BINUS University

Academic Career: ***~~Undergraduate / Master / Doctoral /~~ BINUS Online ~~/ Professional~~**)*			**Class Program:** *Regular ~~/ Global Class~~*)*	
☐ **Mid Exam** ■ **Final Exam**	☐ **Others Exam :**_____		**Term : ~~Odd /~~ Even ~~/ Compact~~*)** **Period (Only for *BINUS Online ~~/ Master~~*) : 1 ~~/ 2~~*)**	
☐ **Kemanggisan** ☐ **Alam Sutera** ☐ **Bekasi**	☐ **Senayan** ☐ **Bandung** ☐ **Malang**	☐ **Semarang** ☐ **Medan** ■ **BiOn**	**Academic Year :** **2025 / 2026**	
Exam Type*	: ~~Onsite / Online /~~ Take Home		Faculty / Dept.	: BINUS Online Learning
Day / Date**	: Senin, 18 Mei 2026 s.d. Senin, 25 Mei 2026		Code - Course	: ISYS6877035 - IT Governance and Security
Time**	: 00:00 WIB s.d. 12:00 WIB (Siang)			
Exam Specification***	: ■ Open Book ☐ Close Book ■ Open E-Book	■ Open Notes ☐ Oral Test	Class	: All Classes
Equipment***	:		Student ID***	: 2802530243
☐ Examination Booklet ■ Calculator ☐ Dictionary	■ Laptop ☐ Tablet ☐ Smartphone	☐ Drawing Paper - A3 ☐ Drawing Paper - A2 ☐ Notes :_____sheet	Name***	: Rizki Rahardiputra
			Signature***	:

) Strikethrough the unnecessary items* *) For Online Exam, this is the due date* ****) Only for Onsite Exam*

Please insert the test paper into the examination booklet and submit both papers after the test.***
The penalty for CHEATING is DROP OUT!

INSTRUCTION

Bacalah ketentuan-ketentuan berikut, sebelum mengerjakan ujian:

1. Cantumkan NIM, Nama Lengkap, Nama Matakuliah dan Kode Kelas pada lembar jawaban.
2. Bahan referensi wajib untuk setiap jawaban:
    1. LN dan atau PPT Matakuliah
    2. Mencantumkan referensi wajib di setiap jawaban
3. Bahan referensi tambahan untuk setiap jawaban:
    1. Harus yang relevan, ilmiah dan dari media resmi
    2. Boleh dari buku, artikel surat kabar, artikel sumber-sumber online, artikel jurnal ilmiah
    3. Mencantumkan referensi yang digunakan untuk setiap jawaban, mencakup: nama penulis, judul buku/artikel, penerbit/link, tahun terbit, halaman
4. Tidak diijinkan mengambil teks secara langsung (plagiat/copy paste) dari sumber referensi, lakukan paraphrasing dengan mengolah dan menulis menggunakan kalimat sendiri.
5. Sertakan link dan atau screen shoot dari Prompts jika menggunakan bantuan Text Generator (ChatGPT, Gemini, dll). Lakukan parafrasing dan jawaban tidak diijinkan copy paste langsung.

1. LO 1: IT governance frameworks (e.g., COBIT) to manage and align information system projects with organizational objectives (10%)

BACALAH STUDI KASUS DIBAWAH INI UNTUK MENJAWAB SEMUA PERTANYAAN

Pemerintah Indonesia mengembangkan platform **SatuSehat** sebagai ekosistem data kesehatan nasional yang mengintegrasikan data dari rumah sakit, BPJS, laboratorium, dan aplikasi kesehatan lainnya. Sistem ini mengelola data sensitif seperti rekam medis, data identitas, dan riwayat kesehatan masyarakat.

Dalam implementasinya, muncul berbagai tantangan:

1. Integrasi sistem lintas organisasi dengan standar yang berbeda
2. Risiko kebocoran data kesehatan
3. Ketergantungan pada cloud dan pihak ketiga

4. Kompleksitas kepatuhan terhadap regulasi internasional (GDPR)
5. Ancaman serangan siber (ransomware, data breach)
6. Belum optimalnya kesiapan incident response nasional

Kasus ini menuntut penerapan IT governance, risk management, compliance, cybersecurity, dan incident response secara terintegrasi.

PERTANYAAN1.

Sebagai konsultan IT governance, analisis implementasi **SatuSehat** menggunakan kerangka **COBIT 2019**.

