# BAB I PENDAHULUAN

## I.1 *State of The Art*

Dalam era perkembangan digital saat ini tentu melibatkan perkembangan digital yang signifikan yang berdampak pada keamanan yang harus dijaga. Beberapa penelitian terbaru telah dilakukan dalam rangka mengembangkan model dan kerangka kerja untuk mengukur kematangan keamanan data yaitu, *"A Comprehensive Maturity Model for Data Security" oleh Penrose et al. (2022)* mengusulkan model kematangan yang komprehensif yang mencakup dimensi seperti kebijakan keamanan, enkripsi, pengelolaan akses, pemantauan, dan keandalan sistem. Di sisi lain, *"Quantifying Data Security Maturity: A Risk-Based Approach" oleh Zhang et al. (2023)* memperkenalkan pendekatan berbasis risiko untuk mengukur kematangan keamanan data dengan menggunakan metrik terkait kebijakan, pemantauan, respons insiden, dan tindakan pencegahan.

Selain itu, *"A Data Security Maturity Assessment Framework for Cloud Environments"* oleh *Li et al. (2021)* fokus pada pengukuran kematangan keamanan data dalam lingkungan cloud dengan menggunakan pendekatan kuantitatif dan kualitatif. Di bidang kesehatan, *"Measuring Data Security Maturity: A Framework for Healthcare Organizations"* oleh *Rahman et al. (2022)* mengusulkan kerangka kerja penilaian yang melibatkan aspek keamanan data seperti kebijakan keamanan, pengelolaan risiko, pelatihan pegawai, dan kepatuhan regulasi.

Untuk sektor keuangan sendiri terdapat beberpa jurnal maupun publikasi terkait, *"Assessing Data Security Maturity in the Financial Sector"* oleh *Gupta et al. (2023)* mengembangkan kerangka kerja penilaian yang melibatkan analisis risiko, kepatuhan regulasi, pengelolaan identitas, serta kebijakan dan prosedur keamanan. Dalam konteks Internet of Things (IoT), *"A Maturity Model for Privacy and Data Protection in IoT Environments" oleh Rodrigues et al. (2022)* mengusulkan model kematangan untuk privasi dan perlindungan data dalam lingkungan IoT.

Penelitian lain yang membahas tentang data security maturity yaitu, "*A Comprehensive Maturity Model for Data Security" oleh Penrose et al. (2022)* penelitian ini mengusulkan model kematangan yang komprehensif untuk keamanan data. Model ini mencakup

beberapa dimensi penting, termasuk kebijakan keamanan, enkripsi, pengelolaan akses, pemantauan, dan keandalan sistem. Penelitian ini menggunakan teknik pengumpulan data dan analisis untuk mengukur kematangan organisasi dalam setiap dimensi dan memberikan wawasan tentang aspek keamanan data yang perlu ditingkatkan.

Penelitian sejenis yang dibahas pada bidang Big Data, IoT dan GDPR dapat dirangkum sebagai berikut *"A Maturity Model for Privacy and Data Protection in IoT Environments" oleh Rodrigues et al. (2022):* Penelitian ini mengusulkan model kematangan untuk privasi dan perlindungan data dalam lingkungan Internet of Things (IoT). Model ini mencakup aspek-aspek seperti kontrol akses, privasi data, transparansi, serta perlindungan data pribadi. Penelitian ini menggunakan survei dan wawancara dengan pakar untuk mengembangkan model dan mengukur tingkat kematangan di lingkungan IoT. *"A Framework for Measuring Data Security Maturity in Industrial Control Systems" oleh Wang et al. (2021):* Penelitian ini fokus pada pengukuran kematangan keamanan data dalam sistem kontrol industri. Penelitian ini mengembangkan kerangka kerja yang mencakup dimensi-dimensi penting seperti pengendalian akses, keamanan jaringan, deteksi ancaman, serta respons dan pemulihan setelah insiden keamanan. Penelitian ini menggunakan metode survei dan analisis untuk mengevaluasi tingkat kematangan keamanan data dalam sistem kontrol industri. *"Measuring Data Security Maturity in Big Data Environments" oleh Chen et al. (2022):* Penelitian ini mengusulkan pendekatan untuk mengukur kematangan keamanan data dalam lingkungan Big Data. Penelitian ini mengidentifikasi faktor-faktor kunci yang mempengaruhi keamanan data dalam konteks Big Data, termasuk pengelolaan akses, enkripsi, pemantauan, serta kepatuhan privasi. Penelitian ini menggunakan analisis statistik untuk mengukur tingkat kematangan dan mengidentifikasi area yang perlu ditingkatkan.*"Data Protection Maturity Assessment in the Era of GDPR" oleh Santos et al. (2023):* Penelitian ini membahas pengukuran kematangan perlindungan data dalam konteks Regulasi Perlindungan Data Umum (GDPR). Penelitian ini mengusulkan kerangka kerja penilaian yang melibatkan aspek-aspek seperti kebijakan keamanan, manajemen risiko, pemantauan, serta tanggapan terhadap pelanggaran data. Penelitian ini menggunakan metode survei dan analisis untuk mengevaluasi tingkat kematangan organisasi dalam menjalankan kepatuhan GDPR. *"A Maturity Model for Cyber Threat*

*Intelligence Capability" oleh Khan et al. (2022):* Penelitian ini berfokus pada pengukuran kematangan kemampuan intelijen ancaman siber. Meskipun tidak secara khusus membahas keamanan data, penelitian ini relevan karena keamanan data seringkali terkait dengan ancaman siber. Penelitian ini mengusulkan model kematangan yang mencakup aspek-aspek seperti pengumpulan data, analisis intelijen, distribusi informasi, serta integrasi dengan sistem keamanan. Penelitian ini memberikan panduan untuk mengukur dan meningkatkan tingkat kematangan dalam hal intelijen ancaman siber.

*"A Maturity Model for Data Privacy Compliance" oleh Kaur et al. (2022):* Penelitian ini mengembangkan model kematangan untuk kepatuhan privasi data. Model ini mencakup aspek-aspek seperti kebijakan privasi, pengelolaan izin, pemantauan, serta respons terhadap pelanggaran privasi. Penelitian ini menggunakan pendekatan berbasis risiko dan metode pengumpulan data untuk mengukur tingkat kematangan kepatuhan privasi data dalam organisasi. *"A Framework for Measuring Data Security Maturity in Cloud Computing" oleh Zhao et al. (2021):* Penelitian ini fokus pada pengukuran kematangan keamanan data dalam komputasi awan (cloud computing). Penelitian ini mengusulkan kerangka kerja yang mencakup aspek-aspek seperti kebijakan keamanan, pengelolaan identitas, enkripsi data, serta pemantauan dan deteksi ancaman. Penelitian ini menggunakan metode survei dan analisis untuk mengukur tingkat kematangan keamanan data dalam lingkungan *cloud computing*.

