ANALISIS ARCHITECTURE TEKNOLOGI MENGGUNAKAN SABSA UNTUK MENINGKATKAN KEAMANAN DI RUMAH SAKIT QUEEN LATIFA

(ANALYSIS OF ARCHITECTURE TECHNOLOGY USING SABSA TO IMPROVE SECURITY at QUEEN LATIFA HOSPITAL)

Alvian Trias Kurniawan[1)], Bambang Soedijono WA[2)], dan Asro Nasiri[3)]
[1,2,3)] Magister Teknik Informatika,
Universitas Amikom Yogyakarta
e-mail: alvian.1322@students.amikom.ac.id[1)], bambang.s@email.com[2)], asro@amikom.ac.id[3)]

ABSTRAK

Penggunaan Internet secara luas dan meningkatnya ketergantungan pada jaringan packet-switched publik untuk e-commerce, telecommuting dll, telah mengakibatkan peningkatan serangan berbahaya pada security & malware di perusahaan. Bisnis pada bidang kesehatan menggunakan jaringan informasi kesehatan dan teknologi informasi yang bekerja sama untuk meningkatkan keselamatan pasien, meningkatkan efektivitas pengobatan, dan meningkatkan efisiensi. Tujuan dari penelitian ini adalah untuk mengatasi masalah keamanan dan privasi dengan Bisnis di bidang kesehatan atau rekam medis yang terintegrasi. Sistem keamanan yang diterapkan pada beberapa Rumah Sakit memerlukan adanya peningkatan dan peninjauan secara berkala demi kenyamanan dan keamanan pihak Rumah Sakit dengan Pasien. Penggunaan framework SABSA pada penelitian ini berfokus pada keamanan TI yang dapat diterapkan di berbagai sektor industri dan organisasi sebagai pengembangan EISA. Paper ini membahas analisa dan meningkatkan EISA melalui pengintegrasian arsitektur keamanan informasi kedalam EA secara sinergis untuk meningkatkan keamanan data dan informasi. Untuk implementasinya menggunakan framework TOGAF untuk Enterprise Architecture, sedangkan untuk arsitektur keamanan informasi akan menggunakan framework SABSA.

***Kata kunci**:* SABSA, TOGAF, *framework*, EISA, *Enterprise Architecture.*

ABSTRACT

Widespread use of Internet and increasing reliance on public packet-switched networks for e-commerce, telecommuting etc., has resulted in an increase in malicious attacks on security & malware in enterprises. Businesses in the healthcare sector use health information networks and information technology that work together to improve patient safety, increase treatment effectiveness, and increase efficiency. The purpose of this study is to address security and privacy concerns with integrated healthcare or medical records businesses. The security system implemented in several hospitals requires periodic improvements and reviews for the comfort and safety of the hospital and the patient. The use of the SABSA framework in this study focuses on IT security that can be applied in various industrial and organizational sectors as an EISA development. This paper discusses analyzing and improving EISA through synergistic integration of information security architecture into EA to improve data and information security. For its implementation using the TOGAF framework for Enterprise Architecture, while for information security architecture it will use the SABSA framework.

***Keyword**:* SABSA, TOGAF, *framework*, EISA, *Enterprise Architecture.*

I. PENDAHULUAN

Penggunaan Internet secara luas dan meningkatnya ketergantungan pada jaringan packet-switched publik untuk e-commerce, telecommuting, dll, telah mengakibatkan peningkatan serangan berbahaya pada security dan malware di perusahaan. Oleh karena itu, kini banyak perusahaan yang berinvestasi dalam keamanan, karena dianggap sebagai faktor penting dan kritis bagi kelangsungan hidup suatu perusahaan, contohnya seperti rumah sakit yang harus menjaga informasi rekam medis dari pasien. Potensi bahaya besar, baik fisik maupun emosional, selalu ada dalam konteks kesehatan ketika teknologi informasi digunakan untuk membantu perawatan pasien. Sistem dasar keamanan informasi harus diikuti ketika mengembangkan kerahasiaan, integritas, aksesibilitas, dan akuntabilitas lingkungan klinis yang saling terintegrasi[1].

