

Data Security Management of the Academic Information System at Kuningan University (SIKADUKU) Using the DAMA-DMBOK Framework

Toni Khalimi^{1*}, Rachmat Ismaya²

^{1,2} Teknik Informatika, Fakultas Ilmu Komputer, Universitas Kuningan, Kuningan, 45513, Indonesia

Informasi Artikel

Diterima : 18 Februari 2025
Revisi : 09 Maret 2025
Publikasi : 20 Maret 2025

Kata Kunci:

Manajemen Keamanan Data
Tata kelola data
Sistem Informasi Akademik
DAMA-DMBOK

ABSTRAK

Manajemen keamanan data menjadi sangat penting bagi sebuah sistem informasi, mengingat data yang sudah menjadi informasi tersebut dapat diakses oleh pengguna manapun. Manajemen keamanan data melindungi aset informasi yang sejalan dengan peraturan privasi dan kerahasiaan serta kebutuhan bisnis. Manajemen keamanan data yang kurang baik dapat berdampak tidak baik bagi proses manajemen yang berjalan. Untuk itu, perlu adanya manajemen data khususnya keamanan data sebagai langkah antisipatif dan penyelesaian terhadap masalah data dan keamanannya. Terdapat beberapa *framework* yang dapat diaplikasikan untuk mengelola keamanan data, salah satunya adalah DAMA-DMBOK. Dengan menggunakan dua area pengetahuan pada *framework* DAMA-DMBOK, yaitu Tata Kelola Data dan Manajemen Keamanan Data untuk membangun suatu sistem informasi akademik, memberikan hasil rekomendasi usulan rancangan tata kelola dan manajemen keamanan data yang kuat untuk sistem informasi akademik (SIA) Universitas Kuningan (SIKADUKU).

ABSTRACT

Data security management is crucial for an information system, considering that data that has been transformed into information can be accessed by any user. Data security management protects information assets in alignment with privacy and confidentiality regulations as well as business needs. Poor data security management can negatively impact ongoing management processes. Therefore, data management, particularly data security, is necessary as a preventive measure and a solution to data-related issues and their security. Several frameworks can be applied to manage data security, one of which is DAMA-DMBOK. By utilizing two knowledge areas within the DAMA-DMBOK *framework*, namely Data Governance and Data Security Management, for an academic information system, a proposed recommendation for governance and data security management design can be formulated for the Academic Information System (SIA) of Universitas Kuningan (SIKADUKU).

This is an open-access article under the [CC BY-SA](#) license



*Penulis Koresponden

Email: toni.khalimi@uniku.ac.id

Cara sitasi IEEE::

T. Khalimi, R. Ismaya, , "Data Security Management of the Academic Information System at Kuningan University (SIKADUKU) Using the DAMA-DMBOK Framework," *Journal of Artificial Intelligence and Software Engineering (J-AISE)*, vol. 5, no. 1, p. 1, Maret 2025. doi:10.30811/jaise.v5i1.6457

1. PENDAHULUAN

Pemanfaatan teknologi informasi dan komunikasi oleh institusi perguruan tinggi sudah merupakan hal yang biasa dan sudah menjadi keharusan. Hal ini agar perguruan tinggi dapat dengan cepat dan efisien merespon kebutuhan *stakeholder* nya. Guna mendukung kebutuhan ini, perguruan tinggi membuat dan menggunakan sistem informasi akademik. Namun pada saat yang sama, perguruan tinggi dihadapkan pada permasalahan data dan informasi, seperti terlalu banyak data dan terus bertambah, data yang tidak jelas dan tidak konsisten, serta tidak mengetahui bagaimana pengelolaan data yang baik dan benar mengingat keterbatasan sumber daya informasi yang dimiliki. Permasalahan ini terjadi akibat tidak diterapkannya tata kelola data yang baik. [1]

Disamping itu, manajemen yang baik akan menghasilkan proses bisnis yang baik. Dalam konteks sistem informasi, manajemen yang baik mencakup manajemen data dan keamanan datanya. Manajemen keamanan data menjadi penting bagi sebuah sistem informasi, mengingat data yang sudah menjadi informasi tersebut dapat diakses oleh pengguna manapun

Keamanan data merupakan proses melindungi *file*, *database*, dan akun pada jaringan dengan mengadopsi serangkaian kontrol, aplikasi, dan teknik yang mengidentifikasi kepentingan relatif dari *dataset* yang berbeda, sensitivitasnya, persyaratan kepatuhan peraturan dan kemudian menerapkan perlindungan yang sesuai untuk mengamankan sumber daya tersebut [2]. Keamanan informasi berarti melindungi informasi dan sistem informasi dari akses, penggunaan, pengungkapan, gangguan, modifikasi, pembacaan dengan teliti, inspeksi, perekaman atau perusakan yang tidak sah. Dengan demikian dapat dikatakan bahwa keamanan informasi mempunyai cakupan yang lebih luas dan kompleks dibandingkan dengan keamanan data.

Salah satu pengelolaan keamanan data adalah pengaturan hak akses. Dengan pengaturan hak akses ini, hanya pengguna tertentu saja yang dapat mengakses informasi sesuai dengan pengaturan hak akses yang ditetapkan. Beberapa kali terjadi penyusupan akses ke data yang bukan haknya dikarenakan sistem pengelolaan hak aksesnya masih lemah bahkan tidak sesuai dengan standarisasi. Hal ini dapat menyebabkan rusak, berubah bahkan hilangnya data.

