ISSN: 1829-667X / E-ISSN: 2460-9021
DOI:10.31515/telematika.v19i2.6534

FRAMEWORK MANAGEMENT TO MINIMIZE RISK IN PROTECTING ENTERPRISE SYSTEMS: SYSTEMATIC LITERATURE REVIEW

PENGELOLAAN *FRAMEWORK* UNTUK MEMINIMALISIR RESIKO DALAM MELINDUNGI SISTEM ENTERPRISE: TINJAUAN PUSTAKA SISTEMATIK

Soni Adiyono[1], Romy Aziz Risaldi[2], Aris Puji Widodo[3], Eko Sediyono[4]

[1,2,3] Magister Sistem Informasi, Universitas Diponegoro, Indonesia
[4] Ilmu Komputer, Universitas Kristen Satya Wacana, Indonesia

[1*]sonisisu@gmail.com, [2]romyrisaldi@gmail.com, [3]arispw@gmail.com , [4]eko@uksw.edu

**: Penulis korenspondensi* (*corresponding author*)

Article's Information / Informasi Artikel
Received: January 2022
Revised: May 2022
Accepted: June 2022
Published: June 2022

Abstract

Purpose: This study aims to determine the efforts to minimize the occurrence of risks in enterprise systems and how far the framework is applied to an organization, as well as what steps must be applied in anticipation of it.
Design/methodology/approach: This study uses a systematic review research method of literature published by international journals in the period 2016 to 2021 which is subscribed to by Diponegoro University.
Findings/result: Most of the selected journals stated that in an effort to secure enterprise systems in an organization, they really consider several aspects in it, especially in terms of cost which is one of the biggest considerations in it, besides that support from policy makers must be needed to make guidelines in implementing framework (framework) regarding the limitations of Authentication access and interaction on a system.
Originality/value/state of the art: the method applied will focus on discussing the realm of enterprise systems, specifically discussing framework management in an effort to minimize risks to enterprise systems.

Abstrak

Tujuan: Penelitian ini bertujuan untuk mengetahui upaya dalam meminimalisir terjadinya resiko pada sistem enterprise dan seberapa jauh framework diterapkan pada suatu organisasi, serta langkah apa saja yang harus diterapkan dalam antisipasi tersebut.

Keywords: Enterprise System Management, Enterprise System Security, framework ERP System, Information Security

Kata kunci: *Enterprise System*

Management, Enterprise System Security, framework ERP System, Information Security

Perancangan/metode/pendekatan: Penelitian ini menggunakan metode penelitian tinjauan sistematis terhadap literatur yang diterbitkan oleh jurnal Internasional pada periode tahun 2016 hingga tahun 2021 yang dilanggan oleh Universitas Diponegoro.
Hasil: Sebagian besar jurnal terpilih menyebutkan bahwa dalam upaya melakukan pengamanan pada sistem enterprise dalam suatu organisasi sangat mempertimbangkan mengenai beberapa aspek di dalamnya, terutama dalam hal biaya yang menjadi salahsau pertimbangan terbesar didalamnya, disamping itu harus diperlukan dukungan dari pembuat kebijakan untuk membuat pedoman dalam menerapkan kerangka kerja (*framework*) mengenai batasan *Autentifikasi* akses dan interaksi pada suatu sistem.
Keaslian/ *state of the art*: pada metode yang diterpkan tersebut akan berfokus pada pembahasan ranah sistem enterprise dengan spesifik membahas mengenai pengelolaan framework dalam upaya meminimalisir risiko pada sistem enterprise.

1. Pendahuluan

Perkembangan teknologi informasi yang terjadi saat ini memiliki pengaruh terhadap banyak hal baik kehidupan masyarakat maupun organisasi. Organisasi atau perusahaan menggunakan atau menerapkan teknologi informasi untuk mendukung kinerja pengambilan keputusan yang lebih efektif dan efisien dalam mencapai tujuan dari proses bisnisnya. Salah satu penerapan teknologi informasi untuk mendukung kinerja organisasi yaitu *Enterprise Resource Planning* (ERP). ERP merupakan suatu sistem terintegrasi dengan tujuan untuk menyederhanakan proses bisnis yang dimiliki oleh organisasi agar lebih efektif dan efisien dengan dukungan dari penerapan teknologi informasi agar dapat menghasilkan informasi untuk mendukung kinerja dari sebuah organisasi [1]. Fungsi dari ERP yaitu melakukan integrasi antara proses-proses bisnis yang terdapat di organisasi atau dapat disebut juga sebagai integrasi antara proses yang dimulainya produk baru berupa bahan mentah sampai dengan produk tersebut menjadi sebuah produk yang siap dipasarkan ke pasaran [2].

