**Kopekan UTS Open-Book Matkul Manajemen dan Infrastruktur Data**

***Tugas Pertemuan 1***

1. **Apa Definisi tata kelola data ?**

Tata kelola data (Data Governance) adalah suatu sistem yang mengatur hak-hak dan akuntabilitas pengambilan keputusan dalam proses-proses terkait informasi, yang dilaksanakan sesuai dengan model-model yang telah disepakati untuk mengatur siapa yang boleh melakukan, terhadap informasi apa, dalam kondisi seperti apa, dan dengan metode apa (Data Governance Institute, 2005).

Dalam implementasinya, menurut Russom (2008), tata kelola data umumnya termanifestasi dalam bentuk dewan tata kelola data di tingkat eksekutif, atau forum serupa yang merumuskan dan menegakkan kebijakan serta prosedur tentang pemanfaatan dan pengelolaan teknis data yang berlaku untuk seluruh organisasi.

Russom juga menyatakan bahwa tujuan umum tata kelola data adalah meningkatkan kualitas data, mengakurkan inkonsistensi data, berbagi data secara luas, memanfaatkan agregasi data untuk memperoleh keunggulan kompetitif, mengelola perubahan data dengan memperhatikan pola penggunaan data, dan mematuhi regulasi internal maupun eksternal serta standar penggunaan data yang disepakati. Pada dasarnya, tata kelola data adalah lembaga organisasi yang mengawasi penggunaan dan kegunaan data sebagai aset organisasi.

1. **Apa konsep dasar tata kelola data?**

Konsep dasar tata kelola data berfokus pada bagaimana sebuah organisasi mengelola, melindungi, dan memaksimalkan nilai data yang dimilikinya. Ada beberapa elemen penting dalam tata kelola data yang harus dipahami:

1. **Kualitas Data (Data Quality):** Tata kelola data bertujuan untuk memastikan bahwa data yang digunakan dalam suatu organisasi akurat, konsisten, dan relevan. Ini berarti menghindari kesalahan, duplikasi, dan data yang tidak lengkap.
2. **Keamanan Data (Data Security)**: Aspek ini melibatkan perlindungan data dari ancaman, baik dari luar maupun dari dalam. Data yang sensitif, seperti informasi pribadi pelanggan, harus diamankan agar tidak jatuh ke tangan yang salah.
3. **Aksesibilitas Data (Data Access)**: Data yang dikelola dengan baik harus bisa diakses oleh orang yang tepat pada waktu yang tepat. Ini memastikan bahwa keputusan bisnis dapat dibuat berdasarkan data yang valid dan up-to-date.
4. **Kepatuhan terhadap Regulasi (Compliance)**: Tata kelola data juga mencakup pemenuhan aturan dan regulasi yang mengatur penggunaan data. Misalnya, banyak negara memiliki undang-undang perlindungan data pribadi yang harus dipatuhi oleh organisasi.
5. **Pengelolaan Siklus Hidup Data (Data Lifecycle Management):** Mengelola data dari awal pengumpulan, penyimpanan, hingga penghapusan, memastikan data yang tidak lagi diperlukan dihapus dengan aman sesuai dengan kebijakan.
6. **Metadataset (Metadata Management):** Mengelola data tentang data (metadata) untuk memudahkan pencarian, pengelompokan, dan penggunaan data dengan lebih efektif.
7. **Tanggung Jawab**: Dalam tata kelola data, penting untuk menetapkan siapa yang bertanggung jawab atas berbagai aspek pengelolaan data. Ini bisa mencakup siapa yang memiliki data, siapa yang boleh mengaksesnya, dan siapa yang bertanggung jawab jika terjadi masalah.

* **3. Apa Pentingnya manajemen data dalam organisasi?**

Manajemen data sangat penting bagi organisasi karena data adalah salah satu aset paling berharga yang mereka miliki. Berikut adalah beberapa alasan utama mengapa manajemen data penting:

* **Pengambilan Keputusan yang Lebih Baik**: Manajemen data yang efektif memastikan bahwa data yang digunakan untuk analisis dan keputusan bisnis akurat dan relevan. Data yang dikelola dengan baik membantu pengambilan keputusan yang lebih cepat dan berbasis fakta.
* **Efisiensi Operasional**: Dengan manajemen data yang baik, organisasi dapat mengurangi redundansi data, mempercepat akses informasi, dan memastikan bahwa sumber daya dimanfaatkan secara efisien.
* **Kepatuhan dan Regulasi** : Banyak industri diatur oleh undang-undang dan regulasi terkait penggunaan dan perlindungan data. Manajemen data yang baik membantu memastikan kepatuhan terhadap peraturan tersebut, seperti GDPR atau HIPAA, yang jika tidak dipatuhi dapat mengakibatkan denda besar.
* **Keamanan Data**: Data yang tidak terorganisir dan dikelola dengan buruk lebih rentan terhadap kebocoran dan serangan siber. Manajemen data yang baik membantu melindungi data dari ancaman eksternal dan internal.
* **Inovasi dan Pertumbuhan**: Dengan manajemen data yang baik, organisasi dapat menganalisis tren, pola, dan informasi pasar, yang membuka peluang untuk inovasi dan pengembangan produk atau layanan baru.
* **4. Apa Hubungan tata kelola data dengan keamanan data?**

Tata kelola data (data governance) dan keamanan data (data security) saling terkait erat karena keduanya berfokus pada pengelolaan dan perlindungan data. Tata kelola data menetapkan aturan, kebijakan, dan proses yang harus diikuti dalam penggunaan dan pengelolaan data, sementara keamanan data memastikan bahwa data terlindungi dari akses yang tidak sah atau pelanggaran keamanan. Berikut adalah hubungan penting antara keduanya:

* **Kebijakan Akses Data:** Tata kelola data menentukan siapa yang memiliki hak untuk mengakses data dan dalam kondisi apa. Keamanan data kemudian mengimplementasikan mekanisme teknis untuk memastikan kebijakan tersebut dijalankan, seperti melalui kontrol akses dan enkripsi.
* **Perlindungan Data Sensitif:** Tata kelola data mengidentifikasi data sensitif yang memerlukan perlindungan ekstra. Keamanan data melindungi data tersebut dari ancaman, baik internal (karyawan yang tidak memiliki wewenang) maupun eksternal (serangan siber).
* **Audit dan Kepatuhan:** Tata kelola data mengharuskan organisasi untuk mematuhi peraturan dan melakukan audit reguler. Keamanan data menyediakan alat dan prosedur untuk memantau dan mencatat akses serta penggunaan data, yang mempermudah proses audit.
* **Respon terhadap Insiden:** Jika terjadi pelanggaran keamanan, tata kelola data menetapkan bagaimana insiden harus ditangani. Keamanan data melaksanakan tindakan pemulihan yang tepat untuk mencegah kerusakan lebih lanjut dan melaporkan insiden sesuai dengan regulasi yang berlaku.
* **5. Apa hubungan tata kelola data dan kualitas data?**

Tata kelola data (data governance) dan kualitas data (data quality) memiliki hubungan yang erat, karena tata kelola data bertujuan untuk memastikan bahwa data yang dikelola di seluruh organisasi memiliki kualitas tinggi. Berikut beberapa cara tata kelola data memengaruhi kualitas data:

* **Standar Data yang Konsisten:** Tata kelola data menetapkan standar dan definisi yang seragam untuk data di seluruh organisasi, yang membantu menghindari kebingungan dan meningkatkan konsistensi data. Kualitas data yang baik bergantung pada standarisasi ini agar data dapat digunakan secara efektif di berbagai departemen.
* **Prosedur Pembersihan Data:** Tata kelola data juga mengatur proses untuk mendeteksi dan mengoreksi kesalahan dalam data, seperti duplikasi, inkonsistensi, atau data yang tidak valid. Proses ini berkontribusi langsung pada peningkatan kualitas data.
* **Monitoring Kualitas Data:** Tata kelola data menetapkan metrik dan proses untuk memantau kualitas data secara terus-menerus. Ini memastikan bahwa data tetap akurat, lengkap, dan up-to-date.
* **Tanggung Jawab terhadap Data :** Tata kelola data menentukan siapa yang bertanggung jawab untuk memastikan kualitas data tetap terjaga, sehingga setiap departemen atau individu yang menggunakan data memiliki peran jelas dalam menjaga kualitas data.

***Tugas Pertemuan 3/Tugas 2 (Kualitas Data di Sistem Perbankan):***

**Kasus:** Sebuah bank besar memiliki beberapa cabang yang tersebar di berbagai negara. Mereka menemukan bahwa data pelanggan sering kali tidak konsisten antara cabang satu dan yang lainnya. Sebagai contoh, beberapa pelanggan memiliki nomor ID yang berbeda di cabang yang berbeda, dan informasi transaksi di satu cabang mungkin tidak cocok dengan informasi di cabang lain.

**Tugas:**

**1. Identifikasi masalah kualitas data yang terjadi pada bank ini.**

Masalah utama yang dihadapi oleh bank ini adalah ketidakkonsistenan data pelanggan antara berbagai cabangnya. Beberapa masalah spesifik yang dapat diidentifikasi meliputi:

* **Ketidakkonsistenan Nomor ID Pelanggan:** Pelanggan yang sama dapat memiliki nomor identifikasi yang berbeda di berbagai cabang.
* **Perbedaan Informasi Transaksi:** Data transaksi pelanggan di satu cabang tidak selalu selaras dengan data yang ada di cabang lain.
* **Redundansi dan Duplikasi Data:** Pelanggan mungkin terdaftar beberapa kali dengan informasi yang berbeda, menyebabkan duplikasi data.
* **Kurangnya Standar Pengelolaan Data yang Konsisten:** Setiap cabang mungkin menggunakan sistem atau format pengelolaan data yang berbeda, sehingga menyulitkan penyatuan data pada level perusahaan.

**2. Bagaimana masalah kualitas data ini dapat mempengaruhi keputusan bisnis dan kepercayaan pelanggan terhadap bank?**

Masalah kualitas data ini berpotensi menimbulkan dampak signifikan pada bank dari berbagai aspek, antara lain:

* **Pengambilan Keputusan yang Tidak Tepat:** Data yang tidak akurat dan tidak konsisten akan mempengaruhi analisis dan laporan manajemen. Misalnya, keputusan mengenai kelayakan kredit atau risiko investasi dapat dibuat berdasarkan informasi yang salah, yang bisa berdampak negatif pada profitabilitas dan stabilitas bank.
* **Kehilangan Kepercayaan Pelanggan:** Pelanggan mengharapkan data mereka dikelola dengan tepat. Ketika informasi seperti saldo atau riwayat transaksi mereka tidak akurat, mereka akan kehilangan kepercayaan terhadap bank. Ini dapat mengarah pada peningkatan keluhan, bahkan penutupan akun.
* **Risiko Regulasi:** Industri perbankan tunduk pada berbagai peraturan terkait perlindungan data dan pelaporan. Ketidakkonsistenan data pelanggan dapat menyebabkan ketidakpatuhan terhadap regulasi ini, yang berpotensi menghasilkan sanksi hukum atau denda.

