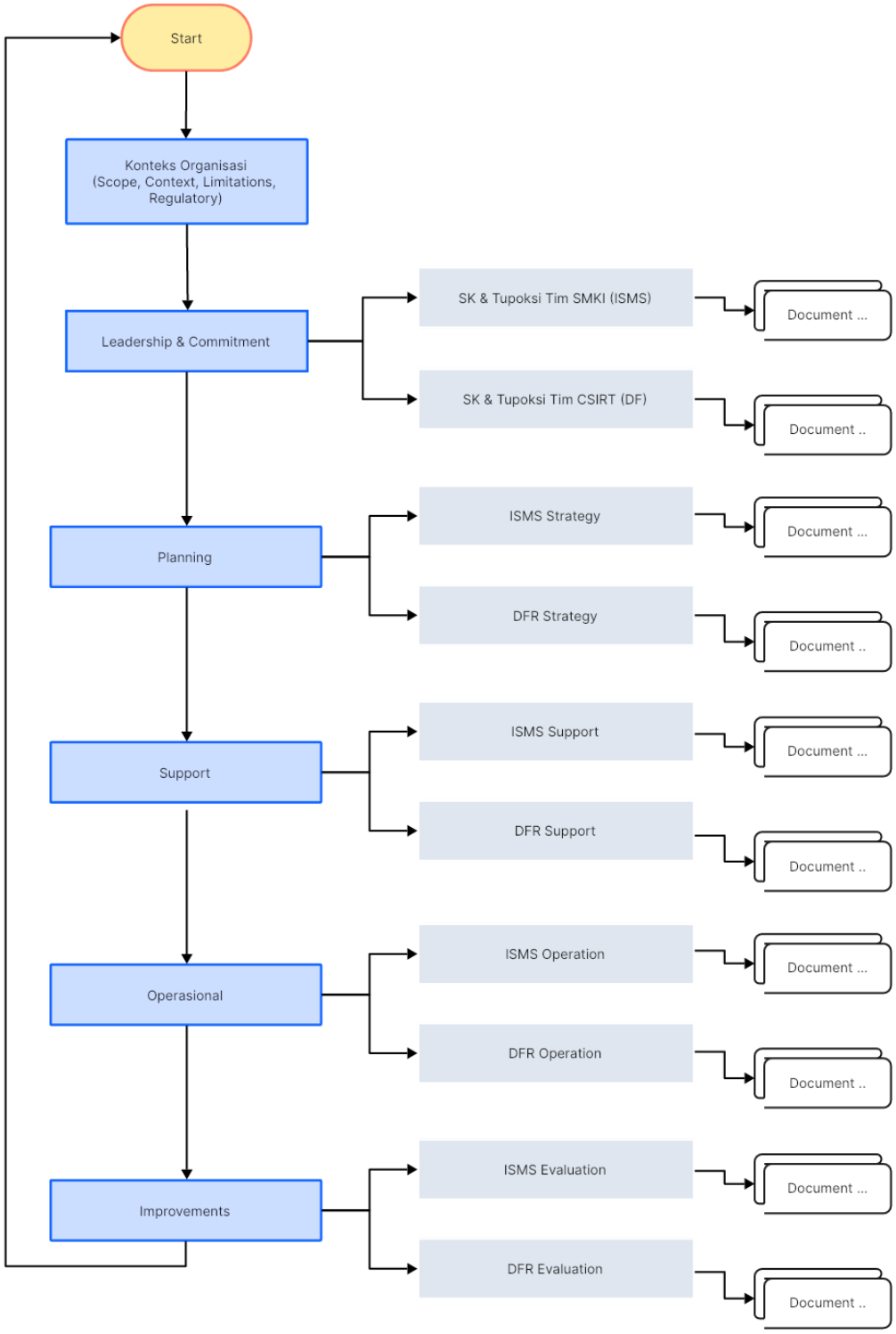
   a. Penambahan komponen tertentu untuk monitoring terhadap aset, proses, *user*, serta anomali yang terjadi. Komponen ini bisa didapat dari menggabungkan poin-poin utama dalam standar ISMS maupun standar DF tertentu

b. Penambahan komponen legal yang berbasis SLA terhadap performa ISMS maupun legal formal yang terkandung pada aspek DF
c. Penambahan komponen Business Continity *Management* berdasarkan ISMS standard yang disesuaikan dengan standard DF yang diacu.
d. Penambahan komponen penilaian berdasarkan *Framework* DFRI kedalam komponen internal audit yang sesuai dengan ISMS