Sistem keamanan yang diterapkan pada beberapa Rumah Sakit seperti contoh Rumah Sakit Queen Latifa perlu adanya peningkatan dan peninjauan secara berkala demi kenyamanan dan keamanan pihak Rumah Sakit dengan pasien mengenai data rekam medis, karena adanya keterlibatan internet dalam integrasi data antar satu rumah sakit dengan pusat dan/atau cabang lainnya.

Penggunaan *framework* SABSA berfokus pada keamanan teknologi informasi yang dapat diterapkan di berbagai sektor industri dan organisasi sebagai pengembangan EISA *(Enterprise Information Security Architecture) dan information assurance* yang menyelaraskan antara keamanan TI dan strategi bisnis berdasarkan risk-driven, dan bertujuan untuk menghasilkan solusi infrastruktur yang aman, karena berfokus dari sudut pandang keamanan atau metodologi business-to-security. Maka, *framework* SABSA digunakan pada penelitian ini sebagai peningkatan dan peninjauan sistem keamanan integrasi data rekam medis pada pasien di Rumah Sakit Queen Latifa[2].

II. STUDI PUSTAKA

Beberapa penelitian terdahulu yang dijadikan acuan dan tinjauan pustaka pada penelitian ini diantaranya;

Penelitian tentang ringkasan model bisnis dan arsitektur keamanan pada framework SABSA dari semua sudut pandang. Penelitian tersebut mencakup resiko operasional dengan mengenali peluang dan ancaman serta proses pengembangan SABSA[3].

Selain itu, penelitian lainnya dilakukan guna meneliti tentang interoperabilitas dan lingkungan klinis yang saling terintegrasi (Integrated Clinical Environment/ ICE). Tujuan ICE adalah untuk meningkatkan keselamatan pasien, efisiensi pengobatan, dan efisiensi alur kerja daripada yang dapat dicapai dengan perangkat medis yang digunakan secara mandiri. Pada penelitian ini framework yang dipakai yaitu NIST dan konsep rekayasa privasi digunakan untuk menunjukkan bagaimana risiko privasi dan keamanan dapat ditangani di seluruh perusahaan klinis[1].

Penelitian lainnya menjelaskan dimensi berbeda dari arsitektur keamanan informasi yang memfasilitasi perusahaan untuk mengamankan akses layanan *cloud SaaS* bisnis yang diakses melalui *Smartphone* BYOD. Pada penelitian tersebut *framework* SABSA dijelaskan sesuai dengan framework arsitektur keamanan SABSA, yang terdiri dari perangkat keras, perangkat lunak dan komponen keamanan berorientasi layanan yang dapat mengurangi risiko tersebut ke tingkat yang dapat diterima[4].

Penelitian berikutnya bertujuan untuk mengevaluasi pengaruh adopsi kerangka kerja terintegrasi yang menggabungkan TOGAF dan SABSA pada SDLC dalam konteks perusahaan spin-off dalam hal efisiensi dan keamanan berbasis komputasi awan dan IASS. Berdasarkan pemetaan artefak SABSA ke fase TOGAF dapat memberikan hasil positif untuk peningkatan keamanan pada SDLC perusahaan spin-off[5].

Penelitian lainnya bertujuan untuk menentukan framework yang sesuai untuk perusahaan pada sistem keamananya. Terlepas dari metodologi atau framework yang digunakan, baik itu SABSA, COBIT atau TOGAF, arsitektur keamanan di perusahaan mana pun harus ditentukan berdasarkan risiko yang tersedia untuk perusahaan itu. karena pada dasarnya framework tersebut dapat menjamin keselarasan arsitektur yang ditentukan dengan tujuan dan sasaran bisnis[6].

Penelitian yang dilakukan untuk mengembangkan *Enterprise Security Framework* (ESF) untuk lembaga pemerintah Indonesia yang disebut SKK Migas (Satuan Kerja Khusus Pelaksana Kegiatan Usaha Hulu Minyak dan Gas Bumi). Kerangka kerja dikembangkan berdasarkan dua standar keamanan yaitu ISO 27000 dan SABSA. *Framework* keamanan yang dihasilkan mencakup 14 domain keamanan yang akan digunakan untuk mengontrol manajemen keamanan informasi di dalam institusi[7].