*"Measuring the Maturity of Data Protection Controls in Organizational Systems" oleh Bhagwat et al. (2023):* Penelitian ini mengusulkan pendekatan untuk mengukur kematangan kontrol perlindungan data dalam sistem organisasi. Penelitian ini mengidentifikasi dimensi-dimensi kunci seperti pengelolaan akses, penggunaan enkripsi, kebijakan privasi, serta pelaporan dan pemulihan insiden. Penelitian ini menggunakan metode survei dan wawancara untuk mengevaluasi tingkat kematangan dan memberikan rekomendasi untuk perbaikan.*"A Maturity Model for Data Governance in the Era of Big Data" oleh Singh et al. (2022):* Penelitian ini berfokus pada pengukuran kematangan tata kelola data dalam era Big Data. Penelitian ini mengembangkan model kematangan yang mencakup aspek-aspek seperti kebijakan dan prosedur, manajemen metadata, kepatuhan, serta manajemen kualitas data. Penelitian ini menggunakan pendekatan berbasis

kuesioner untuk mengukur tingkat kematangan tata kelola data dalam organisasi. *"Measuring Data Security Maturity in the Internet of Medical Things (IoMT)"* oleh Patel et al. (2023): Penelitian ini membahas pengukuran kematangan keamanan data dalam konteks *Internet of Medical Things* (IoMT). Penelitian ini mengusulkan kerangka kerja penilaian yang mencakup aspek-aspek seperti pengelolaan identitas, enkripsi data, kebijakan privasi, serta kepatuhan terhadap regulasi medis. Penelitian ini menggunakan metode survei dan analisis untuk mengevaluasi tingkat kematangan keamanan data dalam lingkungan IoMT. *"A Maturity Model for Data Privacy in Social Media Platforms" oleh Gupta et al. (2022):* Penelitian ini mengusulkan model kematangan untuk privasi data dalam platform media sosial. Model ini melibatkan aspek-aspek seperti pengelolaan izin, transparansi, penghapusan data, serta perlindungan terhadap pelanggaran privasi. Penelitian ini menggunakan pendekatan kombinasi antara analisis deskriptif dan perbandingan untuk mengukur tingkat kematangan privasi data dalam platform media sosial. *"Measuring Data Security Maturity in the Internet of Things (IoT) Devices"* oleh Sharma et al. (2021): Penelitian ini fokus pada pengukuran kematangan keamanan data dalam perangkat Internet of Things (IoT). Penelitian ini mengembangkan kerangka kerja penilaian yang mencakup aspek-aspek seperti enkripsi data, autentikasi, pemantauan, serta respons terhadap serangan keamanan. Penelitian ini menggunakan pendekatan survei dan analisis untuk mengevaluasi tingkat kematangan keamanan data dalam perangkat IoT.

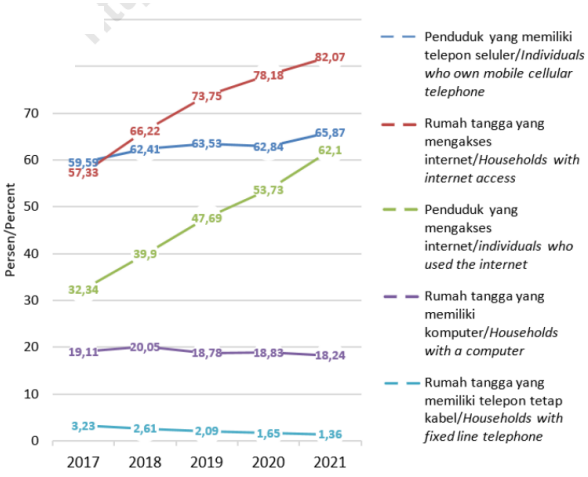
"*A Framework for Assessing Data Security Maturity in Blockchain Systems" oleh Chen et al. (2023):* Penelitian ini membahas pengukuran kematangan keamanan data dalam sistem blockchain. Penelitian ini mengusulkan kerangka kerja penilaian yang melibatkan aspek-aspek seperti pengelolaan kunci kriptografi, kebijakan akses, integritas data, serta privasi dan anonimitas. Penelitian ini menggunakan metode analisis risiko dan evaluasi independen untuk mengukur tingkat kematangan keamanan data dalam sistem blockchain. *"Measuring Data Security Maturity in Supply Chain Management" oleh Liang et al. (2022):* Penelitian ini fokus pada pengukuran kematangan keamanan data dalam manajemen rantai pasok. Penelitian ini mengusulkan kerangka kerja penilaian yang mencakup aspek-aspek seperti pengelolaan identitas, enkripsi data, pengawasan akses, serta kebijakan keamanan. Penelitian ini menggunakan kombinasi metode survei

dan analisis untuk mengevaluasi tingkat kematangan keamanan data dalam manajemen rantai pasok. *"A Maturity Model for Data Protection in Cloud Storage Services" oleh Nguyen et al. (2023)* penelitian ini berfokus pada pengukuran kematangan perlindungan data dalam layanan penyimpanan *cloud*. Penelitian ini mengembangkan model kematangan yang mencakup aspek-aspek seperti enkripsi data, manajemen izin, pemantauan aktivitas, serta pemulihan data. Penelitian ini menggunakan pendekatan berbasis survei dan analisis untuk mengukur tingkat kematangan perlindungan data dalam layanan penyimpanan *cloud*.