1. Jelaskan bagaimana prinsip governance vs management (EDM vs APO/BAI/DSS/MEA) seharusnya diterapkan.

   Jawaban:

   Dalam kerangka COBIT 2019, penting untuk memisahkan tanggung jawab antara pengambil keputusan kebijakan dan pelaksana operasional dengan jelas di SatuSehat. Pemisahan ini harus dilakukan melalui pembagian berikut (Sarungu, 2025):

   - Ranah Governance (Domain EDM - Evaluasi, Arahkan, Pantau): Pimpinan Kementerian Kesehatan berperan sebagai dewan pengarah yang bertugas untuk mengevaluasi kebutuhan peraturan data medis nasional, mengarahkan strategi integrasi dan mitigasi risiko besar, serta memantau kepatuhan platform terhadap ketahanan kesehatan negara (ISACA, 2018). Di tahap ini, perhatian utama adalah untuk memastikan bahwa investasi TI SatuSehat memberikan manfaat bisnis yang terbaik untuk masyarakat (Sarungu, 2025).

   - Ranah Management (Domain APO, BAI, DSS, MEA): Ditugaskan kepada Digital Transformation Office (DTO) dan mitra teknis untuk mengeksekusi arahan strategis melalui siklus operasional harian (Sarungu, 2025). Manajemen bertanggung jawab merencanakan arsitektur integrasi (APO), membangun konektivitas API yang aman pada legacy system rumah sakit (BAI), menjalankan pertahanan siber harian dan respons insiden (DSS), serta mengaudit kinerja platform secara berkala (MEA) (ISACA, 2018).

2. Identifikasi 2 kegagalan alignment antara IT dan business objectives dalam kasus ini.
   Jawaban:

   Berdasarkan kondisi implementasi SatuSehat, terdapat dua indikasi ketidakselarasan utama antara target bisnis (kesehatan) dan kapabilitas teknologi (Sarungu, 2025):
   - Kegagalan Kesesuaian Strategis dalam Interoperabilitas Data: Tujuan bisnis pemerintah adalah untuk mewujudkan pertukaran data medis yang cepat dan tanpa hambatan di seluruh Indonesia (Sarungu, 2025). Namun, dari sisi teknologi informasi, terjadi masalah dalam menyelaraskan standar arsitektur karena adanya berbagai platform lama yang dimiliki oleh setiap fasilitas kesehatan. Hal ini menghambat integrasi yang aman (Mburu, 2023).
   - Kesenjangan antara ketahanan teknologi dan harapan bisnis: Ciri-ciri bisnis layanan kesehatan membutuhkan ketersediaan data yang sempurna (tanpa jeda) karena berkaitan dengan keselamatan pasien (Sarungu, 2025). Kegagalan dalam menyelaraskan hal ini terjadi karena infrastruktur teknologi informasi (TI) belum bisa memenuhi kebutuhan yang mendesak. Hal ini terlihat dari ketergantungan yang tinggi pada layanan cloud dari pihak ketiga tanpa adanya kontrol yang ketat, serta kurangnya kesiapan respons terhadap insiden di tingkat nasional terhadap serangan ransomware (ISACA, 2018).

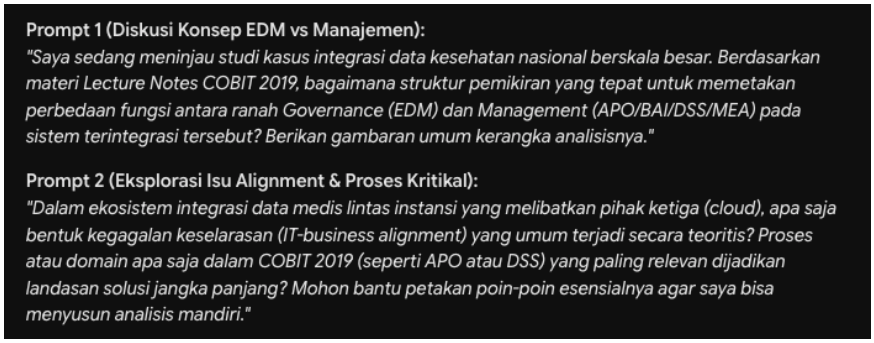
3. Rekomendasikan domain/proses COBIT yang paling kritikal untuk memperbaiki alignment tersebut.
   Jawaban:

   Untuk menjembatani kesenjangan tersebut, manajemen SatuSehat wajib memprioritaskan dua proses COBIT 2019 berikut (Sarungu, 2025):
   - APO03 (Arsitektur Perusahaan yang Dikelola): Proses ini sangat penting untuk mengatasi masalah interoperabilitas. Tim TI perlu membuat satu rencana standar untuk arsitektur data yang harus diikuti oleh semua rumah sakit. Hal ini penting agar integrasi data antara organisasi dapat berjalan dengan baik dan aman (Sarungu, 2025).
   - APO12 (Manajemen Risiko) dan DSS05 (Layanan Keamanan Terkelola): Kerja sama antara kedua proses ini sangat penting untuk mengurangi risiko siber. APO12 digunakan untuk menetapkan batas toleransi risiko dalam penggunaan vendor cloud dari pihak ketiga, sedangkan DSS05 melaksanakan kontrol keamanan teknis secara terus-menerus untuk mencegah kebocoran data penting dan serangan ransomware (Sarungu, 2025).

