Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari

OPEN ACCESS

https://doi.org/10.35870/jimik.v6i1.1172

Evaluasi Keamanan Sistem Informasi Rumah Sakit: Metode Pengujian ISO 27001 di RS Khusus Mata Purwokerto

Rafii Nur Akmal [1*], Tarwoto [2], Deni Dwi Susilo [3], Erik Halma Rouf [4], Kodir [5]

[1*,2,3,4,5] Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Amikom Purwokerto, Kabupaten Banyumas, Provinsi Jawa Tengah, Indonesia.

Email: 21sa2139@mhs.amikompurwokerto.ac.id [1*], tarwoto@amikompurwokerto.ac.id [2], 21sa2026@mhs.amikompurwokerto.ac.id [3], 21sa2161@mhs.amikompurwokerto.ac.id [4], 21sa2059@mhs.amikompurwokerto.ac.id [5]

Histori Artikel:
Dikirim 7 Desember 2024; *Diterima dalam bentuk revisi* 20 Desember 2024; *Diterima* 1 Januari 2025; *Diterbitkan* 10 Januari 2025.

Abstrak

Sudah menjadi kebutuhan saat ini di setiap perusahan mengenai penerapan tata kelola di bidang TIK dalam upaya peningkatan kualitas layanan.Untuk itu maka perlu dilakukan penerapan dan sekaligus melakukan proses audit berkala pada SIMRS di rumah sakit memakai standard ISO 27001. Sesuai dengan hasilaudit serta penelitian ini untuk mengevaluasi keamanan informasi di Rumah Sakit Khusus Mata Purwokerto melalui pendekatan audit berbasis standar ISO/IEC 27001. Sistem Informasi Manajemen Rumah Sakit (SIMRS) yang diterapkan bertujuan untuk mendukung integrasi layanan dan proses administrasi, namun menghadapi berbagai tantangan keamanan seperti kehilangan data dan potensi manipulasi. Audit ini dilakukan melalui observasi, wawancara, dan analisis kebijakan keamanan yang ada. Hasil audit menunjukkan bahwa manajemen insiden keamanan informasi telah sesuai prosedur, meliputi penanganan, pelaporan, dan tindakan korektif, dengan tingkat kematangan keamanan yang cukup tinggi. Studi ini merekomendasikan evaluasi berkala dan peningkatan keamanan untuk memastikan ketangguhan sistem terhadap ancaman di masa depan.

Kata Kunci: Keamanan Informasi; Sistem Informasi; ISO/IEC 27001; Kehilangan Data; Rumah Sakit.

Abstract

As service quality becomes paramount, ICT governance is increasingly important for organizations. This study will audit Purwokerto Eye Specialty Hospital's SIMRS against ISO/IEC 27001 standards to evaluate its information security posture. The implemented Hospital Management Information System (SIMRS) aims to support the integration of services and administrative processes, but faces various security challenges such as data loss and potential manipulation. The audit was conducted through observation, interviews, and analysis of existing security policies. The audit results show that information security incident management is in accordance with procedures, including handling, reporting, and corrective actions, with a fairly high level of security maturity. The study recommends periodic evaluation and security enhancements to ensure system resilience against future threats.

Keyword: Information Security; Information System; ISO/IEC 27001; Data Loss; Hospital.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1172

