BAB III
HASIL DAN ANALISIS JURNAL

A. Hasil

1. Hasil pencarian *Literature*

Tabel 3. 1 Hasil Pencarian *Literature*

No	Author	Tahun	Judul	Metode	Hasil
1.	Lerisa Desti Irlaili, Rohmadi	2018	Tinjauan Keamanan Sistem Informasi Manajemen Rumah Sakit Berdasarkan Aspek *Privacy*, *Integrity* Dan *Authentication* Di Rsud Dr. Soedira Mangun Sumarso Wonogiri	Jenis penelitian ini kualitatif deskriptif dengan pendekatan *cross sectional*.	Hasil penelitian menunjukkan bahwa setiap unit di bagian rumah sakit hanya diterapkan satu modul SIMRS yang diperlukannya saja, sehingga unit lain tidak dapat menggunakan modul SIMRS yang tidak dibutuhkannya saja. Aturan perubahan data pada sistem yaitu dapat dapat dirubah oleh seluruh pengguna SIMRS sedangkan aturan penghapusan data hanyalah kewenangan dari administrator SIMRS
2.	Hendri Nurvianto Saputra, Jamroni	(2017)	Analisis Keamanan Data Sistem Informasi Di Puskesmas Pleret Bantul Yogyakarta	Jenis penelitian ini adalah kualitatif deskriptif dengan pendekatan *cross sectional*.	Berdasarkan hasil penelitian dan pembahasan mengenai analisis system keamanan data SIMPUS di Puskesmas

No	Author	Tahun	Judul	Metode	Hasil
					Pleret Bantul, tidak ada prosedur tetap sistem keamanan dan Pelaksanaan keamanan dilakukan dengan penggunaan *password.* *p*engetahuan petugas puskesmas mengenai system keamanan sudah baik dilihat dari kepahaman petugas mengenai fungsi dari *password*. Tetapi dalam proses pelaksanaan sistem keamanan data SIMPUS masih belum baik karena petugas masih kurang bertanggung jawab dalam pemberian *password.* dalam pelaksanaan sistem keamanan data meliputi pengendalian teknis yaitu dengan menggunakan sistem *back-up* data *server.*
3.	Dea Anjani,	2015	Identifikasi, Penilaian, Dan	Jenis penelitian	Berdasarkan hasil penelitian dan

No	Author	Tahun	Judul	Metode	Hasil
	Dr. Apol Pribadi Subriadi, S.T, M.T, Anisah Hediyanti, S.Kom, M.Sc		Mitigasi Risiko Keamanan Informasi Pada Sistem Electronic Medical Record (Studi Kasus : Aplikasi Healthy Plus Modul Rekam Medis Di Rsu Haji Surabaya)	ini adalah kualitatif	pembahasan mengenai identifikasi, penilaian, dan mitigasi risiko keamanan informasi pada sistem electronic medical record di Rsu Haji Surabaya berdasarkan metode OCTAVE diperoleh bahwa Dari proses identifikasi risiko yang terdapat pada aplikasi healthy plus diperoleh 13 risiko dengan 25 kejadian risik, dengan demikian terdapat risiko yang memiliki kejadian risiko lebih dari satu dikarenakan perbedaan penyebab. Untuk risiko yang paling banyak terjadi terdapat pada aset people dengan risiko penyalahgunaan hak akses dengan total kejadian risiko sebanyak lima kali. Dari proses penilaian risiko menggunakan metode FMEA(*Failure Mode & Effect*

No	Author	Tahun	Judul	Metode	Hasil
					Analysis) didapatkan risiko yang mempunyai skor assessment tertinggi hingga terendah. Untuk risiko very high dengan nilai RPN (*Risk Priority Number*) sebesar 392, yaitu pada kategori risiko people dengan identifikasi risiko Penyalahgunaan hak akses dan untuk risiko paling rendah dengan nilai RPN 18 terdapat pada risiko *Backup data failure.* Dari hasil penilaian risiko menggunakan metode FMEA(*Failure Mode & Effect Analysis*), maka diberikan penanganan atau tindakan pengendalian risiko untuk mengontrol risiko-risiko tersebut. Tindakan pengendalian untuk semua risiko-risiko tersebut mengacu pada ISO 27002 yang berfokus pada standarisasi