**3. Rancang strategi perbaikan yang komprehensif untuk meningkatkan konsistensi, akurasi, dan validitas data di seluruh cabang bank. Pastikan strategi ini melibatkan standar internasional yang relevan untuk pengelolaan kualitas data.**

Untuk memperbaiki masalah kualitas data di bank ini, diperlukan pendekatan menyeluruh yang mencakup proses, teknologi, dan standar yang tepat. Berikut adalah strategi yang dapat diterapkan:

* **Penerapan Kebijakan Data Governance yang Konsisten:** Bank harus menerapkan Data Governance Framework yang komprehensif. Ini harus mencakup kebijakan, standar, dan prosedur untuk memastikan bahwa data di seluruh cabang dikelola dengan cara yang konsisten. Standar seperti ISO 38500 dapat menjadi panduan dalam mengatur tata kelola teknologi informasi dan data.
* **Standar Data yang Seragam di Seluruh Cabang:** Setiap cabang bank harus menggunakan sistem dan format data yang seragam. Ini bisa dicapai dengan mengadopsi standar internasional seperti COBIT, yang mencakup manajemen dan pengendalian data yang efektif, serta ISO 8000, yang berfokus pada kualitas dan integritas data. Semua cabang perlu diintegrasikan ke dalam sistem yang terpusat dengan standar yang jelas tentang bagaimana data harus dikumpulkan, diproses, dan disimpan.
* **Implementasi Master Data Management (MDM) :** Master Data Management (MDM) adalah solusi penting untuk menyatukan dan menyinkronkan data pelanggan dari berbagai cabang. Dengan MDM, bank dapat memastikan bahwa pelanggan memiliki satu identitas tunggal di seluruh cabang. Setiap perubahan atau pembaruan informasi akan tercermin di semua cabang secara otomatis.
* **Penggunaan Teknologi Data Cleansing dan Data Validation:** Teknologi data cleansing dapat digunakan untuk mengidentifikasi dan memperbaiki data yang tidak akurat atau duplikat. Data validation harus diterapkan untuk memastikan bahwa data yang dimasukkan ke dalam sistem memenuhi aturan tertentu, seperti format yang tepat atau hubungan antar-data yang valid.
* **Pelatihan dan Kesadaran Data bagi Pegawai:** Pegawai di setiap cabang perlu dilatih tentang pentingnya pengelolaan data yang baik. Pelatihan ini harus mencakup cara menginput data yang benar, cara memeriksa konsistensi data, dan bagaimana menggunakan sistem data yang terintegrasi.
* **Monitoring dan Audit Berkala:** Bank harus secara rutin melakukan audit data dan monitoring kualitas data di semua cabangnya. Ini dapat dilakukan dengan menggunakan alat otomatis yang melaporkan kesalahan atau ketidakkonsistenan data secara real-time. Dengan audit berkala, bank dapat mengidentifikasi masalah sebelum mereka berkembang menjadi masalah yang lebih besar.

**Implementasi Standar Internasional**

* ISO 38500 memberikan kerangka kerja tata kelola yang membantu memastikan bahwa pengelolaan data di setiap cabang sejalan dengan tujuan bisnis secara keseluruhan. ISO 38500 menekankan pentingnya tanggung jawab manajemen dalam memastikan konsistensi dan akurasi data.
* COBIT menawarkan panduan yang komprehensif untuk mengelola data sebagai aset strategis perusahaan. Dengan menerapkan prinsip-prinsip COBIT, bank dapat memastikan bahwa data pelanggan dikelola secara efektif, terstandar, dan mendukung pengambilan keputusan bisnis.

***Tugas Pertemuan 4 (K3)***

**Soal 1: Konsep Dasar Arsitektur Data.**

**Jelaskan apa yang dimaksud dengan arsitektur data, dan sebutkan 3 komponen utama yang membentuk arsitektur data dalam sebuah organisasi!**

Arsitektur data adalah suatu kerangka kerja yang menggambarkan bagaimana data dikumpulkan, disimpan, dikelola, dan diproses dalam sebuah organisasi. Arsitektur ini bertujuan untuk memastikan data dapat diakses secara efisien, konsisten, dan aman di seluruh organisasi. Selain itu, arsitektur data juga mencakup bagaimana data berinteraksi dengan aplikasi dan sistem lainnya, serta bagaimana data dipertukarkan antara berbagai bagian dalam organisasi. Tiga komponen utama yang membentuk arsitektur data dalam sebuah organisasi adalah:

1. **Data Sumber (Data Sources):** Merupakan tempat asal data yang digunakan dalam organisasi. Data sumber bisa berupa sistem transaksi (seperti ERP atau CRM), sensor, aplikasi lain, atau data eksternal. Data ini adalah bahan baku yang akan diproses untuk mendapatkan informasi yang bermanfaat.
2. **Data Penyimpanan (Data Storage):** Data yang berasal dari berbagai sumber akan disimpan dalam media penyimpanan yang aman dan terstruktur. Ini bisa berupa database relasional, data warehouse, atau sistem penyimpanan lainnya seperti cloud storage. Penyimpanan data ini dirancang untuk memungkinkan akses yang cepat dan efisien.
3. **Data Prosesing dan Analisis (Data Processing and Analytics):** Setelah data disimpan, data perlu diproses dan dianalisis untuk mendapatkan wawasan yang berguna. Proses ini melibatkan teknik ETL (Extract, Transform, Load), pemodelan data, dan analisis statistik atau machine learning. Sistem ini membantu organisasi dalam mengubah data mentah menjadi informasi yang dapat mendukung pengambilan keputusan.

Dengan memiliki ketiga komponen ini, organisasi dapat mengelola data mereka dengan lebih efektif dan memastikan data dapat digunakan untuk mencapai tujuan bisnis.

**Soal 2: Infrastruktur Teknologi untuk Manajemen Data.**

**Apa saja infrastruktur teknologi yang diperlukan untuk mendukung arsitektur data di dalam suatu organisasi? Sebutkan dan jelaskan 4 jenis infrastruktur teknologi yang penting dalam manajemen data!**

Untuk mendukung arsitektur data dalam suatu organisasi, diperlukan berbagai jenis infrastruktur teknologi yang dapat memastikan pengelolaan, penyimpanan, dan akses data berjalan dengan lancar. Berikut adalah empat jenis infrastruktur teknologi yang penting dalam manajemen data:

1. **Sistem Penyimpanan Data (Data Storage Systems):** Infrastruktur ini mencakup sistem yang digunakan untuk menyimpan data dalam jumlah besar, seperti **database** dan **data warehouse**. Database relasional (seperti MySQL atau PostgreSQL) digunakan untuk menyimpan data yang terstruktur, sementara data warehouse (seperti Amazon Redshift atau Google BigQuery) digunakan untuk menyimpan data dalam jumlah besar yang sudah diproses untuk analisis. Selain itu, ada juga penyimpanan data dalam bentuk objek (seperti AWS S3 atau Azure Blob Storage) untuk data tidak terstruktur (misalnya file teks, gambar, atau video).
2. **Sistem Pemrosesan Data (Data Processing Systems):** Infrastruktur ini mencakup sistem yang digunakan untuk memproses dan menganalisis data. Sistem pemrosesan ini dapat berupa **platform pemrosesan batch** seperti Hadoop, atau **platform pemrosesan real-time** seperti Apache Kafka atau Apache Flink. Infrastruktur ini membantu mengolah data mentah menjadi informasi yang dapat dipahami dan digunakan oleh organisasi. Proses pemrosesan bisa berupa ETL (Extract, Transform, Load) untuk mengambil data dari sumber, mengubahnya sesuai kebutuhan, dan memuatnya ke dalam sistem penyimpanan.
3. **Jaringan dan Koneksi (Network and Connectivity):** Infrastruktur jaringan yang handal diperlukan untuk menghubungkan berbagai sistem dan perangkat yang menyimpan serta memproses data. Ini termasuk **cloud services**, **VPN**, **internet bandwidth**, dan **sistem komunikasi internal** yang memastikan data dapat dipindahkan dengan cepat dan aman antar sistem. Infrastruktur jaringan ini juga mencakup protokol dan standar keamanan untuk menjaga integritas dan kerahasiaan data saat dipindahkan atau diakses oleh pengguna.
4. **Platform Analitik dan Business Intelligence (BI):** Infrastruktur untuk analitik dan BI memungkinkan organisasi untuk menganalisis data yang telah disimpan dan diproses. Platform ini termasuk **alat analisis data** (seperti Tableau, Power BI, atau Qlik), yang memungkinkan pengguna untuk membuat visualisasi, laporan, dan dashboard yang membantu dalam pengambilan keputusan bisnis. Infrastruktur ini juga dapat mencakup sistem untuk analisis data menggunakan machine learning atau kecerdasan buatan (AI), yang memungkinkan organisasi untuk menggali wawasan lebih dalam dari data mereka.

Keempat jenis infrastruktur ini saling berhubungan dan mendukung satu sama lain dalam memastikan manajemen data yang efisien dan efektif di dalam organisasi. Infrastruktur yang baik akan meningkatkan kemampuan organisasi dalam mengelola, menganalisis, dan memanfaatkan data untuk mencapai tujuan bisnis mereka.

**Soal 3: Manajemen Data Terdistribusi.**

**Sebuah perusahaan besar memiliki data yang tersebar di beberapa lokasi geografis, dengan kantor pusat dan beberapa cabang di seluruh dunia. Jelaskan dua pendekatan untuk mengelola data yang terdistribusi dan sebutkan tantangan yang mungkin dihadapi dalam masing-masing pendekatan!**

Manajemen data terdistribusi adalah proses mengelola data yang tersebar di berbagai lokasi fisik atau geografis. Dalam perusahaan besar dengan kantor pusat dan beberapa cabang di seluruh dunia, pengelolaan data terdistribusi menjadi sangat penting untuk memastikan aksesibilitas, keamanan, dan konsistensi data. Berikut adalah dua pendekatan yang umum digunakan dalam mengelola data terdistribusi beserta tantangan yang mungkin dihadapi:

**1. Pendekatan Federasi Data (Data Federation):** Pada pendekatan federasi data, data yang tersebar di berbagai lokasi tetap dikelola secara terpisah, namun pengguna atau aplikasi dapat mengakses data tersebut secara terpusat menggunakan **query** atau antarmuka yang menyatukan berbagai sumber data tanpa perlu memindahkan data tersebut ke satu tempat. Sistem federasi memungkinkan aplikasi untuk mengakses dan mengintegrasikan data dari berbagai database atau sumber data secara langsung. **Tantangan dalam federasi data:**

* **Konsistensi data:** Karena data tidak disalin ke satu tempat, menjaga konsistensi data antar lokasi bisa menjadi masalah, terutama jika ada perubahan data yang cepat.
* **Performa:** Query atau permintaan data yang melibatkan beberapa lokasi atau sumber data dapat memperlambat performa, terutama jika ada koneksi jaringan yang lambat atau tidak stabil.
* **Keamanan:** Mengelola kontrol akses dan enkripsi data yang terdistribusi di berbagai lokasi bisa lebih rumit, karena setiap lokasi mungkin memiliki kebijakan keamanan yang berbeda.