Sistem yang dapat diakses dengan ketersediaan yang tinggi saat ini dibutuhkan, keterbukaan dan terdistribusi pasti sudah menjadi keharusan untuk sistem yang terintegrasi. Manajemen keamanan sistem informasi dapat mengurangi terjadinya penyimpangan hak akses oleh pihak tertentu dan pernyalahgunaan data dan informasi sebuah organisasi atau perusahaan. Sasaran keamanan komputer antara lain adalah sebagai perlindungan terhadap informasi. Komponen dari rencana keamanan meliputi: kebijakan, standard dan prosedur keamanan informasi (*policy*), kontrol pengelolaan Sumber Daya Manusia (SDM) untuk keamanan informasi (*people*), dan kontrol teknologi keamanan informasi (*technology*).

Kerahasiaan pribadi (*privacy*) adalah kemampuan satu atau sekelompok individu untuk mempertahankan kehidupan dan urusan personalnya dari publik, atau untuk mengontrol arus informasi mengenai diri mereka. Privasi kadang dihubungkan dengan anonimitas walaupun

ISSN: 1829-667X / E-ISSN: 2460-9021
DOI:10.31515/telematika.v19i2.6534

anonimitas terutama lebih dihargai oleh orang yang dikenal publik. Privasi dapat dianggap sebagai suatu aspek dari keamanan. Kejahatan Komputer adalah perbuatan melawan hukum yang dilakukan memakai komputer sebagai sarana/alat atau komputer sebagai objek, baik untuk memperoleh keuntungan ataupun tidak, dengan merugikan pihak lain. Kejahatan komputer yang diatur dalam UU ITE diatur dalam Bab VII tentang perbuatan dilarang. Perbuatan-perbuatan tersebut dikategorikan

menjadi beberapa kelompok yaitu:

1. Akses tidak sah

2. Penyadapan atau intersepsi tidak sah

3. Gangguan terhadap data komputer.

Kejahatan yang berhubungan erat dengan penggunaan teknologi yang berbasis utama komputer dan jaringan telekomunikasi ini dalam beberapa literatur dan prakteknya dikelompokkan

dalam beberapa bentuk, antara lain:

1. *Unauthorized Acces Computer Sistem and Service*, kejahatan yang dilakukan dengan memasuki/menyusup ke dalam suatu sistem jaringan komputer secara tidak sah, tanpa ijin atau tanpa sepengetahuan dari pemilik sistem jaringan komputer yang dimasukinya.

2. *Contents*, Merupakan kejahatan dengan menggunakan data atau informasi ke internet tentang suatu hal yang tidak benar, tidak etis, dan dapat dianggap melanggar hokum atau mengganggu ketertiban umum.

3. *Data Forgery*, Merupakan kejahatan dengan memalsukan data pada dokumen-dokumen penting yang tersimpan sebagai scriptless document melalui internet.

4. *Cyber Espionage*, Merupakan kejahatan yang memanfaatkan jaringan internet untuk melakukan kegiatan mata-mata terhadap pihak lain, dengan memasuki sistem jaringan komputer pihak sasaran.

5. *Cyber Sabotage and Extortion*, Kejahatan ini dilakukan dengan

membuat gangguan, perusakan atau penghancuran terhadap suatu data, program komputer atau sistem jaringan komputer yang terhubung dengan internet.

6. Offense Against Intellectual Property, Kejahatan ini ditujukan terhadap hak atas kekayaan intelektual yang dimiliki pihak lain di internet. Contoh, peniruan tampilan pada web page suatu situs milik orang lain secara ilegal, penyiaran suatu informasi di internet yang ternyata merupakan informasi rahasia dagang orang lain dan sebagainya Inti dari keamanan komputer adalah melindungi komputer dan jaringannya dengan tujuan mengamankan informasi yang berada di dalamnya. Keamanan komputer sendiri meliputi beberapa aspek, antara lain:

1. *Authentication*, penerima informasi dapat memastikan keaslian pesan, bahwa pesan itu datang dari orang yang dimintai informasi. Dengan kata lain, informasi itu benar- benar datang dari orang yang dikehendaki.

2. *Integrity*, keaslian pesan yang dikirim melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi orang yang tidak berhak.

3. *Non –repudiation*, merupakan hal yang berhubungan dengan si-pengirim. Pengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebut.

4. *Authority*, informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya.

5. *Confidentiality*, merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.

6. *Privacy*, lebih ke arah data-data yang bersifat pribadi.

7. *Availability*, aspek availabilitas berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi.

8. *Access Control*, aspek ini berhubungan dengan cara pengaturan akses ke informasi. Hal ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses seringkali dilakukan dengan menggunakan kombinasi user id dan password ataupun dengan mekanisme lain. Keamanan komputer memberikan persyaratan terhadap komputer yang berbeda dari kebanyakan persyaratan sistem karena sering kali berbentuk pembatasan terhadap apa yang tidak boleh dilakukan komputer. Ini membuat keamanan komputer menjadi lebih menantang karena sudah cukup sulit untuk membuat program komputer melakukan segala apa yang sudah dirancang untuk dilakukan dengan benar. Persyaratan negatif juga sukar untuk dipenuhi dan membutuhkan pengujian mendalam untuk verifikasinya, yang tidak praktis bagi kebanyakan program komputer.