## I.2 Latar Belakang

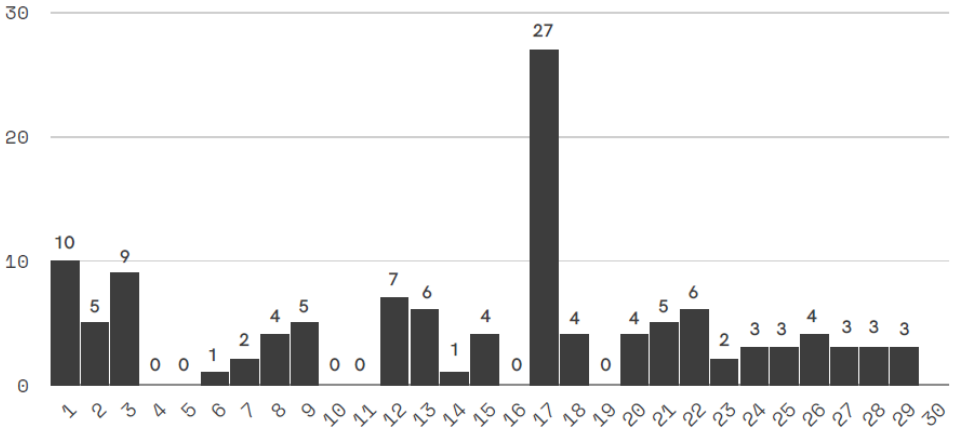
Pada Era digitalisasi yang berkembang dengan pesat saat ini, keamanan data merupakan hal yang krusial baik untuk organisasi maupun individu (Mohamed et al., 2012). Pasalnya, data menjadi salah satu aset berharga yang bisa digunakan dalam pengambilan keputusan bisnis, penyediaan layanan berkualitas tinggi bagi konsumen, serta peningkatan efisiensi operasional (Bertino, 2016; Yang et al., 2020). Namun, apabila data tersebut jatuh ke tangan yang tidak berwenang, maka dapat menimbulkan dampak kerugian yang signifikan bagi organisasi maupun konsumennya. Oleh karena itu, penting untuk melindungi data dengan baik dari ancaman keamanan (Ficco & Palmieri, 2017; Scarfò, 2017). Keamanan data adalah suatu konsep atau praktik yang bertujuan untuk melindungi data dari ancaman, kerusakan, atau kehilangan yang dapat membahayakan integritas, kerahasiaan, dan ketersediaannya (DAMA International Technics, 2017). Dalam konteks organisasi atau perusahaan, keamanan data merupakan suatu kebijakan dan praktik yang penting untuk menjaga kerahasiaan data penting organisasi, seperti data pelanggan, data keuangan, atau data rahasia lainnya (DAMA International Technics, 2017; Mosley, M., Brackett, M., Earley, S. & Henderson, 2009). Ancaman keamanan data bisa datang dari dalam maupun luar organisasi (Chan & Wei, 2008; Kruger et al., 2011). Serangan dari dalam organisasi dapat berasal dari karyawan yang tidak bertanggung jawab atau kurang memahami pentingnya menjaga kerahasiaan data (P. Zhang et al., 2018). Sementara itu, serangan dari luar organisasi bisa datang dari peretas (*hacker*) yang ingin mencuri data, virus komputer yang merusak sistem, atau serangan phishing yang mencuri data pribadi melalui teknik rekayasa sosial (Yaacoub et al., 2023).

Apabila sebuah organisasi tidak memiliki pengelolaan keamanan data yang memadai, maka organisasi tersebut dapat menjadi mudah terkena serangan keamanan data (Ficco & Palmieri, 2017). Tanpa pengelolaan keamanan data yang baik, organisasi dapat kehilangan data, mengalami pencurian identitas, merusak reputasi, dan mengalami kerugian finansial yang signifikan (Wang et al., 2018). Sebagai contoh, pada tahun 2020, sebuah perusahaan teknologi raksasa di Indonesia mengalami kebocoran data besar-besaran, yang menyebabkan kehilangan data pelanggan dan merusak reputasi perusahaan tersebut (Naufal, 2020; Soemitra & Adlina, 2022; Widya, 2020). Kasus lain terjadi kebocoran data BPJS kesehatan yang terjadi pada Mei 2021 data ini di jual oleh pengguna yang tidak bertanggung jawab. Setidaknya terdapat 279 juta data yang bocor (Tempo.co, 2021). Hal ini terjadi seiring dengan perekembangan pemanfaatan jaringan telekomunikasi yang dituliskan dalam laporan Statistik Telekomunikasi Indonesia (Indonesia, 2021), (Badan Pusat Statistik, 2020). Pada November 2022, Badan Siber Sandi Negara (BSSN) mempublikasikan laporan terkait dengan insiden keamanan dan ditemukan 121 kasus peretasan dengan total 56 kasus pada sektor Pendidikan. Dari penyebaran kasus per sektor yang ditampilkan pada Gambar I.2, dapat ditarik kesimpulan bahwa pada bulan November 2022, sektor Pendidikan mengalami jumlah peretasan yang paling banyak. Diketahui juga aktivitas peretasan terbanyak terjadi pada tanggal 17 November 2022 yang mencapai 27 kasus [1].




Gambar I.1Statistik penggunaan telekomunikasi di Indonesia

Sumber: (Indonesia, 2021)




Gambar I.2 Laporan insiden keamanan informasi November 2022

Sumber: [1]

Selain itu, *Consortium for School Networking* (CoSN) yang menunjukkan peningkatan jumlah serangan *cyber* pada sekolah dan distrik pendidikan di Amerika Serikat selama 2018-2019 [2]. Hal tersebut menunjukkan bahwa institusi pendidikan dapat menjadi target serangan siber yang signifikan dan perlu mengambil tindakan untuk memperkuat keamanan informasi mereka. Oleh karena itu, sebagai Yayasan XYZ yang menaungi Lembaga Pendidikan, keamanan informasi menjadi hal penting yang harus diperhatikan sebagai upaya dalam melindungi informasi dari akses yang tidak sah, modifikasi, atau penghapusan. Dengan menjaga keamanan informasi, lembaga di bawah naungan Yayasan XYZ dapat memastikan keberlangsungan bisnis, menjaga kepercayaan pelanggan, dan memenuhi persyaratan peraturan dan undang-undang terkait.