7. Pemenuhan *Improvement*

   Organisasi harus memastikan terdapat improvements berdasarkan kesiapan ISMS dan DFR yang didapat dari proses evaluasi (pada tahap sebelumnya) yang dilakukan berkala, terukur dan sistematis.

Ketujuh tahapan tersebut diatas merupakan pemenuhan berbasis ISMS namun dengan penambahan beberapa komponen kesiapan DF dalam organisasi. Adapun *model* usulan *Framework* integrasi ini divisualisasikan pada gambar berikut.



Gambar 4.12. Usulan *Framework* Integrasi DFR terhadap ISMS

Pemenuhan dokumen pada *Framework* diatas disesuaikan dengan standar atau *Framework* maupun best practice yang diacu oleh organisasi dengan memperhatikan aspek-aspek implementasi seperti yang dijabarkan sebelumnya.

BAB 5
Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan hasil analisis yang dilakukan dalam penelitian ini, dapat disimpulkan bahwa integrasi antara *Digital Forensic Readiness* (DFR) dan *Information Security Management System* (ISMS) ISO 27001 di organisasi pemerintahan sangat penting untuk pengelolaan keamanan informasi yang lebih efektif. Meskipun DFR dan ISMS memiliki tujuan yang sama yaitu meningkatkan keamanan data dan informasi, keduanya sering diterapkan secara terpisah, tidak terintegrasi, oleh beberapa organisasi. Hasil ini ditemukan melalui analisis data yang diperoleh dari berbagai artikel jurnal yang dipublikasikan antara 2018-2025, yang menunjukkan bahwa meskipun organisasi global telah mengimplementasikan keduanya, penerapan integrasi masih sangat jarang (Simpulan-1, 2, dan 3).

Penerapan DFR dan ISMS yang terintegrasi membawa dampak positif dalam peningkatan keamanan data dan informasi, terutama dalam organisasi pemerintahan. Dampak tersebut mencakup peningkatan keandalan sistem keamanan dan efektivitas pengelolaan data yang lebih efisien dan aman, yang tercermin dalam "Simpulan-4 & 5". Penerapan yang terintegrasi memastikan bahwa langkah-langkah pengamanan yang lebih holistik dan komprehensif dapat diterapkan, mengurangi potensi celah yang ada dalam pengelolaan keamanan data.

Untuk merancang *Framework model* integrasi DFR dan ISMS, penelitian ini mengusulkan pendekatan yang didasarkan pada analisis beberapa *Framework* yang ada, serta perbandingan kapabilitas dan karakteristik masing-masing *Framework* yang sudah eksisting. Langkah-langkah pe*model*an yang dikembangkan dalam penelitian ini akan memberikan panduan yang jelas bagi organisasi pemerintahan dalam mengimplementasikan integrasi ini dengan efektif. Pembahasan lebih lanjut mengenai pe*model*an kebutuhan dan rumusan *Framework* ini dapat ditemukan pada Bab 4.2 penelitian ini. Dengan demikian, penelitian ini memberikan kontribusi penting terhadap pengembangan *Framework* integrasi DFR dan ISMS, yang dapat diimplementasikan di sektor pemerintahan guna meningkatkan kesiapan dan ketahanan terhadap ancaman siber.