No	Author	Tahun	Judul	Metode	Hasil
					Sistem Manajemen Keamanan Informasi (SMKI). Untuk risiko yang telah diidentifikasi diatas terdapat 14 sub-klausul yang digunakan, akan tetapi yang sering digunakan ada sub-klausul yaitu *User Access Management*, *Equipment security*, dan *Secure area*.
4.	Rasim , Mayadi	2016	Evaluasi Keamanan Sistem Informasi Rumah Sakit (Studi Kasus Rumah Sakit Umum)	Jenis penelitian ini adalah kualitatif deskriptif	Berdasarkan Hasil Penelitian Dan Pembahasan Mengenai Evaluasi Keamanan Sistem Informasi Rumah Sakit (Studi Kasus Rumah Sakit Umum) ditemukan bahwa Dari aspek performance masih terdapat 15.42% menyatakan kurang baik, sehingga perlu untuk meningkatkan kinerja sistem, Masih terdapat pengguna yang merasakan aspek keamanan dan

No	Author	Tahun	Judul	Metode	Hasil
					kendali dirasakan belum cukup, 25% pengguna merasa kesulitan didalam mengoperasikan system informasi rekam medis, Masih ada pengguna yaitu 12.5% menyatakan bahwa program aplikasi tidak banyak digunakan untuk aplikasi yang lain, Masih ada 2.08% pengguna yang menyatakan bahwa sistem ini masih sangat sulit untuk dipahami dan Sebagian besar pengguna menyatakan bahwa sistem ini sangat membantu dalam memberikan penjelasan kepada pasien, walaupun jumlahnya tidak 100%

B. Analisis Jurnal

Lerisa Desti Irlaili, Rohmadi (2018) menjelaskan bahwa keamanan data yang berhubungan dengan *Privacy* sistem yang ada sudah terintegrasi dimana hak akses antar sistem hanya sebatas data yang diperlukan oleh sistem yang ada

dibagaian tersebut saja yang akan ditampilkan. Untuk pengguna tidak dapat mengakses ke modul-modul SIMRS unit lain karena setiap modu-modul di SIMRS berbeda. Sedangkan unuk *fiture* keamanan data *Integrity* berkaitan dengan informasi yang tersedia hanya diubah dan diolah unk kebutuhan tertentu dan oleh pengguna tertentu yang berhak. Untuk kelengkapan pengisian formulir pengguna SIMRS apabila terdapat kolom yang tidak diisi atau sengaja tidak diisikan oleh petugas maka data tidak dapat disimpan dan akan ada peringatan untuk mengisi semua kolom yang disediakan.

Sistem juga sudah dilengkapi antivirus yang bertujuan untuk menghidarkan hilangnya atau rusaknya data pasien didalam sistem dari virus. Perubahan data dapat dilakukan oleh seluruh pengguna SIMRS, sedangkan penghapusan data kewenangan dari Administrator SIMRS, sehingga setiap adanya penghapusan data pengguna SIMRS harus menghubungi administrator SIMRS dan meminta untuk dilakukan penghapusan data serta memberikan alasan yang jelas meminta untuk dilakukan penghapusan data serta memberikan alasan yang jelas. Fitur Keamanan Data *authentication* berkaitan dengan cara untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud setiap pengguna sistem informasi sudah memiliki *username* dan *password* sendiri-sendiri. *Username* dan *password* awal ditentukan oleh administrator SIMRS dan selanjutnya *password* dapat diubah sendiri oleh pengguna. *Password* yang ada berformat alfanumerik dengan maksimal 10 karakter sedangkan minimal *password* tidak ditentukan, sehingga apabila hanya di- isi dengan hanya satu huruf saja maka bisa digu- nakan. Penggunaan *password* dengan mengisikan abjad atau huruf secara berurutan juga diperbolehkan oleh sistem. *Password* pengguna sistem informasi tidak ditentukan masa berlakunya sehingga pengguna masih menggunakan *password* awal yang dibuatkan oleh Administrator SIMRS.

Hendri Nurvianto Saputra, Jamroni (2017) menjelaskan bahwa pelaksanaan penggunaan program IHIS. Pelaksanaan sistem keamanan data *server* dilaksanakan secara petugas *log in password* SIMPUS untuk masuk ke sistem IHIS data *server*. Pengetahuan petugas puskemas mengenai *password* sebagai sistem keamanan baru berada pada tahap 1 dan 2 yaitu pada tingkatan tahu *(know)* dan tahap memahami *(comphrehension)* bahwa pengamanan data itu penting dan dilakukan dengan cara pemakaian *password.*

Pengetahuan petugas mengenai sistem keamanan ini didapatkan dari pengalaman mereka bekerja dan apa yang mereka lihat selama pemakaian SIMPUS di puskesmas. Petugas tidak mempelajari sistem keamanan lebih mendalam lagi, sehingga pada tahap aplikasi *(Aplication)* pelaksanaannya masih saja ada petugas puskesmas yang bebas memberikan *password* kepada orang lain, padahal petugas itusendiri tahu bahwa *password* tersebut merupakan satu-satunya keamanan yang digunakan data *server* SIMPUS Puskesmas Pleret memberikan hak akses informasi kepada semua petugas puskesmas dan orang luar (mahasiawa yang melakukan observasi) dengan menggunakan *password* dan tanpa ada pengawasan dari petugas. Dengan tidak adanya batasan akses di puskesmas Pleret maka koordinator sistem informasi harus bertanggung jawab atas segala sesuatu yang telah dipilihnya dengan segala risiko, karena koordinator sistem informasi yang bertanggung jawab terhadap *password* data *server.*

Agar penerima informasi dapat memastikan keaslian informasi dari orang yang dimintai informas maka yang berhak dalah koordinator sistem informasi yang memang menjadi pengelola dan penanggung jawab sistem informasi manajemen puskesmas. Cara Menjaga Informasi Agar Tidak Dirubah Puskesmas Pleret menggunakan *password* untuk menjaga informasi data server dari perubahan tanpa ada seizin pemilik informasi. Dalam pengendalian teknis di Puskesmas Pleret telah menggunakan cara yaitu dengan menggunakan sistem *back-up* data yang dilakukan rutin setiap bulan oleh koordinator sistem informasi supaya data yang ada ter *copy.*

Pengendalian formal mencakup penentuan cara berperilaku, dokumentasi, prosedur dan praktik yang diharapkan dan pengawasan serta pencegahan perilaku yang berbeda dari panduan yang berlaku. Karena puskesmas Pleret tidak mempunyai prosedur sistem keamanan, maka dalam pengendalian, formal ini dilakukan dengan adanya koordinator sistem informasi manajemen puskesmas, dimana koordinator ini mempunyai tugas mengendalikan, mengawasi dan menyelesaikan permasalahan yang berkaitan dengan *server* SIMPUS. Pengendalian Informal Pengendalian ini ditujukan untuk menjaga agar para karyawan perusahaan memehami serta mendukung program keamanan tersebut. Dalam pengendalian informal ini yaitu dengan cara petugas puskesmas mengikuti pelatihan perawatan dan penggunaan sistem informasi manajemen puskesmas yang diadakan oleh Dinas Kesehatan kabupaten Bantul.

Dea Anjani, Dr. Apol Pribadi Subriadi, S.T, M.T, Anisah Hediyanti, S.Kom, M.Sc menjelaskan bahwa Dari proses identifikasi risiko yang terdapat pada aplikasi healthy plus diperoleh 13 risiko dengan 25 kejadian risik, dengan demikian terdapat risiko yang memiliki kejadian risiko lebih dari satu dikarenakan perbedaan penyebab. Untuk risiko yang paling banyak terjadi terdapat pada *aset people* dengan risiko penyalahgunaan hak akses dengan total kejadian risiko sebanyak lima kali. Dari proses penilaian risiko menggunakan metode FMEA(*Failure Mode & Effect Analysis*) didapatkan risiko yang mempunyai skor assessment tertinggi hingga terendah. Untuk risiko very high dengan nilai RPN (*Risk Priority Number*) sebesar 392, yaitu pada kategori risiko people dengan identifikasi risiko Penyalahgunaan hak akses dan untuk risiko paling rendah dengan nilai RPN 18 terdapat pada risiko *Backup data failure.*

Dari hasil penilaian risiko menggunakan metode FMEA(Failure Mode & Effect Analysis, maka diberikan penanganan atau tindakan pengendalian risiko untuk mengontrol risiko-risiko tersebut. Tindakan pengendalian untuk semua risiko-risiko tersebut mengacu pada ISO 27002 yang berfokus pada standarisasi

Sistem Manajemen Keamanan Informasi (SMKI). Untuk risiko yang telah diidentifikasi diatas terdapat 14 sub-klausul yang digunakan, akan tetapi yang sering digunakan ada 3 sub-klausul yaitu *User Access Management*, *Equipment security*, dan *Secure area*.

Rasim, Mayadi (2016) Untuk mengevaluasi Sistem Informasi digunakan pada Rumah Sakit umum Bekasi adalah. Dalam kerangka yang dipakai untuk mengklarifikasikan suatu problem, *Opportunities* dan *directives* yang terdapat pada bagian *scope definition* analisa dan perancangan system. Dari aspek performance 84.58% pengguna menilai baik, hanya 10.42% yang mengatakan bahwa output dari system ini sedikit. Waktu tanggap system terhadap pengolahan data dinilai cepat oleh pengguna sebesar 87.50%, walaupun 12.50% pengguna mengatakan kecepatan kerja computer masih lambat Pengguna computer untuk pengolahan informasi rekam medis mengatakan bahwa interface/tampilan dari system informasi mudah dipahami sebesar 81.25%, walaupun 18.75% mengatakan bahwa interface system ini sulit untuk dipahami Kelengkapan system dinilai baik oleh pengguna baik sebesar 89.58%, dan hanya 10.42 % yang merasa bahwa sistem ini kurang lengkap. Sebagian besar pengguna yaitu sebesar 75.00% mengatakan bahwa tidak terdapat kesulitan jika system ini melakukan kesalahan Evaluasi Sistem Informasi mencakup aspek akurasi dan relevansi data, penyajian informasi sesuai dengan kebutuhan serta kemudahan akses data. Ketelitian kerja computer dinilai dari data yang ada diperoleh sebanyak 72.92% menyatakan teliti. Yang cukup signifikan adalah bahwa sebesar 2.08% tidak teliti. Hal ini sering ditemukan dalam daftar rekapitulasi. Indikator masalah lain dari aspek informasi adalah kemudahan jika informasi disesuaikan dengan kebutuhan pengolahan data rekam medis, deskripsi persepsi pengguna menyatakan 72.92% sangat mudah, sedangkan 27.08% menyatakan sulit. Dari aspek ekonomi secara umum 81.25% respondent menyaatakan sangat baik dan baik dan hanya 18.75% menyatakan kurang baik dan tidak baik Indikator yang

digunakan untuk mengukur aspek ekonomi diantaranya adalah aspek reusabilitas yaitu Seberapa banyak program yang dapat dipakai untuk aplikasi lain 42 respoden atau 87.50% bahwa program yang dipakai untuk aplikasi lain sangat banyak dan banyak, sedangkan responden yang menyatakan bahwa program yang dipakai untuk aplikasi lain kurang banyak dan sedikit hanya 6 responden atau sebesar 12.50% saja Sedangkan dari aspek Sumber Daya diperlukan dalam mengembangkan sistem informasi rekam medis ini, 36 responden atau 75% menyatakan bahwa sumber daya yang diperlukan dalam mengembangkan sistem informasi rekam medis ini sangat sedikit dan sedikit, sedangkan yang menyatakan bahwa sumber daya yang diperlukan dalam mengembangkan sistem informasi rekam medis ini tidak terlalu banyak dan banyak haanya 12 responden atau sebesar 25% saja Dari aspek Control and Security sebagian besar responden yaitu 40 responden atau sebesar 83.33% menyatakan sangat baik dan baik dan hanya 8 responden atau sebesar 16.67% menyatakan kurang baik dan tidak baik Indikator lain yang digunakan untuk mengukur aspek ini adalah Integritas yaitu Apakah terdapat kesesuaian batasan akses terhadap pengguna, yang diterapkan oleh sistem informasi ini, jika hak akses tidak dibatasi maka data dapat dibuka oleh siapa saja, dari hasil penelitian diperoleh data bahwa 40 respoden atau 83.33% menyatakan bahwa terdapat kesesuaian antara batasan hak akses terhadap pengguna, dan hanya 8 responden atau 16.67% respoden menyatakan tidak terdapat kesesuaian antara batasan hak akses terhadap pengguna Dari aspek keamanan yaitu Bagaimana keamanan yang diterapkan oleh sistem yang ada untuk menjamin keamanan data yang ada, sebanyak 40 respoden atau 83.33% menyatakan bahwa keamanan yang diterapkan oleh sistem yang ada untuk menjamin keamanan data yang ada sudah sangat aman dan aman, sedangkan yang menyatakan kurang aman dan tidak aman hanya 8 responden atau sebesar 16.67% saja Kontrol dan keamanan data benarbenar harus diperhatikan karena Sistem informasi rekam medis menyimpan data pasien yang harus dijaga kerahasiaannyaoleh Sistem informasi juga harus, mempertimbangkan keamanan

data dalam menghadapi keadaan yang tidak biasa sehinga harus ada mekanisme back up data. Dari aspek Efisiensi sebagian besar responden yaitu 36 responden atau sebesar 73.96% menyatakan sangat baik dan baik dan hanya 12 responden atau sebesar 26.04% menyatakan kurang baik dan tidakbaik Indikator lain yang digunakan untuk mengukur aspek ini adalah Usabilitas yaitu Bagaimana tingkat kesulitan pengguna untuk mempelajari dan mengoperasikan sistem yang ada saat ini. Sebanyak 36 responden atau 75% menyatakan bahwa dalam mempelajari dan mengoperasikan sistem informasi rekam medis saat ini sangat mudah dan mudah, sedangkan yang mengatakan agak sulit sebesar 18.75% dan yang menyatakan sulit dan sangat sulit hanya sebesar 6.18% saja Aspek lain yang diukur adalah Maintanabilitas yaitu Seberapa sulit dalam mencari serta memperbaiki kesalahan yang mungkin terjadi pada sistem informasi ini. Sebanyak 35 responden atau 72.92% menyatakan bahwa dalam memperbaiki kesalahan pada sistem informasi rekam medis saat ini sangat mudah dan mudah, sedangkan yang menyatakan kurang mudah (agak sulit) sebesar 12 responden atau 25% dan yang menyatakan sulit dan sangat sulit sebanyak 2.08% Dari aspek Efisiensi sebagian besar responden yaitu 89.58% menyatakan sangat baik dan baik dan hanya 10.42%responden menyatakan kurang baik dan tidak baik Indikator lain yang digunakan untuk mengukur aspek ini adalah Reliabilitas yaitu Apakah sistem yang ada dapat dipercaya oleh pengguna untuk melakukan pekerjaan yang diminta. Sebanyak 43 responden atau 89.58%menyatakan bahwa sistem yang sangat dipercaya dan dipercaya oleh pengguna untuk melakukan pekerjaan yang diminta, dan hanya 3 responden atau 6.25% menyatakan bahwa sistem informasi rekam medis ini kurang dapat dipercaya untuk melakukan pekerjaan yang diminta, dan 4.16% responden menyatakan bahwa sistem ini tidak dapat dan sangat tidak dapat dipercaya Aspek lain yang diukur adalah Kesederhanaan yaitu Seberapa sulitkah sistem ini dipahami oleh pengguna. Sebanyak 43 responden atau 89.58% menyatakan bahwa sistem informasi ini sangat mudah untuk dipahami oleh pengguna, dan hanya 10.42% pengguna menyatakan kurang

mudah dan sulit untuk memahami sistem informasi ini Aspek berikutnya yang diukur adalah Kemudahan yaitu Apakah sistem informasi rekam medis ini dapat membantu mempermudah dalam memberikan penjelasan kepada pengguna. Sebanyak 43 respoden atau 89.58% responden menyatakan bahwa sistem informasi ini sangat mempermudah dan mempermudah dalam membantu memberikan penjelasan kepada pengguna (pasien), dan sebanyak 3 responden atau 6.25% responden menyatakan bahwa sistem informasi ini kurang dapat membantu dalam memberikan penjelasan kepada pengguna (pasien), serta 4.16% responden menyatakan bahwa sistem informasi ini sulit dan sangat sulit dalam membantu dalam memberikan penjelasan kepada pengguna(pasien)