Adapun beberapa permasalahan yang berkaitan dengan data serta informasi yang terjadi di Yayasan XYZ yaitu adanya celah keamanan yang terjadi berupa serangan *brute force* yang menyerang Cpanel Yayasan XYZ. *Brute force* merupakan sebuah teknik penyerangan keamanan yang dilakukan dengan mencoba seluruh kemungkinan kata sandi atau kunci enkripsi secara terus-menerus hingga sukses mengakses sistem atau data yang diincar. Selain itu, Yayasan XYZ belum menerapkan sistem *Two-Factor Authentication (2FA)* untuk melindungi akun dan data yang dimilikinya sehingga serangan terjadi dengan cepat dan mengakibatkan tidak dapat diaksesnya Cpanel. Adapun kondisi saat ini Yayasan XYZ belum mengimplementasikan secara menyeluruh

pengelolaan data mulai dari keamanan hingga kualitas maupun aspek yang berkaitan dengan menjamin data tersebut bisa termonitor dengan baik karena terdapat keterbatasan sumber daya yang ada. Kondisi tersebut memiliki dampak yang cukup serius, di mana tidak adanya penggunaan file atau file yang terindikasi menjadi *malicious* atau *ransomware* dapat menyebabkan kerugian yang signifikan bagi sebuah organisasi atau perusahaan.

Permasalahan lain dikemukakan bahwa belum adanya pengelolaan terkait dengan siapa saja yang berhak mengakses dan melakukan kontrol terhadap data, fakta ini ditemukan pada hasil asesmen yang dilakukan oleh salah satu konsultan keamanan di Indonesia dan menjadikannya temuan sebagai saran perbaikan bahwa Yayasan XYZ perlu melakukan identifikasi tata kelola keamanan data, melakukan pembuatan kebijakan yang berkaitan dengan keamanan data serta melakukan pemetaan terhadap user atau pengguna aplikasi yang memanfaatkan data beserta membentuk tim dan melakukan proses identifikasi terkait data sensitif yang ada di Yayasan.

Apabila tidak diantisipasi sedini mungkin kerugian tersebut berdampak pada kehilangan data penting yang disebabkan oleh penyebaran virus atau *malware*, yang dapat mengganggu operasional bisnis dan mengakibatkan kehilangan uang, reputasi yang rusak, dan bahkan tuntutan hukum dari pihak yang dirugikan. Oleh karena itu, sangat penting bagi sebuah organisasi atau perusahaan untuk memiliki tata kelola keamanan data yang memadai dan menerapkan praktik keamanan yang tepat untuk melindungi sistem dan data dari ancaman serangan *cyber*, termasuk penerapan dua faktor autentikasi untuk akses ke sistem dan file.

Dalam menjaga keamanan data Yayasan XYZ perlu diimbangi dengan adanya pengelolaan tata kelola data. Pengelolaan tata kelola data mencakup serangkaian praktik, kebijakan, dan prosedur yang bertujuan untuk melindungi data organisasi dari ancaman keamanan data. Dengan memiliki pengelolaan tata kelola data yang baik, organisasi dapat mengidentifikasi ancaman keamanan data, mengevaluasi risiko, dan mengambil tindakan yang tepat untuk mencegah ancaman tersebut. Sebagai contoh, sebuah organisasi harus memiliki pengelolaan tata kelola data yang baik untuk melindungi data pribadi pelanggan, informasi transaksi, dan informasi keuangan lainnya. Pengelolaan tata kelola

data yang baik dapat mencakup penerapan kebijakan keamanan informasi, pelatihan karyawan, penggunaan teknologi keamanan informasi, dan pemantauan keamanan informasi secara teratur. Permasalahan mengenai pengelolaan dan implementasi dari data sering menjadi permasalahan utama dan perlu segera ditangani namun tak banyak dari sebuah organisasi maupun perusahaan menyadari permasalahan ini. Jika kita melihat ke depan banyak perusahaan yang mungkin sudah menerapkan *Good Coorporate Governance* atau bahkan telah memperoleh nilai yang baik dalam hal ini. Namun sering kali kita mendapatkan gap yang cukup jauh terkait dengan pengelolaan data maupun informasi, mengingat fokus utama dari tata kelola teknologi informasi lebih memfokuskan pada bidang investasi dan bagaimana implementasi dari infrastruktur dan perencanaan jangka ke depan, sehingga dirasa pengelolaan data dan informasi ini masih kurang proporsional.

Dalam hal ini keamanan data dan privasi erat kaitannya dengan pengelolaan tata kelola data pada sebuah organisasi atau perusahaan. Dalam membangun tata kelola data yang baik, dapat memberikan manfaat yaitu peningkatan kontributor bisnis langsung, peningkatan efisiensi, monetisasi data dan pengurangan resiko (Ladley, 2019). Tata kelola data yang baik dapat membantu perusahaan untuk mencapai target yang ditentukan, membangun akuntabilitas, dan memungkinkan pengambilan keputusan yang lebih baik (Al-Ruithe et al., 2019). Sebuah perusahaan ataupun organisasi perlu menerapkan tata kelola data dengan baik, sehingga tujuan dari *Good Governance of Data* dapat dicapai dan meningkatkan nilai ataupun *value* dari perusahaan (DAMA International, 2017). Pemanfaatan tata kelola data dalam perusahaan berupa kegiatan untuk memformalkan kebijakan, prosedur serta memantau kepatuhan dari seluruh siklus alur data (Abraham et al., 2019). Adapun dalam memastikan terjaminnya keamanan data perlu mempertimbangkan kualitas data menjadi titik sentral dalam manajemen data yang berdampak pada keputusan strategis. Kualitas data yang buruk akan berpengaruh pada tingginya biaya operasional dan informasi tidak dapat diandalkan untuk membuat keputusan yang strategis (Jimenez et al., 2019).

Dalam mencapai tujuannya sebuah organisasi perlu mendefinisikan beberapa strategi yang mungkin dilakukan hal ini tentu berkaitan dengan serangkaian proses yang ada pada

organisasi. Pada dasarnya setiap pengelolaan proses ini akan berkaitan dengan data yang diolah menjadi sebuah informasi. Semua pihak yang terlibat dalam sebuah organisasi memiliki tanggung jawab untuk menjaga informasi serta dapat memberikan saran maupun upaya pengambilan keputusan yang didasarkan dari data yang berkualitas. Keputusan dan tindakan bisnis yang efektif hanya dapat tercapai melalui penggunaan informasi yang memiliki kualitas tinggi. Dalam konteks ini, penting untuk menerapkan pendekatan yang dapat mengatasi permasalahan terkait data dan informasi, yaitu dengan menerapkan tata kelola data. Perlu dicatat bahwa tata kelola data berbeda dengan tata kelola Teknologi Informasi (TI). Sementara tata kelola TI berkaitan dengan pengambilan keputusan terkait investasi TI, portofolio aplikasi TI, dan portofolio proyek TI, tata kelola data bertujuan untuk menyelaraskan strategi dan tujuan TI dengan strategi dan tujuan perusahaan secara keseluruhan.