1. Pendahuluan

Teknologi dan sistem informasi saat ini mengalami perkembangan yang sangat pesat dan telah merambah berbagai aspek kehidupan manusia (Simatupang, J., & Sianturi, S., 2019; Pangestuti *et al.*, 2024; Fauzi *et al.*, 2023). Sektor-sektor seperti perdagangan, kesehatan, pendidikan, sampai pemerintahan kini memanfaatkan sebuah *teknologi* yang mendukung tahap bisnis mereka (Premana *et al.*, 2020). Sebaliknya, perkembangan cepat ini juga menimbulkan kerentanan terhadap berbagai ancaman keamanan dalam teknologi dan sistem informasi (Lubis & Nasution, 2023). Salah satu bidang yang perlu mendapat perlindungan dari risiko tersebut adalah sektor kesehatan (Ikhwan, 2022). Pelayanan kesehatan masyarakat, terutama di rumah sakit, menjadi tanggung jawab utama institusi terkait (Komalawati & Triswandi, 2022). Kegagalan dalam menjaga aset institusi kesehatan dapat memungkinkan orang yang tidak bertanggung jawab untuk mencuri atau mengganggu tindakan yang terkait dengan data kesehatan pasien. Aset kesehatan adalah bagian penting dari kelancaran operasional rumah sakit, jadi perlu ada perhatian yang lebih besar pada hal ini. Upaya yang serius dan berkelanjutan untuk melindungi aset kesehatan dapat meningkatkan keamanan, melindungi hak pasien, dan menjaga integritas rumah sakit. RS Khusus Mata Purwokerto, sebuah rumah sakit umum tipe C yang berlokasi di Jl. Beringin Raya No.120-116, Bojong, Tanjung, Kecamatan Purwokerto Selatan, Kabupaten Banyumas, Jawa Tengah, sesuai dengan Peraturan Menteri Kesehatan Nomor 82 Tahun 2013, telah menerapkan Sistem Informasi Manajemen Rumah Sakit (SIMRS) dalam berbagai operasi bisnis. Tujuan dari penerapan *SIMRS* di fasilitas kesehatan yang dibahas di sini adalah untuk mengubah dan mengintegrasikan seluruh tahapan pelayanan rumah sakit ke dalam jaringan yang terstruktur dengan baik. Sehingga informasi dapat diperoleh secara akurat dan tepat waktu, sistem ini mencakup pelaporan dan prosedur administrasi. Sistem Informasi Kesehatan secara keseluruhan terdiri dari *SIMRS*.

RS Khusus Mata menjalankan operasinya secara dinamis sesuai dengan peraturan pemerintah daerah dan pusat. Selain itu, jalur proses bisnis yang dapat disesuaikan ini sejalan dengan tujuan utama RS Khusus Mata. Diharapkan *Sistem Informasi Manajemen Rumah Sakit* (*SIMRS*) dapat menyesuaikan diri dengan kebutuhan saat ini dan memengaruhi berbagai aspek proses bisnis. Sektor *IT* rumah sakit bertanggung jawab sepenuhnya atas Sistem Informasi Manajemen Rumah Sakit (SIMRS) di RS Khusus Mata. Sesuai dengan prosedur operasional standar (*SOP*), *SIMRS* disimpan di ruang *server* yang memiliki akses yang sangat terbatas. Meskipun ruang *server* terbatas, masih ada kasus kehilangan data yang cukup sering. Pengguna lokal memiliki otorisasi untuk membuat, membaca, mengubah, dan menghapus data di NAS (*Network Attach Storage*). Namun, data hilang karena otoritas pengguna yang kurang bertanggung jawab. Sejauh ini, RS Khusus Mata belum pernah mengalami kasus pencurian data; namun, laporan hasil rumah sakit yang diubah oleh pihak luar yang menamakan dirinya RS Khusus Mata menunjukkan kasus pencurian data. Karena lalu lintas pertukaran data melalui internet menjadi akses utama dalam proses pelayanan dan administrasi, kasus serangan *virus komputer* cukup sering terjadi. Sistem Informasi Manajemen Rumah Sakit (SIMRS) di rumah sakit yang berfokus pada mata harus diaudit. Melakukan audit sistem informasi menggunakan *framework* ISO/IEC 27001 adalah solusi untuk masalah ini. Tujuan ISO/IEC 27001 adalah untuk melindungi semua aspek keamanan informasi, termasuk kerahasiaan, integritas, dan ketersediaan. ISO/IEC 27001 mencakup 133 kontrol keamanan informasi, dan perusahaan dapat memilih yang paling sesuai dengan keadaan industri mereka saat ini. Tabel di bawah ini akan menjelaskan berbagai penelitian terdahulu yang terkait dengan evaluasi keamanan informasi menggunakan ISO/IEC 27001. Penelitian terkait evaluasi keamanan informasi telah dilakukan oleh berbagai peneliti dengan pendekatan yang berbeda-beda. Silvia Paramita dkk. (2022) melakukan analisis keamanan informasi dengan menggunakan indeks *KAMI* untuk mengukur tingkat kelengkapan dan kematangan sistem. Hasil penelitian menunjukkan bahwa tingkat kelengkapan mencapai nilai 340, dengan tingkat kematangan berada pada level II+. Sementara itu, Mohammad Chevalier Daniswara dkk. (2023) melakukan evaluasi keamanan informasi berdasarkan indeks *maturity*. Penelitian ini memperoleh skor 2,54, yang mengindikasikan bahwa sistem telah menerapkan manajemen keamanan informasi dengan baik.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1172