III. METODE PENELITIAN

Pada bagian di atas, masing-masing dari enam lapisan abstraksi horizontal model arsitektur (kontekstual, konseptual, logis, fisik, komponen dan manajemen layanan) telah diperiksa. Masing-masing bagian juga telah memperkenalkan serangkaian pemotongan vertikal melalui masing-masing lapisan horizontal ini, menjawab pertanyaan:

a) Apa yang coba dilakukan pada lapisan ini? – Aset yang akan dilindungi oleh arsitektur keamanan.
b) Mengapa kamu melakukannya? – Motivasi untuk ingin menerapkan keamanan, dinyatakan dalam istilah risiko.

c) Bagaimana mencoba melakukannya? – Proses dan fungsi yang diperlukan untuk mencapai keamanan.
d) Siapa yang terlibat? – Aspek keamanan orang dan organisasi.
e) Dimanakah melakukannya? – Lokasi di mana menerapkan keamanan Anda.
f) Kapankah melakukannya? – Aspek keamanan yang berhubungan dengan waktu.

Matriks SABSA juga menyediakan keterlacakan dua arah:

1. Kelengkapan: apakah setiap persyaratan bisnis telah terpenuhi? Lapisan dan matriks memungkinkan untuk melacak setiap kebutuhan hingga komponen yang memberikan solusi.

Gambar 1. Lapisan dan matriks Kelengkapan *(Completeness)*

2. Justifikasi Bisnis: apakah setiap komponen arsitektur diperlukan? Ketika seseorang bertanya 'Mengapa kita melakukannya dengan cara ini?' alasannya jelas dengan menelusuri kembali ke persyaratan bisnis yang mendorong solusi spesifik.

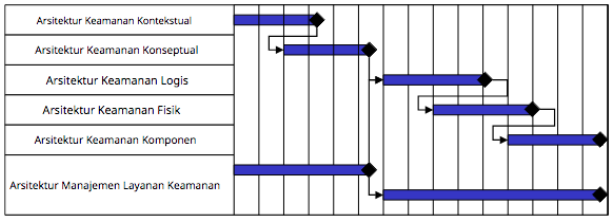
Gambar 2. Lapisan dan matriks Justifikasi Bisnis *(Business Justification)*.

Tabel 1. Matriks SABSA

	ASET (Apa)	MOTIVASI (Mengapa)	PROSES (Cara)	Orang yang)	LOKASI (Dimana)	WAKTU (Kapan)
KONTEKSTUAL ARSITEKTUR	Keputusan Bisnis Taksonomi dari Aset Bisnis, termasuk Tujuan & Tujuan	Resiko bisnis Peluang & Inventarisasi Ancaman	Proses bisnis inventarisasi operasional Proses	Bisnis pemerintahan organisasi Struktur & Perusahaan yang Diperluas	Geografi Bisnis inventarisasi Bangunan, Situs, wilayah, Yurisdiksi, dll.	Waktu bisnis Ketergantungan waktu bisnis tujuan
KONSEPTUAL ARSITEKTUR	Pengetahuan Bisnis & Strategi Risiko Atribut Bisnis Profil	Manajemen risiko Tujuan Pemberdayaan & Tujuan Kontrol; Arsitektur Kebijakan	Strategi untuk Jaminan Proses Proses pemetaan Kerangka; Arsitektur Strategi untuk TIK	Peran & tanggung jawab Pemilik, Penjaga Penyedia jasa & pelanggan	Kerangka Domain Domain Keamanan Konsep & Kerangka	Manajemen waktu Kerangka Risiko Sepanjang Hidup Pengelolaan Kerangka
LOGIS ARSITEKTUR	Aset Informasi Inventarisasi Informasi Aktiva	Manajemen risiko Kebijakan Kebijakan Domain	Peta Proses & Jasa Arus Informasi; Fungsional Transformasi; Arsitektur	Kerangka Skema Entitas; Profil Hak Istimewa	Peta Domain Definisi Domain; Antar domain asosiasi & interaksi	Kalender & Jadwal Mulai Waktu, Siklus Hidup & Tenggat waktu
FISIK ARSITEKTUR	Aset Data Kamus data &	Manajemen risiko Praktek Manajemen risiko Aturan & Prosedur	Proses Mekanisme Aplikasi; Sistem; Keamanan Mekanisme	Antarmuka Manusia Sistem; Mengakses Sistem kontrol	Infrastruktur TIK & jaringan	Pengolahan Jadwal Waktu & Urutan dari Proses dan Sesi
KOMPONEN ARSITEKTUR	Komponen TIK Produk TIK, termasuk Data Repositori dan Prosesor	Manajemen risiko Alat & Standar Alat Analisis Risiko; Register Risiko; Pemantauan Risiko dan Alat Pelaporan	Alat Proses & Standar Alat dan Protokol	Manajemen Personalia Alat & Standar Identitas Pekerjaan Deskripsi; Peran; Fungsi; Tindakan & Daftar Kontrol Akses	Alat Pencari & Standar Node, Alamat dan Pencari lainnya	Langkah Waktu & Alat Pengurutan Jadwal Waktu; Jam, Timer & Interupsi
MELAYANI PENGELOLAAN ARSITEKTUR	Pengiriman Layanan Pengelolaan jaminan dari operasional Kontinuitas & Keunggulan	Risiko operasional Pengelolaan Tugas beresiko; Pemantauan Risiko & Pelaporan; Perlakuan Risiko	Proses Pengiriman Pengelolaan Manajemen & Dukungan Sistem, Aplikasi & jasa	Personil Pengelolaan Akun Penyediaan; Pengguna Mendukung Pengelolaan	Manajemen dari Lingkungan Manajemen dari Bangunan, Situs, Platform & jaringan	Waktu & Performa Pengelolaan Manajemen dari Kalender dan Jadwal