**2. Pendekatan Replikasi Data (Data Replication):** Dalam pendekatan replikasi data, data yang ada di satu lokasi (misalnya, kantor pusat) akan disalin ke beberapa lokasi cabang secara teratur. Dengan demikian, setiap lokasi memiliki salinan data yang serupa, dan setiap cabang dapat mengakses data lokal yang lebih cepat tanpa harus bergantung pada koneksi ke pusat data utama. **Tantangan dalam replikasi data:**

* **Sinkronisasi:** Memastikan bahwa semua salinan data di berbagai lokasi tetap sinkron dapat menjadi tantangan besar, terutama ketika ada pembaruan atau perubahan data secara simultan di berbagai lokasi.
* **Konsistensi dan Ketersediaan:** Dalam sistem replikasi, ada potensi masalah terkait dengan model **CAP theorem** (Consistency, Availability, Partition tolerance). Ketika terjadi gangguan jaringan antar lokasi, sistem harus memutuskan apakah akan menjaga konsistensi data atau menyediakan ketersediaan data. Memilih salah satu dapat mempengaruhi kinerja dan keandalan data.
* **Pemeliharaan dan Biaya:** Replikasi data membutuhkan infrastruktur yang lebih kuat, serta pengelolaan dan pemeliharaan yang lebih intensif, karena banyaknya salinan data yang perlu dijaga agar tetap akurat dan terbarui.

**Kesimpulan:** Kedua pendekatan ini memiliki kelebihan dan kekurangan. Federasi data lebih fleksibel dan hemat biaya karena tidak memerlukan penyimpanan tambahan, namun menghadapi tantangan dalam hal konsistensi dan kinerja. Sementara itu, replikasi data memberikan performa yang lebih baik dan ketersediaan data yang lebih tinggi, namun menimbulkan tantangan dalam hal sinkronisasi dan biaya pemeliharaan. Perusahaan harus memilih pendekatan yang paling sesuai dengan kebutuhan bisnis dan infrastruktur yang ada, serta mempertimbangkan tantangan yang mungkin dihadapi dalam masing-masing pendekatan.

**Soal 4: Peran Data Governance dalam Arsitektur Data**

**Apa yang dimaksud dengan data governance, dan mengapa penting dalam arsitektur data sebuah organisasi? Jelaskan 3 elemen utama yang menjadi fokus dalam penerapan data governance!**

**Data Governance** adalah kerangka kerja yang mencakup kebijakan, prosedur, dan kontrol yang digunakan untuk mengelola, mengatur, dan melindungi data dalam suatu organisasi. Data governance bertujuan untuk memastikan bahwa data dikelola dengan cara yang efektif, efisien, dan sesuai dengan peraturan yang berlaku, serta memberikan kepercayaan kepada pengguna data tentang kualitas dan integritas data yang tersedia. Dalam konteks arsitektur data, data governance memastikan bahwa data yang digunakan dalam organisasi memenuhi standar yang telah ditetapkan untuk pengelolaan data yang baik dan penggunaan yang optimal.

**Mengapa Data Governance Penting dalam Arsitektur Data?** Data governance penting dalam arsitektur data karena:

1. **Meningkatkan Kualitas Data:** Data governance memastikan data yang digunakan di seluruh organisasi adalah akurat, konsisten, dan dapat diandalkan. Tanpa pengelolaan yang tepat, data bisa menjadi tidak terstruktur, tidak valid, atau tidak relevan.
2. **Mengurangi Risiko:** Dengan adanya kebijakan dan kontrol yang jelas, data governance membantu mengurangi risiko terkait dengan pelanggaran privasi, penyalahgunaan data, atau ketidakpatuhan terhadap peraturan yang berlaku (misalnya, GDPR atau UU Perlindungan Data).
3. **Memastikan Kepatuhan:** Data governance memastikan bahwa organisasi mematuhi peraturan dan standar industri yang mengatur pengelolaan dan penggunaan data, menghindari potensi masalah hukum atau reputasi.
4. **Pengambilan Keputusan yang Lebih Baik:** Dengan data yang terkelola dengan baik, organisasi dapat membuat keputusan yang lebih cepat, akurat, dan berbasis data yang terpercaya.

**Tiga Elemen Utama dalam Penerapan Data Governance:**

1. **Kebijakan dan Prosedur (Policies and Procedures):** Elemen ini mencakup aturan dan pedoman yang ditetapkan untuk pengelolaan data di seluruh organisasi. Kebijakan ini meliputi aspek seperti keamanan data, pengelolaan akses, dan penggunaan data. Prosedur operasional yang jelas diperlukan untuk mengelola siklus hidup data dari pengumpulan, penyimpanan, hingga pemusnahan data. Kebijakan ini juga memastikan bahwa semua pihak dalam organisasi memahami dan mematuhi aturan yang telah ditetapkan.
2. **Kualitas Data (Data Quality):** Kualitas data merupakan elemen penting dalam data governance, karena data yang buruk dapat merugikan organisasi dalam pengambilan keputusan dan analisis. Pengelolaan kualitas data melibatkan pengecekan kesalahan (validasi), konsistensi, kelengkapan, dan akurasi data. Organisasi harus memastikan bahwa data yang digunakan adalah data yang dapat dipercaya dan relevan, serta memantau secara berkelanjutan untuk menjaga kualitas data yang tinggi.
3. **Keamanan dan Privasi Data (Data Security and Privacy):** Keamanan data adalah bagian penting dari data governance karena melibatkan perlindungan data dari akses yang tidak sah, kebocoran, atau penyalahgunaan. Kebijakan yang tepat untuk enkripsi data, kontrol akses, serta pemantauan dan audit akses sangat diperlukan untuk menjaga keamanan data. Selain itu, penerapan privasi data juga penting untuk memastikan bahwa data pribadi dilindungi sesuai dengan regulasi yang ada (misalnya, GDPR atau UU Perlindungan Data Pribadi).

**Kesimpulan:** Penerapan data governance yang efektif di dalam arsitektur data organisasi dapat memastikan data yang terkelola dengan baik, aman, dan dapat digunakan secara optimal untuk mendukung keputusan bisnis. Dengan fokus pada kebijakan dan prosedur, kualitas data, serta keamanan dan privasi data, organisasi dapat memanfaatkan data secara efisien dan mengurangi potensi risiko yang terkait dengan pengelolaan data.

**Soal 5: Infrastruktur Cloud dalam Arsitektur Data Modern**

**Sebuah organisasi sedang mempertimbangkan untuk beralih dari infrastruktur lokal (on-premise) ke cloud dalam manajemen datanya. Jelaskan 3 keuntungan utama menggunakan cloud infrastructure untuk arsitektur data organisasi, dan 2 tantangan yang mungkin dihadapi dalam transisi ke cloud.**

Berpindah dari infrastruktur lokal (on-premise) ke infrastruktur cloud untuk manajemen data adalah langkah besar yang banyak dilakukan oleh organisasi untuk memanfaatkan kelebihan yang ditawarkan oleh teknologi cloud. Berikut adalah tiga keuntungan utama dari menggunakan **cloud infrastructure** dalam arsitektur data organisasi serta dua tantangan yang mungkin dihadapi dalam transisi ke cloud:

**3 Keuntungan Utama Menggunakan Cloud Infrastructure untuk Arsitektur Data:**

1. **Skalabilitas yang Fleksibel:** Salah satu keuntungan utama menggunakan cloud adalah kemampuan untuk **menskalakan sumber daya** sesuai dengan kebutuhan organisasi. Dengan cloud, organisasi dapat dengan mudah menambah atau mengurangi kapasitas penyimpanan dan komputasi tanpa harus membeli perangkat keras baru. Ini memungkinkan organisasi untuk menyesuaikan infrastruktur dengan beban kerja yang berubah, baik itu peningkatan atau penurunan volume data, tanpa pemborosan biaya.
2. **Biaya yang Lebih Efisien:** Cloud computing seringkali lebih **hemat biaya** dibandingkan dengan infrastruktur on-premise, terutama dari sisi pengadaan dan pemeliharaan perangkat keras. Dengan cloud, organisasi hanya membayar untuk **sumber daya yang mereka gunakan** (model bayar sesuai pemakaian atau "pay-as-you-go"). Selain itu, biaya untuk pemeliharaan dan pembaruan perangkat keras, serta tenaga kerja untuk operasional, dapat dikurangi karena semuanya dikelola oleh penyedia layanan cloud.
3. **Aksesibilitas dan Kolaborasi yang Lebih Baik:** Cloud memungkinkan data dan aplikasi diakses dari mana saja dan kapan saja selama ada koneksi internet, yang mendukung **kerja jarak jauh** dan kolaborasi antar tim di lokasi geografis yang berbeda. Infrastruktur cloud memberikan **akses yang cepat dan fleksibel** terhadap data, memungkinkan berbagai tim untuk bekerja secara bersamaan tanpa batasan fisik atau waktu.

**2 Tantangan yang Mungkin Dihadapi dalam Transisi ke Cloud:**

1. **Masalah Keamanan dan Privasi Data:** Ketika beralih ke cloud, masalah **keamanan data** menjadi perhatian utama. Data yang disimpan di cloud bisa lebih rentan terhadap ancaman keamanan jika tidak ada langkah-langkah yang tepat untuk **melindungi data**, seperti enkripsi atau kontrol akses yang ketat. Selain itu, jika penyedia cloud tidak memiliki kebijakan atau standar keamanan yang memadai, bisa ada risiko kebocoran data atau pelanggaran privasi, yang dapat merusak reputasi organisasi dan menyebabkan masalah hukum.
2. **Kompleksitas Migrasi dan Integrasi:** Proses **migrasi data** dari sistem lokal ke cloud bisa menjadi tantangan teknis yang besar, terutama jika data sangat besar atau terdistribusi di berbagai sistem. Migrasi memerlukan perencanaan yang matang untuk memastikan **integrasi** yang lancar antara sistem on-premise yang lama dengan infrastruktur cloud yang baru. Selama transisi ini, ada kemungkinan gangguan operasional, kesalahan dalam transfer data, atau masalah dalam kompatibilitas aplikasi yang memerlukan penyesuaian atau modifikasi.