Dalam hal pengelolaan informasi, standar tata kelola TI yang umum digunakan adalah COBIT *(Control Objective For Information and Related Technology)*. Namun demikian, perlu diperhatikan bahwa hanya sebagian kecil dari kerangka kerja COBIT yang membahas pengelolaan informasi secara spesifik. Oleh karena itu, dibutuhkan pendekatan khusus dalam tata kelola data yang fokus pada pengelolaan aset data. Tata kelola data yang efektif dapat meningkatkan kualitas, ketersediaan, dan integritas data perusahaan dengan memperkuat kolaborasi lintas-bidang yang terstruktur sesuai dengan kebijakan yang telah ditetapkan.

Salah satu Kerangka kerja tata kelola data yang dapat digunakan adalah DAMA International. DAMA International adalah sebuah organisasi non-profit yang berfokus pada pengelolaan data di seluruh dunia, didirikan pada tahun 1988 di Los Angeles. Pada tahun 2009, DAMA *Association* memperkenalkan kerangka kerja yang dikenal sebagai DAMA-DMBOK *(Data Management Body of Knowledge)* yang menjadi acuan standar dalam pengelolaan data. DAMA-DMBOK menyediakan pendekatan model tata kelola data yang berfungsi dan menyediakan ruang lingkup pengetahuan bagi organisasi untuk memenuhinya secara mudah, komprehensif, dan terstruktur dalam membangun tata kelola data.

Penelitian ini bertujuan untuk memberikan rekomendasi terkait keamanan data guna meningkatkan pengelolaan tata kelola data di Yayasan XYZ. Kerangka kerja DAMA-DMBOK akan menjadi landasan dalam penelitian ini, dengan harapan bahwa dengan mengimplementasikan kerangka kerja tersebut, proses bisnis yang berjalan di organisasi dapat menjadi lebih efektif dan efisien dalam mencapai strategi bisnis yang telah ditetapkan.

## I.3 Rumusan Masalah

Sebagai salah satu Yayasan yang menaungi pendidikan mulai dari pendidikan dasar dan menegah serta perguruan tinggi tentu Yayasan perlu mempertimbangkan bahwa segala bentuk data dan informasi yang diperoleh dan dikelola haruslah baik dan akurat. Namun dengan adanya masalah seperti belum adanya tata kelola data yang baik, manajemen data yang masih belum terpusat, serta adanya kerentanan keamanan dan kualitas data yang belum dapat dijaminkan, kurangnya meratanya pengetahuan pegawai, serta kesadaran akan keamanan informasi yang masih kurang, banyaknya data yang dikelola masih terdapat redundant, arsitektur data belum terdefinisi, kebijakan terkait dengan pengelolaan data belum ada, dan interaksi data antar unit yang belum terdokumentasi dengan baik serta belum adanya pembagian kewenangan terhadap data yang dikelola menyebabkan permasalahan yang serius berupa pengelolaan data yang terbilang masih dilakukan secara manual seperti dashboard laporan harus dikelola dengan melakukan update menggunakan Excel serta proses berjalan menjadi kurang optimal. Oleh karena itu perlu adanya pengukuran tingkat kedewasaan keamanan data di Yayasan XYZ. Hasil dari pengukuran *maturity* ini diharapkan menjadi sebuah instrument yang memudahkan Yayasan dalam mengidentifikasi kondisi saat ini dan melakukan perencanaan strategis untuk mencapai tujuan yang ingin dicapai baik dalam proses pengelolaan, penyimpanan, arsitektur, dan tata kelola data yang baik terutama dalam memastikan data tersebut tersedia, terjamin integritas datanya dan siapa saja yang berhak mengakses data dapat di identifikasi dan dimanajemen dengan baik oleh Yayasan.

## I.4 Tujuan Penelitian

Tujuan penelitian pada penelitian ini sebagai berikut:

1. Merancang model *maturity assessment* keamanan data yang diterapkan pada Yayasan XYZ agar dapat meningkatkan keamanan data dan informasi.
2. Menilai kondisi saat ini terkait dengan penerapan strategi keamanan data pada Yaysan XYZ.

## I.5 Pertanyaan Penelitian

Berdasarkan tujuan yang telah didefinisikan pada penelitian ini maka permasalahan yang akan digunakan untuk menentukan ketercapaian dari penelitian ini dalam membuat model asesmen *maturity data security* sebagai berikut:

1. Apakah komponen yang diperlukan oleh organisasi untuk menerapkan keamanan data?
2. Apakah faktor yang mempengaruhi kesuskesan Yayasan dalam menerapkan strategi keamanan data?

## I.6 Lingkup Penelitian

Lingkup pada penelitian ini mengacu pada batasan serta jangkauan dari penulis yang dijabarkan sebagai berikut:

1. Ruang lingkup masalah

   Ruang lingkup masalah pada penelitian ini berfokus pada perancangan model asesmen keamanan dan privasi data menggunakan referensi DAMA-DMBOK dan ISO/IEC 38505-1: 2017, COBIT 2019, ISO 27001:2022, *Privacy Maturity Asessment Framework (PMAF), National Institute of Standards and Technology (NIST)*. Penelitian difokuskan dalam pembuatan model asesmen keamanan dan privasi data dan rekomendasi tata kelola data YAYASAN XYZ. Penelitian ini akan memberikan penilaian di masa mendatang dalam penerapan tata kelola data.
2. Lokasi dan objek penelitian

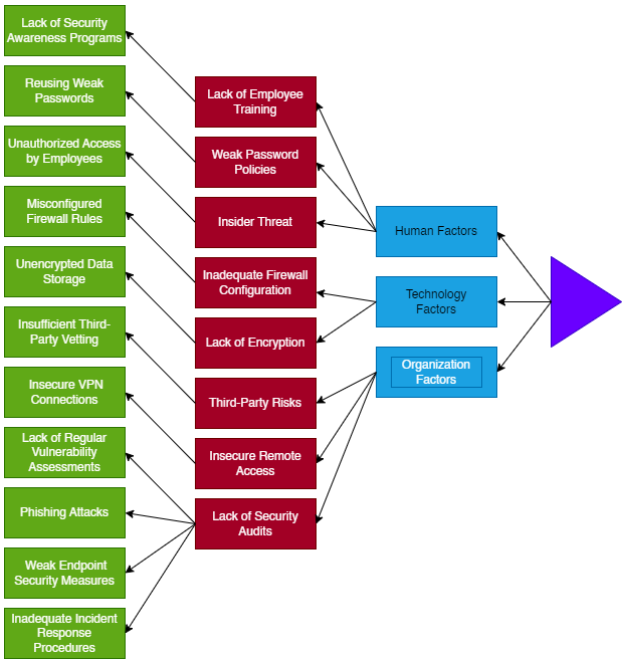
   Lokasi yang digunakan pada penelitian ini merupakan salah satu Yayasan yang berada di wilayah provinsi Jawa Barat, Indonesia. Adapun objek penelitian ini berfokus kepada pegawai yang berada di Yayasan XYZ.