Proses Pembangunan SABSA

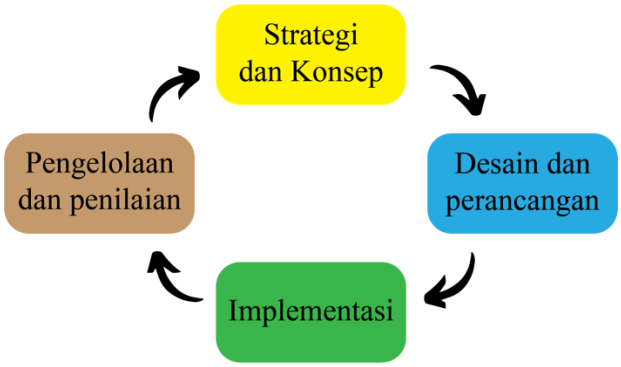
Model SABSA memberikan dasar untuk proses pengembangan arsitektur, karena jelas bahwa melalui pemahaman kebutuhan bisnis, arsitek dapat membuat visi awal. Proses pengembangan itu sendiri ditunjukkan, pada tingkat tinggi, pada gambar 2.



Gambar 3. Proses Pengembangan SABSA

Manajemen dalam proses pengembangan keamanan inteligensia bisnis Proses pengembangan menunjukkan bahwa ada dua jalur pengembangan. Setelah Arsitektur Kontekstual dan Arsitektur Konseptual yang disepakati dan disetujui, kemudian proses berlanjut pada tahap selanjutnya sampai selesai pada Arsitektur Komponen. Sedangkan pada saat bersamaan Arsitektur Manajemen Layanan berjalan dari awal sampai akhir. Siklus dari SABSA dirancang untuk menyelaraskan dengan siklus IT organisasi, sehingga arsitektur keamanan yang dihasilkan akan sesuai dengan siklus TI dari organisasi.

