KEMANAN KOMPUTER

ANALISIS DAN IMPLEMENTASI SISTEM MANAJEMEN INFORMASI (SMKI) BERDASARKAN ISO/IEC 27001 PADA DIVISI IT DI RUMAH SAKIT SEHAT

Disusun Oleh

DONI IRAWAN	221011402176
MUTIA SEPTIFIANI	221011402159

UNIVERSITAS PAMULANG PRODI

TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

2025

DAFTAR ISI

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi yang pesat telah membawa dampak besar terhadap dunia kesehatan, terutama dalam pengelolaan data pasien dan sistem layanan medis digital. Rumah sakit sebagai institusi pelayanan publik yang mengelola informasi sensitif dituntut untuk menjaga kerahasiaan, integritas, dan ketersediaan data secara optimal.
Salah satu standar internasional yang diakui untuk menjamin keamanan informasi adalah ISO/IEC 27001:2022, yang menetapkan kerangka kerja bagi organisasi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI) secara sistematis dan terukur.

Rumah Sakit Sehat (RS Sehat), melalui Divisi Teknologi Informasi (IT), memiliki tanggung jawab besar dalam mengelola berbagai sistem penting seperti rekam medis elektronik (Electronic Health Record), database pasien, dan jaringan rumah sakit. Seiring meningkatnya ancaman keamanan siber seperti ransomware, kebocoran data, dan serangan phishing, RS Sehat memerlukan pendekatan yang terstandar dan komprehensif untuk memastikan keamanan informasi yang dikelola.
Penerapan SMKI berbasis ISO 27001 diharapkan dapat menjadi solusi strategis dalam menjaga kepercayaan pasien, meningkatkan efisiensi sistem IT, serta memastikan kepatuhan terhadap regulasi pemerintah seperti Permenkes No. 24 Tahun 2022 tentang Rekam Medis.

1.2 Rumusan Masalah

1. Bagaimana menganalisis konteks organisasi dan risiko keamanan informasi di Divisi IT RS Sehat?
2. Kontrol keamanan apa yang relevan untuk diterapkan berdasarkan Annex A ISO/IEC 27001:2022?
3. Bagaimana rancangan dokumen utama SMKI yang dapat digunakan sebagai dasar implementasi di RS Sehat?

1.3 Tujuan

1. Menganalisis kondisi dan kebutuhan keamanan informasi di lingkungan Divisi IT RS Sehat.
2. Mengidentifikasi aset, risiko, dan kontrol keamanan yang sesuai dengan standar ISO/IEC 27001:2022.
3. Menyusun rancangan awal dokumen SMKI yang terdiri dari kebijakan, tujuan, dan rencana implementasi keamanan informasi.

1.4 Manfaat

1. Bagi Rumah Sakit Sehat: Memberikan panduan implementasi sistem keamanan informasi yang sistematis dan terukur.
2. Bagi Staf IT dan Manajemen: Meningkatkan kesadaran terhadap pentingnya perlindungan data pasien dan keamanan sistem.
3. Bagi Dunia Akademik: Menjadi referensi studi penerapan ISO/IEC 27001 di sektor kesehatan di Indonesia.

Tahap 1

Pemilihan Organisasi: Rumah Sakit Sehat (Divisi IT)

1. Profil Organisasi

Nama: Rumah Sakit Sehat (RS Sehat)
Jenis Bisnis: Layanan kesehatan umum dan spesialis

Lokasi: Jakarta Selatan, Indonesia

Ruang Lingkup SMKI: Divisi Teknologi Informasi (IT)

Tujuan SMKI: Melindungi kerahasiaan, integritas, dan ketersediaan data pasien, sistem rekam medis elektronik (EHR), dan infrastruktur IT rumah sakit.