Beberapa atribut untuk keamanan data mencakup hal-hal berikut: [3], [4]

1. Kerahasiaan (*Confidentiality / Privacy*)
Data tertentu hanya bisa diakses oleh orang yang berhak / memiliki kewenangan. Data-data seperti NIK, nomor KTP, nomor telepon, nama, alamat, tanggal lahir, nama orang tua dan lainnya merupakan data yang bersifat pribadi atau rahasia. Data-data tersebut mungkin diberikan ke pihak lain untuk kepentingan tertentu, misalnya untuk pendaftaran. Kerahasiaan menjamin data-data tersebut tidak sampai ke pihak yang tidak bertanggung jawab.
2. Keutuhan (*Integrity*) / Keaslian (*Authenticity*)
Merupakan usaha menjaga data dan informasi tidak diubah oleh pihak yang tidak berhak. Keutuhan juga menjamin data tidak mengalami kerusakan. Data yang memiliki keutuhan ialah ketika ia dibutuhkan haruslah tepat waktu, akurat, lengkap, dan konsisten. Keaslian menjamin data diterima oleh orang yang berhak bukan penyusup.
3. Ketersediaan (*Availability*)
Ketersediaan memastikan bahwa sistem bekerja dengan cepat dan layanan tidak ditolak untuk pengguna yang berwenang. Terkait dengan data / informasi, ketersediaan menjamin adanya data dan informasi ketika dibutuhkan oleh pengguna yang berhak.
4. Tidak Ada Pengingkaran (*Non Repudiation*)
Memastikan tidak terjadi pengingkaran terhadap data yang diberikan oleh si pengirim. [5]

Ketiga aspek pertama dikenal sebagai CIA *Triad* dalam sistem informasi dan data sangat penting dijadikan pedoman atau dasar kerangka kerja, yang dapat mencegah terjadinya kejahatan siber yang dapat merugikan organisasi atau perusahaan. Dengan mempertimbangkan ketiga aspek CIA organisasi dapat mengidentifikasi, mengevaluasi, dan mengurangi risiko keamanan secara menyeluruh. [6]

Sistem Informasi Akademik merupakan sumber daya dalam bentuk informasi yang berkaitan dengan masalah-masalah akademik di sebuah institusi perguruan tinggi. Sistem Informasi Akademik saat ini merupakan sistem informasi yang berbasis *web* yang bertujuan untuk membentuk *Knowledge Based System* yang dapat diakses *via* internet. Jenis informasi yang ada di dalam Sistem Informasi Akademik bisa berupa:

1. **Berita**, berisi informasi terbaru yang diterbitkan oleh lembaga pendidikan maupun informasi teknologi dari berbagai sumber berita.
2. **Pendidikan**, berisi informasi yang berkaitan dengan perkuliahan yang terdapat di lembaga pendidikan, misalnya kurikulum, Satuan Acara Perkuliahan (SAP), dosen, materi kuliah, Kerja Praktek, tugas akhir dan penelitian.
3. **Komunitas**, berisi tentang komunitas yang ada di lembaga pendidikan yang akan menginformasikan tentang Sivitas Akademika misalnya staf, mahasiswa, alumni, buletin dan lain-lain.
4. **Data Personal**, berisi Informasi yang berhubungan dengan mahasiswa diantaranya;

- a. **Kartu Rencana Studi (KRS)** sesuai dengan mata kuliah yang telah diprogramkan dalam satu semester.
- b. **Kartu Hasil Studi (KHS)** untuk mengetahui hasil yang telah dicapai selama mengikuti perkuliahan dan hasil evaluasi studi, sekaligus mengetahui indeks prestasinya.
5. **Jadwal Perkuliahan**, yang berisi tentang jadwal kuliah, kegiatan mahasiswa, memonitor jadwal perkuliahan dosen, jumlah kehadiran dalam mengikuti perkuliahan.
6. **Perpustakaan**, berisi tentang informasi buku melalui catalog online.
7. **Surat elektronik** (*electronic mail / e-mail*), fasilitas ini untuk mengirim dan menerima surat/pesan sekaligus dapat dijadikan sebagai sarana atau alat diskusi antar mahasiswa, dosen bahkan karyawan dalam lembaga pendidikan.

Dari sudut pandang entitas dan properti [1], sistem informasi akademik merujuk pada serangkaian sistem dan kegiatan yang digunakan untuk mengatur, memproses, dan menggunakan informasi sebagai sumber dalam suatu organisasi. Output dari informasi yang dihasilkan dari sistem ini akan memberikan informasi kepada para pemimpin atau pembuat keputusan yang dapat diklasifikasikan dalam pemanfaatan yang berbeda dan tujuan yang berbeda, yakni:

1. Sistem Informasi Akademik untuk tujuan menghasilkan laporan dalam berbagai kegiatan seperti akademik, keuangan, pribadi, distribusi siswa ke semua jenis jurusan.
2. Sistem Informasi Akademik untuk tujuan menjawab pertanyaan “bagaimana jika”. Sistem informasi ini menggunakan basis data untuk dibagikan kepada pengguna lain.
3. Sistem Informasi Akademik untuk keperluan mendukung pengambilan keputusan, evaluasi, dan pengembangan sistem. Sistem ini memberikan informasi untuk semua jenis pendidikan tinggi.

Tata kelola data dan manajemen keamanan data untuk sistem informasi akademik yang diterapkan oleh UNIKU belum menggunakan standar nasional maupun internasional. Pengelolaan data dan keamanannya dilakukan hanya berlandaskan pada nalar aktifitas umum mengikuti aturan akademik yang ada dan belum memiliki dokumen khusus yang menjadi acuan. Sehingga, meskipun sudah disistemkan dalam sebuah aplikasi, tetap saja diperlukan adanya strategi dalam menyelesaikan masalah data seperti strategi tata kelola data dan manajemen keamanan data.

Terjadi pelbagai masalah berkenaan dengan manajemen data dan keamanan datanya, seperti migrasi data dari sistem lama, terjadi beberapa permasalahan terkait kompatibilitas, kehilangan, dan kerusakan data penting. Dari sisi keamanan data, terjadi kasus pelanggaran data, yakni staf akademik mengubah nilai mahasiswa. Masalah lain lagi, kebiasaan dan kesadaran *user* dalam penggunaan/pendistribusian *password* untuk *login* ke sistem, beberapa masih belum menganggap hal yang sangat rahasia sehingga masih ada *password* yang ditempel di meja, diberikan ke rekan kerja lain dan sebagainya.

DAMA International atau The Data Management Association merupakan organisasi debut pertama bagi para profesional data di seluruh dunia yang bertujuan mempromosikan pemahaman, pengembangan, dan praktek pengelolaan data dan informasi untuk mendukung strategi bisnis. Sedangkan, DAMA Foundation adalah afiliasi penelitian dan pendidikan DAMA International, yang didedikasikan untuk mengembangkan profesi manajemen data dan mempromosikan kemajuan konsep dan praktek untuk mengelola data dan informasi sebagai aset perusahaan.