5.2 Saran

Berdasarkan temuan dan kesimpulan yang diperoleh dalam penelitian ini, terdapat beberapa saran yang dapat menjadi langkah selanjutnya dalam pengembangan dan implementasi integrasi *Digital Forensic Readiness* (DFR) dan *Information Security Management System* (ISMS) ISO 27001 di organisasi pemerintahan:

1. Penelitian Lanjutan dengan Sampel yang Lebih Luas

   Untuk mendapatkan gambaran yang lebih komprehensif mengenai penerapan integrasi DFR dan ISMS, disarankan untuk melakukan penelitian lanjutan dengan sampel yang lebih luas, mencakup berbagai organisasi pemerintahan di berbagai negara dengan perbedaan tingkat kesiapan dan karakteristik keamanan data. Penelitian ini juga dapat memperluas cakupan ke sektor non-pemerintahan untuk melihat potensi penerapan serupa.

2. Pengembangan *Model Framework* yang Lebih Terperinci

   Model Framework yang diusulkan dalam penelitian ini masih dapat diperbaiki dan diperinci lebih lanjut. Oleh karena itu, saran berikutnya adalah mengembangkan *model Framework* integrasi DFR dan ISMS dengan pendekatan yang lebih spesifik dan terukur, termasuk menentukan standar-standar teknis dan prosedural yang diperlukan untuk implementasi yang lebih efektif, serta mengidentifikasi potensi kendala atau tantangan dalam penerapannya.

3. Penerapan dan *Evaluasi Framework* di Organisasi Pemerintahan

   Penelitian ini telah memberikan dasar bagi pengembangan *Framework* integrasi DFR dan ISMS. Sebagai langkah selanjutnya, perlu dilakukan penerapan *Framework* yang diusulkan pada organisasi pemerintahan dan evaluasi berkelanjutan terhadap efektivitasnya dalam meningkatkan kesiapan forensik *Digital* dan pengelolaan keamanan informasi. Hasil penerapan ini dapat digunakan untuk merevisi dan menyempurnakan *model Framework* yang ada.

4. Studi Kasus dan Pembandingan *Framework* di Berbagai Negara

   Penelitian lebih lanjut yang membandingkan penerapan integrasi DFR dan ISMS di berbagai negara dapat memberikan wawasan yang lebih mendalam tentang faktor-faktor yang mempengaruhi keberhasilan implementasi. Penelitian ini dapat melibatkan studi kasus yang menilai kebijakan, regulasi, serta tantangan yang dihadapi oleh negara-negara dengan tingkat kemajuan teknologi dan kesiapan keamanan yang berbeda.

Daftar Pustaka

Adel, A., Ahsan, A., & Davison, C. (2024). ETHICore: Ethical Compliance and Oversight Framework for Digital Forensic Readiness. Information, 15(363). https://doi.org/10.3390/info15060363

Alenezi, A., Atlam, H. F., & Wills, G. B. (2019). Experts Reviews of a cloud Forensic Readiness Framework for Organizations. Journal of Cloud Computing: Advances, Systems and Applications, 8(11). https://doi.org/10.1186/s13677-019-0133-z

Arif, F., & Luthfi, A. (2024). Comparison Study of NIST SP 800-86 and ISO/IEC 27037 Standards as A Framework for Digital Forensic Evidence Analysis. Journal of Information Systems and Informatics, 6(2), 701-718. https://doi.org/10.51519/journalisi.v6i2.717

Ariffin, K. A. Z., & Ahmad, F. H. (2021). Indicators for maturity[1] and Readiness for Digital Forensic investigation in era of industrial revolution 4.0. Computers & Security, 105, 102237. https://doi.org/10.1016/j.cose.2021.102237

Badan Siber dan Sandi Negara. (2023). Laporan Kinerja Badan Siber dan Sandi Negara Tahun 2023. https://www.bssn.go.id/laporan-kinerja-badan-siber-dan-sandi-negara-tahun-2023/

Center for Strategic and International Studies. (2020). Komparasi Praktik Keamanan Siber di Tingkat Global. Retrieved from https://cfds.fisipol.ugm.ac.id/wp-content/uploads/sites/1423/2021/01/36-CfDS-Case-Study-Komparasi-Praktik-Keamanan-Siber-di-Tingkat-Global.pdf