Siklus Hidup SABSA



Gambar 4. SABSA *lifecycle*

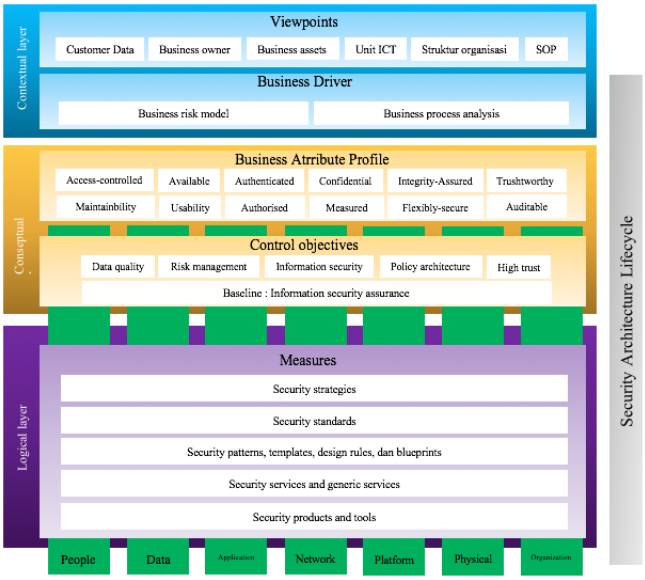
Siklus arsitektur keamanan inteligensia bisnis Dalam siklus SABSA, fase pertama dari Proses Pembangunan arsitektur dikelompokkan menjadi aktivitas yang disebut konsep dan strategi. Selanjutnya diikuti dengan aktivitas yang disebut desain, yang mencakup desain logik, fisik, arsitektur komponen dan operasional. Siklus yang ketiga adalah implementasi diikuti oleh pengelolaan dan penilaian. Penilaian merupakan awal proses untuk menetapkan metrik target. Setelah operasional, sangat penting untuk mengukur kinerja aktual terhadap target, dan untuk mengelola setiap penyimpangan yang terjadi. Pengelolaan seperti ini mungkin hanya melibatkan parameter operasional, tetapi juga dapat menjadi masukan untuk siklus baru pengembangan. Sebuah perbaikan lebih lanjut adalah penggunaan SABSA

Atribut Inteligensia Bisnis.

IV. HASIL DAN PEMBAHASAN

Langkah selanjutnya pada fase IV adalah membuat perancangan model format arsitektur keamanan organisasi Rumah Sakit Queen Latifa berdasarkan poin-point dari hasil mapping antara artefak security SABSA dengan komponen-komponen dalam TOGAF. Pada paper ini, peneliti membatasi model format Enterprise Security Architecture (ESA) tersebut hanya dalam 3 (tiga) layer teratas, yaitu Contextual Layer, Conceptual Layer dan Logical Layer. Struktur layout rancangan model format ESA adalah sebagai berikut :

a) Contextual Layer : Viewpoints AND Business Driver
b) Conceptual Layer : Business Attribute AND Control Objectives
c) Logical Layer : Measures
d) Conceptual AND Logical Layer : (People, Data, Application, Network, Platform, Physical & Organization).



Gambar 4. Format *Enterprise Security Architecture* Rumah Sakit Queen Latifa

Adapun penjelasan mengenai artefak security, komponen dan deskripsi aktifitas pada format *Enterprise Security Architecture* pada Rumah Sakit Queen Latifa di setiap layernya, sebagai berikut;

A. Contextual layer

Tabel 2. Deskripsi aktifitas pada *security artifact component (Contextual Layer)*

Artefak security	Komponen *artefak*	Deskripsi aktifitas
Business viewpoint	Business assets (*Security requirement*)	a. Identifikasi persyaratan keamanan untuk system assurance. b. Memanfaatkan aset bisnis sebagai value untuk mendukung kebutuhan bisnis terhadap keamanan informasi. c. Identifikasi kebutuhan bisnis untuk keamanan sistem informasi. d. Identifikasi persyaratan keamanan untuk menjamin kontinuitas operasional bisnis.
Business Driver	Business Risk Model (*Risk Assessment*)	Organisasi atau perusahaan harus melakukan penilaian terhadap risiko binis dan memiliki respon resiko yang mungkin terjadi di beberapa area, diantaranya; *loss prevention, business continuity, fraud protection, brand protection, confidence of stakeholders dan operational risk.*
	Business Process Analysis (*Security for business process*)	Mengidentifikasi dan menganalisa pada persyaratan keamanan yang dilakukan (*driven*) oleh *business process*, diantaranya; a. Komunikasi *business* antar *process* yang terjadi. b. Perlu identifikasi dan otentikasi entitas dari *business process* untuk Interaksi *business.*

B. Conceptual Layer

Tabel 3. Deskripsi aktifitas pada *security artifact component* (*Conceptual Layer*)

Artefak security	Komponen *artefak*	Deskripsi aktifitas
Business Attribut *Profile*	Implementasi Atribut *security* pada *(Business attribut profile)*	a. Mapping atribut *security* (SABSA) kedalam *business drivers*, meliputi : *a. Access-control*