Eri Riana dkk. (2023) menganalisis tingkat keamanan informasi dengan pendekatan indeks *maturity* yang didasarkan pada standar ISO 27001:2013. Hasil audit menunjukkan bahwa PT Indonesia Game telah menerapkan manajemen keamanan informasi dengan sangat baik, dengan nilai rata-rata 97,45% pada level 5 (*Optimized*). Wenceslaus Candraditya P. dan Fahmy Trimuti S. (2020) juga melakukan evaluasi keamanan informasi dengan menggunakan indeks *KAMI*. Penelitian mereka menunjukkan tingkat kelengkapan sebesar 520 dan tingkat kematangan pada level III. Terakhir, Piski Sundari dan Wella (2020) memfokuskan penelitiannya pada manajemen risiko *PUSDATIN* dengan menggunakan indeks *KAMI*. Penelitian ini menunjukkan tingkat kelengkapan sebesar 300, dengan tingkat kematangan berada pada level I+. ISO 27001 adalah serangkaian pedoman yang menetapkan persyaratan untuk mengembangkan, menerapkan, memantau, dan secara berkala meningkatkan kontrol terkait sumber daya manusia, proses, dan teknologi informasi di sebuah perusahaan. Dengan manajemen risiko sebagai elemen utama, Standar ini dibuat untuk memastikan bahwa prosedur keamanan yang diterapkan dapat melindungi aset informasi dari berbagai ancaman dan memberikan para pemangku kepentingan jaminan keamanan. (Riana, E., *et al.*, 2023). Perbedaan antara penelitian ini dan penelitian sebelumnya terletak pada fokusnya yang menekankan audit manajemen keamanan informasi di RS Khusus Mata Purwokerto dengan mengacu pada standar ISO 27001. Melalui penelitian ini, akan diungkapkan apakah penerapan Framework ISO 27001 telah dilakukan secara efektif atau belum.

2. Metode Penelitian

Audit Manajemen Keamanan Informasi harus dilakukan melalui berbagai tahapan dari awal penelitian hingga akhir penelitian untuk menghasilkan hasil audit yang tepat sasaran.

1) Observasi dan Wawancara
   Dalam audit keamanan IT rumah sakit, tahap observasi melibatkan pengamatan langsung terhadap infrastruktur teknologi yang digunakan, seperti perlengkapan keamanan fisik, jaringan, dan sistem komputer. Penilaian ini juga mencakup penilaian pelaksanaan kebijakan keamanan, tata kelola akses, dan pengawasan aktivitas pengguna. Selain itu, wawancara langsung dilakukan dengan karyawan penting di rumah sakit, seperti petugas keamanan IT dan administrator sistem yang menggunakan teknologi tersebut. Tujuan wawancara ini adalah untuk mendapatkan pemahaman tentang praktik keamanan yang digunakan dan kesadaran akan keamanan informasi, serta untuk mendapatkan pemahaman langsung tentang masalah keamanan yang mungkin dihadapi rumah sakit saat menggunakan teknologi informasi.
2) Pengumpulan Informasi
   Proses pengumpulan berbagai sumber daya dan referensi, seperti literatur, artikel jurnal ilmiah, dan sumber lainnya, digunakan dalam tahap pengumpulan informasi. Dalam audit keamanan sistem informasi rumah sakit, langkah ini mencakup pengumpulan referensi terkait peraturan keamanan informasi serta literatur tentang teknik audit keamanan IT. Mendapatkan pemahaman yang mendalam tentang literatur ini akan membantu membangun fondasi teoritis dan membangun pendekatan audit yang berhasil untuk menilai keamanan sistem informasi rumah sakit.
3) Perumusan Masalah
   Tujuan utama dari perumusan masalah adalah untuk menentukan secara jelas apa yang ingin kita teliti dan menetapkan batasan-batasan penelitian agar kita dapat menemukan solusi yang efektif.
4) Penentuan Kontrol Objektif
   Pada tahap ini, kita akan merancang penelitian dengan cermat. Kita akan memilih metode penelitian yang paling tepat dan menentukan bagian mana dari standar ISO 27002:2013 yang akan kita jadikan fokus utama. Tujuannya adalah untuk memastikan bahwa penelitian kita relevan dan memberikan hasil yang berharga.