3. Waktu dan periode penelitian

   Penelitian ini dilakukan dalam kurun waktu dua tahun yaitu sejak tahun 2021 hingga tahun 2023. Adapun proses yang dikelola dan perlu monitoring oleh peneliti berupa melakukan identifikasi langsung ke Yayasan dan melakukan interviu.

## I.7 Kesenjangan Penelitian

*Gap analysis* adalah suatu alat analisis yang dirancang untuk mengevaluasi perbedaan antara kondisi aktual atau kinerja suatu organisasi pada suatu periode waktu tertentu dengan kondisi yang diharapkan atau potensial di masa depan. Menurut Kemenkoan Komenfo Kabinet KM ITB (2022), alat ini digunakan untuk mengidentifikasi kesenjangan antara keadaan sekarang dan harapan di masa depan. Dalam konteks ini, alat yang digunakan adalah diagram tulang ikan *(fishbone diagram)* untuk menggambarkan kesenjangan yang terjadi dalam proses penelitian eksisting mengenai pengenalan wajah, dengan tujuan untuk membantu proses penelitian ini.




Gambar I.3 *Fishbone Diagram* (Kesenjangan Penelitian)

Kesenjangan penelitian dalam asesmen kematangan keamanan data adalah bahwa ada kebutuhan yang belum terpenuhi untuk memahami dan mengukur kematangan

keamanan data secara menyeluruh. Meskipun telah ada upaya untuk mengembangkan kerangka kerja dan metode asesmen, masih ada beberapa aspek yang perlu dieksplorasi dan dipelajari lebih lanjut.

Salah satu kesenjangan utama adalah kurangnya konsensus tentang indikator dan metrik yang dapat digunakan untuk mengukur kematangan keamanan data. Meskipun ada beberapa kerangka kerja yang ada, belum ada standar yang diakui secara luas untuk mengukur tingkat kematangan keamanan data secara komprehensif. Oleh karena itu, perlu dilakukan penelitian lebih lanjut untuk mengidentifikasi dan mengembangkan indikator yang dapat memberikan gambaran yang akurat tentang tingkat kematangan keamanan data dalam konteks yang berbeda.

Selain itu, ada kebutuhan untuk menyelidiki faktor-faktor yang mempengaruhi kematangan keamanan data dan bagaimana aspek-aspek ini dapat diukur. Ini termasuk pemahaman yang lebih baik tentang faktor organisasional, teknis, dan manusia yang berkontribusi pada kematangan keamanan data. Dalam penelitian lebih lanjut, dapat dilakukan analisis yang lebih mendalam terhadap pengaruh dari kebijakan, proses, budaya organisasi, infrastruktur teknologi, serta tingkat kesadaran dan keterampilan personel terhadap kematangan keamanan data.

Selanjutnya, ada kebutuhan untuk mengeksplorasi hubungan antara kematangan keamanan data dengan kinerja organisasi. Penelitian lebih lanjut dapat mengeksplorasi apakah organisasi yang memiliki tingkat kematangan keamanan data yang lebih tinggi cenderung mencapai kinerja yang lebih baik dalam hal keamanan informasi, kepuasan pelanggan, efisiensi operasional, dan keunggulan kompetitif. Studi ini akan memberikan wawasan yang berharga tentang manfaat nyata dari mengembangkan dan meningkatkan kematangan keamanan data.

Terakhir, penting untuk mencatat bahwa lingkungan keamanan data terus berkembang dengan cepat. Ancaman keamanan baru terus muncul, teknologi terus berevolusi, dan regulasi terus diperbarui. Oleh karena itu, penelitian kesenjangan ini juga harus mengakomodasi perubahan yang terjadi dalam lingkungan keamanan data. Diperlukan kajian yang terus-menerus dan upaya penelitian yang berkelanjutan untuk menjaga kebaharuan dan relevansi penelitian dalam asesmen kematangan keamanan data.

## I.8 Batasan Penelitian

Adapun batasan pada penelitian ini sebagai berikut:

1. Penelitian ini berfokus pada identifikasi dan proses pengelolaan keamanan data.
2. Penelitian hanya dilakukan dalam proses perancangan dan validasi serta melakukan identifikasi penilaian kondisi eksisting serta memberikan saran perbaikan kedepannya. Penelitian tidak mengakomodir proses pembuatan *tools maturity* asesmen keamanan data secara digital.

## I.9 Manafaat Penelitian

Asesmen kematangan keamanan data merupakan suatu proses yang memiliki signifikansi penting dalam mengevaluasi dan mengukur sejauh mana suatu organisasi telah mencapai tingkat kematangan dalam aspek keamanan data. Dalam konteks ini, asesmen kematangan memiliki potensi untuk memberikan wawasan yang berharga bagi organisasi dalam mengidentifikasi kelemahan dan area yang memerlukan peningkatan, dengan tujuan meningkatkan tingkat keamanan data yang ada.

Dalam pelaksanaannya, asesmen kematangan memberikan kerangka evaluatif yang sistematis untuk mengukur dan menganalisis sejumlah dimensi kritis yang terkait dengan keamanan data. Melalui proses ini, organisasi dapat mengidentifikasi dan menganalisis celah keamanan, praktik yang rentan terhadap ancaman, serta kebijakan dan prosedur yang mungkin perlu diperbarui atau diperkuat.

Dengan memanfaatkan hasil asesmen kematangan, organisasi dapat merumuskan rencana tindakan yang tepat dan strategis untuk meningkatkan tingkat keamanan data secara efektif. Rekomendasi yang dihasilkan dari proses asesmen tersebut dapat menyediakan panduan yang spesifik dan terarah bagi organisasi dalam mengidentifikasi dan mengatasi kelemahan yang ada, menerapkan solusi teknis yang relevan, serta memperkuat kerangka kebijakan dan prosedur keamanan data.