2. Struktur Organisasi (Singkat)

Direktur Utama
|
├ Wakil Direktur Pelayanan Medis
|
├ Wakil Direktur Administrasi & Keuangan
|
└─ Kepala Divisi IT
  ├ Tim Infrastruktur Jaringan
  ├ Tim Keamanan Informasi
  ├ Tim Pengembangan Sistem
  └─ Tim Dukungan Teknis

3. Layanan Utama Divisi IT

- Pemeliharaan server rekam medis elektronik (EHR System)
- Pengelolaan database pasien dan sistem keuangan rumah sakit
- Manajemen akses pengguna (dokter, perawat, staf administrasi)
- Pengelolaan keamanan jaringan dan backup data
- Dukungan teknis untuk seluruh unit rumah sakit

4. Aset Informasi Penting

No	Aset Informasi	Deskripsi	Nilai Kepentingan
1	**Database Pasien**	Berisi data pribadi dan rekam medis pasien	Sangat tinggi
2	**Server EHR (Electronic Health Record)**	Sistem aplikasi rekam medis utama	Sangat tinggi
3	**Sistem Keuangan Rumah Sakit**	Menyimpan data transaksi, tagihan, dan pembayaran	Tinggi
4	**Jaringan Internal Rumah Sakit**	Menghubungkan sistem antar divisi	Tinggi
5	**Akun Akses Pegawai IT**	Digunakan untuk administrasi dan konfigurasi sistem	Tinggi
6	**Backup Data Pasien**	Salinan data kritis untuk pemulihan bencana	Sangat tinggi

Tahap 2

Analisis Konteks Organisasi (RS Sehat – Divisi IT)

1. Analisis Isu Internal dan Eksternal

Jenis Isu	**Deskripsi**	**Dampak terhadap Keamanan Informasi**
Internal – Infrastruktur TI	Server dan jaringan masih bergantung pada sistem lokal tanpa cloud backup otomatis.	Risiko kehilangan data jika terjadi kerusakan hardware atau bencana.
Internal – SDM IT	Kurangnya pelatihan keamanan siber bagi staf IT dan pengguna umum.	Potensi human error dan serangan phishing meningkat.
Internal – Kebijakan	Belum ada kebijakan keamanan informasi formal berbasis ISO 27001.	Tidak ada pedoman resmi dalam pengelolaan aset informasi.
Eksternal – Regulasi	Peraturan Kementerian Kesehatan terkait perlindungan data pasien (Permenkes No. 24/2022).	Harus ada kepatuhan terhadap aturan perlindungan data pribadi.
Eksternal – Ancaman Siber	Meningkatnya kasus ransomware pada sektor kesehatan.	Ancaman terhadap ketersediaan dan kerahasiaan data pasien.
Eksternal – Teknologi Cloud	Migrasi sebagian sistem ke cloud publik (mis. AWS, GCP).	Membutuhkan kontrol tambahan untuk keamanan akses dan enkripsi data.

2. Pihak Berkepentingan (Stakeholders) dan Kebutuhan Mereka

Stakeholder	Kepentingan / Kebutuhan	Relevansi terhadap Keamanan Informasi
Direktur Rumah Sakit	Kepastian operasional rumah sakit berjalan lancar dan data pasien aman.	Menuntut sistem keamanan yang andal dan audit berkala.
Kepala Divisi IT	Implementasi sistem keamanan informasi yang sesuai standar ISO 27001.	Butuh kebijakan, SOP, dan kontrol keamanan yang jelas.
Tim IT & Network Administrator	Perlindungan terhadap server, jaringan, dan akses pengguna.	Perlu kontrol teknis seperti firewall, IDS, enkripsi, dan backup rutin.
Tenaga Medis (Dokter/Perawat)	Akses cepat dan aman ke data pasien.	Diperlukan sistem autentikasi dan otorisasi yang efisien.
Pasien	Privasi dan keamanan data pribadi serta rekam medis.	Butuh jaminan data tidak bocor atau disalahgunakan.
Pemerintah (Kemenkes)	Kepatuhan terhadap peraturan dan standar nasional.	Harus ada pelaporan dan kepatuhan terhadap kebijakan data pasien.
Vendor IT / Penyedia Cloud	Pengelolaan server dan sistem pihak ketiga.	Diperlukan perjanjian keamanan data (Data Processing Agreement).

3. Ringkasan Konteks

Divisi IT Rumah Sakit Sehat beroperasi dalam lingkungan dengan risiko tinggi terkait data sensitif pasien dan ancaman siber. Oleh karena itu, penerapan **Sistem Manajemen Keamanan Informasi (SMKI)** berbasis **ISO/IEC 27001:2022** menjadi prioritas utama untuk menjamin perlindungan data, kepatuhan regulasi, serta keberlanjutan layanan TI.