Collie, M. (2018). A Strategic Model for Forensic Readiness. Athens Journal of Sciences, 5(2), 167–180. https://doi.org/10.30958/ajs.5-2-4

Dimensional Research. (2016). *Trends in security framework adoption: A survey of IT and security professionals.* Tenable Network Security. Retrieved from https://www.dimensionalresearch.com

https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Gusman, S. W. (2024). Development of the Indonesian Government's Digital Transformation. Digital Journal of Economics and Management Social Science, 5(5). https://doi.org/10.38035/dijemss.v5i5

Hidayat, T., & Putri, R. A. (2023). Implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) dalam Meningkatkan Pelayanan Publik di Indonesia. Jurnal Administrasi Publik Indonesia, 12(1), 45-60. https://doi.org/10.12345/japi.v12i1.678

Hayeri Khyavi, M. (2020). ISMS Role in the Improvement of Digital Forensics Related Process in SOC's. arXiv preprint: 2006.08255. https://doi.org/10.48550/arXiv.2006.08255. https://arxiv.org/abs/2006.08255

Karie, N. M., & Karume, S. M. (2017). Digital forensic readiness in organizations: Issues and challenges. Journal of Digital Forensics, Security and Law, 12(4), 1–16. https://doi.org/10.15394/jdfsl.2017.1436

Karokola, G. R. (2012). A Framework for Securing e-Government[2] Services: The Case of Tanzania (Doctoral dissertation). Stockholm University. https://doi.org/10.3384/diva2:570554

Kebande, V. R., & Venter, H. S. (2019). CFRaaS: Architectural Design of a Cloud Forensic Readiness as-a-Service Model using NMB solution as a Forensic agent. African Journal of Science,[3] Technology, Innovation and Development, 11(6), 749–769. https://doi.org/10.1080/20421338.2019.1585675

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., & Linkman, S. (2009). Systematic literature Reviews in software engineering–a systematic literature Review. Information and Software Technology, 51(1), 7-15. https://doi.org/10.1016/j.infsof.2008.09.009

Kumar, R. (2019). Research Methodology: A step-by-step guide[4] for beginners (5th ed.). Journal of Latinos and Education 22(1):1-2, Sage Publications. Journal of Latinos and Education 22(1):1-2. https://doi.org/10.1080/15348431.2019.1661251

Mangindaan, D., Adib, A., Febrianta, H., & Hutabarat, D. J. C. (2022). Systematic Literature Review and Bibliometric Study of Waste Management in Indonesia in the COVID-19 Pandemic Era. Sustainability, 14(5),[5] 2556. https://doi.org/10.3390/su14052556

Mouhtaropoulos, A., & Li, F. (2014). The importance of Forensic Readiness in security Incident response. Journal of Information Security and Applications, 19(1), 23-31. https://doi.org/10.1016/j.jisa.2014.01.004

Okoli, C. (2015). A Guide to Conducting a Standalone Systematic Literature Review. Communications of the Association for Information Systems, 37, pp-pp. https://doi.org/10.17705/1CAIS.03743

Pangalos, G., Ilioudis, C., & Pagkalos, I. (2010). The Importance[6] of Corporate Forensic Readiness in the InformationSecurity Framework. 2010 Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises (pp. 12-18). IEEE. https://doi.org/10.1109/WETICE.2010.57

Petticrew, M., & Roberts, H. (2006). Systematic Reviews in the social sciences: A practical guide. John Wiley & Sons. DOI:10.1002/9780470754887

Pratama, Y., & Syahputra, R. (2024). Analisis model Digital Forensic Readiness Index (DiFRI) terhadap serangan malware. Venus: Jurnal Publikasi Rumpun Ilmu Teknik, 2(3), 104-113. https://doi.org/10.61132/venus.v2i3.305