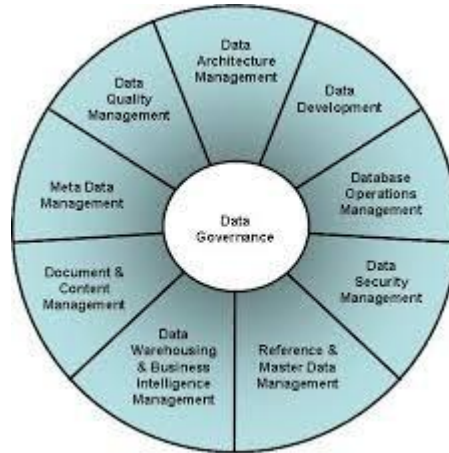
Misi gabungan DAMA International dan DAMA Foundation, secara kolektif dikenal sebagai DAMA, adalah untuk memimpin profesi manajemen data menuju kematangan (*maturity*). DAMA mempromosikan pemahaman, pengembangan, dan praktek pengelolaan data, informasi, dan pengetahuan sebagai aset utama perusahaan, terlepas dari *vendor*, teknologi, dan metode tertentu. DAMA International menghasilkan dokumen The Guide to the Data Management Body of Knowledge (the DAMA-DMBOK Guide). [7], [8]

Framework DAMA-DMBOK terdiri atas 10 fungsi komponen utama dengan tata kelola data (*data governance*) sebagai intinya dimana setiap fungsi memiliki cakupannya sendiri (Gambar 1). Tata Kelola Data melaksanakan otoritas perencanaan (*planning*), pengawasan (*supervision*) dan kontrol (*control*) serta penegakan (*enforcement*) atas manajemen dan penggunaan data. Fungsi Tata Kelola Data ini berinteraksi dengan dan mempengaruhi masing-masing dari sepuluh fungsi manajemen data di sekitarnya, termasuk fungsi Manajemen Keamanan Data. [7]

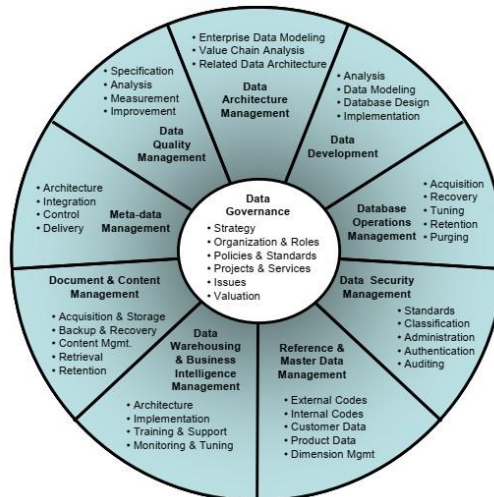
Terdapat 10 fungsi dan 102 aktivitas. Jika terdapat lebih dari 12 aktivitas dalam satu fungsi, aktivitas dikelompokkan ke dalam dua atau lebih subfungsi. Fungsi dan subfungsi diberi nama dengan frasa kata benda, sedangkan aktivitas diberi nama dengan frasa kata kerja (Gambar 2). Setiap aktivitas dikategorikan sebagai milik salah satu dari empat grup:

1. Aktivitas Perencanaan (P), menetapkan arah strategis dan taktis untuk aktivitas manajemen data lainnya. Aktivitas perencanaan dapat dilakukan secara berulang.
2. Aktivitas Kontrol (C), dilakukan secara berkelanjutan.
3. Aktivitas Desain (D), dilakukan dalam proyek dan diakui sebagai bagian dari *systems development lifecycle* (SDLC), menciptakan hasil data melalui analisis, desain, pembangunan, pengujian, dan penerapan.

4. Aktivitas Operasional (O), merupakan aktivitas layanan dan dukungan yang dilakukan secara berkelanjutan.

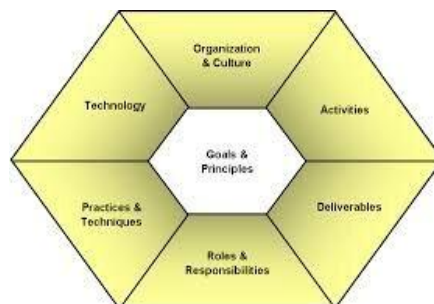


Gambar 1. Fungsi-fungsi Manajemen Data



Gambar 2. Ringkasan Lingkup Fungsi-fungsi Management Data

Selain mengidentifikasi 10 fungsi manajemen data, Kerangka kerja ini juga mengidentifikasi 7 Elemen Lingkungan, 7 Elemen Lingkungan menyediakan cara yang logis dan konsisten untuk menggambarkan setiap fungsi (Gambar 3). [8]



Gambar 3. Element-elemen Lingkungan

Elemen Lingkungan itu sendiri terbagi menjadi dua kategori: **dasar** (Sasaran dan Prinsip, Aktifitas, Hasil Utama, dan Peran dan Tanggung Jawab) dan **pendukung** (Praktek dan Teknik, Teknologi, dan Organisasi dan Budaya). Adapun ruang lingkup masing-masing Elemen Lingkungan ditunjukkan pada Gambar 3. [7]

Elemen Lingkungan dasar adalah: [7], [8], [9]

- Sasaran dan Prinsip (*Goals and Principles*): sasaran bisnis terarah dari setiap fungsi dan prinsip dasar yang memandu kinerja masing-masing fungsi.
- Aktifitas (*Activity*): Setiap fungsi terdiri dari kegiatan tingkat bawah. Beberapa kegiatan dikelompokkan ke dalam sub kegiatan. Kegiatan selanjutnya didekomposisi menjadi tugas dan langkah.
- Hasil Utama (*Main Delivery*): Informasi dan basis data fisik dan dokumen yang dibuat sebagai keluaran sementara dan akhir dari masing-masing fungsi. Beberapa hasil sangat penting, beberapa umumnya direkomendasikan, dan yang lain opsional tergantung pada keadaan.
- Peran dan Tanggung Jawab (*Roles and Responsibilities*): Peran bisnis dan TI yang terlibat dalam melakukan dan mengawasi fungsi itu, dan tanggung jawab spesifik masing-masing peran dalam fungsi itu. Banyak peran akan berpartisipasi dalam berbagai fungsi.