Tahap 3

Penilaian Risiko Keamanan Informasi (RS Sehat – Divisi IT)

1. Identifikasi Aset, Ancaman, dan Kerentanan

No	Aset Informasi	Ancaman	Kerentanan	Dampak	Kemungkinan	Level Risiko	Tindakan Mitigasi
1	Database Pasien	Serangan ransomware / kebocoran data	Tidak ada enkripsi dan backup harian	Sangat tinggi	Tinggi	Ekstrem	Terapkan enkripsi database, backup harian terenkripsi, dan segmentasi jaringan.
2	Server Rekam Medis (EHR)	Akses tidak sah oleh staf internal	Pengendalian akses lemah, tidak ada log audit	Tinggi	Sedang	Tinggi	Implementasi autentikasi multi-faktor dan audit log sistem.
3	Jaringan Internal Rumah Sakit	Serangan dari luar (malware, DDoS)	Firewall belum optimal, update tidak rutin	Tinggi	Tinggi	Ekstrem	Pasang firewall berlapis, IDS/IPS, dan patch keamanan berkala.
4	Sistem Keuangan Rumah Sakit	Phishing dan credential theft	Kurang edukasi keamanan pengguna	Tinggi	Sedang	Tinggi	Pelatihan keamanan siber dan kebijakan password kuat.
5	Akun Administrator IT	Penyalahgunaan hak akses	Tidak ada prinsip least privilege	Sangat tinggi	Rendah	Sedang	Terapkan kontrol akses berbasis peran (RBAC) dan review berkala akun.

6	Backup Data Pasien	Kehilangan media backup / pencurian	Backup disimpan di lokasi yang sama	Sangat tinggi	Sedang	Tinggi	Simpan backup terenkripsi di lokasi berbeda (off-site/cloud).

No	**Aset Informasi**	**Ancaman**	**Kerentanan**	**Dampak**	**Kemungkinan**	**Level Risiko**	**Tindakan Mitigasi**
7	Email Rumah Sakit	Phishing, malware attachment	Filter email belum memadai	Sedang	Tinggi	Tinggi	Implementasikan email security gateway dan awareness training.
8	Sistem Cloud (AWS/GCP)	Misconfiguration, kebocoran API key	Pengaturan akses cloud belum standar	Tinggi	Sedang	Tinggi	Gunakan IAM policy ketat dan audit konfigurasi cloud rutin.
9	Website RS Sehat	SQL Injection, defacement	Kode aplikasi tidak diuji keamanan	Sedang	Sedang	Sedang	Lakukan vulnerability assessment dan pengetesan keamanan aplikasi.
10	Perangkat Komputer Staff	Malware, USB tidak aman	Tidak ada endpoint protection	Sedang	Tinggi	Tinggi	Pasang antivirus terpusat dan batasi penggunaan USB.

2. Metode Analisis Risiko

Pendekatan yang digunakan adalah **analisis risiko kualitatif**, dengan skala sederhana:

Nilai	Dampak	Kemungkinan
Rendah (1)	Gangguan kecil, tidak mempengaruhi layanan utama	Jarang terjadi
Sedang (2)	Mengganggu sebagian sistem, dapat pulih cepat	Kadang terjadi
Tinggi (3)	Mengganggu layanan utama, menimbulkan kerugian signifikan	Sering terjadi
Sangat Tinggi (4)	Menyebabkan gangguan besar, kehilangan data kritis	Sangat sering terjadi

Nilai risiko diperoleh dari:
Level Risiko = Dampak × Kemungkinan
Kemudian dikategorikan sebagai berikut:

- **1–3** → Rendah
- **4–6** → Sedang
- **7–9** → Tinggi
- **>9** → Ekstrem

3. Ringkasan Hasil Analisis

Dari hasil penilaian risiko, aset dengan prioritas mitigasi tertinggi adalah:

1. Database pasien
2. Server EHR
3. Jaringan internal dan backup data

Fokus utama kontrol keamanan diarahkan pada **perlindungan data pasien, pencegahan akses tidak sah, dan kesiapan pemulihan data**.