**Kesimpulan:** Meskipun beralih ke cloud menawarkan banyak keuntungan seperti **skalabilitas**, **biaya efisien**, dan **aksesibilitas**, organisasi harus memperhatikan tantangan yang mungkin muncul, seperti masalah **keamanan data** dan **kompleksitas migrasi**. Keputusan untuk beralih ke cloud harus didasarkan pada analisis kebutuhan organisasi, kesiapan teknologi, dan kemampuan untuk menangani tantangan yang ada.

A close-up of a sign

Description automatically generated

**Outline Framework IT Governance**

* COBIT (Control Objectives for Information and Related Technologies)
* ITIL (Information Technology Infrastructure Library)
* ISO 17799 (The International Organization for Standardization 17799)
* ISO 27000 (The International Organization for Standardization 27000)
* ISO/IEC 38500 (The International Organization for Standardization /International Electrotechnical Commission 38500)
* COSO (Committee of Sponsoring Organizations of the Treadway Commission)
* IT Governance Nasional

**Mengapa dibutuhkan framework ?**

1. Sisi Konseptual
2. Agar pemahaman menyeluruh
3. Menentukan arah
4. Menjamin keteraturan

**Framework Tata Kelola TI**

|  |  |
| --- | --- |
| ITIL (IT Infrastructure Library) | COSO |
| ISO 17799 | ISO/IEC 17799:2000 |
| ISO/IEC TR 13335 | ISO/IEC 15408 |
| TickIT | NIST 800-14 |
| ASL | SAC |
| SAS70 | BS 15000 |
| SysTrust | PRINCE2 |
| SOX | Six Sigma |
| CMM/CMMI | SASs |

Framework yang sering dijadikan acuan oleh instistusi untuk membangun Tata Kelola TI (hasil survey ITGI) :

1. COBIT
2. IT Infrastructure Library
3. ISO 17799
4. ISO 27000
5. ISO/EIC 38500
6. Australian Standart 8015

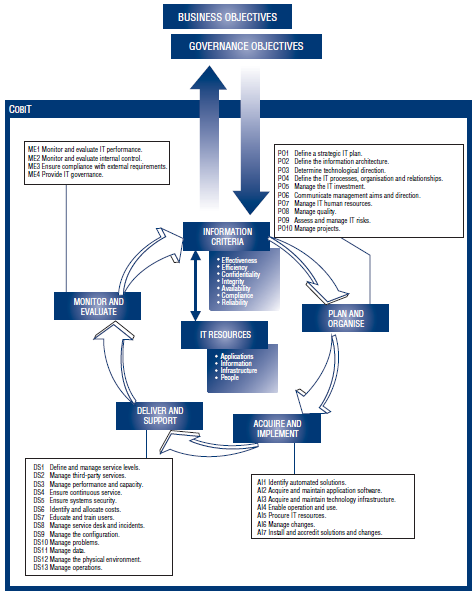
\* Serta yang bersifat lokal/nasional

**COBIT**

* *Control Objectives for Information and related Technology* (COBIT) adalah seperangkat pedoman umum (best practice) untuk **manajemen TI**.
* Asal mula standar COBIT dikembangkan oleh **ISACF** (Information Systems Audit and Control Foundation) lembaga penelitian untuk Information Systems Audit and Control Association (**ISACA**).
* Tahun 1999, **tugas ISACF** untuk COBIT di transfer ke IT Governance Institute (**ITGI**) yang merupakan badan independen di dalam ISACA.
* COBIT versi pertama pada tahun 1996.
* COBIT versi kedua pada tahun 1998.
* COBIT versi 3.0 pada tahun 2000.
* COBIT 4.0 pada tahun 2005.
* COBIT 4.1 pada tahun 2007.
* COBIT 5 pada tahun 2012.

COBIT memiliki 4 cakupan domain dan memiliki 34 proses dan mencakup 137 control objectives yang dikategorikan ke dalam 4 domain :

1. **Perencanaan dan organisasi** (plan and organise/PO) : proses perencanaan dan penyelarasan strategi TI dengan strategi organisasi.
2. **Pengadaan dan implementasi** (Acquire & Implement/AI) : proses pemilihan, pengadaan, dan penerapan penggunaan TI yang digunakan.
3. **Layanan dan dukungan** (Deliver and Support (DS)) : proses pelayanan TI dan dukungan teknisnya
4. **Pengawasan dan evaluasi** (Monitor and Evaluate (ME)) : proses pengawasan dan mengevaluasi pengelolaan TI pada organisasi



* Cobit mempunyai **model kematangan** (*maturity model*) untuk mengontrol proses-proses TI, dengan menggunakan metode penilaian (*scoring*), sehingga suatu organisasi dapat menilai proses-proses TI yang dimilikinya mulai dari skala non-existent sampai dengan optimized (dari 0-5).
* **Maturity model ini akan memetakan**:

1. Current status dari organisasi, untuk melihat posisi organisasi saat ini.
2. Current status dari kebanyakan industri saat ini, sebagai perbandingan.
3. Current status dari standar internasional, sebagai perbandingan tambahan.
4. Strategi organisasi dalam rangka perbaikan, level yang ingin dicapai oleh organisasi.

COBIT juga memiliki **pengukuran** lainnya :

1. Critical Success Factors (CSF), yaitu mendefinisian hal-hal atau **kegiatan penting** yang dapat digunakan manajemen untuk dapat mengontrol proses-proses TI di organisasinya.
2. Key Goal Indicators (KGI), yaitu mendefinisikan ukuran-ukuran yang akan memberikan **gambaran** kepada manajemen apakah proses-proses TI yang ada telah memenuhi kebutuhan proses bisnis yang ada.

KGI biasanya berbentuk **kriteria informasi**:

1. Ketersediaan informasi yang diperlukan dalam mendukung kebutuhan bisnis.
2. Tidak adanya resiko integritas dan kerahasiaan data.
3. Efisiensi biaya dari proses dan operasi yang dilakukan
4. Konfirmasi reliabilitas, efektifitas, dan compliance

Key Performance Indicators (KPI) yaitu mendefinisikan ukuran-ukuran untuk menentukan kinerja proses-proses TI dilakukan untuk mewujudkan tujuan yang telah ditentukan. KPI biasanya berupa indikator-indikator kapabilitas, pelaksanaan, dan kemampuan sumber daya TI.

**ITIL**

* ITIL atau **Information Technology Infrastructure Library** (Bahasa Inggris, diterjemahkan Pustaka Infrastruktur Teknologi Informasi), adalah **suatu rangkaian konsep dan teknik pengelolaan infrastruktur, pengembangan, serta operasi teknologi informasi(TI).** ITIL diterbitkan dalam suatu rangkaian buku yang masing-masing membahas suatu topik pengelolaan TI. Nama ITIL dan IT Infrastructure Library merupakan merek dagang terdaftar dari Office of Government Commerce (OGC) Britania Raya.
* Walaupun dikembangkan sejak dasawarsa 1980-an, penggunaan ITIL baru meluas pada pertengahan**1990-an** dengan spesifikasi versi keduanya (ITIL v2) yang paling dikenal dengan dua set bukunya yang berhubungan dengan ITSM (IT Service Management), yaitu Service Delivery (AntarLayanan) dan Service Support (Dukungan Layanan).
* Pada 30 Juni 2007, OGC menerbitkan versi ketiga ITIL (ITIL v3) yang intinya terdiri dari lima bagian dan lebih menekankan pada **pengelolaan siklus hidup layanan** yang disediakan oleh teknologi informasi. Kelima bagian tersebut adalah:

1. Service Strategy
2. Service Design
3. Service Transition
4. Service Operation
5. Continual Service Improvement

* ITIL memberikan deskripsi detil tentang beberapa praktik TI penting dengan daftar cek, tugas, serta prosedur yang menyeluruh yang dapat disesuaikan dengan segala jenis organisasi TI.

Kelima bagian tersebut dikemas dalam buku **“core guidance publications”.** Setiap buku dalam kelompok utama ini berisi:

1. Practice fundamentals – menjelaskan latar belakang tahapan lifecycle serta kontribusinya terhadap pengelolaan layananTI secara keseluruhan.
2. Practice principles – menjelaskan konsep-konsep kebijakan serta tata kelola tahapan lifecycle yang menjadi acuan setiap proses terkait dalam tahapan ini.
3. Lifecycle processes and activities – menjelaskan berbagai proses maupun aktivitas yang menjadi kegiatan utama tahapan lifecycle. Misalnya proses financial management dan demand management dalam tahapan Service Strategy.
4. Supporting organization structures and roles – proses-proses ITIL tidak akan dapat berjalan dengan baik tanpa defini roles dan responsibilities. Bagian ini menjelaskan semua aspek yang terkait dengan kesiapan model dan struktur organisasi.
5. Technology considerations – menjelaskan solusi-solusi otomatisasi atau software ITIL yang dapat digunakan pada tahapan lifecycle, serta persyaratannya.
6. Practice Implementation – berisi acuan/panduan bagi organisasi TI yang ingin mengimplementasikan atau yang ingin meningkatkan proses-proses ITIL.
7. Complementary guide line – berisi acuan model-model best practice lain selain ITIL yang dapat digunakan sebagai referensi bagian tahapan lifecycle.
8. Examples and templates – berisi template maupun contoh-contoh pengaplikasian proses

**ISO**

* **Organisasi Internasional untuk Standardisasi** (bahasa Inggris: International Organization for Standardization disingkat ISO atau Iso) adalah **badan penetap standar internasional yang terdiri dari wakil-wakil dari badan standardisasi nasional setiap negara.** Pada awalnya, singkatan dari nama lembaga tersebut adalah IOS, bukan ISO. Tetapi sekarang lebih sering memakai singkatan ISO, karena dalam bahasaYunani isos berarti sama (equal). Penggunaan ini dapat dilihat pada kata isometrik atau isonomi.
* Didirikan pada 23 Februari 1947, ISO menetapkan standar-standar industrial dan komersial dunia. ISO, yang merupakan lembaga nirlaba internasional, pada awalnya dibentuk untuk membuat dan memperkenalkan standardisasi internasional untuk apa saja. Standar yang sudah kita kenal antara lain standar jenis film fotografi, ukuran kartu telepon, kartu ATM Bank, ukuran dan ketebalan kertas dan lainnya.
* Dalam menetapkan suatu standar tersebut mereka mengundang wakil anggotanya dari1 30 negara untuk duduk dalam KomiteTeknis (TC), Sub Komite (SC) dan Kelompok Kerja (WG).