Fungsi Manajemen Keamanan Data – fungsi keempat *framework* DAMA-DMBOK – menjamin privasi (*privacy*), kerahasiaan (*confidentiality*), dan akses yang tepat. Fungsi ini menjabarkan bagaimana melakukan perencanaan, pengembangan, dan pelaksanaan kebijakan dan prosedur keamanan untuk menyediakan otentikasi (*authentication*), otorisasi (*authorization*), akses (*access*), dan audit data dan informasi yang tepat. Kebijakan dan prosedur keamanan data yang efektif memastikan bahwa orang yang tepat dapat menggunakan dan memperbarui data dengan cara yang benar, dan bahwa semua akses dan pembaruan yang tidak pantas dibatasi. Sedangkan fungsi tata kelola data memandu dan mengontrol bagaimana fungsi manajemen keamanan data itu dilakukan [7], [8]. Dengan demikian, *framework* DAMA-DMBOK dapat dijadikan acuan untuk membantu menerapkan (*implement*) dan meningkatkan (*improve*) pengelolaan keamanan data SIKADUKU.

Beberapa penelitian yang mengadopsi *framework* DAMA telah dilakukan sebelumnya, diantaranya oleh Ferra Arik Tridalestari, dan Hanung Nindito Prasetyo. dengan topik Pembangunan Roadmap Tata Kelola Data di Perguruan Tinggi X dengan Menggunakan *Framework* DAMA. Penelitian ini berhasil menyusun *roadmap* Tata Kelola Data untuk Perguruan Tinggi dengan Menggunakan *Framework* DAMA International. [10]

Penelitian lainnya dilakukan oleh Hanung Nindito Prasetyo, dan Kridanto Surendro. Mereka berdua melakukan perbandingan *framework* Tata Kelola Data DGI dan DAMA International. Mereka menyimpulkan bahwa DAMA International memberikan pendekatan model tata kelola data secara fungsional atau lebih tepatnya memberikan ruang-ruang berupa artefak bagi organisasi atau perusahaan untuk ‘mengisi’-nya. Namun model ini dominan fokus pada manajemen data dan kurang menyentuh sisi tata kelola (*governance*) secara menyeluruh. [11]

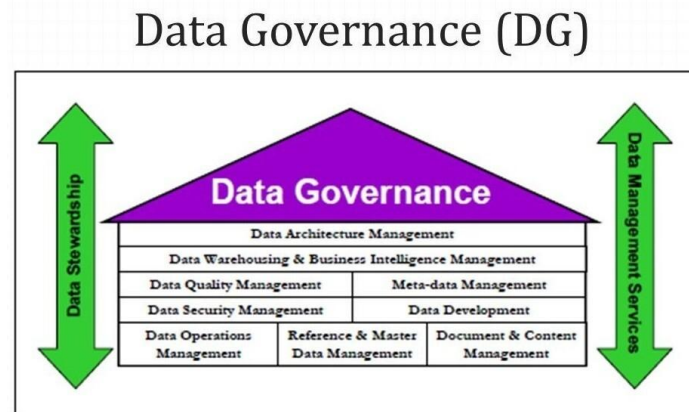
Selanjutnya, penelitian yang dilakukan oleh Muhammad Fajrin yang mencoba menyusun Pedoman Manajemen Data untuk Implementasi *Open Data* di Indonesia untuk 5 (lima) *knowledge area framework* DAMA-DMBOK, yaitu Tata Kelola Data, Manajemen Operasi Data, Manajemen Data Master dan Referensi, Manajemen Data Warehouse dan Business Intelligence, Manajemen Dokumen dan Konten). Penelitian ini menghasilkan Dokumen Pedoman Manajemen Data untuk Implementasi *Open Data* untuk 5 (lima) *knowledge area framework* DAMA-DMBOK tersebut. [12]

Penelitian lainnya dilakukan oleh Ferra Arik Tridalestari, dan Hanung Nindito Prasetyo. Peneliti melakukan identifikasi fungsi Tata Kelola Data *Framework* DAMA International pada Universitas X, dan menghasilkan dokumen fungsi tata kelola data untuk perguruan tinggi berdasarkan *framework* DAMA International. [13]

Terakhir, penelitian yang dilakukan oleh Hanung Nindito Prasetyo. Beliau melakukan peninjauan terhadap tingkat kematangan tata kelola data di perguruan tinggi menggunakan acuan model pengukuran tata kelola data IBM dan DAMA International. Penelitian memperlihatkan bahwa DAMA lebih fokus pada pencapaian manajemen data teknis. Sehingga peneliti menyimpulkan bahwa apabila organisasi ingin mengukur tingkat kematangan tata kelola data berdasarkan pemenuhan struktur tata kelola data, dapat menggunakan pendekatan DAMA International karena sifatnya yang lebih teknis. [14]

Beberapa penelitian tersebut memperlihatkan bahwa pembangunan model tata kelola data dan keamanan data, apalagi untuk data-data yang tersedia secara bebas untuk di akses dan dimanfaatkan oleh masyarakat luas (*open data*) merupakan hal yang penting. Dari sejumlah penelitian tersebut belum ada yang fokus pada *knowledge area* Manajemen Keamanan Data (fungsi keempat) *framework* DAMA International.