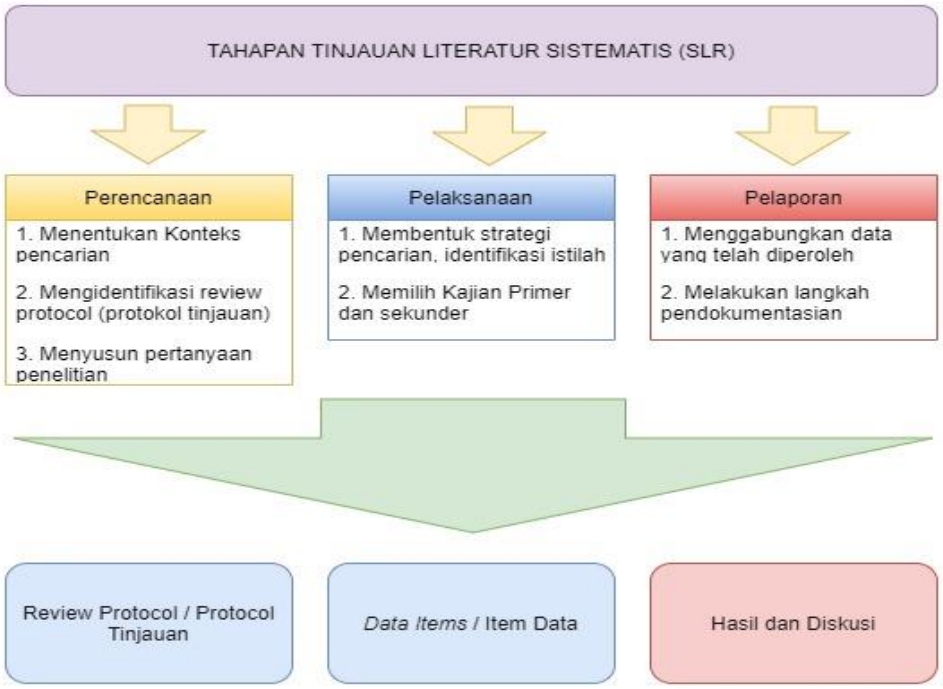
Aspek keamanan informasi meliputi sepuluh aspek diantaranya: kebijakan keamanan, pengorganisasian keamanan, klasisfikasi dan *control asset*, pengamanan personil, keamanan fisik dan lingkungan, komunikasi dan manajemen operasi, pengontrolan akses, pengembangan dan pemeliharaan sistem, menejemn kelangsungan bisnis, kesuaian.

Hal ini berarti, bahwa dari banyaknya penelitian sebelumnya yang telah dilakukan untuk mengetahui sejauh mana *framework* yang diterapkan pada berbagai macam organisasi dalam upaya pengelolaan keamanan sistem enterprise di organisasi tersebut. Atas dasar inilah, Maka penelitian ini bertujuan untuk mengetahui upaya dalam meminimalisir terjadinya resiko pada sistem enterprise dan seberapa jauh *framework* diterapkan pada suatu organisasi, serta langkah apa saja yang harus diterapkan dalam antisipasi tersebut serta dapat mejadi dasar bagi pengambilan keputusan untuk kepentingan masa depan yang lebih baik dengan menggunakan metode tinjauan literatur sistematis dikarenakan mengacu pada aspen peninjauan penelitian-penelitian sebelumnya.

2. Metode

Pada Penelitian ini menerapkan metode penelitian tinjauan pustaka atau lebih familiar disebut dengan *systematic literature review* (SLR). Tahapan yang terdapat dalam metode SLR tersebut disederhanakan oleh Adrian, Abdullah, Atan, & Jusoh (2016) sehingga menjadi terdiri dari tiga tahapan yang mencakup perencanaan, pelaksanaan, dan pembuatan laporan seperti yang ditampilkan pada gambar dibawah ini:

ISSN: 1829-667X / E-ISSN: 2460-9021
DOI:10.31515/telematika.v19i2.6534



Gambar 1. Metodologi Penelitian SLR

2.1. Perencanaan

Systematic literature review (SLR) merupakan metode yang akan diterpkan pada tahapan perencanaan dalam penelitian ini. Penelitian ini dilakukan dengan tujuan untuk mengetahui pengelolaan keamanan ERP pada suatu perusahaan, dengan demikian untuk mencapai tujuan tersebut, maka dapat dirumuskan masalah sebagai berikut:

Tabel 1. Cakupan dalam penyusunan pertanyaan penelitian

No	Kriteria	Cakupan
1	Populasi	Pengelolaan Sistem Enterprise / *Framework* keamanan pada Sistem enterprise / Resiko dalam Sistem Enterprise
2	Intervensi	Batasan penelitian berfokus pada keamanan pada Sistem Enterprise dalam suatu jurnal yang diterbitkan oleh publisher
3	Komparasi	*Tidak tersedia*
4	Hasil	Pengelolaan *framework* untuk meminimalisir resiko dalam melindungi Sistem Enterprise
4	Konteks	Tinjauan literatur mengenai faktor keamanan dan pengelolaan Sistem Enterprise

Pada Tabel 1 diatas kriteria pertanyaan ini disusun berdasarkan cakupan pada point tabel diatas yang berdasarkan merujuk pada PICOC (*Population, Intervention, Comparison, Outcomes and Context*) (2006, Petticrew & Robert). Berdasarkan kriteria dan cakupan tersebut

pada Tabel 1, ada tiga pertanyaan penelitian (PP) yang disusun, yaitu:

a. PP1: Apakah dalam mengelola keamanan sistem enterprise sering kali menggunakan *Framework* dalam penerapannya?

b. PP2: Resiko apa saja yang mempengaruhi keamanan sistem Enterprise?
c. PP3: Apa saja langkah yang dilakukan dalam melindungi Sistem Enterprise?