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1172

5) Penyusunan Pertanyaan
Tujuan dari tahap ini adalah untuk menciptakan pertanyaan audit yang spesifik dan terukur yang akan membantu kita mengevaluasi sejauh mana organisasi telah menerapkan persyaratan ISO 27001 terkait manajemen insiden keamanan informasi.

6) Penulisan Pertanyaan
Pada tahap ini, kami mendefinisikan secara spesifik setiap tujuan kontrol yang terkait dengan Manajemen Insiden Keamanan Informasi (MIKI) sesuai dengan standar ISO 27001:2013. Definisi yang jelas ini akan menjadi dasar untuk menyusun pertanyaan audit yang relevan. Proses ini memastikan bahwa pernyataan kontrol yang dihasilkan sepenuhnya selaras dengan persyaratan ISO 27001:2013. Hal ini memungkinkan kita untuk melakukan audit keamanan IT secara komprehensif dan sesuai dengan standar internasional. Setelah menganalisis data, kami menilai sejauh mana sistem telah menerapkan praktik keamanan terbaik dengan menggunakan skala penilaian dari 0 hingga 5.

7) *Maturity* Level
Penilaian keamanan informasi melibatkan tiga aspek utama: model kematangan (Tabel 1), kontrol objektif (Tabel 2), dan pertanyaan penilaian (Tabel 3). Kombinasi ketiga aspek ini memberikan gambaran yang komprehensif mengenai tingkat kematangan keamanan informasi organisasi (Nurhadi, D. 2024) (Nayang, C., *et al.*, 2024).

Tabel 1. Skala *Indeks Maturity*

Skala	Index	Deskripsi
0.00-0.50	*Not Performed*	Proses tidak lengkap; tidak dilaksanakan atau tidak menghasilkan hasil yang diinginkan.
0.51-1.50	*Performed Informally*	Proses telah selesai dan tujuan telah dicapai.
1.51-2.50	*Planned and Tracked*	Prosesnya telah dilakukan dengan lebih teratur, dan hasilnya telah ditetapkan, diawasi, dan dipelihara dengan baik.
2.51-3.50	*Well Defined*	Proses telah dilakukan sesuai dengan aturan dan prosedur yang ditetapkan dan menghasilkan hasil yang diharapkan.
3.51-4.50	*Quantitatively Controlled*	Untuk mencapai hasil yang diharapkan, prosedur telah dilakukan sesuai dengan aturan yang telah ditetapkan.
4.51-5.00	*Continuously Improving*	Untuk mencapai tujuan yang diharapkan saat ini dan di masa mendatang, proses yang ada secara berkala dan berkesinambungan dioptimalkan.

Tabel 2. Kontrol Objektif

A.16.1 Manajemen Peristiwa dan Peningkatan Keamanan Informasi
16.1.1 Prosedur dan Tanggung Jawab
16.1.2 Laporkan Kejadian Kemanan Informasi
16.1.3 Laporkan kekurangan Keamanan Informasi
16.1.4 Penilaian dan Keputusan tentang Peristiwa Keamanan Informasi
16.1.5 Menimpali kejadian Keamanan Informasi
16.1.6 Pembelajaran dari kejadian Keamanan Informasi

Tabel 3. Susunan Pertanyaan

No.	A.16.1 Manajemen Insiden Keamanan Sistem Informasi
1	Apa jabatan atau fungsi dan tugas Anda di divisi yang diberikan?
2	Di bagian ini apa yang Anda lakukan?
3	Prosedur bisnis apa saja yang diawasi di divisi ini?
4	Apakah ada hambatan yang timbul selama proses menerapkan sistem informasi tersebut?
5	Apakah ada penilaian yang dilakukan secara berkala?
6	Apakah data dan aset perusahaan telah dilindungi?

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1172

3. Hasil dan Pembahasan

3.1 Hasil

Bagian ini menyajikan hasil audit yang telah dilakukan terkait manajemen insiden dan peningkatan keamanan sistem informasi berdasarkan standar ISO/IEC 27001. Hasil evaluasi diuraikan secara rinci dalam tabel-tabel yang mencakup berbagai aspek pengelolaan keamanan informasi, seperti tanggung jawab dan prosedur, pelaporan kejadian, serta pembelajaran dari insiden keamanan. Setiap hasil yang disajikan didasarkan pada data yang dikumpulkan melalui observasi, wawancara, dan analisis dokumen terkait.