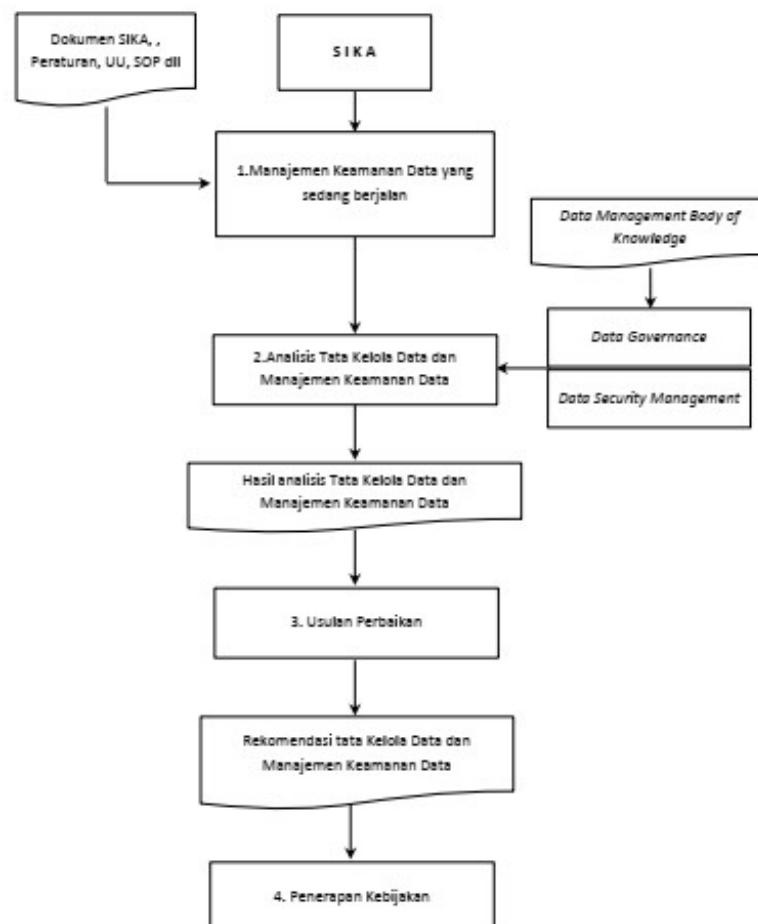
Tata Kelola Data merupakan area fungsional utama dari *framework* Manajemen Data DAMA seperti yang ditunjukkan pada Gambar 1 dan 3, yang berinteraksi dengan dan memengaruhi masing-masing dari sepuluh fungsi manajemen data di sekitarnya. Oleh karena itu, tata kelola data menjadi jantung dari pengelolaan aset data sehingga harus diperhatikan dan diungkap untuk menjaga efisiensi dan efektifitas manajemen data. Tata kelola data Posisi kontrol dari tata kelola data, digambarkan sebagai "atap manajemen" atas fungsi-fungsi manajemen data lainnya, seperti yang ditunjukkan oleh Gambar 4.



Gambar 4. Tata Kelola Data, *Stewardships*, dan Layanan

2. METODE

Penelitian ini menggunakan metode deskriptif yakni melakukan analisis pekerjaan dan aktifitas [15]. dengan mengambil studi kasus Sistem Informasi Akademik Universitas Kuningan (SIKADUKU). Dengan demikian, penelitian ini bersifat kualitatif [16]. Adapun kerangka berfikir dalam melakukan penelitian ini tersaji pada Gambar 5.



Gambar 5. Kerangka berfikir penelitian

Dalam melaksanakan penelitian metode analisis pekerjaan dan aktifitas dibutuhkan data-data terkait manajemen keamanan data dengan objek SIKADUKU ini. Berdasarkan sumber data dari tempat penelitian, diperoleh 2 jenis data yang diperlukan sebagai berikut.

1. Data Primer

Data primer dihimpun langsung dari tempat penelitian, yakni dari UNIKU dan PUSINFO, lembaga yang bertanggungjawab mengelola Sistem Informasi Akademik Terpadu UNIKU. Dokumen yang diperoleh: *blue print* pengembangan TIK, arsitektur, infrastruktur, konektivitas jaringan internet dan intranet, *software* sistem informasi akademik, *software* aplikasi dan layanan elektronik lainnya.

Fungsi Bisnis		Data Logik																					
		Mahasiswa	Dosen	FMB	Prodi	Fakultas	Marakuliah	Nilai	Pengajaran Dosen	Penilaian	Konversi	Absensi	Proposal	Skripsi/Tesis	Sidang	Wisuda	SPP	Total SPP	Registrasi	Biaya Lain	Tahun Akademik	Kalender	KRS
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
	Penerimaan Pendaftaran Mahasiswa Baru	1		CRUD																			
	Administrasi Mahasiswa baru	2	R														CRUD	R	CRUD	CRUD	R		
	Penetapan Mahasiswa Baru	3	CRUD		R												R	R	R	R	R		
	Data Mahasiswa Baru	4	CRUD		R																		
	Konfigurasi Registrasi Mahasiswa	5	R																				
	Registrasi Mahasiswa	6	R																				
	Administrasi Mahasiswa	7	R														CRUD	R	CRUD	CRUD	R		
	Data Mahasiswa	8	CRUD					R	R		R		CRUD				R	R	R	R	R		
	Konversi Nilai Mahasiswa	9	R					R					CRUD										
	Master Data Akademik	10		CRUD		CRUD	CRUD														CRUD		
	Master Kurikulum	11		R		R	R	CRUD				CRUD										R	
	Penetapan Kalender Akademik	12																				R	CRUD
	Herregistrasi Mahasiswa	13	R																		CRUD	R	R
	Perubahan Rencana Studi	14	R	R		R	R	R		R												R	CRUD
	Penilaian	15	R	R		R	R					CRUD										R	
	Perkuliahan	16	R	R		R	R	R	R														R
	Administrasi Keuangan	17	R														CRUD	CRUD	CRUD	CRUD	R	R	R
	Penilaian	18	R	R		R	R	R	CRUD	R												R	R
	Status Mahasiswa	19	U																			R	
	Drop Out	20	U																			R	
	Penyunduran Diri	21	U																			R	
	Sidang Proposal	22	R																			R	R
	Sidang Akhir	23	R																			R	R
	Pembuatan Ijazah	24	R			R	R	R	R													R	R
	Pembuatan Transkrip Akademik	25	R			R	R	R	R													R	R
	Wisuda	26	U														CRUD					R	R

Gambar 6. Matriks Komponen Data dan Fungsi Bisnis

Data primer diperoleh melalui:

- Observasi / pengamatan langsung SIKADUKU UNIKU selama kurang lebih 3 tahun. Dari observasi langsung ini diperoleh tabel Matriks Komponen Data dan Fungsi Bisnis yang menggambarkan ketersediaan sistem informasi, integrasi dan operasionalisasi sistem informasi dan layanan lainnya. (Gambar 6)
- Wawancara mendalam atau *in-depth interview* dengan Wakil Rektor, Kepala Biro, Dekan, Kepala Unit, dan dosen untuk memperoleh data dan informasi serta kebijakan.