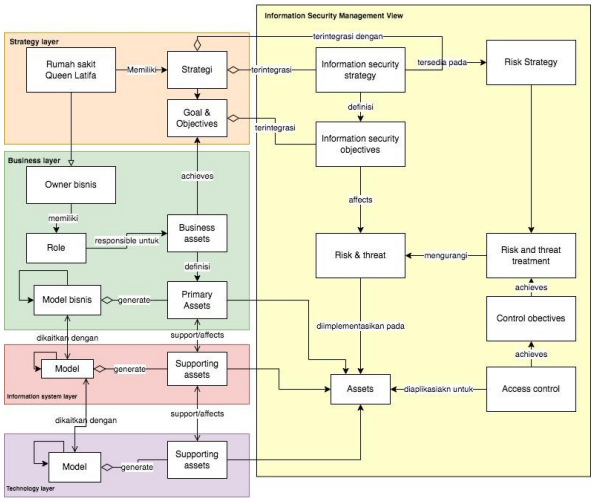
	kedalam *business assets.*	*b. Availability* *c. Authenticated* *d. Confidential* *e. Integrity* *f. Trustworthy* *g. Maintainability* *h. Usability* *i. Authorised* *j. Measured* *k. Flexible Secure* *l. Auditable* b. *Business assets* membutuhkan proteksi keamanan ketika identifikasi.
Control Objectives	Security Audits dan Assurance Level *(Information Security Assurance*)	*Control objectives* (tujuan pengendalian) dibutuhkan untuk mengkonseptualkan strategi mitigasi dalam upaya mengatasi resiko bisnis yang terjadi. Definisi *control objectives* adalah : *a. Data Quality* *b. Risk Management* *c. Information Security* *d. Policy* e. *High Trust*

C. Logical Layer

Tabel 4. Deskripsi aktifitas pada *security artifact component* (Logical Layer)

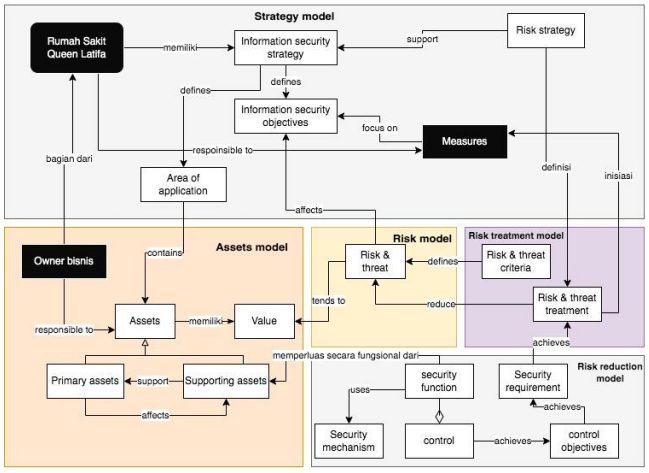
Artefak security	Komponen *artefak*	Deskripsi aktifitas
Measures	*Security Strategies* *Security Standards* *Security Patterns* *Security Services* *Security Products & Tools*	a. Identifikasi pengukuran standar keamanan arsitektur dengan melihat tingkat kematangan arsitektur. b. Mengidentifikasi strategi untuk arsitektur dan kebijakan keamanan. c. Mengidentifikasi pengukuran layanan security pada seluruh entitas yang terlibat pada arsitektur keamanan organisasi atau perusahaan.

Tahap berikutnya pada fase IV ini adalah membuat model konseptual integrasi *Information Security Management System* (ISMS) kedalam *framework* TOGAF berdasarkan artefak-artefak hasil identifikasi yang dilakukan pada tahap sebelumnya. Pada tahapan ini, peneliti mengintegrasi model tersebut hanya pada 4 tahap ADM saja, diantaranya; *Strategy, Business, Information System, dan Technology*.



Gambar 5. Model Integrasi ISMS dengan *Enterprise Architecture*

Tahap terakhir yaitu membuat model konseptual akhir dari integrasi proses ISMS kedalam EA sebagai satu kesatuan proses *business* yang saling *support*. Pada tahapan ini, peneliti mengintegrasikan artefak security (ISMS) sebagai core business di dalam *Enterprise Architecture* Rumah Sakit Queen Latifa.