Penerapan ISO di suatu perusahaan berguna untuk:

1. Meningkatkan citra perusahaan
2. Meningkatkan kinerja lingkungan perusahaan
3. Meningkatkan efisiensi kegiatan
4. Memperbaiki manajemen organisasi dengan menerapkan perencanaan, pelaksanaan, pengukuran dan tindakan perbaikan (plan, do, check, act)
5. Meningkatkan penataan terhadap ketentuan peraturan perundang – undangan dalam hal pengelolaan lingkungan
6. Mengurangi risiko usaha
7. Meningkatkan daya saing
8. Meningkatkan komunikasi internal dan hubungan baik dengan berbagai pihak yang berkepentingan
9. Mendapat kepercayaan dari konsumen/mitrakerja/pemodal

**ISO 17799**

* ISO 17799 merupakan suatu struktur dan rekomendasi pedoman yang diakui secara internasional untuk keamanan informasi.
* Suatu proses keamanan informasi yang menyeluruh yang dapat diusahakan atau di implementasikan bagi perusahaan agar memperoleh manfaat keamanan yang diinginkan.
* Proses evaluasi, implementasi, pemeliharaan dan pengaturan keamanan informasi yang singkat.
* Upaya penggunaan oleh konsorsium perusahaan untuk memenuhi kebutuhan industri.
* ISO 17799 merupakan proses yang seimbang antara fisik, keamanan secara teknikal dan prosedur, serta keamanan pribadi.
* Secara internal keuntungan-keuntungan menerapkan suatu ISO 17799 Sistem Manajemen Keamanan Informasi (ISMS) dapat digunakan sebagai:

1. Suatu pengukuran untuk keamanan perusahaan
2. Satu set kendali
3. Suatu metoda untuk menentukan target dan mengusulkan peningkatan
4. Basis untuk standard keamanan informasi intern perusahaan

* Organisasi menerapkan ISO 17799 mempunyai **suatu alat untuk mengukur, mengatur dan mengendalikan informasi yang penting kepada operasi system mereka**. Pada gilirannya ini dapat mendorong kearah kepercayaan pelanggan, yang lebih efisien dan sistem internal efektif serta suatu tanda kelihatan dari kesanggupan suatu organisasi
* 10 control clauses (10 pasal pengamatan)
* 36 control objectives (36 objek/sasaran pengamanan)
* 127 controls securiTy(127 pengawasan keamanan)

**Keluarga ISO 27000**

* ISO 27000: dokumen defenisi-defenisi keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.
* ISO 27001: berisi aspek-aspek pendukung realisasi serta implementasi sistem manajemen keamanan informasi perusahaan
* ISO 27002: terkait dengan dokumen ISO 27001, namun dalam dokumen ini terdapat panduan praktis pelaksanaan dan implementasi sistem manajemen keamanan informasi perusahaan.
* ISO 27003: panduan implementasi sistem manajemen keamanan informasi perusahaan.
* ISO 27004: dokumen yang berisi matriks dan metode pengukuran keberhasilan implementasi sistem manajemen keamanan informasi.
* ISO 27005: dokumen panduan pelaksanaan manajemen risiko.
* ISO 27006: dokumen panduan untuk sertifikasi sistem manajemen keamanan informasi perusahaan.
* ISO 27007: dokumen panduan audit sistem manajemen keamanan informasi perusahaan.
* ISO 27799: panduan ISO 27001 untuk industri kesehatan.
* ISO 27001: 2005 digunakan sebagai icon sertifikasi ISO 27000

**ISO/IEC 38500**

* suatu standar internasional untuk Tata Kelola TI yang diterbitkan bersama oleh Organisasi Internasional untuk Standardisasi (ISO) dan International Electrotechnical Commission (IEC).
* Kerangka kerja bagi pemerintahan yang efektif untuk membantu mereka pada tingkat tertinggi dari organisasi untuk memahami dan memenuhi **kewajiban hukum, peraturan, dan etika mereka dalam hal penggunaan organisasi mereka di bidang TI.**

**Australian Standart 8015**

* Standar ini menyediakan prinsip panduan bagi direktur atau top level management organisasi untuk penggunaan teknologi komunikasi dan informasi yang efektif, efisien, dan dapat diterima dengan baik didalam organisasi (Australian Standard, 2005).
* Australian Standard 8015 (AS 8015) merupakan panduan bagi terciptanya suatu sistem dimana penggunaan Teknologi Informasi dan Komunikasi(TIK) pada saat ini dan dimasa depan dapat terarah dan terkendali.

**Prinsip AS 8015**

1. **Menetapkan tanggungjawab terhadap TIK yang dapat dipahami secara jelas**–memastikan individu atau group dalam organisasi memahami dan menerima tanggungjawabnya dalamTIK.
2. **Merencanakan TIK untuk sebaik mungkin mendukung organisasi** – memastikan rencana TIK sesuai dengan kondisi sekarang dan kebutuhan yang sedang berjalan dan rencana TIK mendukung rencana organisasi
3. **Mengadakan sarana TIK secara benar** –memastikan akuisisi TIK dibuat dengan alasan yang disetujui pada level tertentu dan analiasa yang sesuai. Selain itu terdapat keseimbangan antara biaya, risiko, serta keuntungan jangka pendek maupun panjang.
4. **Memastikan TIK berjalan baik**, kapanpun diperlukan –memastikan TIK sesuai dengan tujuannya untuk mendukung organisasi, responsive terhadap kebutuhan bisnis dan menyediakan dukungan pada bisnis ketika dibutuhkan.
5. **Memastikan TIK memenuhi aturan-aturan formal** –memastikan TIK sesuai dengan peraturan-peraturan eksternal dan sejalan dengan standard dan kebijakan organisasi
6. **Memastikan TIK memperhatikan faktor manusia** –memastikan TIK memenuhi kebutuhan saat ini dan mencakup semua orang di dalam proses

**ISO / IEC 38500**

* ISO/IEC 38500:2008, Pertama kali dibuat oleh Standards Australia (dikenal dengan nama AS8015:2005) dan kemudian diadopsi oleh Joint Technical Committee ISO/IEC JTC 1.
* Tujuannya dari kerangka ini : untuk menyediakan sebuah framework dasar bagi pimpinan untuk melakukan **evaluasi, pengarahan dan monitoring terhadap pemanfaatan TI dalam organisasi.**
* ISO / IEC 38500 berlaku untuk organisasi dari semua ukuran, termasuk publik dan perusahaan swasta, lembaga pemerintah, dan organisasi nirlaba.
* Standar ini memberikan prinsip-prinsip panduan untuk direktur organisasi pada penggunaan efektif, efisien, dan dapat diterima Teknologi Informasi (TI) dalam organisasi mereka.
* Kerangka kerja ini terdiri dari definisi, prinsip dan model.
* Enam prinsip tata kelola TI:

1. Tanggung jawab
2. Strategi
3. Akuisisi
4. Kinerja
5. Kesesuaian
6. Perilaku manusia

Dokumen referensi yang bisa digunakan untuk mengetahui lebih dalam mengenai standar ini antara lain:

1. Report of the Committee on the Financial Aspects of Corporate
2. Governance,Sir Adrian Cadbury, London, 1992 ISBN 0 85258 913 1
3. OECD Principles of Corporate Governance, OECD, 1999 and 2004
4. ISO Guide 73 2002 – Risk management — Vocabulary — Guidelines for use in standards

Dan masih banyak Framework Tata Kelola TI yang lain

**COSO**

* COSO (Committee of Sponsoring Organization of the Treadway Commission), sebuah organisasi di Amerika yang berdedikasi dalam meningkatkan **kualitas pelaporan finansial mencakup etika bisnis, kontrol internal dan corporate governance.** Komite ini didirikan pada tahun 1985 untuk mempelajari faktor-faktor yang menunjukkan ketidaksesuaian dalam laporan finansial
* Pada awal tahun 90-an, Price waterhouse Couper bersama komite ini melakukan extensive study mengenai kontrol internal, yang menghasilkan COSO Framework yang digunakan untuk mengevaluasi efektifitas kontrol internal suatu perusahaan. Sejak itu, komunitas finansial global, termasuk badan-badan regulator seperti public accounting dan internal audit professions, telah mengadopsi COSO. Hal ini juga bernilai untuk perusahaan manapun yang ingin memastikan sistem kontrol internalnya dengan menggunakan standar internasional.

Kerangka kerja COSO terdiri atas 3 dimensi :

1. Komponen kontrol COSO. COSO mengidentifikasi 5 komponen kontrol yang diintegrasikan dan dijalankan dalam semua unit bisnis, dan akan membantu mencapai sasaran kontrol internal, yakni ***monitoring, information and communications, control activities, risk assessment, dan control environment***.
2. Sasaran kontrol internal. Sasaran kontrol internal dikategorikan menjadi beberapa area, yakni :

* Operations, efisisensi dan efektifitas operasi dalam mencapai sasaran bisnis yang juga meliputi tujuan performansi dan keuntungan.
* Financial reporting, persiapan pelaporan anggaran finansial yang dapat dipercaya.
* Compliance, pemenuhan hukum dan aturan yang dapat dipercaya.

1. Unit/aktifitas terhadap organisasi. Dimensi ini mengidentifikasikan unit/aktifitas pada organisasi yang menghubungkan kontrol internal. Kontrol internal menyangkut keseluruhan organisasi dan semua bagianbagiannya. Kontrol internal seharusnya diimplementasikan terhadap unit-unit dan aktifitas organisasi.