Penelitian terdahulu mengemukakan adanya beberapa penilaian pada sektor kesehatan, fokus pada pengelolaan *Cloud, Big Data, IoT* serta pada sector kesehatan maupun keuangan. Penelitian terkait dengan asesmen keamanan data di Indonesia sendiri

terbilang minim dibandingkan dengan penelitian di negara lain. sehingga perlu adanya penyesuaian pada framework ataupun kriteria serta pembuatan model perancangan yang cocok digunakan untuk melakukan asesmen keamanan data di Indonesia.

Oleh karena itu, asesmen kematangan keamanan data memainkan peran penting dalam membantu organisasi dalam memahami tingkat kematangan keamanan yang telah dicapai dan mengidentifikasi langkah-langkah yang diperlukan untuk meningkatkan keamanan data yang ada.

## I.10 Rasionalisasi Penelitian

Rasionalisasi penelitian mengenai *maturity assessment* keamanan data digunakan untuk memberikan pemahaman secara holistik terhadap pentingnya pengelolaan keamanan data pada Yayasan. Tentunya harapan dengan adanya proses pengelolaan tata kelola keamanan data yang baik akan memberikan kemudahan bagi Yayasan untuk mengelola program strategis memastikan bahwa Yayasan telah mematuhi peraturan dan prosedur sesuai dengan standar pengelolaan keamanan data baik dalam negeri maupun luar negeri seperti ISO 27001, GDPR, dan UU PDP.

Penelitian tentang keamanan data dapat membantu Yayasan melakukan identifikasi dan praktik terbaik untuk meningkatkan efektivitas dari pengelolaan secara tata kelola, sumber daya maupun secara operasional terkait dengan keamanan data sehingga dapat meningkatkan *awareness* dan kemampuan Yayasan dalam memastikan terwujudnya tujuan dari Yayasan itu sendiri.

## I.11 Signifikansi Penelitian

Penelitian tentang keamanan data memiliki signifikansi yang penting dalam konteks teknologi informasi dan dunia bisnis saat ini. Salah satu hal yang diupayakan dalam penelitian ini adalah melindungi informasi yang bersifat rahasia dan sensitif dari akses yang tidak sah. Dalam era digital yang terus berkembang, data menjadi aset berharga bagi organisasi, dan menjaga kerahasiaan data merupakan hal yang krusial untuk menjaga keunggulan kompetitif serta mencegah kerugian finansial atau reputasi yang serius. Selain itu, penelitian tentang keamanan data juga membantu mengidentifikasi

dan mencegah pelanggaran data, seperti peretasan, pencurian identitas, atau penyalahgunaan informasi pribadi. Dengan pemahaman yang lebih baik tentang ancaman dan kerentanan yang ada, organisasi dapat mengambil tindakan proaktif dalam melindungi data mereka dari serangan yang berpotensi merugikan. Selain itu, penelitian ini juga berperan dalam membangun kepercayaan pelanggan. Pelanggan cenderung merasa lebih percaya dan nyaman berinteraksi dengan organisasi yang memiliki langkah-langkah keamanan yang kuat untuk melindungi informasi pribadi mereka. Penelitian dalam bidang keamanan data membantu organisasi mengadopsi praktik terbaik dan standar keamanan untuk membangun kepercayaan pelanggan yang lebih tinggi. Selain itu, penelitian keamanan data juga penting untuk memastikan kepatuhan organisasi terhadap peraturan dan hukum yang berlaku, seperti GDPR di Uni Eropa. Dengan pemahaman yang baik mengenai persyaratan hukum, organisasi dapat mengembangkan kebijakan dan praktik yang sesuai. Keamanan data yang kuat juga membantu mencegah gangguan operasional yang serius bagi organisasi. Serangan *malware, DDoS*, atau *ransomware* dapat menyebabkan gangguan operasional yang signifikan, mengganggu produktivitas, dan merusak reputasi bisnis. Melalui penelitian keamanan data, risiko dapat diidentifikasi dengan baik dan strategi pencegahan dan respons yang efektif dapat dikembangkan. Terakhir, penelitian keamanan data juga berkontribusi pada inovasi teknologi yang lebih aman. Dengan mempelajari serangan dan celah keamanan yang ada, para peneliti dapat mengembangkan solusi baru dan teknologi yang lebih kuat dalam melindungi data. Ini memungkinkan organisasi untuk terus berinovasi tanpa mengorbankan keamanan informasi. Oleh karena itu, penelitian keamanan data menjadi penting dalam menjaga keberhasilan, mematuhi regulasi, dan memastikan operasional yang aman bagi organisasi dan institusi.

## I.12 Motivasi Penelitian

Motivasi penulis dalam merancang asesmen keamanan data salah satunya karena hal ini menjadi krusial dalam konteks yang semakin kompleks dan seringnya terjadi pelanggaran keamanan data. Dengan meningkatnya jumlah serangan siber dan ancaman terhadap informasi sensitif, organisasi harus memiliki pemahaman yang mendalam tentang keamanan data mereka. Studi asesmen keamanan data bertujuan untuk

mengidentifikasi dan mengevaluasi kelemahan dalam sistem keamanan, mengukur tingkat kematangan keamanan data, serta merumuskan strategi yang efektif untuk mengurangi risiko keamanan. Dengan melakukan asesmen yang komprehensif, organisasi dapat mengidentifikasi celah keamanan yang ada, mengimplementasikan langkah-langkah perbaikan yang sesuai, dan melindungi data sensitif mereka dari serangan yang berpotensi merugikan. Studi ini akan memberikan landasan yang kuat bagi organisasi untuk meningkatkan keamanan data mereka, memenuhi kebutuhan regulasi yang berlaku, dan membangun kepercayaan pelanggan serta pemangku kepentingan yang lain. Dalam era di mana data menjadi aset yang sangat berharga, penelitian dalam asesmen keamanan data menjadi semakin penting untuk menjaga integritas, kerahasiaan, dan ketersediaan informasi yang vital bagi kesuksesan suatu organisasi.

## I.13 Tantangan Penelitian

Tantangan dalam penelitian asesmen *maturity* keamanan data melibatkan berbagai faktor yang kompleks. Pertama, ketersediaan data yang memadai menjadi tantangan utama karena sulitnya menemukan data keamanan yang relevan dan representatif. Terkadang, data yang tersedia tidak lengkap, tidak konsisten, atau tidak terstruktur dengan baik, menghambat identifikasi pola keamanan dan analisis kematangan keamanan secara komprehensif.