Setelah tersusun point-point diatas akan menjadi *protocol* tinjauan dan sebagai acuan dalam melangkah ketahapan selanjutnya.

2.2. Pelaksanaan

Pada tahapan pelaksanaan, strategi pencarian akan dilakukan untuk memasukkan perumusan istilah pencarian, dan mencari sumber data dari *database online*, merumuskan kriteria inklusi dan ekslusi.

a. Istilah Pencarian

Dalam melakukan pencarian mengenai penelitian ini, istilah pencarian yang digunakan adalah istilah yang berasal dari bahasa Inggris dan merupakan gabungan kata-kata kunci dengan menggunakan operator *Boolean* AND sebagai berikut: Maintaining AND authenticity AND archives AND "digital age"

b. Sumber-sumber Literatur

Sumber-sumber literatur yang digunakan dalam tinjauan ini dengan menggunakan fasilitas pencarian *E-Resources UNDIP* berdasarkan pada fitur portal SSO UNDIP (*Single Sign On*) akses mahasiswa oleh Universitas Diponegoro dimana terdapat 3 sumber referensi terpercaya sebagai acuan dalam penelitian ini, yaitu: *Scopus, Springer Link, Science Direct.* Beberapa artikel dikutip menggunakan teknik pencarian bola salju (*snowballing technique search*) melalui database elektronik. Sumber-sumber yang relevan kemudian disimpan dalam alat manajemen referensi untuk dilakukan pemilihan literatur yang dikutip dalam tinjauan ini dengan mempertimbangkan publikasi yang hanya diterbitkan pada periode tahun 2016 hingga akhir 2021.

c. Kriteria Inklusi dan Eksklusi

Kriteria inklusi (penyertaan) dan eksklusi (pengecualian) digunakan untuk mengeluarkan artikel atau jurnal yang tidak relevan dengan jawaban pertanyaan penelitian.

d. Penilaian Kualitas Penelitian

Penilaian kualitas dirumuskan untuk mengevaluasi kelengkapan daripada jurnal maupun artikel prosiding yang akan di evaluasi menggunakan beberapa kriteria inklusi dan eksklusi serta menguntungkan ekstraksi data, lalu pertanyaan yang akan dimasukkan dalam evaluasi sebagai berikut, yang dalam satu variable nya terdapat 3 atau 2 jawaban dan untuk nilai maksimum pada tiap jutnalnya adalah 10. (1)

3. Hasil dan Pembahasan

Berdasarkan kriteria tersebut maka didapatkan hasil dengan jumlah paper yang bervariatif dalam jumplahnya di setiap *publisher*. Setelah memilah berdasarkan kata kunci yang telah ada dapat dimasukkan lai kedalam beberapa kreteria eksklusi dan inklusi dalam hasil pencarian yang sudah ada, sehingga akan lebih spesifik dari hasil beberapa jurnal yang masuk dalam kriteria dalam penelitian ini, antara lain sebagai berikut:

Tabel 2. Penentuan kriteria Inklusi dan Eksklusi

No	***Inklusi* / Penyertaan**	***Eksklusi* / Pengecualian**
1	Semua Literatur yang termasuk kedalam kategori artikel jurnal	Semua literature yang **tidak** termasuk dalam kategori artikel jurnal
2	Semua literature yang diterbitkan periode tahun 2016 - 2021	Semua literature yang diterbitkan **< 2016 dan atau (AND, OR)** di luar cakupan
3	Semua literature yang dapat diakses full	Semua litaratur yang **tidak** dapat diakses full
4	Semua litaratur yang diterbitkan dalam Bahasa Inggris	Semua literatur yang **tidak** menggunakan Bahasa Inggris
5	Semua literatur dalam ranah disiplin ilmu *Computer Science*	Semua literatur yang **tidak** dalam ranah disiplin Ilmu *Computer Science*

Setelah tiap jurnal dimasukkan langkah seperti tabel 2, barulah masuk di langkah selanjutnya yakni menentukan kualifikasi penilaian di tiap jurnalnya, penilaian tersebut dapat dijabarkan kedalam Tabel 3 dibawah ini.