**IT Governance Nasional**

**Latar Belakang :**

1. Perlunya rencana TIK nasional yang lebih harmonis:
2. Hampir semua institusi memiliki Rencana TIK, tetapi integrasi dan sinkronisasi di level nasional masih lemah.
3. Perlunya pengelolaan yang lebih baik untuk merealisasikan flagship nasional :
4. Flagship nasional yang merupakan inisiatif TIK strategis memerlukan pendekatan yang lebih baik, khususnya dalam hubungan antar lembaga dan hubungan dengan penyedia layanan.
5. Perlunya peningkatan efisiensi dan efektifitas belanja/investasi TIK : Diperlukan mekanisme yang memungkinkan menghindari kemungkinan terjadinya redundansi inisiatif TIK, sehingga meningkatkan efisiensi dan efektivitas belanja/investasi TIK nasional.
6. Perlunya pendekatan yang meningkatkan pencapaian value dari implementasi TIK Nasional :
7. Value yang dapat diciptakan dengan implementasi TIK, khususnya yang dapat dirasakan langsung oleh publik

**Referensi penyusunan :**

1. COBIT (Control Objective for Information and Related Technology) yang dikeluarkan oleh ISACA (Information System Audit & Control Association) versi 4.1
2. ITIL (Information Technology Infrastructure Library)
3. ISO 27000 (Information Security Management System)
4. AS 8015-2005 (Australian Standard on Corporate Governance of Information & Communication Technology)
5. Riset CISR MIT (Center for Information System Research – MIT) tentang IT Governance
6. Keppres 20 tahun 2006 tentang Dewan TIK Nasional
7. Keppres 80 tahun 2003 tentang Pedoman Pelaksanaan Pengadaan Barang/Jasa Pemerintah
8. PP No. 20 tahun 2004 tentang Rencana Kerja Pemerintah
9. PP No. 21 tahun 2004 tentang Penyusunan Rencana Kerja dan Anggaran Kementrian Negara/Lembaga
10. UU No. 32 tentang Pemerintahan Daerah

* Panduan ini berisi prinsip dan model.
* Untuk prinsip terdiri dari 5 prinsip yang mendasari model dan tingkat kedalaman implementasi model.
* Sedangkan model dibagi 2 bagian utama yaitu

1. Struktur dan peran tata kelola
2. Proses tata kelola

*Terima kasih atas perhatiannya dan sampai jumpa pada pertemuan berikutnya*

***Pertemuan 3***

**Dimensi kualitas data:**

* akurasi,
* konsistensi,
* kelengkapan,
* dan validitas

**1. Akurasi (Accuracy)**

**Pengertian**: Akurasi merujuk pada tingkat di mana data menggambarkan kondisi nyata atau kebenaran dari objek atau entitas yang diwakilinya. Data yang akurat berarti data tersebut benar, tepat, dan mencerminkan informasi yang valid tanpa ada kesalahan atau distorsi.

**Contoh**: Jika data pelanggan menunjukkan bahwa seseorang berusia 30 tahun, maka akurasi berarti usia tersebut benar-benar 30 tahun, bukan 29 atau 31.

**Kriteria Akurasi:**

* Data harus bebas dari kesalahan faktual atau kesalahan pengukuran.
* Pengumpulan data harus dilakukan dengan proses yang andal dan terpercaya.

**2. Konsistensi (Consistency)**

**Pengertian**: Konsistensi berarti data yang ada di berbagai sistem atau sumber harus bersifat harmonis dan tidak bertentangan satu sama lain. Data yang konsisten adalah data yang tetap sama di seluruh proses atau database yang berbeda, tanpa adanya perbedaan atau ketidaksesuaian dalam format atau nilai.

**Contoh**: Jika nama pelanggan dalam sistem penjualan adalah "John Doe", nama yang sama harus muncul di sistem penagihan, inventaris, dan CRM tanpa perubahan seperti "J. Doe" atau "Jonathan Doe".

**Kriteria Konsistensi:**

* Data yang diupdate di satu sistem harus tercermin secara akurat di semua sistem lain yang menggunakan data tersebut.
* Aturan bisnis yang sama harus diterapkan di seluruh proses untuk menjaga keseragaman data.

**3. Kelengkapan (Completeness)**

**Pengertian**: Kelengkapan mengacu pada sejauh mana data yang tersedia mencakup semua informasi yang diperlukan atau diharapkan. Data yang lengkap berarti tidak ada elemen atau bagian penting yang hilang dari set data tersebut.

**Contoh**: Sebuah formulir pendaftaran pelanggan seharusnya mencakup semua kolom yang diperlukan seperti nama, alamat, nomor telepon, dan email. Jika salah satu kolom tersebut kosong, data dianggap tidak lengkap.

**Kriteria Kelengkapan:**

* Semua informasi wajib yang dibutuhkan oleh organisasi harus disediakan.
* Data harus memiliki semua atribut atau elemen yang diharapkan atau diperlukan untuk tujuan operasional.

**4. Validitas (Validity)**

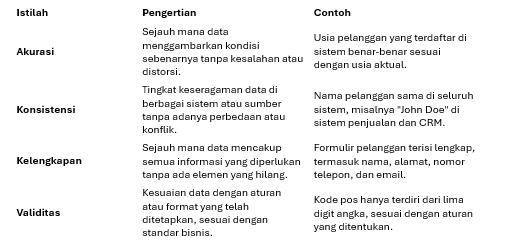
**Pengertian**: Validitas mengacu pada kesesuaian data dengan aturan atau format yang telah ditetapkan. Data yang valid berarti sesuai dengan aturan bisnis, format, dan standar yang diterapkan, dan tidak melanggar batasan-batasan yang telah ditentukan. Validitas juga mencakup bahwa data sesuai dengan tipe yang diharapkan (misalnya, angka pada kolom umur).

**Contoh**: Jika ada aturan bahwa kode pos harus terdiri dari lima digit angka, maka validitas data berarti bahwa semua entri kode pos dalam sistem hanya terdiri dari lima digit angka, bukan huruf atau format lain.

**Kriteria Validitas:**

* Data harus mematuhi aturan, standar, dan batasan yang telah ditentukan (misalnya, format tanggal harus sesuai dengan format yang telah ditetapkan, seperti DD/MM/YYYY).
* Setiap kolom atau atribut data harus memiliki tipe data yang benar (misalnya, angka untuk jumlah, teks untuk nama, dan sebagainya).

**RINGKASAN**



**Pentingnya Menerapkan Keempat Aspek Kualitas Data:**

* **Akurasi** memastikan bahwa data yang digunakan dalam pengambilan keputusan benar dan dapat diandalkan.
* **Konsistensi** menjaga keseragaman data antar sistem, menghindari kebingungan atau masalah dalam sinkronisasi data.
* **Kelengkapan** memastikan tidak ada informasi penting yang hilang sehingga tidak ada keputusan yang didasarkan pada data yang tidak cukup.
* **Validitas** menggaransi bahwa data mematuhi aturan bisnis dan format yang tepat, menghindari kesalahan saat pemrosesan data atau analisis.

Dalam **tata kelola dan infrastruktur data**, **Manajemen Kualitas Data** adalah aspek yang sangat penting untuk memastikan bahwa data yang digunakan dalam pengambilan keputusan dan proses bisnis lainnya valid, konsisten, dan dapat diandalkan. Namun, terdapat sejumlah permasalahan umum yang sering dihadapi dalam manajemen kualitas data.

Beberapa permasalahan yang mungkin terjadi serta solusi yang dapat diterapkan, antara lain:

**Permasalahan Utama dalam Manajemen Kualitas Data:**

1. Data yang Tidak Akurat
2. Data yang Tidak Konsisten
3. Data Duplikasi
4. Data yang Hilang atau Tidak Lengkap
5. Tidak Adanya Governance yang Jelas
6. Masalah Keamanan dan Privasi Data
7. Tidak Ada Mekanisme Pemantauan dan Pengukuran Kualitas Data
8. Integrasi Sistem yang Buruk

**Data yang Tidak Akurat**

**Permasalahan**: Data yang dimasukkan ke dalam sistem sering kali tidak akurat karena kesalahan manusia, proses otomatisasi yang buruk, atau data yang usang. Data yang tidak akurat dapat mengakibatkan keputusan bisnis yang salah dan penurunan kepercayaan terhadap sistem data. **Solusi**:

* Implementasi validasi data otomatis selama input data untuk memastikan data yang dimasukkan sesuai dengan format dan aturan yang telah ditetapkan.
* Melakukan pembersihan data secara berkala untuk memperbaiki data yang salah atau usang.
* Pelatihan personel terkait dengan pentingnya memasukkan data yang akurat dan menerapkan audit data secara rutin.

**Data yang Tidak Konsisten:**

**Permasalahan**: Data sering kali berasal dari berbagai sumber, dengan format dan standar yang berbeda. Ini dapat menyebabkan inkonsistensi, seperti perbedaan format tanggal, nama, atau kode unik. **Solusi**:

* Menerapkan **standarisasi data** melalui penerapan format dan konvensi yang seragam di seluruh organisasi. Ini bisa dilakukan dengan menggunakan **Master Data Management (MDM)** untuk mendefinisikan dan menjaga definisi yang konsisten.
* Menggunakan **ETL (Extract, Transform, Load)** tools untuk melakukan transformasi data secara otomatis, memastikan konsistensi di berbagai sumber data.

**Data Duplikasi**

**Permasalahan**: Data yang diinput lebih dari sekali, misalnya data pelanggan yang sama dimasukkan berkali-kali dengan nama atau ID yang berbeda. Hal ini menyebabkan redundansi dan kebingungan dalam analisis data. **Solusi**:

* Menerapkan deduplikasi data menggunakan algoritma yang bisa mengidentifikasi dan menghapus data yang redundant.
* Menggunakan kunci unik (unique keys) atau identifiers yang kuat, seperti nomor identifikasi nasional atau ID pelanggan yang tidak dapat diulang untuk menghindari duplikasi.

**Data yang Hilang atau Tidak Lengkap**

**Permasalahan**: Data yang hilang atau tidak lengkap sering kali menghambat analisis, pengambilan keputusan, dan integrasi dengan sistem lain. Misalnya, beberapa kolom penting mungkin kosong atau tidak sesuai dengan format yang diharapkan. **Solusi**:

* Implementasi **mekanisme wajib input data** untuk memastikan bahwa setiap kolom kritis diisi dengan benar.
* Menggunakan **data enrichment** untuk melengkapi informasi yang hilang, misalnya dengan menggabungkan data dari sumber lain atau melakukan estimasi berdasarkan data yang ada.
* **Automasi pengisian data** dan pengingat untuk bagian yang tidak lengkap dapat membantu dalam menangani masalah ini.

**Masalah Keamanan dan Privasi Data**

**Permasalahan**: Data yang berkualitas baik tidak hanya harus akurat dan konsisten, tetapi juga harus dilindungi dari akses yang tidak sah. Jika tidak, data yang sensitif dapat bocor, menyebabkan kerugian finansial dan reputasi. **Solusi**:

* Menerapkan **kontrol akses** dan **enkripsi data** untuk melindungi data sensitif dan memastikan bahwa hanya pengguna yang berwenang yang dapat mengaksesnya.
* Mematuhi **regulasi privasi data** seperti **GDPR** (General Data Protection Regulation) atau **Undang-Undang Perlindungan Data Pribadi** di negara lain, dan memastikan adanya transparansi dalam penggunaan data.

**Tidak Ada Mekanisme Pemantauan dan Pengukuran Kualitas Data**

**Permasalahan**: Organisasi mungkin tidak memiliki mekanisme untuk mengukur kualitas data secara terus-menerus, sehingga masalah kualitas data tidak teridentifikasi sampai menimbulkan dampak signifikan. **Solusi**:

* Menggunakan **Key Performance Indicators (KPIs)** dan **tools monitoring kualitas data** untuk secara proaktif memantau kualitas data dan mendeteksi potensi masalah sejak dini.
* Menerapkan **proses audit dan review data** secara berkala untuk menilai apakah kualitas data tetap sesuai standar.

**Integrasi Sistem yang Buruk**

**Permasalahan**: Sistem yang berbeda dalam sebuah organisasi mungkin menggunakan format data yang tidak sesuai atau tidak terhubung dengan baik, sehingga menyebabkan masalah integrasi data dan kualitas data yang rendah saat data dipindahkan di antara sistem-sistem tersebut. **Solusi**:

* Menerapkan solusi **middleware** atau **platform integrasi data** yang dapat mengakomodasi berbagai format data dan memastikan transisi data yang mulus antar sistem.
* Mengadopsi **arsitektur data modern** seperti **data lakes** atau **data warehouses** untuk menyatukan data dari berbagai sumber dalam format yang konsist

**Langkah-Langkah Penerapan Manajemen Kualitas Data yang Efektif:**

1. **Identifikasi Pemilik Data**: Menentukan siapa yang bertanggung jawab atas kualitas data di setiap bagian atau departemen, termasuk kebijakan pemrosesan data.
2. **Pembuatan Kebijakan Kualitas Data**: Menetapkan pedoman yang jelas terkait pengumpulan, pemrosesan, dan penyimpanan data yang sesuai dengan standar organisasi.
3. **Penggunaan Teknologi Pendukung**: Menggunakan alat-alat otomatisasi untuk pemantauan, validasi, dan pembersihan data secara berkala.
4. **Pelatihan dan Kesadaran Kualitas Data**: Melatih karyawan tentang pentingnya kualitas data dan bagaimana memasukkan serta mengelola data dengan benar.
5. **Evaluasi dan Audit Berkala**: Melakukan audit kualitas data secara berkala untuk memastikan bahwa standar kualitas tetap terjaga dan bahwa tindakan perbaikan dilakukan sesuai kebutuhan.

**Materi Pertemuan 5  
Peran dan Tanggung Jawab dalam Tata Kelola Data**

**Latar Belakang**

* Jika Anda berada di awal perjalanan tata kelola data, salah satu langkah pertama yang perlu Anda ambil adalah mengidentifikasi siapa di organisasi Anda yang akan menjadi bagian dari tim tata kelola data.
* Menunjuk orang yang salah pada peran kunci dapat mengakibatkan inisiatif yang dipikirkan secara matang menjadi gagal dengan cepat, jadi menyiapkan hal-hal mendasar dengan benar dan membentuk tim yang paling efektif dan tepat sejak awal akan sangat membantu Anda dalam penerapan tata kelola data yang sukses.
* Untuk menunjuk orang yang paling tepat untuk peran ini, penting untuk memahami apa saja yang mereka libatkan dan apa saja tanggung jawab mereka. Ini adalah peran dan tanggung jawab tata kelola data.

**Executive sponsor (Sponsor eksekutif)**

* Sponsor eksekutif adalah karyawan senior yang bertanggung jawab untuk mengoordinasikan aktivitas dan program tata kelola data. Peran sponsor eksekutif adalah bertindak sebagai penghubung antara pemangku kepentingan paling senior dan pimpinan atau dewan tata kelola data dan berwenang untuk membuat keputusan dan mengambil tindakan.
* Tanggung jawab sponsor eksekutif dapat bervariasi tergantung pada budaya organisasi dan tergantung apakah mereka mengambil peran yang lebih pasif atau peran yang lebih aktif. Jika mereka mengambil peran yang lebih aktif, tanggung jawabnya meliputi bekerja dengan tim tata kelola data dan bertanggung jawab atas implementasi dan proses tata kelola data yang sedang berlangsung. Tugas mereka adalah memastikan tujuan program, rencana tata kelola data, dan strategi lembaga selaras.

**Executive sponsor (Sponsor eksekutif)**

>> Peran penting lainnya adalah bagi mereka untuk membuat:

* Peran pemimpin program tata kelola data (misalnya ini bisa menjadi posisi Chief Data Officer)
* Dewan tata kelola data

>> Mereka juga bertugas mengamankan pendanaan untuk program tersebut dan memastikan anggota

tim diberikan waktu yang cukup di luar tugas harian untuk memenuhi peran mereka dalam tim tata kelola data. Ini berarti sponsor eksekutif harus memiliki senioritas yang relatif tinggi dalam organisasi Anda.

>. Jika mereka mengambil peran yang lebih pasif, tanggung jawab mereka umumnya hanya mencakup pengamanan pendanaan dan memastikan bahwa hasil tata kelola data terkait dengan prioritas bisnis

**Tanggung jawab seorang CDO (Chief Data Officer) meliputi hal-hal berikut:**

* **Tata Kelola** : Memberikan saran, memantau, dan mengatur data perusahaan.
* **Operasi** : Memastikan data dapat digunakan, tersedia, dan efisien.
* **Inovasi** : Mendorong transformasi digital, mengurangi biaya, dan menghasilkan pendapatan.
* **Analitik** : Mendukung analitik dan pelaporan pada produk, pelanggan, operasi, dan pasar

**Data governance lead (Pemimpin tata kelola data)**

* Pimpinan tata kelola data bertanggung jawab atas semua aspek dalam mendefinisikan dan mengoperasikan kebijakan tata kelola data serta mendukung berbagai domain data. Mereka bertanggungjawab untuk mengimplementasikan visi program tata kelola data, mempromosikan peran tata kelola, dan menegakkan kebijakan, sekaligus mengikuti praktik terbaik tata kelola data.
* Secara tradisional, peran ini berada di bawah TI dan cenderung menjadi tanggung jawab Chief Information Officer (CIO) atau bahkan Chief Technology Officer (CTO). Masih ada beberapa organisasiyang masih melakukan hal ini, tetapi tidak lagi direkomendasikan.
* Bergantung pada ukuran organisasi Anda, budayanya, kebutuhannya, tujuannya, serta model operasinya, peran pemimpin tata kelola data juga dapat jatuh ke tangan orang-orang berikut: Direktur/manajer tata kelola data ; Kepala Petugas Data ; Pimpinan kepatuhan dan keamanan informasi
* Kepada siapa pun peran itu diberikan, tanggung jawab utamanya adalah memberikan kepemimpinan, dukungan, sponsor, dan pemahaman tentang tata kelola data kepada departemen lain.

**Data governance council (Dewan tata kelola data)**

* Ini adalah satu-satunya peran dalam daftar ini yang bukan milik individu. Peran ini milik sekelompok individu. Ada kelompok lain sebagai bagian dari hierarki organisasi tata kelola data, tetapi saya akan membahasnya dalam artikel terpisah.
* Jadi, apa itu dewan tata kelola data? Sederhananya, dewan ini adalah badan pengelola yang bertanggung jawab atas arahan strategis program tata kelola data, penentuan prioritas proyek dan inisiatif tata kelola data, persetujuan kebijakan dan standar data di seluruh organisasi, serta memungkinkan dukungan, pemahaman, dan kesadaran berkelanjutan terhadap program tata kelola data.
* Intinya, badan ini menetapkan arah strategis tentang APA yang perlu dicapai oleh program tata kelola data dan KAPAN program tersebut perlu mencapainya. Sebaliknya, pimpinan tata keloladata memutuskan bagaimana hal-hal ini harus dicapai

**Tanggung jawab Dewan Tata Kelola data meliputi:**

* Menangani kebijakan tata kelola data, standar, proses, dan persyaratan lainnya
* Kontrol dan penegakan standar tata kelola data
* Menyediakan kerangka kerja untuk komunikasi dan kolaborasi yang efektif antara departemen TI dan unit bisnis
* Mengawasi berbagai jenis kebijakan atau strategi manajemen data yang membahas proses persetujuan
* Saran dan rekomendasi tentang aktivitas kualitas data
* Menyelaraskan persyaratan data, prioritas, dan masalah di berbagai entitas
* Menyelesaikan perselisihan terkait tata kelola data
* Mengubah kebijakan sesuai kebutuhan
* Mengkoordinasikan masalah umum dan terperinci yang terkait dengan strategi data

**Data owner (Pemilik Data)**

* Pemilik data adalah orang dalam organisasi Anda yang memiliki wewenang untuk membuat keputusan tentang definisi istilah bisnis, kualitas data, aksesibilitas, dan persyaratan penyimpanan yang terkait dengan kebutuhan bisnis.
* Pemilik data Anda juga perlu mengetahui, atau setidaknya menyadari, peraturan, kebijakan, undang-undang yang mengatur privasi data dan memahami kebutuhan bisnis serta aturan, prosedur, dan batasan bisnis, karena hal ini terkait dengan area kepemilikan data mereka sendiri. Setidaknya di dunia yang ideal. Lebih sering mereka mendapatkan saran tentang hal-hal ini dari kantor tata kelola data dan dewan tata kelola data
* Secara umum, saat menunjuk pemilik data, Anda akan menginginkan seseorang yang memiliki pengetahuan mendalam dan pemahaman bisnis yang baik tentang data yang mereka miliki. Sekarang, kita tahu bahwa tidak seorang pun dapat mengetahui segalanya tentang setiap bit data dari setiap departemen di satu organisasi. Ini berarti Anda mungkin memiliki sejumlah pemilik data dalam program tata kelola data Anda, dengan masing-masing bertanggung jawab atas data dalam area bisnis mereka sendiri.
* Pemilik data biasanya adalah manajer senior dari berbagai area fungsional bisnis. Area bisnis ini adalah pemangku kepentingan utama dari domain data tertentu.

**Data Steward (Pengelola Data)**

* Sebagian besar pengelola data berasal dari departemen bisnis masing-masing. Anda akan menginginkan pengelola data
* yang memahami data dan kebutuhan bisnis serta aturan yang mengaturnya, fasilitator yang baik, dan memiliki pola pikir
* analitis. Yang terpenting, pengelola data Anda haruslah orang-orang yang memiliki pengetahuan praktis tentang data
* dan memahami bagaimana data tersebut digunakan oleh bisnis sehari-hari. Sederhananya, pengelola data Anda
* berinvestasi dalam data.
* Seorang pengurus data berada di bawah pemilik data dan umumnya ditunjuk oleh pemilik data untuk bekerja dengan
* mereka atau bertindak sebagai perwakilan mereka dalam rapat kelompok domain pengelolaan data. Dalam hierarki tata
* kelola data, mereka menjadi bagian dari setidaknya satu kelompok domain pengelolaan data.
* Pemilik data tetap bertanggung jawab, tetapi mereka akan mendelegasikan tanggung jawab sehari-hari kepada
* pengurus data. Pengurus data sering kali cenderung menjadi pakar dalam bidang tersebut tetapi masih cukup senior
* karena mereka harus dipercaya oleh pemilik data.
* Jika Anda ambil contoh, departemen keuangan, kemungkinan besar direktur keuangan atau wakilnya akan menjadi
* pemilik data untuk semua data keuangan, kemudian kepala setiap sub tim dalam keuangan akan ditunjuk sebagai
* pengurus data.
* Ada juga konsep Pengelola Data Utama, yang bertanggung jawab atas hasil kelompok domain pengelolaan data mereka
* dan mereka merupakan penghubung antara pengelola data dan dewan tata kelola data

**Tanggung Jawab Seorang Pengelola Data**

* Memenuhi persyaratan data komunitas pengguna
* Mengumpulkan, merakit, dan menilai isu dan permasalahan berdasarkan fakta
* Disarankan untuk mendelegasikan tugas pengelolaan sehubungan dengan pokok bahasan atau bidang usaha.
* Menyelaraskan peran pengelolaan di sepanjang batasan Entitas Data Utama (KDE) dalam kasus Manajemen Data Induk (MDM).
* Penting juga untuk melaporkan berbagai masalah yang menonjol kepada masing-masing orang yang mungkin terpengaruh.
* Standarisasi definisi, aturan, dan deskripsi data untuk menyediakan konteks pada aset data.
* Pastikan kualitas dan standar data dinilai, dikontrol, dan diperiksa di seluruh bisnis.
* Mengadopsi praktik terbaik tata kelola keamanan data untuk diintegrasikan dengan tujuan tata kelola, kebijakan, norma, dan peraturan.
* Identifikasi dan klasifikasikan tingkat akses data, memastikan pengguna bisnis yang tepat dapat mengakses data yang diperlukan

**Data Stakeholder (Pemangku Kepentingan)**

* Pemangku kepentingan dalam program tata kelola data apa pun adalah individu atau kelompok yang dapat memengaruhi atau dipengaruhi oleh keputusan, proses, kebijakan, standar, dan lain-lain tata kelola data. Contoh pemangku kepentingan yang jelas adalah peneliti institusional, pengelola data, arsitek data, dan staf intelijen bisnis.
* Selain mereka yang lebih erat kaitannya dengan peran manajemen data, kelompok lain juga perlu dipandang sebagai pemangku kepentingan. Misalnya, seorang rektor universitas yang melihat laporan dasbor tentang persentase pengajar yang mengajar mata kuliah daring perlu mengetahui bagaimana "pengajar" didefinisikan dan apakah asisten dosen atau dosen diikutsertakan. Program tata kelola data yang efektif memiliki informasi dan definisi yang tepat yang tertanam dalam dasbor sehingga rektor dapat memahami dan menafsirkan data dengan benar.
* Program tata kelola data perlu dibangun untuk mendukung konsumen data dalam berbagai kelompok dalam institusi.
* Anda menginginkan pemangku kepentingan data yang: Memahami pentingnya data dan dampaknya; Bersifat kolaboratif dan ingin terlibat; Adalah seorang juara di bidang keahliannya

**Data Custodian (Penjaga Data)**

* Penjaga data biasanya merupakan bagian dari departemen TI. Hal ini membuatnya berbeda secara mendasar dari peran lainnya - seperti pemilik data dan pengurus data - karena semuanya berkaitan dengan bisnis.
* Penjaga data biasanya dibagi lagi berdasarkan area keahliannya, seperti: pemodelan data, arsitektur data, dan administrasi basis data. Mereka bertanggung jawab utama untuk memelihara, mengarsipkan, memulihkan, mencadangkan data, mencegah kehilangan/kerusakan data, dan lain-lain.
* Anda menginginkan penjaga data yang: Memiliki pengetahuan, keterampilan, dan pengalaman teknis yang diperlukan; Mengikuti praktik terbaik pengelolaan data yang baik; Mengetahui peraturan, kebijakan, dan standar yang mengatur data yang mereka gunakan
* Sederhananya, mereka bertanggung jawab untuk memelihara data pada sistem Anda sesuai dengan persyaratan bisnis. Menjadi kustodian data berarti memelihara data dan sistem, memindahkan data antar sistem, menggabungkan, dan mentransformasikan data sesuai dengan persyaratan bisnis.
* Penjaga data cenderung berkolaborasi dengan pengelola data dan pemangku kepentingan data dan semuanya dapat menjadi bagian dari grup domain pengelolaan data yang sama

**Tanggung jawab seorang Penjaga Data meliputi:**

* Mengotorisasi dan mengendalikan akses ke data
* Penentuan pengurus data untuk setiap tipe data
* Mempertahankan proses diskursif sehingga data tetap berkelanjutan
* Kolaborasi dengan pengurus data untuk menangani masalah kualitas data
* Menerapkan kontrol teknis untuk melindungi data
* Verifikasi Konsistensi Data dengan bantuan model data umum
* Memelihara cadangan data Master, serta mendokumentasikan proses pembaruan.
* Mempertimbangkan penerapan proses manajemen perubahan dalam pemeliharaan database

**Bagaimana Anda Menetapkan Tanggung Jawab kepada Tim Tata Kelola Data?**

• Menetapkan tanggung jawab kepada tim tata kelola data Anda penting untuk memastikan setiap orang tahu apa yang seharusnya mereka lakukan. Ini membantu menjaga segala sesuatunya tetap teratur dan memastikan bahwa data dikelola dengan baik.

• Namun, penugasan tanggung jawab kepada tim tata kelola data melibatkan beberapa langkah penting untuk memastikan kejelasan dan efektivitas:

**1. Tentukan Peran**

• Peran dalam tata kelola data menjadi dasar bagi pengelolaan aset dan aktivitas data yang efektif di seluruh organisasi. Setiap peran menentukan tanggung jawab, memastikan akuntabilitas yang jelas, konsultasi dengan pemangku kepentingan, dan memberi tahu semua pihak tentang tugas-tugas terkait data yang relevan.

• Pada perusahaan rintisan teknologi kecil, peran dalam tata kelola data mungkin terlihat seperti ini:

• **Pengelola Data** : Bertanggung jawab untuk menjaga kualitas data dalam basis data pelanggan dan memastikan kepatuhan terhadap peraturan perlindungan data.

• **Administrator Data** : Mengelola infrastruktur basis data, memastikan aksesibilitas dan keamanan data untuk tim pengembangan.

• **CDO** : Mengawasi strategi data secara keseluruhan, menyelaraskan inisiatif data dengan tujuan bisnis untuk mendorong pertumbuhan dan inovasi

**2. Identifikasi Tanggung Jawab**

• Berikutnya adalah menetapkan tanggung jawab untuk peran-peran ini. Biasanya, Chief Data Officer (CDO) memimpin dalam mengawasi upaya tata kelola data. Tanggung jawab utama CDO adalah memastikan bahwa kebijakan data mendukung tujuan strategis organisasi.

• Hal ini melibatkan penetapan tugas dan tanggung jawab yang jelas bagi setiap peran untuk memastikan mereka berkontribusi secara efektif dalam mencapai tujuan tata kelola data

**3. Mencocokkan Keterampilan dan Pengalaman**

• Langkah selanjutnya setelah mengidentifikasi tanggung jawab adalah mencocokkannya dengan keterampilan dan pengalaman yang tepat. Misalnya, seseorang yang ahli dalam manajemen kualitas data akan fokus pada upaya memastikan keakuratan data di seluruh organisasi.

• Dengan cara ini, setiap anggota tim dapat menangani tugas yang paling mampu mereka kelola, dan tata kelola data Anda akan berjalan dengan baik.

**4. Menetapkan Akuntabilitas**

• Langkah ini secara jelas mendefinisikan siapa yang bertanggung jawab atas setiap tugas atauarea manajemen data tertentu. Misalnya, Chief Data Officer mungkin bertanggung jawab atas strategi data secara keseluruhan dan kepatuhan terhadap kebijakan data dalam tim tata kelola data perusahaan.

• Sementara itu, seorang Data Steward dapat bertanggung jawab untuk memastikan kualitas dan integritas data pelanggan yang digunakan dalam kampanye pemasaran.

• Dapatkah Anda melihat kejelasannya di sini? Hal ini memastikan bahwa setiap aspek tata kelola data Anda memiliki pemilik khusus yang dapat bertanggung jawab atas keberhasilan dan hasilnya.

**5. Memberikan Pelatihan**

• Untuk memastikan tim tata kelola data Anda memahami peran dan tanggung jawab mereka secara efektif, berikan pelatihan dan sumber daya.

• Misalnya, perusahaan jasa keuangan menerapkan program di mana Chief Data Officer memastikan pengelola data menerima pelatihan kualitas data dan kepatuhan. Mereka menghadiri lokakarya dan memperoleh sertifikasi.

• Anda perlu menawarkan dukungan berkelanjutan dengan pedoman terkini, sesi pelatihan rutin, dan bimbingan. Dengan cara ini, tim tata kelola data Anda dapat mempertahankan standar data yang tinggi.

**Kesimpulan**

• Dari atas hingga bawah suatu organisasi, sangat penting bagi inisiatif tata kelola data Anda untuk mengidentifikasi orang yang tepat untuk menjalankan masingmasing peran penting ini dan mereka juga memahami peran apa yang dimainkan satu sama lain dalam gambaran besar.

• Sekali lagi, mendapatkan dasar-dasar yang benar dan tim yang paling efektif dan cocok sejak awal akan sangat membantu Anda dalam penerapan tata kelola data yang sukses.

**Tanya jawab umum**

**Bagaimana tata kelola data meningkatkan pengambilan keputusan organisasi?**

• Kerangka tata kelola data berperan penting dalam meningkatkan pengambilan keputusan organisasi. Kerangka ini memastikan bahwa data yang digunakan dalam proses pengambilan keputusan akurat, andal, dan aman

**Tantangan apa yang dihadapi organisasi dalam menerapkan tata kelola data?**

• Menerapkan kerangka tata kelola data memiliki sejumlah tantangan tersendiri. Organisasi sering kali kesulitan dalam menetapkan kebijakan yang jelas, menciptakan kolaborasi lintas departemen, dan mengelola praktik tata kelola data yang sedang berjalan secara efektif

**Bagaimana tata kelola data berhubungan dengan kepatuhan regulasi?**

• Tata kelola data terkait erat dengan kepatuhan terhadap peraturan. Tata kelola data melibatkan pembuatan dan penerapan kebijakan serta prosedur yang memastikan praktik penanganan data organisasi mematuhi standar dan peraturan hukum