   Referensi:

   - ISACA. (2018). COBIT 2019 Framework: Introduction and Methodology. Information Systems Audit and Control Association (ISACA).
   - Mburu, S. (2023). Guiding the Development of Interoperable Health Information Systems: A Conceptual IT Governance Framework. ResearchGate.
   - Sarungu, C. M. (2025). Lecture Notes Week 1: EGIT, Alignment, Value Introduction. BINUS University Online Learning.
   - Sarungu, C. M. (2025). Lecture Notes Week 2: Business/IT Alignment. BINUS University Online Learning.
   - Sarungu, C. M. (2025). Lecture Notes Week 4: COBIT Foundation 1. BINUS University Online Learning.
   - Sarungu, C. M. (2025). Lecture Notes Week 5: COBIT Foundation 2. BINUS University Online Learning.

Screen shoot Prompt:



2. LO 2: risk management strategies in IT projects by identifying and mitigating potential risks to ensure project success and security. (20%)

PERTANYAAN 2:

Gunakan pendekatan risk management (ISO 31000) untuk menganalisis risiko pada SatuSehat.

1. Identifikasi minimal lima risiko utama (strategic, operational, cybersecurity, compliance, reputational).

   Jawaban:

   Berdasarkan proses identifikasi risiko dalam kerangka kerja ISO 31000, terdapat lima domain risiko kritikal dalam ekosistem SatuSehat:

   - Risiko Strategis (Keterikatan Vendor & Ketergantungan): Terlalu bergantung pada penyedia layanan cloud pihak ketiga tanpa memiliki rencana keluar yang jelas. Ini bisa menyebabkan biaya operasional yang meningkat tanpa kontrol dan juga mengurangi fleksibilitas kedaulatan data dalam jangka panjang.
   - Risiko Operasional (Kegagalan Interoperabilitas Sistem): Masalah dalam ketersediaan platform yang disebabkan oleh kesulitan dalam mengintegrasikan sistem lama (legacy system) dari ribuan fasilitas kesehatan yang masing-masing memiliki standar kinerja yang berbeda. Masalah ini bisa menyebabkan terganggunya akses untuk bertukar data medis ketika pelayanan pasien sedang berlangsung.
   - Risiko Keamanan Siber (Ransomware & Pencurian Data): Serangan siber yang ditargetkan untuk memanfaatkan celah keamanan pada integrasi API antara organisasi. Dampak utama dari hal ini adalah enkripsi data secara besar-besaran atau pencurian data medis yang bersifat sensitif oleh pihak-pihak yang berbahaya dari luar.
   - Risiko Kepatuhan: Kegagalan dalam sistem atau proses tata kelola SatuSehat untuk memenuhi aturan hukum yang melindungi data, baik dari peraturan dalam negeri (UU PDP) maupun yang internasional (GDPR), disebabkan oleh lemahnya pengawasan terhadap hak subjek data dan pencatatan audit yang tidak memadai.

     Risiko Reputasi (Krisis Kepercayaan Publik): Kehilangan kepercayaan dari masyarakat dan komunitas medis secara besar-besaran terhadap keandalan platform pemerintah jika ada insiden kebocoran data yang terjadi berulang kali, yang bisa menyebabkan masyarakat menolak untuk menggunakan ekosistem digital nasional.

2. Lakukan analisis likelihood vs impact terhadap 2 risiko paling kritis.

   Jawaban:

   Untuk menentukan prioritas penanganan, dilakukan analisis mendalam terhadap dua dimensi utama—kemungkinan terjadinya (likelihood) dan dampak yang ditimbulkan (impact) pada dua risiko paling kritis:

   - **Risiko Keamanan Siber (Serangan Ransomware / Kebocoran Data)**

     Kemungkinan – Tinggi: Ekosistem kesehatan menjadi sasaran utama serangan siber di seluruh dunia karena data rekam medis memiliki nilai yang sangat tinggi di pasar gelap. Beragamnya standar keamanan di ribuan lokasi integrasi rumah sakit daerah meningkatkan kemungkinan terjadinya ancaman.