Untuk kebutuhan wawancara ini, disusun daftar pertanyaan berkaitan dengan tata kelola data dan manajemen keamanan data sesuai *framework* DAMA.

2. **Data Sekunder**

Data sekunder digunakan untuk melengkapi data primer. Data sekunder diperoleh dari beberpa referensi berupa jurnal, paper, laporan hasil penelitian, arsip dan situs serta peraturan perundangan yang berlaku.

3. **HASIL DAN PEMBAHASAN**

Hasil proses penilaian atau *assessment* terhadap hasil wawancara maupun pengumpulan, dan penafsiran temuan bukti pada SIKADUKU untuk aktifitas Tata Kelola Data dan Manajemen Keamanan Data disajikan dalam Tabel 1 dan 2.

Tabel 1. Hasil proses indentifikasi tata kelola data

Aktivitas	Tersedia	
	Ya	Tidak
Tata Kelola Data		
1. Perencanaan Manajemen Data		
1.1. Memahami Kebutuhan Data Strategis Perusahaan	√	
1.2. Membangun dan Memelihara Strategi Data	√	
1.3. Menetapkan Peran Data Profesional dan Organisasi		√
1.4. Mengidentifikasi dan Menunjuk Data <i>Stewards</i>		√
1.5. Membentuk Organisasi Tata Kelola Data dan Penatalayanan (<i>Stewardship</i>)		√

1.6.	Mengembangkan dan Menyetujui Kebijakan, Standar, dan Prosedur Data	√	
1.7.	Meninjau dan Menyetujui Arsitektur Data	√	
1.8.	Merencanakan dan Mensponsori Proyek dan Layanan Manajemen Data		√
1.9.	Memperkirakan Nilai dan Biaya yang terkait dengan Aset Data		√
2.	Pengawasan Manajemen Data		
2.1.	Mengawasi Organisasi dan Staf Data Profesional		√
2.2.	Mengelola dan Menyelesaikan Masalah yang Berkaitan dengan Data	√	
2.3.	Memantau dan Memastikan Kepatuhan Regulasi		√
2.4.	Memantau dan Memberlakukan Kesesuaian Kebijakan, Standar, dan Arsitektur Data		√
2.5.	Mengawasi proyek dan layanan manajemen data.		√
2.6.	Mengkomunikasikan dan mendorong peningkatan nilai dari aset data.		√

Tabel 2. Hasil proses identifikasi manajemen keamanan data

Aktivitas	Tersedia	
	Ya	Tidak
Manajemen Keamanan Data		
1. Memahami Kebutuhan Keamanan Data dan Persyaratan Pengaturan (<i>Regulatory Requirements</i>)		√
2. Mendefinisikan Kebijakan Keamanan Data		√
3. Mendefinisikan Standar Keamanan Data		√
4. Mendefinisikan Kontrol dan Prosedur Keamanan Data		√
5. Mengelola Users, Passwords, and Grup Keanggotaan (Group Membership)	√	
6. Mengelola View dan Permission Akses Data	√	
7. Memantau User Authentication dan Access Behavior	√	
8. Mengklasifikasi Kerahasiaan Informasi		√
9. Mengaudit Keamanan Data		√

Berdasarkan hasil identifikasi pemenuhan aktivitas Tata Kelola Data dan Manajemen Keamanan Data, ternyata pada SIKADUKU masih ditemukan aktivitas yang belum sesuai dengan *framework* DAMA International. Hal ini karena memang secara umum SIKADUKU belum menerapkan satu pun manajemen data atau informasi berstandar internasional semisal DAMA International, DGI, ISO/IEC atau lainnya. Padahal, penelitian dalam domain tata kelola data semakin berkembang di bidang sistem informasi karena semakin banyak organisasi termasuk perguruan tinggi yang menganggap data sebagai aset yang berharga. [5]

Hasil pengolahan menunjukkan bahwa sistem informasi akademik tersebut belum memenuhi artefak standar keamanan data seperti yang ditetapkan oleh *framework* DAMA International. Dari aktivitas tata kelola data misalnya, belum terbentuk Organisasi Tata Kelola Data dan Penatalayanan (*Stewardship*). Hal ini tentunya akan kesulitan dan tentunya menjadi kendala dalam penyusunan manajemen keamanan datanya. Adapun untuk pemenuhan peran dalam Dewan Tata Kelola Data di Universitas Kuningan tersaji pada Tabel 3.

Tabel 3. Peran dalam dewan tata kelola UNIKU

Peran	Deskripsi	Pekerjaan dalam Perguruan Tinggi
Dewan tata kelola data	Adalah kelompok yang dibentuk untuk menerapkan Program tata kelola data pada Universitas	<ul style="list-style-type: none"> • Rektor • Wakil Rektor • Dekan • Wakil Dekan • Prodi • DII
Data Steward	Data Steward bertanggung jawab untuk meminimalkan penggunaan, penyimpanan, dan paparan informasi sensitif, terutama informasi pribadi. Selain itu memiliki tanggung jawab untuk membatasi penggunaan dan paparan informasi tersebut kepada unit atau individu lain yang membutuhkan data organisasi	<ul style="list-style-type: none"> • Kepala TU • Kepala PUSINFO • dan staf
Data Kustodian	Manajer dan / atau administrator sistem atau media yang memiliki informasi berada, termasuk namun tidak terbatas pada komputer pribadi, komputer laptop, PDA, <i>smartphone</i> , <i>server</i> , database perusahaan, sistem penyimpanan, CD/DVD, USB drive, file-file	<ul style="list-style-type: none"> • Kepala PUSINFO

	kertas, dan perangkat lainnya yang <i>removable</i> atau <i>portable</i> atau penyimpanan teknologi	
Pengguna Data (<i>Users</i>)	Individu yang mengelola sekaligus juga Pengguna data di perguruan tinggi	Siapa saja yang berkaitan dengan proses pengelolaan dan penggunaan data

Sebelum menyusun dan menetapkan rekomendasi penerapan Manajemen Keamanan Data dibuat pemetaan pengolahan/aktivitas untuk Manajemn Keamanan Data (Tabel 4). Setelah itu, dengan mengacu pemetaan ini, disusun dan ditetapkan rekomendasi rancangan usulan perbaikan Sistem Informasi Akademik SIKADUKU UNIKU.

