SISTEM KEAMANAN SIMRS DI RUMAH SAKIT

[1]Puguh Ika Listyorini*, [2]Intan Sintya
[1]Universitas Duta Bangsa Surakarta.puguh_ika@udb.ac.id
[1]Universitas Duta Bangsa Surakarta.intancintya064@gmail.com
**Penulis Korespondensi*

ABSTRAK

System informasi manajemen rumah sakit merupakan system yang kritis menyangkut kehidupan seseorang. Upaya perlu dilakukan agar system tersebut dapat tetap aman, terjaga dari berbagai ancaman yang dapat menggangu keberjalanan system. Penelitian ini bertujuan untuk mengetahui ancaman terhadap keamanan system manajemen resiko keamanan data di rumah sakit. Penelitian ini menggunakan metode studi literatur dengan melakukan Teknik purposive sampling yang berjumlah 5 jurnal sehingga menghasilkan pembahasan dan kesimpulan yang terpadu. Keamanan dan kerahasiaan data saat ini menjadi isu yang sangat penting dan terus berkembang. Beberapa kasus menyangkut keamanan data saat ini menjadi suatu pekerjaan yang membutuhkan biaya penanganan dan pengamanan yang sedemikian besar. Dapat disimpulkan bahwa Keamanan data pasien dapat terbongkar karena banyak kejahatan pencurian data pasien di rumah sakit.

Kata Kunci : studi literatur, ancaman keamanan, system informasi Kesehatan, manajemen rumah sakit

ABSTRACT

Hospital management information system is a critical system concerning a person's life. Efforts need to be made so that the system can remain safe, protected from various threats that can interfere with the operation of the system. This study aims to determine the threats to the security of the data security risk management system in hospitals. This study uses a literature study method by conducting a purposive sampling technique totaling 5 journals so as to produce an integrated discussion and conclusion. Data security and confidentiality is currently a very important issue and continues to grow. Several cases concerning data security are currently a job that requires such large handling and security costs. It can be concluded that the security of patient data can be exposed because there are many crimes of theft of patient data in hospitals.

Keywords: literature study, security threats, health information system, hospital management

PENDAHULUAN

Di era informasi ini, rumah sakit dituntut untuk meningkatkan kinerja dan daya saing sebagai badan usaha dengan tidak mengurangi misi sosial yang diembannya. Rumah sakit harus merumuskan kebijakan-kebijakan strategis pada internal organisasi, manajemen, dan SDMnya serta harus mampu secara cepat dan tepat mengambil keputusan untuk peningkatan kualitas pelayanan kesehatan kepada masyarakat luas agar dapat menjadi organisasi yang responsif, inovatif, efektif, efisien dan tentu saja menguntungkan bagi pemilik modal dengan tidak mengabaikan misi sosialnya.

Sistem Informasi Manajemen Rumah Sakit adalah sebuah sistem komputer yang memproses dan mengintegrasikan seluruh alur proses bisnis layanan kesehatan dalam bentuk jaringan koordinasi, pelaporan dan prosedur administrasi untuk memperoleh informasi secara cepat, tepat dan akurat. Saat ini Sistim Informasi Manajemen (SIM) berbasis komputer rumah sakit (SIMRS) merupakan sarana pendukung yang sangat penting, bahkan bisa dikatakan mutlak untuk mendukung pengelolaan operasional rumah sakit.

Berbagai rumah sakit yang masih tetap bertahan menggunakan sistim administrasi konvensional telah menunjukan banyaknya kehilangan kesempatan memperoleh laba akibat dari lemahnya koordinasi antar departemen maupun kurangnya dukungan informasi yang cepat, tepat, akurat, dan terintegrasi. Hal ini tentu saja akan mempengaruhi kualitas layanan yang diberikan kepada para pemangku kepentingan khususnya pasien. Rumah sakit ini umumnya tertinggal dalam

persaingan dengan rumah sakit yang menggunakan SIMRS. Sebagai contoh, pada system administrasi konvensional, pencatatan biaya perawatan dibagian keuangan dikumpulkan secara bertingkat mulai dari bangsal, bangsal belum dapat membuat perhitungan biaya karena menunggu informasi harga obat yang diberikan kepada pasien dari apotik, bangsal juga menunggu informasi catatan biaya dari laboratorium, seandainya ada jaminan uang yang dibayarkan ke kasir juga harus menunggu keabsahan data tersebut, demikian seterusnya sehingga pasien yang akan melakukan pembayaran di akhir perawatan harus menunggu untuk waktu yang cukup lama. Belum lagi ada unsur subyektifitas penghitungan yang dilakukan oleh masing-masing bangsal/ruangan karena ada rumah sakit yang memberi wewenang kapada kepala ruangan untuk mengestimasi sendiri tingkat kemampuan pasien dan berapa tindakan perawatan ataupun obat-obatan yang tidak ditagihkan ke pasien. Kondisi pemberian potongan di masing-masing ruangan ini jelas akan menimbulkan akibat yang kurang baik, dimana pendapatan rumah sakit menjadi berkurang dan insentif untuk jasa medis dipotong secara sepihak yang pada akhirnya akan menimbulkan standar ganda perawatan.

METODE

Rancangan penelitian ini menggunakan adalah *literature review*, yaitu dengan menganalisis dan kajian bebas pada jurnal, e-book, maupun buku teks yang berkaitan dengan keamanan data SIM RS di rumah sakit. Jurnal atau artikel yang digunakan pada *literature review* ini adalah jurnal atau artikel yang didapatkan dari *google scholar, google book, library*. Kata kunci yang digunakan untuk pencarian antara lain SIMRS, dan keamanan SIMRS.

HASIL DAN PEMBAHASAN

1. Rumah Sakit

Rumah sakit merupakan suatu institusi yang fungsi utamanya memberikan pelayanan kesehatan kepada masyarakat. Tugas rumah sakit adalah melaksanakan upaya kesehatan secara berdaya guna dan berhasil guna dengan mengutamakan upaya penyembuhan dan pemulihan yang dilaksanakan secara serasi dan terpadu dengan peningkatan dan pencegahan serta melaksanakan rujukan.Untuk dapat menyelenggarakan upaya-upaya tersebut dan mengelola rumah sakit agar tetap dapat memenuhi kebutuhan pasien dan masyarakat yang dinamis, maka setiap komponen yang ada di rumah sakit harus terintegrasi dalam satu sistem (Soejitno, 2002).

2. Konsep Keamanan Informasi

Sarno dan Iffano, 2009, keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (business continuity), meminimalisasi risiko bisnis (reduce business risk) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang. Untuk mengamankan informasi, maka diperlukan adanya audit sistem informasi. Audit secara umum adalah proses terpadu dalam pengumpulan dan penilaian terhadap informasi sebagai satu kesatuan organisasi oleh seorang ahli . Pengertian audit sistem informasi adalah proses pengumpulan dan evaluasi bukti-bukti untuk menentukan apakah sistem komputer yang digunakan telah dapat melindungi aset milik organisasi, mampu menjaga integritas data, dapat membantu pencapaian tujuan organisasi secara efektif, serta menggunakan sumber daya yang dimiliki secara efisien.

Menurut Sabarguna (2008) bahwasanya keamanan dalam system komputerisasin terdiri atas empat aspek yaitu privacy, integrity, authentication, availability, sedangkan untuk dunia kesehatan terdapat aspek lain yang juga tak aklah pentingnya yang harus diperhatikan yaitu access control dan *non-repudiation.* Adapun penjelasan dari system komputerisasin berikut ini.

a. Privasi.

Privasi merupakan sebuah upaya untuk menjaga informasi dari pihak-pihak yang tidak memiliki hak untuk mengakses informasi tersebut. Data rekam medis yang berisi riwayat kesehatan pasien yang merupakan dokumen rahasia harus senantiasa dijaga kerahasiaanya, sebab itu infomasi tersebut merupakan milik pasien.

b. Integritas.
   Integritas pengamanan atau proteksi yang lebih yaitu tidak begitu saja menghapus data yang tersimpan dalam rekam kesehatan elektronik tersebut dan segala perubahanya dapat diketahui.
c. Otentifikasi.
   Otentifikasi perlu adanya pembatasan akses khusus untuk hanya orang tertentu yang dapat mengaksesnya dan dibubuhi nama, waktu, dan tanda tangan petugas yang memberikan pelayanan atau tindakan".
d. Ketersediaan.
   Ketersediaan merupakan aspek yang menekankan bahwa informasi ketika dihubungkan oleh pihak-pihak yang terkait tersedia secara cepat (just in time).
e. Kontrol terhadap akses.
   Kontrol terhadap akses adalah aspek yang menekankan pada proses dan teknis yang harus dilakukan dalam mengatur akses terhadap informasi.
f. Non-Penolakan.
   Pada aspek ini berkaitan erat dengan dengan suatu transaksi atau perubahaninformasi. Aspek ini membantu mencegah seseorang untuk tidak menyanggah bahwa dirinya telah melakukan transaksi atau perubahan terhadap suatu informasi.

Resiko keamanan data yang sering terjadi biasanya terdapat pada jaringan komputer. virus komputer juga merupakan hasil karya seorang programmer yang punya niat jahat atau hanya untuk memuaskan nafsu programmingnya yang berhasil menyusupkan virus kedalam sistem komputer orang lain. Virus menyusup masuk ke dalam sistem komputer melalu berbagai cara antara lain :

a. Pertukaran file, misalnya mengambil file (*copy-paste*) dari komputer lain yang telah tertular virus.
b. E-mail, membaca e-mail dari sumber yang tidak dikenal bias berisiko tertular virus, karena virus telah ditambahkan (*attach*) ke file e-mail.
c. IRC, saluran chatting bisa dijadikan jalan bagi virus untuk masuk ke komputer. Sedangkan resiko pencurian hanya sebagian kecil saja, dikarenakan setiap penyedia atau pengguna terkadang lebih mengutamakan dalam ancaman yang ini.

Dengan melihat beberapa aspek yang menjadi ancaman bagi keamanan sistem infomasi kesehatan yang disampaikan dalam makalah-makalah yang ditinjau, beberapa hal yang perlu diperhatikan oleh pengelola sistem informasi yaitu:

a. Melakukan perlindungan yang memadai dalam menopang aspek kerahasiaan, integritas dan ketersediaan untuk investigasi. Penyelidikan lebih lanjut untuk mengidentifikasi ancaman keamanan di kesehatan sistem informasi.
b. Melakukan perlindungan yang menyangkut kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman.
c. Melakukan analisis resiko keamanan untuk melindungi aset informasi menjamin keamanan sistem.

3. Konsep Sistem Informasi Rumah Sakit

Pembangunan sistem informasi rumah sakit berbasis komputer akan membentuk rumah sakit digital yang dapat dipahami dengan merujuk pada definisi perusahaan digital dimana hampir semua proses bisnis dan hubungan dengan pelanggan, pemasok, mitra kerja dan pihak internal perusahaan, serta pengelolaan aset-aset perusahaan yang meliputi properti intelektual,

kompetensi utama, keuangan dan sumber daya manusia (SDM) dilakukan secara digital (Laudon, 2004).

Pembentukan SI tersebut tentu saja bukan sekedar mengotomatisasikan prosedur lama, tetapi menata dan memperbarui bahkan menciptakan aliran data yang baru yang lebih efisien, menetapkan prosedur pengolahan data yang baru secara tepat, sistematis dan sederhana, menentukan model penyajian yang informatif dan standar, serta mendistribusikan informasi secara efektif (Oetomo, 2002).

SI merupakan infrastruktur dasar pembentuk rumah sakit digital, karena suatu rumah sakit dapat dikategorikan sebagai rumah sakit digital (secara administratif manajerial), bila empat SI utamanya telah dikelola secara digital, yaitu: Supply Chain Management Sistem, Customer Relationship Management Sistem, Enterprise Sistem dan Knowledge Management Sistem (Laudon, 2004).

a. Supply Chain Management Sistem. SI ini berfungsi untuk mendigitalisasikan Supply Chain Management Sistem, sehingga hubungan antara rumah sakit dengan para pemasok dapat dioptimalkan. Kegiatan perencanaan, pemesanan dan pasokan bahan baku, obat maupun peralatan medis dapat dikoordinasikan dengan baik dan efisien. Dalam hal rantai pasokan ini, rumah sakit perlu mengelola aliran informasi dengan pemasok, khususnya untuk menjamin tersedianya bahan dan peralatan medis. SI ini diharapkan dapat menciptakan efisiensi dalam pengelolaan persediaan. Dimana SI tersebut memungkinkan penerapan sistem Just in Time bahkan Stockless Inventory Method (Laudon, 2004), sehingga rumah sakit dapat menghemat biaya penyimpanan dan mengurangi resiko kerusakan, namun persediaan bahan dan peralatan medis tetap terjamin.
b. Enterprise Sistem. SI ini berfungsi untuk mengkomputerisasi Enterprise Sistem dalam hal ini sistem rumah sakit, sehingga dapat mengkoordinasikan proses-proses internal utama dari rumah sakit, mengintegrasikan data dari semua unit, seperti front office, layanan rawat inap, rawat jalan, poliklinik, apotik, laboratorium, keuangan, SDM, investasi dan persediaan. Komputerisasi yang terintegrasi dari setiap unit yang ada memungkinkan pengelola untuk mengetahui kondisi objektif rumah sakit baik secara keseluruhan maupun per unit melalui laporan-laporan manajerial yang dapat disusun setiap saat secara cepat dan akurat, sehingga pengelola dapat membuat keputusan-keputusan yang tepat dan melakukan kontrol kualitas terhadap layanan maupun produk medis lainnya. Sementara itu, para pasien dapat memperoleh informasi secara rinci tentang biaya-biaya yang harus ditanggung tanpa harus mondar-mandir ke unit-unit yang memberikan layanan.
c. Customer Relationship Management Sistem. SI ini berfungsi untuk mendigitalisasikan Customer Relationship Management Sistem, sehingga dapat mengintegrasikan dan memelihara relasi antara rumah sakit dengan pasien, pengguna jasa kesehatan dan pihak-pihak terkait lainnya. Rumah sakit perlu terus menerus membangun dan menjaga relasi dengan semua pihak yang terkait, agar dapat menciptakan rasa aman dan nyaman bagi pihak-pihak yang menggunakan jasa layanan medis dan melakukan kerjasama baik dalam hal pemenuhan kebutuhan rumah sakit, pengembangan jasa layanan medis dan penyediaan infrastruktur. SI akan memungkinkan rumah sakit untuk mengelola data semua pihak yang terkait, sehingga rumah sakit dapat memberi perhatian kepada pihak-pihak yang terkait tersebut dengan lebih baik lagi, misalnya memberikan ucapan selamat kepada pasien yang melahirkan, memberikan penawaran pertama kepada rekanan penyedia infrastruktur saat rumah sakit akan membangun dan lain sebagainya.
d. Knowledge Management Sistem. SI ini berfungsi untuk mengkomputerisasikan Knowledge Management Sistem, sehingga mendukung pencatatan, penyimpanan dan penyebaran dari pengetahuan dan keahlian. Sistem ini tidak saja mengolah data transaksi untuk menghasilkan informasi berupa laporan manajerial, melainkan menghasilkan suatu pengetahuan baru. Pengelola dapat mengeksplorasi data warehouse untuk menemukan

data mining yang memberi pengetahuan baru berupa gambaran pola atau korelasi dari pengguna jasa kesehatan di rumah sakit yang dikelolanya atau pola-pola yang terjadi di setiap unit. Pengetahuan-pengetahuan yang diperoleh tersebut, tentu sangat berperan untuk menyusun rencana jangka panjang, mennyusun strategi dan menciptakan program-program layanan dan sistem pengelolaan yang inovatif.

Saat ini, menggunakan sistem informasi dalam layanan kesehatan dapat memberikan banyak manfaat yang potensial seperti meningkatkan kualitas pelayanan, mengurangi kesalahan medis, meningkatkan pembacaan ketersediaan fasilitas dan aksesibilitas informasi. Namun demikian, ancaman terhadap keamanan Sistem Informasi Kesehatan juga meningkat secara signifikan. Sebagai contoh, selama periode 2006 - 2007, terdapat lebih dari 1,5 juta kesalahan data yang terjadi di rumah sakit (HIMSS Analytics, 2008). Oleh karena itu, menyimpan informasi kesehatan dalam bentuk elektronik dapat menimbulkan kekhawatiran bagi pasien maupun manajemen rumah sakit. Pada dasarnya, ancaman dan tindakan yang disengaja dapat sangat merusak sistem informasi kesehatan dan akibatnya dapat mencegah profesional untuk menggunakannya di kemudian hari. Selain itu, kurangnya perlindungan yang memadai dalam menopang aspek kerahasiaan, integritas dan ketersediaan untuk investigasi juga menjadi ancaman, terutama di domain sistem informasi kesehatan. Hal ini memerlukan pengelolaan lebih dalam keamanan informasi serta perhatian khusus dari sektor publik dan swasta.Penyelidikan lebih lanjut diperlukan untuk mengidentifikasi ancaman keamanan sistem informasi kesehatan adalah wajib.

4. Pelaksanaan Sistem Keamanan SIMRS di Rumah Sakit

Beberapa rumah sakit telah menggunakan SIMRS, dan menerapkan sistem keamanan SIMRS, antara lain dalam penelitian Irlaili dan Rohmadi (2017), hasil penelitiannya di RSUD dr. Soediran Mangun Sumarso Wonogiri 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. Seluruh kolom harus diisikan secara lengkap, apabila tidak lengkap maka diminta kembali untuk melengkapi. Lamanya data dapat diakses oleh pengguna SIMRS tidak ditentukan.Penerapan maksimal password berjumlah 10 digit, tetapi dengan penggunaan batas minimal password tidak ditentukan. Belum adanya kebijakan yang mengatur tentang wewenang administrator.

Sedangkan penelitian yang dilakukan oleh Waisantoro, Rohmadi, dan Mulyono (2014), menunjukan bahwa Menunjukkan bahwa RSUD Surakarta menggunakan SIMRS dengan Otentifikasi system keamanan yang kurang, dikarenakan otentifikasi keamanan dari SIMRS tidak dapat mengidentifikasi user pada sistem tersebut. Otentifikasi keamanan yang ada hanya sebagai jalur dimana user dapat memasuki sistem tersebut. Sedangkan untuk keamanan data yang ada pada SIMRS harusnya otentifikasi adalah bagian dari sesuatu juga berperan penting. Walaupun pada dasarnya setiap petugas sudah memiliki password sendiri-sendiri, Itu tidak menjamin bahwa sistem keamanannya sudah berjalan dengan baik.Maka dari itu Otentifikasi diharuskan dapat menidentifikasi dan mengotorisasi user sehingga pihak yang tidak berkepentingan terhadap kemanan sistem komputer dapat diketahui sedini mungkin, bila otentifikasi (Validasi user) didalam SIMRS sudah sesuai, Makarumah sakit akan terjaga keamanan datanya dengan baik.

Pada RSU Haji Surabaya, dalam penelitian Yaner, Tanuwijaya, dan Sutomo (2011) Instalasi SIM-RS memiliki kekurangan pada keamanan fisik dan lingkungan disebabkan karena belum adanya kontrol, aturan, kebijakan, standar untuk perlindungan keamanan fisik dan lingkungan dan masih belum lengkapnya batas parimeter, peralatan otentikasi, fasilitas untuk mendukung dalam pemeliharaan dan perlindungan keamanan fisik dan lingkungan. Penyalahgunaan password disebabkan belum adanya dokumen maupun pernyataan tertulis

untuk membuat manajemen password, belum terdapat pemberian sanksi bagi pengguna yang melanggar password dan masih banyaknya pengguna password yang belum memiliki kesadaran untuk menjaga keamanan password. Belum adanya pencatatan mengenai insiden kelemahan keamanan informasi yang disebabkan karena tidak terdapat kebijakan, prosedur maupun aturan untuk menanggulangi insiden kelemahan sistem informasi, serta belum adanya kebijakan dan prosedur untuk melakukan pembahasan keamanan fisik dan lingkungan, kontrol akses, dan akuisis sistem infomasi, pembangunan dan pemeliharaan, belum terdapat kontrol keamanan yang diterapkan dimana terdapat bukti bahwa masalah keamanan ada dan perlu ditangani, tidak ada kontrol untuk mengatasi masalah ini dan kurangnya pendokumentasian prosedur, kebijakan dan peraturan.

Beberapa penelitian diatas menyebutkan bahwa pada dasarnya setiap rumah sakit telah memiliki sistem keamanan pada SIMRSnya, akan tetapi dalam pelaksanaannya masih saja terdapat kekurangan. Akan tetapi tetap saja tidak bisa dipungkiri bahwa keberadaan SIMRS sangat penting untuk pengelolaan data di rumah sakit.

Pengelolaan data Rumah Sakit sesungguhnya cukup besar dan kompleks, baik data medis pasien maupun data-data administrasi yang dimiliki oleh rumah Sakit sehingga bila dikelola secara konvensional tanpa bantuan SIMRS akan mengakibatkan beberapa hal berikut:

a. Redudansi Data, pencatatan data medis yang sama dapat terjadi berulang-ulang sehingga menyebabkan duplikasi data dan ini berakibat membengkaknya kapasitas penyimpanan data. Pelayanan menjadi lambat karena proses retreiving (pengambilan ulang) data lambat akibat banyaknya tumpukan berkas.
b. Unintegrated Data, penyimpanan dan pengelolaan data yang tidak terintegrasi menyebabkan data tidak sinkron, informasi pada masing-masing bagian mempunyai asumsi yang berbeda-beda sesuai dengan kebutuhan masing-masing unit /Instalasi.
c. Out of date Information, dikarenakan dalam penyusunan informasi harus direkap secara manual maka penyajian informasi menjadi terlambat dan kurang dapat dipercaya kebenarannya
d. Human Error, kelemahan manusia adalah kelelahan, ketelitian dan kejenuhan hal ini berakibat sering terjadi kesalahan dalam proses pencatatan dan pengolahan data yang dilakukan secara manual terlebih lagi jika jumlah data yang dicatat atau di olah sangatlah besar. Pemasukan data yang tidak sinkron untuk pasien atau barang yang sama tentu saja akan meyulitkan pengolahan data dan tidak jarang berdampak pada kerugian materi yang tidak sedikit bagi rumah sakit (Handiwijojo, 2009)

KESIMPULAN

Sekarang ini setiap rumah sakit sudah harus memiliki SIMRS untuk pengelolaan data rumah sakit. Data rumah sakit akan diolah menjadi informasi, sehingga keamanannya harus dijaga.

DAFTAR PUSTAKA

C. Laudon, P. Jane Laudon, Kenneth. 2004. *Management Information Systems*. Pearson International.

Handiwijojo, Wimmie. 2009. Sistem Informasi Manajemen Rumah Sakit. *Media Neliti* (https://media.neliti.com/media/publications/78723-ID-none.pdf)

HIMSS Analytics Report, 2008. *Security Of Patient Data*. (https://pubmed.ncbi.nlm.nih.gov/15460243/)

Irlaili, Lerisa Desti, dan Rohmadi. 2017. Tinjauan Keamanan Sistem Informasi Manajemen Rumah Sakit Berdasarkan Aspek Privacy, Integrity dan Authentication di RSUD dr. Soediran Mangun Sumarso Wonogiri. *Jurnal Rekam Medis, Vol. 11. No.1.*

Oetomo, Budi Sutedjo Dharma. 2002. *Perencanaan dan Pembangunan Sistem Informasi*. Jakarta: Penerbit Andi

Sabarguna B S. 2008. Rekam Medis Terkomputerisasi. Jakarta: UI Press

Soejitno, S (2002). *Reformasi Perumahsakitan Indonesia*. Jakarta. Bagian Penyusunan Program Dan Laporan Ditjen Pelayanan medik depkes RI.

Sarno, R. dan Iffano, I. 2009. Sistem Manajemen Keamanan Informasi. Surabaya: ITS Press.efisien

Waisantoro, Data Unggul; Rohmadi; dan Mulyono, Sri. 2014. Tinjauan Penerapan Atentifikasi Keamanan Sistem Informasi Managemen Rumah Sakit Umum Daerah Surakarta. *Jurnal Rekam Medis, Vol. 8. No.1. 2014*

Yaner, Annisa Destiara; Tanuwijaya, Haryanto; dan Sutomo, Erwin. 2011. Audit Keamanan Sistem Informasi Pada Instalasi Sistem Informasi Management (SIM-RS) Berdasarkan Standar ISO 27002. *Jurnal JSIK. Vol 1. No.1 2021*