     Dampak – Sangat Tinggi: Kehilangan kontrol atas data penting dapat menyebabkan hukuman hukum yang serius, denda uang, dan risiko bahaya fisik jika catatan medis pasien diubah atau tidak bisa diakses saat terjadi keadaan darurat.

   - **Risiko Operasional (Kegagalan Interoperabilitas & Downtime Sistem)**

     Kemungkinan – Sedang-Tinggi: Kesulitan dalam menggabungkan data dari berbagai organisasi dengan arsitektur, format data, dan infrastruktur jaringan yang tidak seimbang sering menyebabkan terjadinya kegagalan dalam sinkronisasi, terutama di fase operasional awal.

     Dampak – Tinggi: Jika sistem pusat tidak berfungsi, proses administrasi rujukan, verifikasi BPJS, dan akses riwayat alergi obat pasien di unit gawat darurat akan terhenti di seluruh negara, mengganggu stabilitas layanan kesehatan publik.

3. Rancang strategi mitigasi risiko yang selaras dengan keberlanjutan layanan kesehatan nasional.

   Jawaban:

   Guna memastikan keberlanjutan layanan kesehatan nasional (business continuity), strategi penanganan risiko (risk treatment) dirancang sebagai berikut:

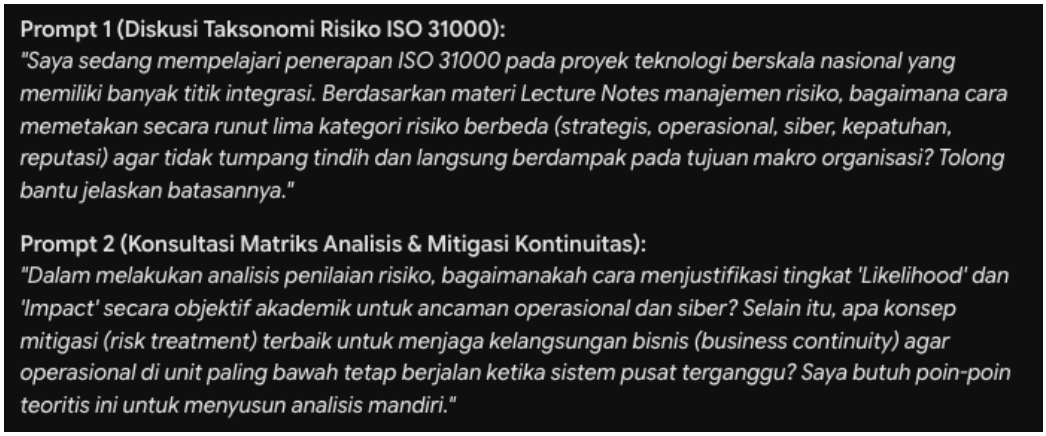
   - Mitigasi Risiko Siber (Teknis & Prosedural): Mengimplementasikan enkripsi tingkat tinggi di semua level data (at rest dan in transit), menerapkan arsitektur kontrol akses yang ketat, serta mewajibkan audit keamanan periodik bersama tim tanggap insiden nasional untuk mendeteksi ancaman secara real-time.

   - Mitigasi Risiko Operasional (Arsitektur Ketahanan): Mewajibkan penyedia cloud menyediakan klaster redundansi (multi-zone availability) dengan jaminan SLA tinggi. Di sisi lain, sistem aplikasi lokal di rumah sakit harus dilengkapi dengan fitur offline caching, sehingga dokter tetap dapat menginput dan melihat data medis esensial pasien secara lokal meskipun koneksi ke pusat SatuSehat terputus sementara. Hal ini memastikan operasional medis di lapangan tetap berjalan tanpa disrupsi fatal.

   Referensi:

- ISO. (2018). ISO 31000:2018 Risk Management – Guidelines. International Organization for Standardization.
- Sarungu, C. M. (2025). Lecture Notes Week 7: Risk Management in EGIT (ISO 31000). BINUS University Online Learning.

   Screen shoot Prompt:



3. LO 3: regulatory and compliance standards (e.g., GDPR, HIPAA) to ensure information system projects meet legal and organizational requirements. (20%)

PERTANYAAN 3:

Evaluasi kesiapan SatuSehat dalam memenuhi standar GDPR dan regulasi perlindungan data kesehatan.

1. Jelaskan prinsip GDPR yang paling relevan untuk data kesehatan.

   Jawaban:

   Dalam pengelolaan data ekosistem SatuSehat, terdapat dua prinsip utama GDPR yang paling krusial untuk diterapkan:

   - Integrity and Confidentiality (Integritas dan Kerahasiaan): Prinsip ini mewajibkan data pribadi diproses dengan cara yang menjamin keamanan tingkat tinggi, termasuk perlindungan terhadap pemrosesan yang tidak sah, kehilangan, atau kerusakan secara tidak sengaja. Dalam kasus SatuSehat, prinsip ini sangat relevan untuk mendasari kewajiban penerapan enkripsi kuat dan kontrol akses berlapis demi melindungi rekam medis dari ancaman kebocoran data dan serangan siber lintas organisasi.