Tahap 4
Pemilihan dan Rancangan Kontrol Keamanan Informasi

4.1 Dasar Pemilihan Kontrol

Pemilihan kontrol keamanan informasi dilakukan berdasarkan hasil penilaian risiko pada Tahap 3, dengan fokus utama pada:

- Perlindungan data pasien dan rekam medis elektronik (EHR)
- Pencegahan akses tidak sah
- Ketersediaan sistem layanan rumah sakit
- Kepatuhan terhadap regulasi kesehatan dan perlindungan data

Kontrol diambil dari Annex A ISO/IEC 27001:2022 yang dikelompokkan ke dalam kontrol organisasi, manusia, fisik, dan teknologi.

4.2 Daftar Kontrol Keamanan yang Dipilih dan Rancangannya

Berikut minimal 10 kontrol keamanan yang relevan untuk Divisi IT RS Sehat:

No	Kontrol Annex A ISO 27001:2022	Deskripsi Kontrol	Alasan Pemilihan	Rancangan Penerapan di RS Sehat
1	**A.5.1 – Kebijakan Keamanan Informasi**	Menetapkan kebijakan formal keamanan informasi	RS belum memiliki kebijakan tertulis	Menyusun dan mengesahkan kebijakan keamanan informasi oleh Direktur RS
2	**A.5.15 – Kontrol Akses**	Mengatur hak akses pengguna	Risiko akses tidak sah ke EHR	Penerapan role-based access control (RBAC)
3	**A.5.17 – Informasi Autentikasi**	Pengelolaan password dan autentikasi	Banyak akun sensitif IT	Password kuat dan multi-factor authentication (MFA)
4	**A.5.23 – Keamanan Informasi pada Penggunaan Cloud**	Perlindungan data di lingkungan cloud	Migrasi sistem ke AWS/GCP	IAM policy ketat dan enkripsi data cloud
5	**A.6.3 – Kesadaran dan Pelatihan Keamanan Informasi**	Pelatihan SDM	Human error & phishing	Pelatihan keamanan siber tahunan
6	**A.7.4 – Pemantauan Keamanan Fisik**	Perlindungan server fisik	Risiko akses fisik tidak sah	CCTV dan akses kartu di ruang server

No	Kontrol Annex A ISO 27001:2022	Deskripsi Kontrol	Alasan Pemilihan	Rancangan Penerapan di RS Sehat
7	**A.8.2 – Hak Akses Istimewa**	Pengelolaan akun administrator	Risiko penyalahgunaan hak akses	Review akun admin setiap 6 bulan
8	**A.8.7 – Perlindungan terhadap Malware**	Pencegahan malware	Risiko ransomware	Antivirus terpusat & email filtering
9	**A.8.9 – Manajemen Konfigurasi**	Keamanan konfigurasi sistem	Risiko salah konfigurasi	Standar konfigurasi dan audit rutin
10	**A.8.13 – Backup Informasi**	Menjamin ketersediaan data	Risiko kehilangan data	Backup harian terenkripsi dan off-site

4.3 Ringkasan Tahap 4

Kontrol yang dipilih telah disesuaikan dengan risiko prioritas tinggi pada RS Sehat, terutama yang berkaitan dengan **database pasien, server EHR, jaringan, dan sistem cloud**. Implementasi kontrol ini menjadi fondasi utama dalam penerapan SMKI secara efektif.

Tahap 5
Rancangan Dokumen Utama Sistem Manajemen Keamanan Informasi (SMKI)

5.1 Kebijakan Keamanan Informasi (Information Security Policy)

Tujuan Kebijakan
Menetapkan komitmen Rumah Sakit Sehat dalam melindungi keamanan informasi sesuai ISO/IEC 27001:2022.

Ruang Lingkup
Kebijakan ini berlaku untuk seluruh sistem informasi, data, pegawai, dan pihak ketiga yang terlibat dalam pengelolaan informasi RS Sehat.