Tabel 4. Manajemen Insiden dan Peningkatan Keamanan Sistem

A.16.1	Manajemen Insiden dan Peningkatan Keamanan Sistem Informasi				
16.1.1	Tanggung Jawab dan Prosedur				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5
1	Tanggung jawab dan prosedur manajemen untuk penanganan insiden keamanan informasi telah ditetapkan dan didokumentasikan.	1	✓		4
2	Tanggung jawab dan prosedur manajemen untuk penanganan insiden keamanan informasi telah dikomunikasikan kepada semua staf yang relevan.	1	✓		4
3	Tanggung jawab dan prosedur manajemen untuk penanganan insiden keamanan informasi telah ditinjau dan diperbarui secara berkala.	1	✓		4

Dilihat dari tabel 4, menunjukan bahwa manajemen insiden dan peningkatan keamanan sistem informasi dari segi tanggung jawab dan prosuder sudah sesuai dengan memiliki nilai index keseluruhan adalah 4 dari 3 pertanyaan yang sudah ditanyakan ke narasumber yaitu mas Wiwik yang mengatakan bahwa "Tanggung jawab dan prosedur manajemen untuk penanganan insiden keamanan informasi dilakukan oleh divisi IT dan prosedur penanganan sesuai dengan prosedur dari KOMINFO"

Tabel 5. Pelaporan Kejadian

16.1.2	Pelaporan Kejadian Keamanan Informasi				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5
1	Memiliki prosedur yang terdokumentasi untuk pelaporan insiden keamanan informasi.	1	✓		4
2	Menindaklanjuti semua insiden keamanan informasi sesuai dengan prosedur yang terdokumentasi.	1	✓		4
3	Mengumpulkan bukti sesegera mungkin setelah insiden terjadi.	1	✓		4

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1172

Dari tabel diatas di dapatkan bahwa manajemen insiden dan peningkatan keamanan sistem informasi dari segi pelaporan kejadian keamanan informasi sudah sesuai dengan pelaporan prosuder dari KOMINFO dan memiliki nilai index keseluruhan adalah 4 dari 3 pertanyaan yang sudah ditanyakan ke narasumber yaitu mas Wiwik mengatakan "Memiliki prosedur yang terdokumentasi dari KOMINFO jika ada pelaporan kejadian keamanan informasi".

Tabel 6. Pelaporan Kelemahan

16.1.3	Pelaporan Kelemahan Keamanan Informasi				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5
1	Pelaporan masalah ke titik kontak secepat mungkin untuk mencegah insiden keamanan informasi	1	✓		4
2	Mekanisme Pelaporan yang mudah, dapat diakses dan tersedia	1	✓		4
3	Adanya panduan tertulis dan mudah diakses mengenai proses pelaporan masalah	1	✓		4

Dari tabel diatas menunjukan bahwa manajemen insiden dan peningkatan keamanan sistem informasi dari segi pelaporan kelemahan keamanan informasi sudah sesuai dengan prosuder dari KOMINFO dan memiliki nilai index keseluruhan adalah 4 dari 3 pertanyaan yang sudah ditanyakan ke narasumber yaitu mas Wiwik mengatakan "Jika terjadi pelaporan kelemahan keamanan informasi akan langsung di tindak lanjuti dan untungnya insiden ini belum pernah kejadian".

Tabel 7. Penilaian dan Keputusan

16.1.4	Penilaian dan Keputusan Pada Kejadian Keamanan Informasi				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5
1	Pencatatan hasil evaluasi apakah peristiwa keamanan informasi telah dianalisis dengan cermat untuk menentukan klasifikasinya sebagai insiden keamanan informasi.	1	✓		4
2	Penilaian dan keputusan insiden keamanan informasi dilakukan oleh personil yang kompeten dan berwenang.	1	✓		4
3	Hasil penilaian dan keputusan insiden keamanan informasi dicatat secara rinci untuk referensi dan verifikasi di masa mendatang.	1	✓		4

Dari tabel diatas menunjukan bahwa manajemen insiden dan peningkatan keamanan sistem informasi dari segi Penilaian dan Keputusan Pada Kejadian Keamanan Informasi sudah sesuai dan memiliki nilai index keseluruhan adalah 4 dari 3 pertanyaan yang sudah ditanyakan ke narasumber yaitu mas Wiwik mengatakan "Untuk evaluasi sistem sering dlakukan secara berkala yang dilakukan oleh divisi IT dan di dampingi oleh manajemen RS Khusus Mata Purwokerto".