   - Purpose Limitation (Pembatasan Tujuan): Data kesehatan masyarakat harus dikumpulkan untuk tujuan yang spesifik, eksplisit, dan sah, serta tidak boleh disalahgunakan untuk aktivitas lain yang tidak kompatibel dengan tujuan awal. Platform SatuSehat wajib menjamin bahwa rekam medis yang diintegrasikan dari berbagai rumah sakit dan laboratorium murni digunakan untuk kepentingan pelayanan kesehatan dan jaminan sosial, bukan untuk komodifikasi data atau pelacakan tanpa persetujuan (consent) eksplisit dari pasien.

2. Identifikasi dua potensi pelanggaran compliance dalam kasus ini.

   Jawaban:

   Berdasarkan kerentanan operasional platform SatuSehat, terdapat dua potensi pelanggaran serius terhadap aspek kepatuhan regulasi:

- Pelanggaran Akuntabilitas Pengawasan Pihak Ketiga (Processor Oversight Failure): Ketergantungan yang tinggi pada penyedia cloud pihak ketiga tanpa adanya ikatan kontrak Data Processing Agreement (DPA) yang ketat merupakan pelanggaran serius. Di bawah GDPR, Kemenkes selaku Data Controller tetap memegang tanggung jawab penuh atas kegagalan sistem keamanan yang terjadi di sisi vendor cloud selaku Data Processor.

- Kegagalan Pemenuhan Hak Subjek Data (Data Subject Rights Violation): Kompleksitas integrasi dengan standar yang berbeda antar-organisasi berpotensi memicu kegagalan sistem dalam mengakomodasi hak-hak konstitusional pemilik data. Hal ini mencakup potensi ketidakmampuan platform untuk memfasilitasi hak akses (right of access), hak pembetulan data yang keliru (right to rectification), atau hak penghapusan (right to be forgotten) secara sinkron di seluruh jaringan rumah sakit yang terhubung.

3. Rekomendasikan langkah strategis agar sistem memenuhi aspek legal, governance, dan accountability.

   Jawaban:

   Untuk memastikan sistem SatuSehat memenuhi kriteria kepatuhan secara menyeluruh, manajemen direkomendasikan mengambil langkah strategis berikut:

   - Aspek Legal: Menyusun dan mengimplementasikan klausul Data Processing Agreement (DPA) yang seragam dan mengikat secara hukum dengan seluruh fasilitas kesehatan mitra dan penyedia cloud. Selain itu, sistem harus membangun mekanisme persetujuan (consent management) yang transparan dan mudah diakses oleh masyarakat.

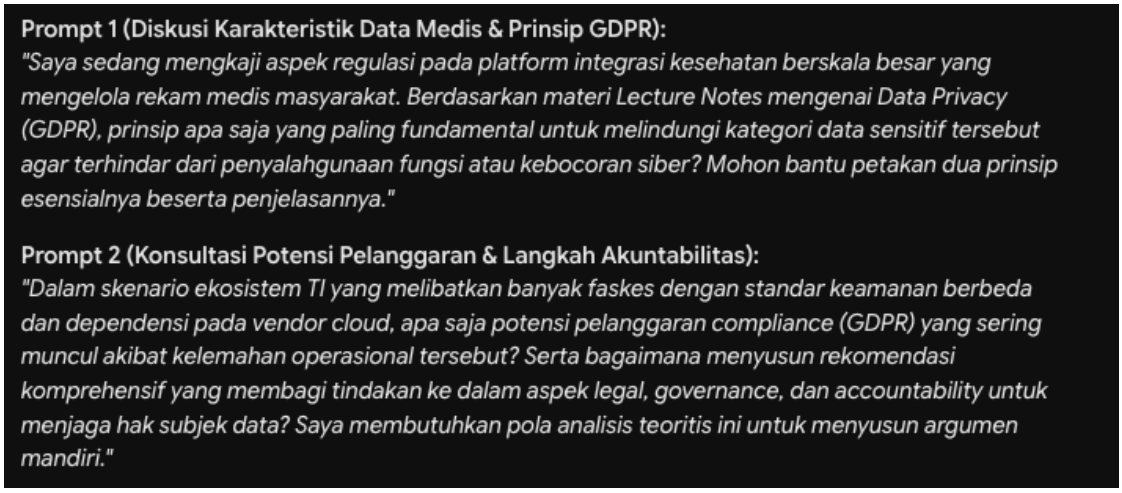
   - Aspek Governance: Menunjuk dan menempatkan Pejabat Perlindungan Data atau Data Protection Officer (DPO) yang independen di level otoritas pusat SatuSehat. DPO ini bertugas mengawasi kepatuhan harian, memberikan saran tata kelola data lintas instansi, serta menjadi narahubung utama bagi lembaga regulator dan subjek data.