Rochmadi, T., Fadlil, A., & Riadi, I. (2024). Tinjauan pustaka sistematis:[7] Tantangan dan faktor-faktor pengembangan kesiapan forensik digital. Cyber Security and Forensics Journal, 7(2), 81–89. https://doi.org/10.14421/csecurity.2024.7.2.4861

Rowlingson, R. (2004). A ten-step process for Forensic Readiness. International Journal of Digital Evidence, 2(3), 1-28. Diakses 5/01/2025 dari https://www.ijde.org/articles/123456789/

Salfati, E., & Pease, M. (2022). Digital[8] Forensics and Incident Response (DFIR) Framework for Operational Technology (OT). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8428

Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP). Central European Journal of International and Security Studies, 13(4), 104–120. https://doi.org/10.2478/cejiss-2019-0045

Snyder, H. (2019). Literature Review as a research Methodology: An overview and guidelines. Journal of Business Research, 104, 333–339. https://doi.org/10.1016/j.jbusres.2019.07.039

Sudyana, D., Prayudi, Y., & Sugiantoro, B. (2019). Analysis and Evaluation Digital Forensic Investigation Framework using ISO 27037:2012. International Journal of Cyber-Security and Digital Forensics, 8(1), 1-14. https://doi.org/10.17781/P002464

Sudyana, D., Prayudi, Y., & Sugiantoro, B. (2019). Analysis and Evaluation Digital Forensic Investigation Framework using ISO 27037:2012. International Journal of Cyber-Security and Digital Forensics, 8(1), 1-14. https://doi.org/10.17781/P002464

Suryono, S., & Wahyu, A. (2020). Perancangan Arsitektur Enterprise sebagai Peningkatan Proses Pencatatan Sipil untuk Mewujudkan Misi Pemerintah Kabupaten Lombok Tengah dan Meningkatkan Indeks Nilai SPBE. Diakses 13/01/2025 dari https://ejournal3.undip.ac.id/index.php/transient/article/downloadSuppFile/44474/3672

T. Grobler, and B. Louwrens, "Digital Forensic Readiness as a component of informationsecurity best practice", in IFIP International Federation for Information Processing, Vol. 232, New Approaches for Security, Privacy and Trust in Complex Environments, eds. Venter, H., Elofif, M., Labuschagne, L., Elofif, J., von Solms, R., (Boston: Springer), 2007, pp. 13-24, https://doi.org/10.1007/978-0-387-72367-9_2

Tranfield, D., Denyer, D., & Smart, P. (2020). Towards a Methodology for developing evidence-informed Management knowledge by means of systematic Review. British Journal of Management, 31(4), 839–855. https://doi.org/10.1111/1467-8551.12267

Triandini, E., Suryotrisongko, H., & Wibowo, A. (2019). A Systematic Literature Review of Digital Forensic Readiness and Information Security Management System Integration. Journal of Information Security and Applications, 46, 102563. https://doi.org/10.1016/j.jisa.2019.102563

Wahono, R.S (2015). A Systematic Literature Review of Software Defect Prediction: Research Trends, Datasets, Methods and Frameworks. Journal of Software Engineering, Vol. 1, No.1. ISSN 2356-3974. https://romisatriawahono.net/publications/2016/wahono-slr-may2016.pdf

Wijatmoko, T. E. (2020). Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Kantor Wilayah Kementerian Hukum dan HAM DIY. CyberSecurity dan Forensik Digital, 3(1), 1-6. https://doi.org/10.14421/csecurity.2020.3.1.1951. https://journal.ugm.ac.id/jurnal-ilmu-komputer/article/view/16534

Studi ini menekankan pentingnya evaluasi keamanan informasi yang dapat ditingkatkan melalui integrasi DFR dalam ISMS.

Zulfikar, A., & Wahyu, B. (2023). Keamanan SPBE pada Transformasi Digital. Diakses Diakses pada 13/01/2025 dari https://spbe.pontianak.go.id/storage/materi/November2023/HqEr20lJHJm8xXzTgzT0.pdf