Jurnal Indonesia : Manajemen Informatika dan Komunikasi
https://journal.stmiki.ac.id
E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1172

Tabel 8. Tanggapan terhadap Insiden Keamanan Informasi

16.1.5	Tanggapan Terhadap Insiden Keamanan Informasi				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5
1	Menyusun dan mendokumentasikan prosedur respon terhadap insiden keamanan informasi	1	✓		4
2	Tim respons insiden keamanan telah ditetapkan dan dijelaskan dalam prosedur yang terdokumentasi	1	✓		4
3	Insiden keamanan informasi dilaporkan secara tepat waktu sesuai dengan prosedur yang telah ditetapkan	1	✓		4

Dari tabel diatas menunjukan bahwa manajemen insiden dan peningkatan keamanan sistem informasi dari segi Tanggapan Terhadap Insiden Keamanan Informasi sudah sesuai dan memiliki nilai index keseluruhan adalah 4 dari 3 pertanyaan yang sudah ditanyakan ke narasumber yaitu mas Wiwik mengatakan " Jika ada kejadian terkait insiden keamanan informasi maka divisi IT langsung merespon tanggapan insiden tersebut dan mengikuti prosedur-prosedur dari KOMINFO".

Tabel 9. Pembelajaran Insiden Keamanan Informasi

16.1.6	Pembelajaran dari Insiden Kemanan Informasi				
No.	Pernyataan	Bobot	Dilakukan		Nilai
			Ya	Tidak	1-5
1	Menyusun dan mendokumentasikan prosedur respon terhadap insiden keamanan informasi	1	✓		4
2	Tim respons insiden keamanan telah ditetapkan dan dijelaskan dalam prosedur yang terdokumentasi	1	✓		4
3	Insiden keamanan informasi dilaporkan secara tepat waktu sesuai dengan prosedur yang telah ditetapkan	1	✓		4

Dari table diatas menunjukan bahwa manajemen insiden dan peningkatan keamanan sistem informasi dari segi Pembelajaran dari Insiden Kemanan Informasi sudah sesuai dan memiliki nilai index keseluruhan adalah 4 dari 3 pertanyaan yang sudah ditanyakan ke narasumber yaitu mas Wiwik mengatakan "Sebelumnya sudah ada pembelajaran dan juga SIMRS dibuatkan oleh KOMINFO dan memiliki prosedur-prosedur dari KOMINFO".

3.2 Pembahasan

Hasil audit yang dilakukan pada RS Khusus Mata Purwokerto menunjukkan bahwa manajemen insiden dan peningkatan keamanan sistem informasi telah memenuhi standar ISO/IEC 27001. Berdasarkan data pada tabel 4, tanggung jawab dan prosedur manajemen keamanan informasi telah dirancang dan diterapkan dengan baik. Penanganan insiden keamanan, termasuk pelaporan, dokumentasi, dan tindakan korektif, telah sesuai dengan pedoman Kementerian Komunikasi dan