Gambar 6. Model Akhir Integrasi Proses ISMS

Fase terakhir adalah expert judgement yang dilakukan presentasikan kepada stakeholder dan/atau manajer Rumah Sakit Queen Latifa, adapun yang dilakukan adalah; Memilih dan mengonfirmasikan aktivitas yang akan dianalisis; Membuat daftar pernyataan dan/atau pertanyaan;

Memilih para ahli; Meminta para ahli memberikan penilaian / jawaban mereka; Membuat laporan dan mengirimkan ke semua orang; Meminta para ahli untuk melakukan revisi jawaban mereka; dan Membuat laporan kedua.

V. KESIMPULAN

EISA merupakan bagian dari Enterprise Architecture yang menyelaraskan antara keamanan TI dan strategi bisnis. Perancangan EISA dapat dilakukan dengan menggunakan standar dari SABSA yang berfokus pada sudut pandang keamanan. Setiap layer pada SABSA merupakan pandangan dari sisi pemain atau user yang berbeda dalam proses menetukan, merancang, membangun, dan menggunakan sistem bisnis.

Studi kasus pada Rumah Sakit Queen Latifa memperlihatkan bahwa arsitektur keamanan SABSA dapat diintegrasikan secara sinergis dengan arsitektur organisasi (TOGAF) untuk menghasilkan sebuah Enterprise Security Architecture yang baik. Hasil dari penelitian ini menjadi pertimbangan kepada pihak Rumah Sakit Queen Latifa sebagai pemegang keputusan mengenasi implementasi dari hasil analisa dan peningkatan sistem keamanan dengan *framework* SABSA.

Peneliti menyarankan kepada stakeholder dan pimpinan Rumah Sakit Queen Latifa turut berpartisipasi dalam pengembangan EISA sehingga informasi mengenasi proses bisnis dan komponen didalamnya dapat digali lebih dalam sehingga dapat menciptakan EISA yang lebih baik lagi.

DAFTAR PUSTAKA

[1] *and Privacy of the Integrated Clinical Environment Part I"*. Health Care Finance, 2019.

[2] Syamsudin, A., (2015, June). Arsitektur Keamanan Enterprise untuk Pengembangan Inteligensia Bisnis. [Online]. Available: https://www.kompasiana.com/ariessyamsuddin/552e092c6ea8348d258b4576/arsitektur-keamanan-enterprise-untuk-pengembangan-inteligensia-bisnis

[3] Sherwood, J., Clark, A. and Lynas, D. *Enterprise Security Architecture*. SABSA White Paper, 6, 43-54. 2009.

[4] Samaras, V. et.al. "*An enterprise security architecture for accessing SaaS cloud services with BYOD"*. Australia. 2014.

[5] Maketas D. and Zisopoulos I., "*Integration of TOGAF and SABSA on the Increased Effectiveness and Security of a Software Development Life Cycle, in the Context of a Spinoff Company"*. Luleå University of Technology. 2013.

[6] Zadeh R. G., "*Enterprise Security Architecture— A Top-down Approach"*. ISACA. 2017.

[7] Najib W. et. al,. "*Development of Enterprise Security Framework in SKK Migas Based on Integration of ISO 27000 and SABSA Model"*. Universitas Gadjah Mada, Indonesia. 2018.

[8] Mouratidis, H., Giorgini, P., Manson, G. "*Integrating Security and Systems Engineering: Towards the Modelling of Secure Information Systems"*.Springer, Berlin, Heidelberg. 2003.

[9] Mouratidis, H., Giorgini, P., Manson, G. "*When security meets software engineering: a case of modelling secure information systems"***.** University of Sheffield, UK. 2005.

[10] Devanbu, P. and Stubblebine, S. "*Software Engineering for Security: A Roadmap. Proceedings of the Conference on The Future of Software Engineering"*, 227-239. 2000

[11] Kurniawan, N.B. "*Perancangan Enterprise Security Architecture Melalui Integrasi Arsitektur Keamanan Informasi dengan Enterprise Architecture (SABSA Dan TOGAF 9.1)"*. Institut Teknologi Bandung, Indonesia. 2013.