Prinsip Keamanan Informasi

1. Kerahasiaan (Confidentiality)
2. Integritas (Integrity)
3. Ketersediaan (Availability)

Kebijakan Utama

- Data pasien wajib dilindungi dari akses tidak sah
- Setiap pengguna memiliki hak akses sesuai perannya
- Semua insiden keamanan wajib dilaporkan
- Backup data dilakukan secara rutin dan aman
- Kepatuhan terhadap regulasi kesehatan dan perlindungan data

5.2 Tujuan Keamanan Informasi (Information Security Objectives)

No	Tujuan Keamanan Informasi	Indikator Keberhasilan
1	Menjamin keamanan data pasien	Tidak ada kebocoran data
2	Mencegah akses tidak sah ke EHR	Implementasi MFA & RBAC
3	Menjaga ketersediaan sistem IT	Downtime < 1% per tahun
4	Meningkatkan kesadaran keamanan	Pelatihan minimal 1x/tahun
5	Memastikan backup dan recovery	Uji restore berhasil 100%

5.3 Rencana Implementasi SMKI (Implementation Plan)

Tahap	Aktivitas	Penanggung Jawab	Waktu
1	Pembentukan tim SMKI	Direktur & Kepala IT	Bulan 1
2	Penyusunan kebijakan & SOP	Tim Keamanan Informasi	Bulan 1–2
3	Implementasi kontrol teknis	Tim Infrastruktur & Security	Bulan 2–4
4	Pelatihan keamanan informasi	HR & IT	Bulan 3
5	Audit internal SMKI	Auditor Internal	Bulan 5
6	Tinjauan manajemen	Manajemen RS	Bulan 6

Tahap 6
Kesimpulan

6.1 Kesimpulan

Berdasarkan hasil analisis dan perancangan SMKI di Divisi IT Rumah Sakit Sehat, dapat disimpulkan bahwa:

1. RS Sehat memiliki aset informasi kritis dengan tingkat risiko tinggi, khususnya data pasien dan sistem EHR.
2. Penerapan SMKI berbasis ISO/IEC 27001:2022 sangat diperlukan untuk mengelola risiko keamanan informasi secara sistematis.
3. Kontrol keamanan dari Annex A yang dipilih mampu mengurangi risiko utama yang teridentifikasi.
4. Rancangan dokumen SMKI menjadi dasar implementasi keamanan informasi yang berkelanjutan.

6.2 Rekomendasi

Agar RS Sehat dapat menuju **sertifikasi ISO/IEC 27001**, disarankan:

1. Melanjutkan implementasi SMKI secara bertahap dan konsisten
2. Melakukan audit internal dan perbaikan berkelanjutan
3. Meningkatkan anggaran keamanan informasi
4. Melibatkan seluruh pegawai dalam program kesadaran keamanan
5. Menggunakan tools pendukung SMKI seperti template risk assessment atau software ISMS

DAFTAR PUSTAKA

International Organization for Standardization. (2022).
ISO/IEC 27001:2022 ***Information Security, Cybersecurity and Privacy Protection — Information Security Management Systems — Requirements***. Geneva: ISO.

International Organization for Standardization. (2022).
ISO/IEC 27002:2022 ***Information Security, Cybersecurity and Privacy Protection — Information Security Controls***. Geneva: ISO.

Kementerian Kesehatan Republik Indonesia. (2022).
Peraturan Menteri Kesehatan Republik Indonesia Nomor 24 Tahun 2022 tentang Rekam Medis. Jakarta: Kemenkes RI.

Whitman, M. E., & Mattord, H. J. (2021).
Principles of Information Security (7th ed.). Boston: Cengage Learning.

Peltier, T. R. (2016).
Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Boca Raton: CRC Press.

Calder, A., & Watkins, S. (2018).
IT Governance: An International Guide to Data Security **and ISO/IEC 27001/27002**. London: Kogan Page.

Behl, A., & Behl, K. (2017).
Cyberwar: The Next Threat to National Security and What to Do About It. New York: Oxford University Press.

Farizi, H. A., Saputra, H. K., Hendriyani, Y., & Budayawan, K. (2025).
Implementasi sistem manajemen keamanan informasi berbasis ISO/IEC 27001 pada organisasi layanan publik.
Jurnal Pendidikan Tambusai, 9(2), 27627–27636.
https://doi.org/10.31004/jptam.v9i2.31314

Stallings, W. (2020).
Effective Cybersecurity: A Guide to Using Best Practices and Standards. Boston: Addison-Wesley.

NIST. (2018).
Framework for Improving Critical Infrastructure Cybersecurity (Version **1.1)**. National Institute of Standards and Technology.