Tabel 3. Kriteria penilaian kualitas penelitian

ID Kualitas	**Pertanyaan penilaian kualitas**	**Jawaban**	**Range Nilai**
P1	Apakah dalam jurnal atau artikel prosiding terdapat penjelasan yang cukup terhadap tujuan dan sasaran dari penelitian ?	Sebagian / Ya / Tidak	**Ya = 8 – 10** **Sebagian 7 - 5** **Tidak < 5**
P2	Apakah jurnal atau artikel prosiding tersebut membahas tentang keamanan Sistem Enterprise? (termasuk framework, dan teknik keamanannya)	Sebagian / Ya / Tidak	
P3	Apakah jurnal atau artikel prosiding tersebut membahas tentang keamanan information security ? (termasuk management didalamnya)	Ya / Tidak	
P4	Apakah jurnal atau artikel prosiding tersebut memberikan solusi dalam sisi keamanannya	Ya / Tidak	
	Total		10

Setelah menerapkan tahapan dalam metode SLR yang digunakan dalam penelitian ini, seperti Gambar 1, pencarian digital dilakukan pada sumber terpercaya dan serta dilakukan penyeleksian proses berdasarkan judul, yang menggunakan beberapa kata kunci yaitu *Enterprise System Management, Enterprise System Security, framework ERP System, Information Security*. Literatur yang diperoleh dari hasil pencarian yaitu sebagai berikut:

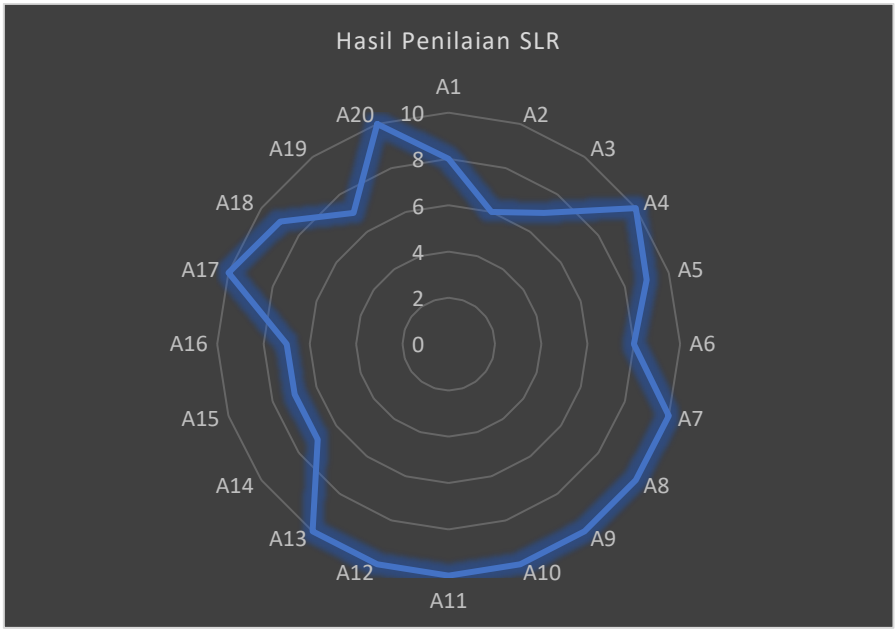
ISSN: 1829-667X / E-ISSN: 2460-9021
DOI:10.31515/telematika.v19i2.6534

Tabel 4. Hasil Pencarian Berdasarkan keyword (kata kunci)

no	Keywords	Sumber		
		Scopus	**Science Direct**	**Springer Link**
1	*Information Security*	2,522	1,622	47,921
2	*Enterprise system management*	748	419	8,606
3	*Enterprise system security*	310	272	5,274
4	*Framework ERP System*	34	53	727
Total		3,614	2,366	62,528

3.1. Pembahasan

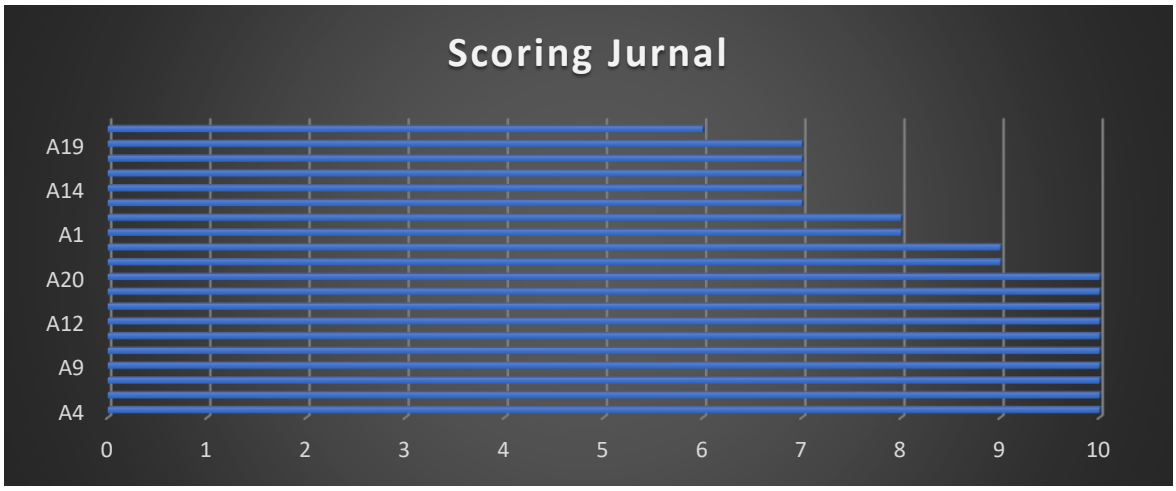
Setelah melakukan penelusuran dan pencarian sumber-sumber informasi berupa jurnal dan artikel prosiding dari beberapa sumber terpercaya dan relevan maka didapatkan hasil dari penilaian di tiap jurnal terpilih dari ketiga sumber bereputasi tersebut, berikut hasil yang diperoleh berkaitan dengan pertanyaan penelitian ini yang sudah disampaikan pada bagian sebelumnya. Jawaban dari kriteria pertanyaan ditampilkan pada Gambar 2.