Selanjutnya, kompleksitas lingkungan keamanan data menjadi tantangan yang signifikan. Lingkungan keamanan data terdiri dari sistem, aplikasi, infrastruktur, dan entitas yang beragam. Peneliti harus memahami dan mengelola kerumitan ini dengan memperoleh pemahaman mendalam tentang teknologi yang digunakan, kebijakan dan prosedur keamanan yang ada, serta dinamika organisasi yang mempengaruhi keamanan data.

Keterbatasan kerangka kerja dan metode juga menjadi tantangan yang harus dihadapi dalam penelitian ini. Meskipun ada beberapa kerangka kerja dan metode yang tersedia, belum ada kerangka kerja standar yang diakui secara luas. Peneliti harus mengadaptasi kerangka kerja yang sesuai dengan kebutuhan, konteks, dan tujuan spesifik organisasi.

Selain itu, pengembangan metode yang akurat, dapat diandalkan, dan praktis juga menjadi fokus penelitian yang kompleks ini.

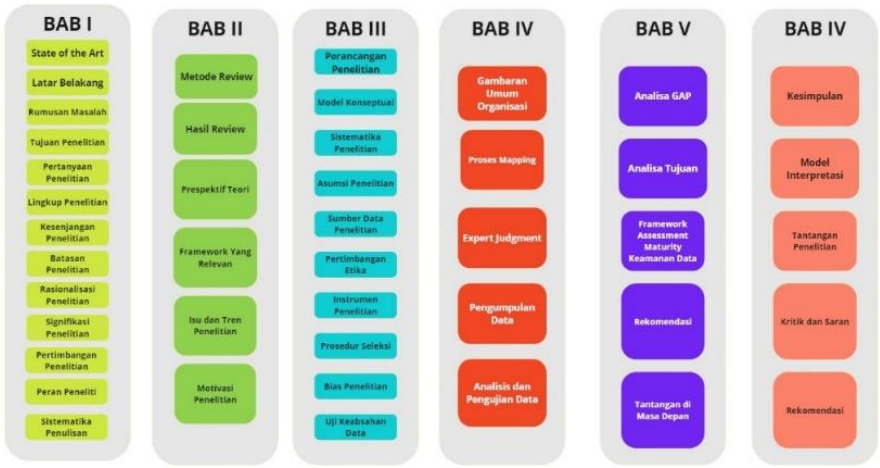
Perubahan dalam lingkungan keamanan data juga menjadi tantangan yang perlu ditangani. Teknologi terus berkembang, ancaman baru terus muncul, dan regulasi terus diperbarui. Penelitian asesmen tingkat kedewasaan keamanan data harus mengikuti perubahan ini dan mengantisipasi tren serta tantangan baru yang muncul. Pembaruan konstan pada kerangka kerja dan metode penelitian yang digunakan, serta pemahaman yang mendalam tentang tren keamanan data terbaru, menjadi penting dalam mengatasi tantangan ini.

Untuk mengatasi tantangan dalam penelitian ini, penting bagi peneliti untuk mengadopsi pendekatan yang holistik, melibatkan pemangku kepentingan yang relevan, dan terus memperbarui pengetahuan dan keterampilan dalam bidang keamanan data. Kolaborasi dengan praktisi keamanan data dan pemanfaatan kerangka kerja dan metode yang terbukti dapat membantu mengatasi tantangan ini dan menghasilkan penelitian berkualitas dalam asesmen *maturity* keamanan data.

## I.14 Sistematika Penulisan

Sistematika penulisan ini terbagi menjadi beberapa bab pokok pembahasan. Pada Bab I menjelaskan terkait dengan *state-of-the art* penelitian *maturity assessment* keamanan data. Adapun latar belakang diidentifikasi berdasarkan permasalahan serta melakukan pendekatan dalam menyolusikan permasalahan yang terjadi. Selain itu proses penetapan tujuan penelitian dan formulasi serta rumusan dari pertanyaan penelitian juga dituliskan pada Bab I. limitasi penelitian tentu perlu diidentifikasi dan perlu adanya rasionalisasi penelitian mengingat akan pentingnya dari penelitian ini untuk memberikan manfaat dan dampak dari penelitian dengan melakukan beberapa pertimbangan untuk dilanjutkan dengan ringkasan dari struktur penulisan penelitian ini. Bab II merangkum metode review yang digunakan oleh penulis, hasil dari review yang didapatkan dengan dukungan teori-teori yang diperoleh oleh penulis untuk memperkuat penelitian. Bagaimana *framework* yang cocok digunakan dalam penelitian dan isu maupun tren dalam penelitian keamanan data. Bab II berisi perancangan dari penelitian,

metode konseptual yang digunakan berupa model *Tree of Research*, untuk menjelaskan secara rinci sistematika penelitian, asumsi dari penelitian yang dilakukan serta sumber daya uang digunakan dalam penelitian. Selain itu terdapat etika penelitian, instrumen yang digunakan dalam penelitian, prosedur dalam memilih para ahli ataupun e*xpert judgment*, penentuan dari lingkup populasi responden kuesioner. Adapun langkah terakhir yang dilakukan yaitu melakukan validasi konten untuk memastikan penelitian data kualitatif tersebut tidak bias. Adapun tahapan keduanya melakukan validasi dan reliabilitas dari penelitian kuantitatif yang diperoleh dari hasil kuesioner responden.




Gambar I.4 Sistematika Penelitian

Bab IV berisi mengenai deskripsi singkat dari Yayasan, menjelaskan mengenai hasil perancangan asesmen dan validasi dengan *expert*, perancangan untuk kuesioner dan melakukan validasi dan reliabilitas dari hasil kuesioner tersebut. Bab V berisi analisis GAP dan hasil dari pengukuran maturity level dari keamanan data. Kemudian peneliti akan melakukan analisis dan menyusun rekomendasi pada setiap domain yang telah ditentukan nilai hasil akhirnya, kemudian melakukan rekomendasi dan saran perbaikan untuk Yayasan dapat meningkatkan nilai maturity yang telah diperoleh. Bab VI merupakan bab terakhir dalam penelitian ini berupa kesimpulan dari penelitian *maturity* asesmen keamanan data dan metode interpretasi dan tantangan yang dihadapi selama proses penelitian serta saran dan kritik untuk proses rekomendasi.