   - Aspek Accountability: Mewajibkan pelaksanaan Penilaian Dampak Perlindungan Data atau Data Protection Impact Assessment (DPIA) secara berkala sebelum melakukan interkoneksi sistem baru. Seluruh aktivitas pemrosesan, mutasi data, dan hak akses juga harus terdokumentasi dalam audit trail yang komprehensif guna membuktikan akuntabilitas platform saat dilakukan audit eksternal.

   Referensi

   - Dibble, S. (2020). GDPR for Dummies. John Wiley & Sons, Inc.
   - Sarungu, C. M. (2026). Lecture Notes Week 9: Data Privacy (General Data Protection Regulation). BINUS University Online Learning.
   - Voigt, P., & Von dem Bussche, A. (2017). The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer.

   Screen shoot Prompt:



4. LO 4: cybersecurity best practices, such as access controls and encryption, to protect data and maintain system integrity within information system projects. (20%)

PERTANYAAN 4:

Sebagai auditor keamanan, evaluasi penerapan cybersecurity best practices pada SatuSehat.

1. Analisis kelemahan dalam:
   1. access control
   2. encryption
   3. network security

   Jawaban:

   Analisis Kelemahan pada Tiga Elemen Utama Keamanan
   - Kontrol Akses: Masalah utama ada pada berbagai cara autentikasi yang digunakan di ribuan fasilitas kesehatan yang menjadi mitra. Kurangnya manajemen identitas terpusat (Identity and Access Management / IAM) yang konsisten menimbulkan risiko penggunaan kata sandi yang lemah di fasilitas kesehatan kecil. Selain itu, belum ada kewajiban

untuk menggunakan Multi-Factor Authentication (MFA) bagi semua operator, dan penerapan prinsip hak akses minimum (least privilege) dalam mengakses rekam medis pasien juga masih lemah.

- Enkripsi: Berbagai standar yang berbeda antar organisasi menambah risiko terjadinya eksploitasi data. Kelemahan yang mungkin ada termasuk penggunaan algoritma enkripsi yang sudah tua pada sistem lama rumah sakit saat mengirim data ke SatuSehat (data yang sedang dikirim), serta manajemen kunci enkripsi yang belum berjalan dengan baik untuk data medis yang disimpan di penyedia cloud pihak ketiga (data yang disimpan).

- Keamanan Jaringan: Menghubungkan ribuan organisasi dengan tingkat kematangan TI yang tidak sama menyebabkan adanya celah yang besar di perimeter jaringan. Kelemahan utama adalah belum adanya pemeriksaan yang mendalam terhadap lalu lintas API antar instansi, sehingga jalur integrasi ini menjadi rentan terhadap penyebaran malware secara lateral atau serangan ransomware dari fasilitas kesehatan mitra yang sudah terkena masalah.

2. Jelaskan bagaimana prinsip:
    1. Zero Trust
    2. Defense in Depth

dapat diterapkan dalam sistem ini.

Jawaban:

Penerapan Prinsip Zero Trust dan Defense in Depth

- Prinsip Zero Trust ("Never Trust, Always Verify"): Pendekatan ini wajib diterapkan dengan mengasumsikan bahwa ancaman bisa datang dari dalam maupun luar jaringan. Pada SatuSehat, Zero Trust diimplementasikan melalui autentikasi dan otorisasi berkelanjutan; setiap permintaan akses data dari faskes mana pun harus diverifikasi secara ketat berdasarkan konteks pengguna, perangkat, dan lokasi, bukan hanya karena mereka berada di dalam jaringan tepercaya. Selain itu, dilakukan mikro-segmentasi jaringan untuk mengisolasi klaster data sensitif agar jika satu faskes terserang, dampaknya tidak menyebar ke seluruh ekosistem.

- Prinsip Defense in Depth (Pertahanan Berlapis): Prinsip ini diterapkan dengan menyusun kombinasi kontrol organisasi, sumber daya manusia, fisik, dan teknologi secara bertingkat. Jika lapisan pertahanan terluar (seperti firewall jaringan) berhasil ditembus oleh peretas, data rekam medis SatuSehat tetap aman karena dilindungi oleh lapisan pertahanan berikutnya, seperti kontrol akses berbasis peran yang ketat, enkripsi data tingkat tinggi, dan pemantauan anomali harian secara otomatis.