Gambar 2. Hasil Penilaian penyaringan artikel terpilih

Gambar 2 menjelaskan dimana tiap jurnal atau artikel prosiding terpilih akan mendapatkan hasil penilaian dari beberapa penyaringan dan review sesuai dengan seleksi di tiap tahapannya berikut detail bibliografi dan hasil penilaian secara rinci pada pengambilan data terpilih diperlihatkan pada Gambar 3.

ISSN: 1829-667X / E-ISSN: 2460-9021
DOI:10.31515/telematika.v19i2.6534



Gambar 3. Grafik Hasil Penilaian Artikel terpilih

Tabel 5. Rincian bibliografis dan hasil penelitian jurnal dan artikel prosiding

Kode	Penulis	Tahun Terbit	Judul	Nama Jurnal	Nilai
A1	Hankin, P., Almanei, M., & Salonitis, K.	2021	An ISM analysis of the critical success factors in ERP implementation.	Advances in Transdisciplinary Engineering	8
A2	Freitag, C., Berners-Lee, M., Widdicks, K., Knowles, B., Blair, G. S., & Friday, A.	2021	The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations.	Patterns,	6
A3	Hurni, T., Huber, T. L., & Dibbern, J.	2021	Power dynamics in software platform ecosystems.	In Information Systems Journal	7
A4	Rožman, N., Diaci, J., & Corn, M.	2021	Scalable framework for blockchain-based shared manufacturing.	obotics and Computer-Integrated Manufacturing	10
A5	Fan, Z., & Guan, Y. peng.	2021	A deep learning framework for face verification without alignment.	Journal of Real-Time Image Processing	9
A6	Ssegawa, J. K., & Muzinda, M.	2021	Feasibility assessment framework (FAF): A systematic and objective approach for assessing the viability of a project.	Procedia Computer Science	8
A7	Ben Dhaou Dakhli, S.	2021	Architectural deviations and inconsistencies management: A framework based on information systems urbanization.	Procedia Computer Science	10
A8	Reddy, S. S. T., & Shyam, G. K.	2020	A machine learning based attack detection and mitigation using a secure SaaS framework.	Journal of King Saud University - Computer and Information Sciences	10

A9	Shrestha, M., Johansen, C., Noll, J., & Roverso, D.	2020	A Methodology for Security Classification applied to Smart Grid Infrastructures.	International Journal of Critical Infrastructure Protection	10
A10	Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I.	2020	Digital forensics framework for reviewing and investigating cyber attacks.	Array	10
A11	Dewi, R. S.	2019	Maturity level assessment for ERP systems investment using val IT framework.	Procedia Computer Science	10
A12	Kohli, M.	2018	Using machine learning algorithms on data residing in SAP ERP application to predict equipment failures.	International Journal of Engineering and Technology(UAE)	10
A13	Olson, D. L., Johansson, B., & De Carvalho, R. A.	2018	Open source ERP business model framework.	Robotics and Computer-Integrated Manufacturing	10
A14	B, K. M., Nagami, T., Sugase, Y., & Takemura, A.	2017	Assessing Organization-System Fit in ERP Selection Procedures – A Literature Review	Development and Multimodality	7
A15	Scholtz, B. M., Kapeso, M., & de Villiers, M. R. R	2017	The usefulness and ease of use of a mobile simulation application for learning of ERP systems	South African Computer Journal	7
A16	Fernandez, D., Zainol, Z., & Ahmad, H.	2017	The impacts of ERP systems on public sector organizations	Procedia Computer Science	7
A17	Oseni, T., Foster, S., Rahim, M., & Smith, S. P.	2017	A framework for ERP post-implementation amendments: A literature analysis	Australasian Journal of Information Systems	10
A18	Chatzoglou, P., Fragidis, L., Chatzoudes, D., & Symeonidis, S.	2016	Critical success factors for ERP implementation in SMEs.	Proceedings of the 2016 Federated Conference on Computer Science and Information Systems	9
A19	Ruivo, P., Rodrigues, J., Johansson, B., Oliveira, T., & Rebelo, J.	2016	Using TOE and RBV Theories to Define a Theoretical Model to Assess ERP Value Across Iberian MANUFACTURING and Services SMEs	Procedia Computer Science	7
A20	Jayawickrama, U., Liu, S., & Hudson Smith, M.	2016	Empirical evidence of an integrative knowledge competence framework for ERP systems implementation in UK industries.	Computers in Industry	10