Tabel 4. Pemetaan rekomendasi aktivitas manajemen keamanan data

Grup Aktivitas	Aktivitas	Aktivitas Praktek Terbaik	Keluaran
Perencanaan (P)	Manajemen Keamanan Data		
	1. Memahami Kebutuhan Keamanan Data dan Persyaratan Pengaturan (<i>Regulatory Requirements</i>)	<ul style="list-style-type: none"> Memahami arah dan tujuan organisasi. Menganalisis kondisi organisasi saat ini Menganalisis kebutuhan data strategis organisasi Menganalisis kebutuhan data untuk aplikasi SIKADUKU) 	<ul style="list-style-type: none"> Daftar kebutuhan data strategis organisasi. Kebijakan, standar, dan prosedur terkait data. Roadmap implementasi manajemen data. Penatalayanan data organisasi.
Perencanaan (P)	2. Mendefinisikan Kebijakan Keamanan Data	<ul style="list-style-type: none"> Menganalisis persyaratan keamanan data yang diperlukan organisasi. Meninjau persyaratan keamanan data organisasi. Mengidentifikasi kebijakan keamanan data untuk organisasi. 	<ul style="list-style-type: none"> Kebijakan keamanan data teridentifikasi. Kebijakan keamanan data.
Perencanaan (P)	3. Mendefinisikan Standar Keamanan Data	<ul style="list-style-type: none"> Menganalisis insiden keamanan data yang terjadi. Menganalisis standar keamanan data yang diperlukan organisasi. Meninjau persyaratan keamanan data organisasi. Mengidentifikasi standar keamanan data untuk organisasi. 	<ul style="list-style-type: none"> Standar keamanan data terdefinisi. Standar keamanan data.
Desain (D)	4. Mendefinisikan Kontrol dan Prosedur Keamanan Data	<ul style="list-style-type: none"> Melakukan pelacakan dan pemanantauan perubahan data dari waktu ke waktu. Mengidentifikasi data pribadi yang bersifat rahasia seperti data keuangan, gaji dan sebagainya. Memahami regulasi terkait prosedur dan kontrol penggunaan data. Menyusun prosedur dan kontrol keamanan data. 	<ul style="list-style-type: none"> Dokumen prosedur dan kontrol keamanan data .
Operasional (O)	5. Mengelola <i>Users, Passwords, and Group Keanggotaan (Group Membership)</i>	<ul style="list-style-type: none"> Mengidentifikasi sumber daya (<i>platform</i>, sistem aplikasi, perangkat keras dan komunikasi) dan kemampuan sistem informasi. Menganalisis kemampuan mekanisme sinkronisasi antara sumber daya dan kemampuan sistem informasi bagi kemudahan manajemen <i>password</i> pengguna. Menetapkan kebijakan penetapan, perubahan, dan tingkat kompleksitas <i>password</i>. 	<ul style="list-style-type: none"> Ditetapkannya grup keanggotaan aplikasi dan profil pengguna. Ditetapkannya aturan dan persyaratan penggunaan <i>password</i>.
Operasional (O)	6. Mengelola <i>View dan Permission Akses Data</i>	<ul style="list-style-type: none"> Melakukan kontrol akses berbasis peran. Pemberian ijin kepada setiap anggota dari grup peran. Membatasi akses ke bidang yang lebih rahasia. Merancang <i>view</i> aplikasi yang nyaman bagi administrator. 	<p>Semua pengguna dalam suatu grup pengguna diberikan hak akses sesuai dengan perannya dalam pemakaian sistem SIKADUKU).</p>

Control (C)	7.	Memantau <i>User Authentication</i> dan <i>Access Behavior</i>	<ul style="list-style-type: none"> • Memutuskan apa yang perlu dipantau dan seberapa lama pemantauan dilakukan, serta melakukan tindakan bila terjadi peringatan. • Melakukan pemantauan secara aktif dan <i>real-time</i> untuk data-data yang mengandung informasi rahasia seperti data keuangan. • Melakukan pemantauan pasif dengan melacak perubahan dari waktu ke waktu dengan mengambil snapshot keadaan sistem saat ini secara berkala. • Membandingkan kecenderungan perubahan dengan tolok ukur atau sekumpulan kriteria yang ditetapkan. 	<ul style="list-style-type: none"> • Laporan hasil pemantauan baik secara aktif, <i>real-time</i> maupun pasif. • Daftar langkah / tindakan yang diambil untuk menangani masalah.
	Desain (D)	8.	Mengklasifikasi Kerahasiaan Informasi	<ul style="list-style-type: none"> • Menganalisis tingkat kerahasiaan data organisasi. • Menetapkan tingkat kerahasiaan data organisasi dengan benar. • Memberi label tingkat kerahasiaan yang sesuai untuk setiap dokumen. • Melakukan evaluasi klasifikasi tingkat kerahasiaan data organisasi.
Control (C)	9.	Mengaudit Data Keamanan	<ul style="list-style-type: none"> • Menganalisis kebijakan dan standar keamanan data terhadap praktik dan kebutuhan terbaik. • Menganalisis prosedur implementasi dan praktik aktual untuk memastikan konsistensi dengan sasaran, kebijakan, standar, pedoman, dan hasil keamanan data yang diinginkan. • Menilai apakah standar dan prosedur yang ada memadai dan sesuai dengan persyaratan bisnis dan teknologi. • Memverifikasi bahwa organisasi mematuhi persyaratan peraturan. • Meninjau keandalan dan keakuratan data audit keamanan data. • Mengevaluasi prosedur eskalasi dan mekanisme pemberitahuan jika terjadi pelanggaran keamanan data. • Meninjau kontrak, perjanjian berbagi data, dan kewajiban keamanan data vendor luar dan eksternal, memastikan mereka memenuhi kewajiban mereka, dan memastikan organisasi memenuhi kewajibannya untuk data yang bersumber eksternal. • Melaporkan kepada manajemen senior, pelayan data, dan pemangku kepentingan lainnya tentang "Keadaan Keamanan Data" (<i>State of Data Security</i>) di dalam organisasi dan kematangan praktiknya. • Merekomendasikan desain keamanan data, operasional, dan peningkatan kepatuhan 	Audit Keamanan Data.

Dalam melaksanakan penerapan *framework* DAMA-DMBOK (penyusunan dan penerapan rekomendasi) diperhatikan juga Elemen-elemen Lingkungan (Gambar 2). Pelengkapan Elemen Lingkungan ini bisa megacu kepada peraturan perundangan, dan tridharma perguruan tinggi, sehingga dihasilkan manajemen keamanan data yang baik sebagai berikut:

1. Komitmen pimpinan universitas dalam mendorong penerapan *framework* DAMA-DMBOK.
2. Memahami dengan seksama dan bijaksana kultur manajemen universitas
3. Dibentuk tim khusus yang terdiri dari data profesional dan data *stewards*.

4. KESIMPULAN

Penelitian ini berhasil melakukan identifikasi pemenuhan area fungsi Tata Kelola Data dan Manajemen Keamanan Data berdasarkan *framework* DAMA-DMBOK pada SIKADUKU Universitas Kuningan. Dan menghasilkan luaran berupa usulan rekomendasi rancangan Manajemen Keamanan Data terhadap sistem informasi akademik SIKADUKU Universitas Kuningan dalam bentuk dokumen.

Sebaiknya penelitian diawali dengan identifikasi dan penyusunan Tata Kelola Data secara lebih mendalam guna efisiensi dan efektifitas dari fungsi area Manajemen Keamanan Data. Penelitian ini dapat dikembangkan dengan menambah fungsi area lain dari *framework* DAMA International, seperti Database Operations Management dan sebagainya.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada semua pihak yang telah berkontribusi dan mendukung penelitian ini. Ucapan terima kasih disampaikan kepada pihak Universitas Kuningan atas bantuan kebijakan dan finansial, khususnya Pusinfo yang telah memberikan materi dan bahan serta waktunya guna penyelesaian penelitian, dan juga mendorong penyusunan jurnalnya.

REFERENSI

- [1] E. Indrayani, "Management of academic information system (AIS) at higher education in the city of Bandung," *Procedia-Social and Behavioral Sciences*, vol. 103, pp. 628-636, 2013.
- [2] M. Buckbee, "Data security: Definition, explanation and guide," *Retrieved December*, vol. 20, p. 2019, 2019.
- [3] R. A. Azdy, "Tanda tangan digital menggunakan algoritme keccak dan RSA," *Jurnal Nasional Teknik Elektro dan Teknologi Informasi*, vol. 5, no. 3, pp. 184-191, 2016.
- [4] T. W. Edgar and D. O. Manz, *Research methods for cyber security*. Syngress, 2017.
- [5] I. Alhassan, D. Sammon, and M. Daly, "Data governance activities: an analysis of the literature," *Journal of Decision Systems*, vol. 25, no. sup1, pp. 64-75, 2016.
- [6] A. H. H. Harahap, C. D. Andani, A. Christie, D. Nurhaliza, and A. Fauzi, "Pentingnya Peranan CIA Triad Dalam Keamanan Informasi dan Data Untuk Pemangku Kepentingan atau Stakholder," *Jurnal Manajemen dan Pemasaran Digital*, vol. 1, no. 2, pp. 73-83, 2023.
- [7] M. Mosley, M. Brackett, and S. Earley, "The DAMA Guide to The Data Management Body of Knowledge (DAMA-DMBOK Guide)," 2009.
- [8] M. Mosley, "DAMA DMBOK Functional Framework (version 3.02)," *DAMA International*, 2008.
- [9] D. International, *DAMA-DMBOK: Data management body of knowledge*. Technics Publications, LLC, 2017.
- [10] F. A. Tridalestari and H. N. Prasetyo, "Pembangunan Roadmap Tata Kelola Data di Perguruan Tinggi X dengan Menggunakan Framework Dama International," 2014.
- [11] H. N. Prasetyo and K. Surendro, "Perbandingan Framework Tata Kelola Data DGI dan DAMA International," in *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*, 2013.
- [12] M. Fajrin, "Pedoman Manajemen Data untuk Implementasi Open Data di Indonesia, (Area Tata Kelola Data, Manajemen Operasi Data, Manajemen Data Master dan Referensi, Manajemen Data Warehouse dan Business Intelligence, Manajemen Dokumen dan Konten)," 2015. STEI ITB.
- [13] F. A. Tridalestari and H. N. Prasetyo, "Identifikasi Fungsi Tata Kelola Data Framework Dama International Pada Universitas X," *Jurnal Ilmiah Teknologi Infomasi Terapan*, vol. 2, no. 1, 2015.
- [14] H. N. Prasetyo, "A review of data governance maturity level in higher education," *Jurnal Ilmiah Teknologi Infomasi Terapan*, vol. 3, no. 1, 2016.
- [15] D. Rahmat, "Perencanaan Sistem Manajemen Keamanan Informasi Menggunakan Standar Sni Iso/Iec 27001: 2013," *COMPUTING/ Jurnal Informatika*, vol. 6, no. 2, pp. 37-41, 2019.
- [16] D. Priharsari and D. Y. Liliana, "Persoalan Sistem Informasi Dan Metode Yang Dapat Dipilih Untuk Mempelajarinya: Information Systems Problems And Approaches To Study The Problems," *Jurnal Sistem Informasi, Teknologi Informasi, dan Edukasi Sistem Informasi*, vol. 1, no. 2, 2020.