1. Berikan rekomendasi teknis dan strategis untuk meningkatkan keamanan data.

Jawaban:

- Rekomendasi Teknis: Mewajibkan implementasi Multi-Factor Authentication (MFA) bagi seluruh tenaga medis yang mengakses platform, menerapkan enkripsi standar industri (AES-256 untuk data at rest dan TLS 1.3 untuk data in transit), serta memasang solusi Endpoint Detection and Response (EDR) di setiap titik integrasi faskes untuk mendeteksi aktivitas mencurigakan secara real-time.

- Rekomendasi Strategis: Menerbitkan regulasi standardisasi keamanan siber nasional yang mengikat dan wajib dipenuhi oleh seluruh faskes sebagai syarat interkoneksi SatuSehat (selaras dengan kontrol teknologi ISO 27001:2022). Selain itu, manajemen harus melakukan uji penetrasi (penetration testing) secara berkala serta membentuk Security Operations Center (SOC) terpusat untuk memantau ancaman siber nasional.

Referensi:

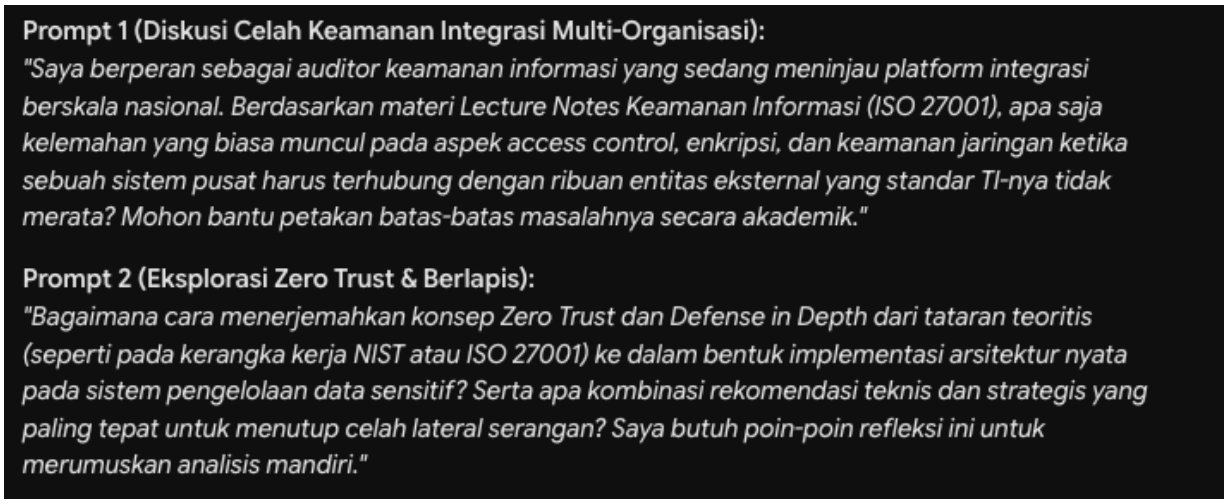
- Kenyon, B. (2024). ISO 27001 Controls: A Guide to Implementing and Auditing. IT Governance Publishing.

- National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0. U.S. Department of Commerce.

- Sarungu, C. M. (2025). Lecture Notes Week 8: Keamanan Informasi (ISO 27001:2022). BINUS University Online Learning.

- Sarungu, C. M. (2025). Lecture Notes Week 10: National Institute of Standards and Technology (NIST). BINUS University Online Learning.

Screen shoot Prompt:



5. LO 5: incident response plans to address security breaches and minimize disruption in information system operations. (30%)

PERTANYAAN 5:

SatuSehat menghadapi potensi serangan ransomware yang melumpuhkan sistem nasional.

1. Rancang incident response plan yang mencakup:
    1. detection
    2. containment
    3. eradication
    4. recovery

2. Jelaskan peran stakeholder dalam setiap tahap (IT, manajemen, regulator).

Jawaban: Berikut jawaban untuk nomer 1 dan 2

Manajemen insiden SatuSehat dirancang melalui empat tahapan terstruktur dengan pembagian peran pemangku kepentingan (stakeholder) sebagai berikut:

1. Tahap Detection (Deteksi)
    - Tindakan Teknis: Melakukan pemantauan dan analisis terhadap indikasi awal serangan, seperti lonjakan aktivitas enkripsi file yang tidak sah pada server data rekam medis atau peringatan anomali lalu lintas API dari sistem Endpoint Detection and Response (EDR).
    - Peran Stakeholder:
        - Tim IT & Keamanan: Melakukan penilaian teknis, mengonfirmasi jenis ransomware, dan menetapkan tingkat keparahan insiden.
        - Manajemen: Menerima laporan pertama yang lebih serius tentang keadaan teknis.
        - Regulator (BSSN/Kominfo): Menerima notifikasi awal mengenai adanya ancaman siber berskala nasional.