4. Kesimpulan dan Saran

Sebagian besar dalam jurnal maupun artikel prosiding yang membahas mengenai keamanan sistem enterprise termasuk didalamnya *framework* yang diterapkan pada suatu organisasi tertentu dan juga memberikan cara dan metode baru untuk dapat mengembangkan keamanan suatu ERP yang sudah berjalan sangat diperlukan pengambilan suatu kebijakan yang diambil oleh Top menegement, serta mempertimbangkan dampak atau kerugian-kerugian yang timbul dari keseluruhan aspek yang nantinya dapat dipetakan kedalam kerangka kerja.

Dengan demikian sudah menjadi hal yang mendasar apabila adanya keamanan pada setiap transaksi atau kegiatan dibutuhkan sebagai berikut:

1. *autentifikasi* pada setiap posisi karyawan pada suatu organisasi, tentunya dengan yang berlapis menjadi salah satu bagian terpenting dan mendasar pada keamanan di dalam ERP yang sudah ada pada perusahaan atau organisasi.
2. Dalam sisi *Networking* pada sistem ERP akan lebih secure jika pada akses protocolnya juga dilengkapi VPN sebagai langkah keamanan berlapis, sehingga lebih terjaga pada sisi jaringan.
3. Jika pada sisi pengelolaan SDM pada suatu organisasi pada individu yang berhubungan langsung dengan sistem terutama pada bagian TI harus mempunyai ikatan yang lebih terhadap suatu organisasi dikarenakan seluruh data yang bersifat vital pada organisasi juga ikut berperan didalamnya.

Terlihat pada Gambar 3, dimana hasil penilaian dari literature yang didapatkan pada kode *paper* A4, A7, A8, A9, A10, A11, A12, A13, A17, A20 mendapatkan point 10, kemudian pada rentan penilaian score 9 – 7 dengan kode *paper* A5, A18, A1, A6, A3, A14, A15, A16, A19 sementara untuk kode *paper* A2 mendapatkan nilai 6 dengan kriteria mengacu pada Tabel 3.

Daftar Pustaka

[1] P. Hofmann, "ERP is dead, long live ERP," *IEEE Internet Comput.*, vol. 12, no. 4, pp. 84–88, 2008, doi: 10.1109/MIC.2008.78.

[2] T. Q. Ferbia, "Analisis Penggunaan Sistem ERP untuk Transformasi Proses Bisnis Studi Kasus: Supermarket Bangunan dan Furniture," *JUTIM (Jurnal Tek. Inform. Musirawas)*, vol. 3, no. 2, pp. 74–82, 2018, doi: 10.32767/jutim.v3i2.313.

[3] Hankin, P., Almanei, M., & Salonitis, K. (2021). An ISM analysis of the critical success factors in ERP implementation. Paper presented at the *Advances in Transdisciplinary Engineering, , 15* 383-389. doi:10.3233/ATDE210066

[4] Pekša, J. and Grabis, J. (2018). Integration of Decision-Making Components in ERP Systems. In *Proceedings of the 20th International Conference on Enterprise Information Systems - Volume 1: ICEIS*, ISBN 978-989-758-298-1; ISSN 2184-4992, pages 183-189. DOI: 10.5220/0006779601830189

[5] Russman, R.; Seymour, L. and van Belle, J. (2017). Integrating BI Information into ERP

ISSN: 1829-667X / E-ISSN: 2460-9021
DOI:10.31515/telematika.v19i2.6534

Processes - Describing Enablers. In *Proceedings of the 19th International Conference on Enterprise Information Systems - Volume 3: ICEIS*, ISBN 978-989-758-247-9; ISSN 2184-4992, pages 241-248. DOI: 10.5220/0006292302410248

[6] Catherine, C., & Abdurachman, E. (2018). ERP system adoption analysis using TOE framework in permata hijau group (PHG) medan. *International Journal of Enterprise Information Systems*, *14*(3), 91-105. doi:10.4018/IJEIS.2018070105

[7] Tamara Babaian, Jennifer Xu & Wendy Lucas | Ken Peffers (Guest Editor), Tuure Tuunanen (Guest Editor) & Björn Niehaves (Guest Editor) (2018) ERP prototype with built-in task and process support, European Journal of Information Systems, 27:2, 189-206, DOI: 10.1057/s41303-017-0060-3

[8] G. Gallardo, J. Hernantes and N. Serrano, "Designing SaaS for Enterprise Adoption Based on Task, Company, and Value-Chain Context," in IEEE Internet Computing, vol. 22, no. 4, pp. 37-45, Jul./Aug. 2018, doi: 10.1109/MIC.2018.043051463.

[9] Kohli, M. (2018). Using machine learning algorithms on data residing in SAP ERP application to predict equipment failures. *International Journal of Engineering and Technology(UAE)*, *7*(2), 312–319. https://doi.org/10.14419/ijet.v7i2.28.12952

[10] Scholtz, B. M., Kapeso, M., & de Villiers, M. R. R. (2017). The usefulness and ease of use of a mobile simulation application for learning of ERP systems. *South African Computer Journal*, *29*(2), 87–105. https://doi.org/10.18489/sacj.v29i2.475

[11] Fernandez, D., Zainol, Z., & Ahmad, H. (2017). The impacts of ERP systems on public sector organizations. *Procedia Computer Science*, *111*, 31–36. https://doi.org/10.1016/j.procs.2017.06.006

[12] Freitag, C., Berners-Lee, M., Widdicks, K., Knowles, B., Blair, G. S., & Friday, A. (2021). The real climate and transformative impact of ICT: A critique of estimates, trends, and regulations. *Patterns*, *2*(9), 100340. https://doi.org/10.1016/j.patter.2021.100340

[13] Rožman, N., Diaci, J., & Corn, M. (2021). Scalable framework for blockchain-based shared manufacturing. *Robotics and Computer-Integrated Manufacturing*, *71*, 102139. https://doi.org/10.1016/j.rcim.2021.102139

[14] Hurni, T., Huber, T. L., & Dibbern, J. (2021). Power dynamics in software platform ecosystems. In *Information Systems Journal*. https://doi.org/10.1111/isj.12356

[15] Olson, D. L., Johansson, B., & De Carvalho, R. A. (2018). Open source ERP business model framework. *Robotics and Computer-Integrated Manufacturing*, *50*(October 2015), 30–36. https://doi.org/10.1016/j.rcim.2015.09.007

[16] Dewi, R. S. (2019). Maturity level assessment for ERP systems investment using val IT framework. *Procedia Computer Science*, *161*, 250–257. https://doi.org/10.1016/j.procs.2019.11.121

[17] Krumbholz, M., Arthur, N., & Maiden, M. (2000). How culture might impact on the implementation of enterprise resource planning packages. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1789*, 279–293. https://doi.org/10.1007/3-540-45140-4_19

[18] Ssegawa, J. K., & Muzinda, M. (2021). Feasibility assessment framework (FAF): A systematic and objective approach for assessing the viability of a project. *Procedia Computer Science*, *181*(2019), 377–385. https://doi.org/10.1016/j.procs.2021.01.180

[19] Jayawickrama, U., Liu, S., & Hudson Smith, M. (2016). Empirical evidence of an integrative knowledge competence framework for ERP systems implementation in UK industries. *Computers in Industry*, *82*, 205–223. https://doi.org/10.1016/j.compind.2016.07.005

[20] Dimitriadis, A., Ivezic, N., Kulvatunyou, B., & Mavridis, I. (2020). D4I - Digital forensics framework for reviewing and investigating cyber attacks. *Array*, *5*(October 2019), 100015. https://doi.org/10.1016/j.array.2019.100015

[21] Chatzoglou, P., Fragidis, L., Chatzoudes, D., & Symeonidis, S. (2016). Critical success factors for ERP implementation in SMEs. *Proceedings of the 2016 Federated Conference on Computer Science and Information Systems, FedCSIS 2016*, *8*, 1243–1252. https://doi.org/10.15439/2016F37

[22] Hankin, P., Almanei, M., & Salonitis, K. (2021). An ISM analysis of the critical success factors in ERP implementation. *Advances in Transdisciplinary Engineering*, *15*, 383–389. https://doi.org/10.3233/ATDE210066

[23] B, K. M., Nagami, T., Sugase, Y., & Takemura, A. (2017). *Human-Computer Interaction. User Interface Design, Development and Multimodality*. *10271*, 593–608. https://doi.org/10.1007/978-3-319-58071-5

[25] Oseni, T., Foster, S., Rahim, M., & Smith, S. P. (2017). A framework for ERP post-implementation amendments: A literature analysis. *Australasian Journal of Information Systems*, *21*, 1–21. https://doi.org/10.3127/ajis.v21i0.1268

[24] Ben Dhaou Dakhli, S. (2021). Architectural deviations and inconsistencies management: A framework based on information systems urbanization. *Procedia Computer Science*, *181*(2019), 1122–1130. https://doi.org/10.1016/j.procs.2021.01.309

ISSN: 1829-667X / E-ISSN: 2460-9021
DOI:10.31515/telematika.v19i2.6534

[26] Fan, Z., & Guan, Y. peng. (2021). A deep learning framework for face verification without alignment. *Journal of Real-Time Image Processing*, *18*(4), 999–1009. https://doi.org/10.1007/s11554-020-01037-z

[27] Shrestha, M., Johansen, C., Noll, J., & Roverso, D. (2020). A Methodology for Security Classification applied to Smart Grid Infrastructures. *International Journal of Critical Infrastructure Protection*, *28*, 100342. https://doi.org/10.1016/j.ijcip.2020.100342

[28] Reddy, S. S. T., & Shyam, G. K. (2020). A machine learning based attack detection and mitigation using a secure SaaS framework. *Journal of King Saud University - Computer and Information Sciences*, *xxxx*. https://doi.org/10.1016/j.jksuci.2020.10.005