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1172

Informatika (Kominfo). Hal ini sejalan dengan temuan Paramita *et al.* (2022), yang menekankan pentingnya dokumentasi prosedur dalam menjaga keamanan informasi. Prosedur terkait tanggung jawab dan penanganan insiden juga telah dikomunikasikan secara efektif kepada staf yang relevan, menunjukkan adanya kesadaran organisasi yang tinggi terhadap pentingnya perlindungan data. Sebagaimana dinyatakan oleh Komalawati dan Triswandi (2022), tanggung jawab profesional dalam sektor kesehatan, terutama dalam pengelolaan data pasien, merupakan hal yang krusial untuk memastikan pelayanan kesehatan yang aman. Sistem keamanan informasi di RS Khusus Mata Purwokerto telah mencapai tingkat kematangan yang tinggi, sebagaimana dinilai menggunakan pendekatan indeks *maturity*. Ini mengindikasikan pengelolaan keamanan yang konsisten dan terstruktur, mirip dengan hasil yang diperoleh oleh Riana *et al.* (2023) dalam analisis mereka tentang tingkat kematangan keamanan informasi berdasarkan standar ISO 27001. Evaluasi berkala terhadap prosedur keamanan juga menjadi prioritas, seperti yang direkomendasikan oleh Chevalier Daniswara *et al.* (2023), untuk meningkatkan ketahanan sistem terhadap ancaman yang berkembang. Penanganan insiden yang cepat dan terorganisir juga diidentifikasi sebagai faktor penting dalam mencegah eskalasi kerugian akibat ancaman keamanan. Lubis dan Nasution (2023) menyoroti bahwa perkembangan teknologi informasi tidak hanya membawa manfaat tetapi juga risiko yang perlu diantisipasi melalui strategi mitigasi yang efektif. Hal ini tercermin dalam respons cepat divisi IT RS Khusus Mata terhadap insiden keamanan informasi, seperti yang diungkapkan dalam hasil wawancara. Dengan melihat pentingnya perlindungan data pasien di sektor kesehatan, temuan penelitian ini sejalan dengan argumen Ikhwan dan Yuniana (2022) bahwa pengelolaan risiko yang efektif dapat membantu menjaga integritas institusi kesehatan. Evaluasi keamanan sistem informasi di RS Khusus Mata Purwokerto tidak hanya mendukung keberlanjutan operasional, tetapi juga memastikan perlindungan hak-hak pasien dan kepercayaan masyarakat terhadap institusi kesehatan.

4. Kesimpulan dan Saran

Kesimpulan dari penilitian ini adalah bahwa Rumah Sakit Khusus Mata Purwokerto sudah menggunakan Sistem Informasi Manajemen Rumah Sakit (SIMRS) yang membantu mengintegrasikan pelayanan dan proses administrasi dengan baik. Meski demikian, terdapat tantangan terkait keamanan informasi, termasuk kehilangan data dan ancaman manipulasi data. Penelitian ini melakukan audit keamanan informasi berbasis ISO/IEC 27001 untuk mengevaluasi kesiapan dan penerapan manajemen keamanan informasi di rumah sakit khusus mata Purwokerto. Hasil audit menunjukkan bahwa manajemen insiden keamanan informasi telah berjalan sesuai prosedur, meliputi penanganan insiden, pelaporan kejadian, serta tindakan korektif yang telah didokumentasikan dan dikomunikasikan dengan baik kepada staf terkait. Setiap tahapan dalam penerapan standar ISO 27001 di rumah sakit ini telah memenuhi indikator keamanan dengan baik, menunjukkan tingkat kematangan keamanan yang cukup tinggi. Saran dari penelitian ini, perlunya evaluasi berkala dan peningkatan keamanan sistem informasi agar rumah sakit lebih tangguh dalam menghadapi ancaman keamanan data yang mungkin timbul di masa mendatang.

5. Daftar Pustaka

Daniswara, M. C., Putrawanto, D. I., Najib, M., Achmadha, Z., Islami, M. C. S., & Mukaromah, S. (2023). Evaluasi Keamanan Informasi di Lingkungan Rumah Sakit: Pendekatan Audit ISO 27001 di RS Rahman Rahim Sidoarjo. *Journal of Digital Ecosystem for Natural Sustainability*, *3*(2), 64-69.

E-ISSN: 2723-7079 | P-ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1172

Fauzi, A. A., Kom, S., Kom, M., Budi Harto, S. E., Mm, P. I. A., Mulyanto, M. E., ... & Rindi Wulandari, S. (2023). *Pemanfaatan Teknologi Informasi di Berbagai Sektor Pada Masa Society 5.0*. PT. Sonpedia Publishing Indonesia.

Handiwidjojo, W. (2015). Sistem informasi manajemen rumah sakit. *Jurnal Eksplorasi Karya Sistem Informasi dan Sains*, *2*(2).

Hariana, E., Sanjaya, G. Y., Rahmanti, A. R., Murtiningsih, B., & Nugroho, E. (2013). Penggunaan sistem Informasi manajemen rumah sakit (SIMRS) di DIY. *SESINDO 2013*, *2013*.

Igiany, P. D. (2019, December). Systematic Review: Faktor yang Mempengaruhi Implementasi Sistem Informasi Manajemen Rumah Sakit (SIMRS). In *Prosiding Seminar Nasional INAHCO 2019* (Vol. 1).

Ikhwan, A., & Yuniana, A. N. (2022). Strategy management semi-islamic boarding schools. *Al-Hayat: Journal of Islamic Education*, *6*(1), 74-86. https://doi.org/10.35723/ajie.v6i1.222.

Komalawati, V., & Triswandi, E. F. (2022). Tanggung Jawab Dokter Atas Insiden Keselamatan Pasien Dalam Pelayanan Kesehatan Di Rumah Sakit Sebagai Institusi Kesehatan. *Jurnal Bina Mulia Hukum*, *6*(2), 174-186. https://doi.org/10.23920/jbmh.v6i2.687.

Lubis, N. S., & Nasution, M. I. P. (2023). Perkembangan Teknologi Informasi Dan Dampaknya Pada Masyarakat. *Kohesi: Jurnal Sains dan Teknologi*, *1*(12), 41-50. https://doi.org/10.3785/kohesi.v1i12.1311.

Pamungkas, W. C., & Saputra, F. T. (2020). Evaluasi Keamanan Informasi Pada SMA N 1 Sentolo Berdasarkan Indeks Keamanan Informasi (KAMI) ISO/IEC 27001: 2013. *Jurnal Sistem Komputer dan Informatika (JSON)*, *1*(2), 101-106.

Paramita, S., Siregar, S. A., Damanik, R. A., & Irawan, M. D. (2022). Analisis Manejemen Resiko Keamanan Data Sistem Informasi Berdasarkan Indeks Keamanan Informasi (KAMI) ISO 27001: 2013. *Bulletin of Information Technology (BIT)*, *3*(4), 374-379. https://doi.org/10.47065/bit.v3i4.421.

Pertiwi, T. P., Pangestuti, D. D., Febrian, W. D., Nove, A. H., Megavitry, R., & Imanirubiarko, S. (2024). Strategi Pengembangan Kompetensi Dosen Untuk Menanggapi Tantangan Pendidikan Abad Ke-21. *Jurnal Review Pendidikan Dan Pengajaran (JRPP)*, *7*(1), 2586-2596. https://doi.org/10.31004/jrpp.v7i1.25779.

Premana, A., Fitralisma, G., Yulianto, A., Zaman, M. B., & Wiryo, M. A. (2020). Pemanfaatan teknologi informasi pada pertumbuhan ekonomi dalam era disrupsi 4.0. *Journal of Economic and Management (JECMA)*, *2*(2), 1-6. https://doi.org/10.46772/jecma.v1i01.219.

Riana, E., Sulistyawati, M. E. S., & Putra, O. P. (2023). Analisis Tingkat Kematangan (Maturity Level) Dan PDCA (Plan-Do-Check-Act) Dalam Penerapan Audit Sistem Manajemen Keamanan Informasi Pada PT Indonesia Game Menggunakan Metode ISO 27001: 2013. *Journal of Information System Research (JOSH)*, *4*(2), 632-640. https://doi.org/10.47065/josh.v4i2.2552.

Setyawan, D. (2016). Analisis Implementasi Pemanfaatan Sistem Informasi Manajemen Rumah Sakit (Simrs) Pada Rsud Kardinah Tegal. *IJCIT (Indonesian Journal on Computer and Information Technology)*, *1*(2). https://doi.org/10.31294/ijcit.v1i2.1503.

E - ISSN: 2723-7079 | P - ISSN: 2776-8074
Vol. 6 No. 1 (2025) | Januari
OPEN ACCESS
https://doi.org/10.35870/jimik.v6i1.1172

Simatupang, J., & Sianturi, S. (2019). Perancangan sistem informasi pemesanan tiket bus pada po. Handoyo berbasis online. *Jurnal Intra-Tech*, *3*(2), 11-25.

Sundari, P., & Wella, W. (2021). SNI ISO/IEC 27001 dan Indeks KAMI: Manajemen Risiko PUSDATIN (PUPR). *Ultima InfoSys: Jurnal Ilmu Sistem Informasi*, *12*(1), 35-42. https://doi.org/10.31937/si.v12i1.1701.