2. Tahap Containment (Isolasi)
    - Tindakan Teknis: Memutus koneksi jaringan internet pusat SatuSehat dan mengisolasi server yang terinfeksi secara cepat guna menghentikan penyebaran lateral (lateral movement) ransomware ke infrastruktur rumah sakit mitra.
    - Peran Stakeholder:
        - Tim IT & Keamanan: Mengeksekusi karantina jaringan dan menonaktifkan akun pengguna yang terkompromi.
        - Manajemen: Mengaktifkan Komite Manajemen Krisis dan menyusun strategi komunikasi publik untuk meredam kepanikan.
        - Regulator: Memantau jalannya isolasi agar dampak siber tidak merembes ke jaringan infrastruktur kritis negara lainnya.

3. Tahap Eradication (Eradikasi)
    - Tindakan Teknis: Mengidentifikasi titik masuk awal peretasan (patient zero), menghapus seluruh varian malware dari sistem, serta menambal celah kerentanan (vulnerability) yang dieksploitasi peretas.
    - Peran Stakeholder:
        - Tim IT & Keamanan: Membersihkan instalasi server dan membangun kembali sistem operasi menggunakan citra (image) yang aman.
        - Manajemen: Melakukan koordinasi dengan aparat penegak hukum untuk investigasi forensik kriminal siber.

- Regulator: Menyediakan bantuan tim ahli forensik siber negara dan memberikan panduan teknis pembersihan sistem.

4. Tahap Recovery (Pemulihan)
   - Tindakan Teknis: Memulihkan data rekam medis masyarakat dari sistem cadangan terisolasi yang dipastikan steril, menguji integritas data, serta mengaktifkan kembali koneksi interkoneksi faskes secara bertahap.
   - Peran Stakeholder:
     - Tim IT & Keamanan: Melakukan restore data, memantau stabilitas performa sistem pasca-pemulihan, dan melakukan peninjauan kembali (lessons learned).
     - Manajemen: Mengumumkan secara resmi pemulihan penuh layanan SatuSehat kepada publik dan media.
     - Regulator: Melakukan audit kepatuhan pasca-insiden untuk memastikan kelayakan platform sebelum diizinkan beroperasi normal kembali.

3. Jelaskan bagaimana memastikan business continuity dan minimal disruption pada layanan kesehatan.

Jawaban:

Untuk menjamin kelangsungan layanan kesehatan nasional agar tidak terjadi disrupsi fatal pada pelayanan pasien di rumah sakit saat SatuSehat lumpuh, strategi kontingensi berikut harus diterapkan:

- Mengaktifkan Mode Offline dan Prosedur Manual Lokal: Aplikasi SIMRS (Sistem Informasi Manajemen Rumah Sakit) di setiap fasilitas kesehatan harus dirancang dengan fitur penyimpanan sementara offline. Saat koneksi SatuSehat terputus, dokter masih bisa memasukkan rekam medis, melihat riwayat alergi, dan meresepkan obat secara lokal dengan menggunakan database internal rumah sakit, tanpa perlu bergantung pada jaringan pusat.
- Isolasi Arsitektur Cadangan (Cadangan Tak Berubah): Proses pengelolaan risiko mengharuskan SatuSehat memiliki sistem cadangan data yang memakai teknologi air-gapped atau cadangan tak berubah (data cadangan yang terkunci dan tidak bisa diubah atau dihapus oleh ransomware). Ini memastikan bahwa data penting negara bisa dipulihkan dengan cepat tanpa harus membayar tebusan kepada penyerang, sehingga layanan medis di negara bisa segera kembali berjalan normal.

Referensi:

- National Institute of Standards and Technology. (2024). NIST Cybersecurity Framework 2.0. U.S. Department of Commerce.
- Sarungu, C. M. (2025). Lecture Notes Week 7: Risk Management in EGIT (ISO 31000). BINUS University Online Learning.
- Sarungu, C. M. (2025). Lecture Notes Week 8: Keamanan Informasi (ISO 27001:2022). BINUS University Online Learning.
- Sarungu, C. M. (2025). Lecture Notes Week 10: National Institute of Standards and Technology (NIST). BINUS University Online Learning.

Screen shoot Prompt: