TESIS

PERANCANGAN *ENTERPRISE SECURITY ARCHITECTURE* MENGGUNAKAN INTEGRASI *FRAMEWORK* SABSA DAN TOGAF 9.1 DI SCALEOUT CREATIVE AGENCY

Disusun oleh:

Nama	**: Alvian Trias Kurniawan**
NIM	**: 20.51.1322**
Konsentrasi	**: Informatics Technopreneurship**

PROGRAM STUDI S2 TEKNIK INFORMATIKA

PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2023

TESIS

PERANCANGAN *ENTERPRISE SECURITY ARCHITECTURE* MENGGUNAKAN INTEGRASI *FRAMEWORK* SABSA DAN TOGAF 9.1 DI SCALEOUT CREATIVE AGENCY

ENTERPRISE SECURITY ARCHITECTURE DESIGN USING SABSA AND TOGAF 9.1 *FRAMEWORK* INTEGRATION ON SCALEOUT CREATIVE AGENCY

Diajukan untuk memenuhi salah satu syarat memperoleh derajat Magister

Disusun oleh:

Nama : **Alvian Trias Kurniawan**
NIM : **20.51.1322**
Konsentrasi : **Informatics Technopreneurship**

PROGRAM STUDI S2 TEKNIK INFORMATIKA
PROGRAM PASCASARJANA UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA
2023

HALAMAN PENGESAHAN

PERANCANGAN *ENTERPRISE SECURITY ARCHITECTURE* MENGGUNAKAN INTEGRASI *FRAMEWORK* SABSA DAN TOGAF 9.1 DI SCALEOUT CREATIVE AGENCY

ENTERPRISE SECURITY ARCHITECTURE DESIGN USING SABSA AND TOGAF 9.1 *FRAMEWORK* INTEGRATION ON SCALEOUT CREATIVE AGENCY

Dipersiapkan dan Disusun oleh

Alvian Trias Kurniawan

20.51.1322

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Selasa, 4 Juli 2023

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, 4 Juli 2023
Rektor

Prof. Dr. M. Suyanto, M.M.
NIK. 190302001

HALAMAN PERSETUJUAN

PERANCANGAN *ENTERPRISE SECURITY ARCHITECTURE* MENGGUNAKAN INTEGRASI *FRAMEWORK* SABSA DAN TOGAF 9.1 DI SCALEOUT CREATIVE AGENCY

ENTERPRISE SECURITY ARCHITECTURE DESIGN USING SABSA AND TOGAF 9.1 *FRAMEWORK* INTEGRATION ON SCALEOUT CREATIVE AGENCY

Dipersiapkan dan Disusun oleh

Alvian Trias Kurniawan

20.51.1322

Telah Diujikan dan Dipertahankan dalam Sidang Ujian Tesis
Program Studi S2 Teknik Informatika
Program Pascasarjana Universitas AMIKOM Yogyakarta
pada hari Selasa, 4 Juli 2023

Pembimbing Utama	Anggota Tim Penguji
Prof. Dr. Bambang Soedijono W.A	Hanafi, S.Kom., M.Eng., Ph.D.
NIK. 555126	NIK. 190302024
	Hanif Al Fatta, M.Kom., Ph.D
Pembimbing Pendamping	NIK. 190302096
Drs. Asro Nasiri, M.Kom.	Tonny Hidayat, M.Kom., Ph.D
NIK. 190302152	NIK. 190302106

Tesis ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Magister Komputer

Yogyakarta, 4 Juli 2023
Direktur Program Pascasarjana

Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN TESIS

HALAMAN PERNYATAAN KEASLIAN TESIS

Yang bertandatangan di bawah ini,

Nama mahasiswa : Alvian Trias Kurniawan
NIM : 21.51.1322
Konsentrasi : Informatics Technopreneurship

Menyatakan bahwa Tesis dengan judul berikut:
Tuliskan Judul Tesis Bahasa Indonesia

Dosen Pembimbing Utama : Prof. Dr. Bambang Soedijono W.A
Dosen Pembimbing Pendamping : Drs. Asro Nasiri, M.Kom.

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Tim Dosen Pembimbing
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi

Yogyakarta, tanggal ujian tesis
Yang Menyatakan,

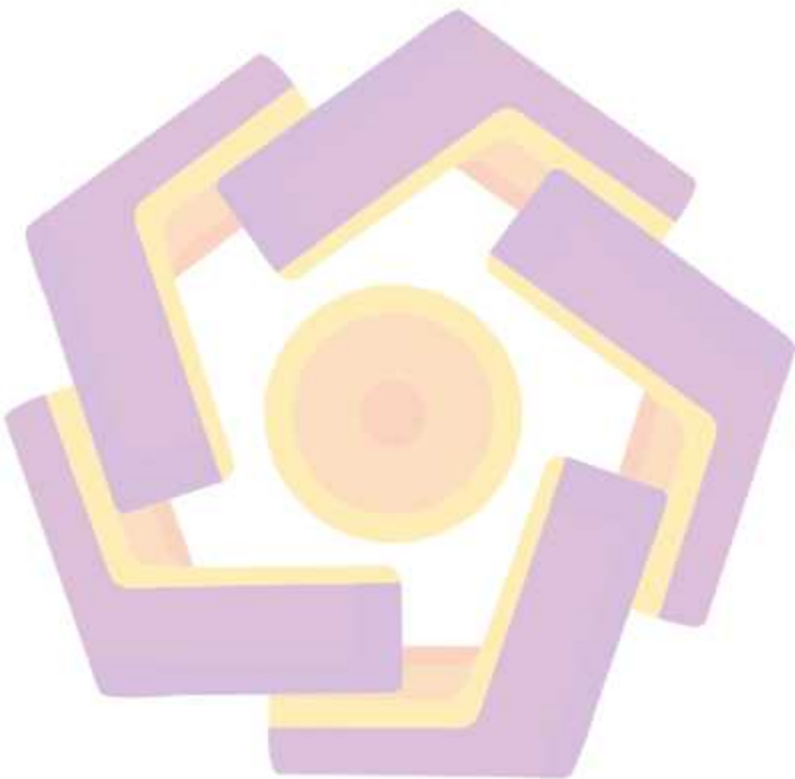
Alvian Trias Kurniawan

HALAMAN PERSEMBAHAN

Dengan segala rasa syukur dan tulus ikhlas, tesis ini Penulis persembahkan untuk semua orang yang selalu memberikan dukungan, inspirasi, dan doa-doa terbaik dalam perjalanan kami. Terima kasih atas semua bantuan dan semangat yang tak tergantikan. Semoga hasil penelitian ini dapat bermanfaat bagi perkembangan ilmu pengetahuan dan kebermanfaatan bagi banyak orang.

HALAMAN MOTTO

"Sesungguhnya Allah tidak akan mengubah keadaan suatu kaum, sebelum mereka mengubah keadaan diri mereka sendiri." (QS. Ar-Ra'd Ayat 11)



KATA PENGANTAR

Puji syukur Penulis panjatkan kehadirat Allah SWT atas segala rahmat, karunia, dan petunjuk-Nya, yang telah melimpahkan berkah-Nya sehingga Penulis dapat menyelesaikan penulisan tesis ini dengan lancar. Penulisan tesis ini bertujuan untuk menganalisa dan merancang *blueprint* sistem keamanan pada Scaleout Creative Agency menggunakan *framework* SABSA dan TOGAF 9.1. Penulis menyadari bahwa tesis ini tidak akan terselesaikan tanpa adanya dukungan, bantuan, bimbingan, doa, dan nasehat dari berbagai pihak selama penyusunan tesis ini. Pada kesempatan ini Penulis mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Dr. M. Suyanto, MM. selaku Rektor Universitas Amikom Yogyakarta.
2. Prof. Dr. Bambang Soedijono W.A dan Drs. Asro Nasiri, M.Kom. atas bimbingan, dukungan, dan arahan yang berharga selama proses penulisan tesis ini.
3. Orang tua, saudara, teman-teman seangkatan, serta keluarga besar yang selalu memberikan semangat, dukungan, dan doa agar tesis ini dapat terselesaikan dengan baik. Kebersamaan dan kerjasama selama proses penelitian menjadi salah satu faktor kunci kesuksesan penyelesaian tesis ini.
4. Seluruh jajaran direksi perusahaan Scaleout Creative Agency yang telah berkontribusi dalam menyelesaikan penelitian ini. Termasuk dalam memberikan data dan informasi yang berharga dalam penelitian ini.

Kontribusi dari pihak-pihak tersebut menjadi landasan penting untuk menunjang keakuratan dan validitas penelitian ini.

5. Orang tercinta yang selalu meluangkan waktu dan memberikan dorongan, serta memberikan semangat pada saat proses penulisan Tesis sedang berlangsung.
6. Semua pihak yang turut membantu dan memberikan dukungan dalam berbagai bentuknya selama proses penulisan tesis ini.

Semoga tesis ini dapat memberikan kontribusi yang bermanfaat dan inspirasi bagi pengembangan ilmu pengetahuan dan praktik keamanan informasi di agensi kreatif. Penulis menyadari bahwa tesis ini masih jauh dari kesempurnaan, oleh karena itu, perlu adanya penerapan dan evaluasi untuk perbaikan dan pengembangan lebih lanjut.

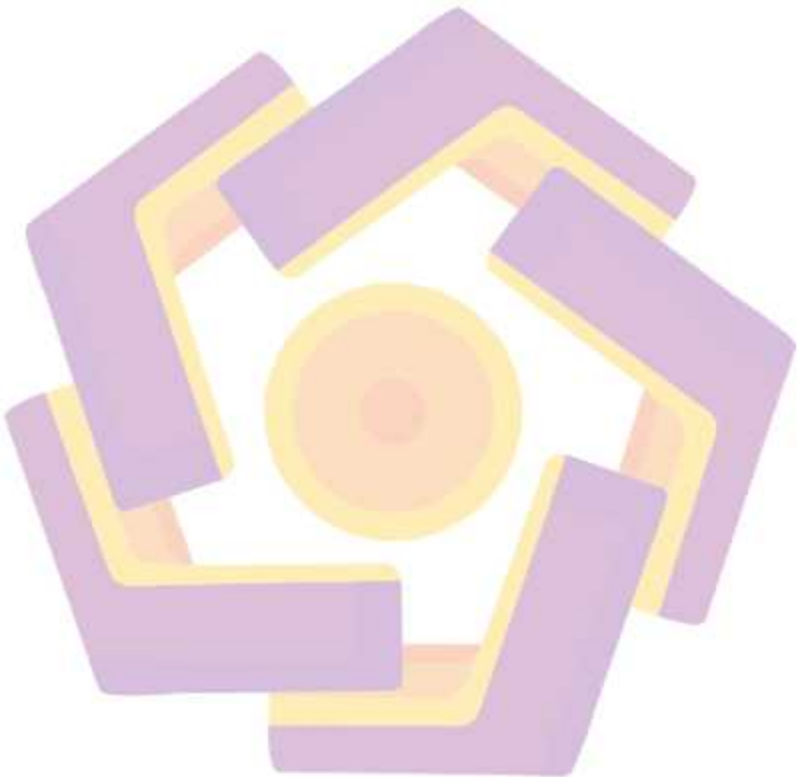
Akhir kata, Penulis berharap agar tesis ini dapat memberikan manfaat bagi para pembaca dan menjadi bagian dari sumbangsih pengetahuan dan teknologi dalam mewujudkan sistem keamanan yang terintegrasi, efektif, dan berdaya guna di masa yang akan datang.

Terima kasih.

Yogyakarta, 31 Juli 2023

Penulis

DAFTAR ISI



DAFTAR TABEL

DAFTAR GAMBAR

INTISARI

Dalam era digital saat ini, agensi kreatif dituntut untuk tetap beradaptasi dan mengikuti perkembangan teknologi dan informasi yang terus berkembang. Salah satu hal yang menjadi fokus utama bagi agensi kreatif adalah memastikan aksesibilitas dan fleksibilitas dalam sistem keamanannya, terutama dengan semakin banyaknya karyawan yang bekerja dari jarak jauh. Oleh karena itu, diperlukan sebuah *framework* keamanan yang dapat membantu agensi kreatif untuk mengintegrasikan dan memperkuat sistem keamanannya.

Scaleout Creative Agency merupakan sebuah agensi kreatif dan rumah produksi yang bergerak di bidang pemasaran digital berbasis audiovisual dengan tujuan branding dan selling. Dengan banyakanya klien dan karyawan yang ada, tentunya perlunya sistem keamanan yang sangat diperlukan untuk melindungi aset digital yang ada, seperti data klien, karya, dan kekayaan intelektual.

Dalam penelitian ini, digunakan pendekatan kualitatif dengan merancang *Enterprise Security Architecture* yang mana studi kasusnya adalah Scaleout Creative Agency. Data diperoleh melalui wawancara dan dokumentasi. Hasil penelitian menunjukkan bahwa *blueprint* dari integrasi *framework* SABSA dan TOGAF 9.1 membantu agensi kreatif dalam membangun sistem keamanan yang efektif dan efisien untuk memastikan keamanan data dan informasi, serta menjaga aksesibilitas dan fleksibilitas karyawan jarak jauh.

Kata kunci: SABSA, TOGAF, *framework, Enterprise Security Architecture, blueprint.*

ABSTRACT

In today's digital era, creative agencies are required to continue to adapt and keep abreast of technological and information developments that continue to evolve. One of the key areas of focus for creative agencies is ensuring accessibility and flexibility in their security systems, especially with an increasing number of employees working remotely. Therefore, there is a need for a security framework that can help creative agencies integrate and strengthen their security systems.

Scaleout Creative Agency is a creative agency and production house engaged in audiovisual-based digital marketing with the aim of branding and selling. With so many existing clients and employees, of course, a security system is needed to protect existing digital assets, such as client data, work, and intellectual property.

In this study, a qualitative approach was used in designing an Enterprise Security Architecture with a case study of the Scaleout Creative Agency. Data obtained through interviews and documentation. The results of the study show that the SABSA and TOGAF 9.1 framework integration blueprint helps creative agencies build an effective and efficient security system to ensure data and information security, as well as maintain the accessibility and flexibility of remote employees.

Keyword: SABSA, TOGAF, *framework, Enterprise Security Architecture, blueprint.*

BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Dalam era digital saat ini, aksesibilitas dan fleksibilitas menjadi hal yang sangat penting bagi perusahaan, termasuk agensi kreatif. Namun, hal ini juga menimbulkan masalah keamanan, terutama dalam hal aksesibilitas dan fleksibilitas yang berkaitan dengan data dan informasi penting perusahaan. Oleh karena itu, perlu ada sistem keamanan yang baik untuk memastikan bahwa aksesibilitas dan fleksibilitas tidak mengorbankan keamanan data dan informasi perusahaan.

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 (Devanbu dan Stubblebine, 2000, p. 227). Oleh karena itu, dengan semakin banyaknya perusahaan yang berinvestasi dalam keamanan, hal tersebut kini dianggap sebagai faktor penting dan kritis bagi kelangsungan hidup suatu perusahaan. Terlepas dari keamanan komputer dan jaringan yang dikenal luas, di mana penggunaan *hardener*, sistem deteksi intrusi, sistem pencegahan intrusi, daftar kontrol akses dan firewall banyak digunakan, beberapa peneliti juga telah mengidentifikasi kebutuhan untuk menambahkan keamanan dalam proses pengembangan sistem informasi (Mouratidis et al., 2003, dan Mouratidis et al., 2005).

Bisnis pada bidang pemasaran seperti rumah produksi, agensi kreatif, *advertising*, pemasaran digital, dan sebagainya termasuk sintesis penyedia layanan dan perangkat pemasaran, jaringan informasi dan teknologi informasi yang bekerja sama untuk meningkatkan kepuasan pelanggan, meningkatkan efektivitas produktivitas, dan meningkatkan *efisiensi*. Tujuan dari penelitian ini adalah untuk mengatasi masalah aksesibilitas dan fleksibilitas dalam sistem keamanan Scaleout Creative Agency, yang mana semakin banyaknya karyawan yang bekerja dari jarak jauh. Sayangnya, konsep tersebut lahir dengan sedikit fokus pada sistem keamanan dan privasi. Potensi bahaya besar, baik fisik maupun emosional, selalu ada dalam konteks agensi kreatif dan/atau marketing ketika teknologi informasi digunakan untuk membantu pemasaran dari sebuah brand. Sistem dasar keamanan informasi harus diikuti ketika mengembangkan kerahasiaan, integritas, aksesibilitas, dan akuntabilitas lingkup agensi pemasaran yang saling terintegrasi (William, J.L. 2019).

Selain itu, masalah privasi yang digariskan dalam Prinsip Praktik Informasi yang adil dalam peng-aksesan dan amandemen, akuntabilitas, otoritas, minimalisasi, kualitas dan integritas, partisipasi individu, spesifikasi tujuan dan batasan penggunaan, keamanan, dan transparansi juga harus ditangani saat menciptakan lingkungan bisnis yang saling terintegrasi. Integrasi tanpa keamanan dan privasi bukanlah interoperabilitas. Sebuah perusahaan marketing digital tidak dapat mengoperasikan lingkungan agensi kreatif yang terintegrasi dalam lingkungan hukum dan peraturan saat ini, tanpa jaminan keamanan dan privasi yang direkayasa ke dalam sistem. Namun, saat ini ada kerangka kerja yang

memungkinkan perusahaan agensi kreatif untuk mengelola risiko keamanan dan privasi di dalam sebuah perusahaan secara sistematis (William, J.L. 2019).

Seluruh proses bisnis yang ada dalam agensi kreatif dapat diintegrasikan dengan teknologi informasi, termasuk di bidang keamanannya. Pengintegrasian teknologi dalam merencanakan pelayanan yang baik membutuhkan suatu perencanaan yang terarah, terstruktur, dengan prosedur yang tepat. salah satunya merupakan aset digital, dimana data-data tersebut merupakan hal yang sangat penting dan rahasia. Agensi kreatif merupakan salah satu perusahaan yang memiliki proses bisnis yang cukup kompleks mulai dari diskusi dengan calon klien sampai dengan pengolahan data klien ke output konten digital setelah melakukan kesepakatan. Penelitian ini akan mengimplementasikan *framework* SABSA (*Sherwood Applied Business Security Architecture*) yang diintegrasikan dengan TOGAF 9.1 untuk menganalisa sistem keamanan pada Scaleout Creative Agency, supaya dapat memberikan gambaran kerangka kerja dalam perencanaan layanan teknologi yang *terintegrasi* dengan proses bisnis yang sesuai.

Framework SABSA digunakan untuk mengembangkan arsitektur keamanan informasi dan jaminan informasi perusahaan yang digerakkan oleh risiko dan untuk memberikan solusi infrastruktur *keamanan* yang mendukung inisiatif bisnis penting. Ini adalah standar terbuka, terdiri dari sejumlah kerangka kerja, model, metode dan proses, gratis untuk digunakan oleh semua, tanpa lisensi yang diperlukan untuk organisasi pengguna akhir yang menggunakan standar dalam

mengembangkan dan mengimplementasikan arsitektur dan solusi (Sherwood, J. et al,. 2009).

Kesadaran tentang sistem keamanan di bidang agensi kreatif sangat minim, terutama tentang aksesibilitas dan fleksibilitas-nya. Sistem keamanan yang diterapkan pada beberapa agensi kreatif khususnya Scaleout Creative Agency belum seratus persen maksimal, perlu adanya peningkatan dan peninjauan secara berkala demi kenyamanan dan keamanan pihak agensi dengan karyawan dan/atau klien. Isu yang terjadi di masyarakat tentang banyaknya data atau formula klien yang bocor, hal tersebut menjadikan stigma baru di kalangan *brand owner* untuk lebih waspada dalam memilih sebuah agensi kreaitf untuk memberikan data *brand*-nya. Hingga kini, banyak *brand owner* mulai berpindah dari agensi kreatif satu ke agensi kreatif lainnya untuk mendapatkan pelayanan yang terbaik dan terjamin khususnya di bidang keamanan data klien. Hal ini tentunya menjadi permasalahan agensi kreatif yang krusial karena persaingan bisnis antar agensi kreatif menjadi masalah yang cukup besar. Salah satu pelayanaan yang dapat dilihat saat ini yaitu pendataan, penyimpanan, dan pengolahan data milik klien.

Aksesibilitas dan fleksibilitas pada agensi kreatif dianggap penting karena dalam era digital saat ini, banyak pekerjaan yang bisa dilakukan secara jarak jauh atau *remote*. Hal ini membuka peluang bagi agensi kreatif untuk mempekerjakan karyawan dari berbagai tempat dan memberikan kesempatan kepada karyawan untuk bekerja secara fleksibel. Namun, hal ini juga menimbulkan tantangan dalam hal keamanan data dan informasi yang harus diakses dan digunakan oleh karyawan

dari tempat yang berbeda-beda. Oleh karena itu, penting untuk menjamin aksesibilitas dan fleksibilitas yang aman untuk memastikan keamanan data dan informasi pada agensi kreatif.

Penggunaan *framework* SABSA (*Sherwood Applied Business Security Architecture*) pada penelitian ini karena *framework* ini berfokus pada keamanan TI 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 pada dasarnya *framework* SABSA merupakan pengembangan dari *framework* Zachman yang berfokus dari sudut pandang keamanan atau metodologi *business-to-security* (Syamsudin, A., 2015).

Penelitian ini membahas konsep peningkatan Enterprise Security Architecture (ESA) pada Scaleout Creative Agency dengan mengintegrasikan arsitektur keamanan informasi kedalam *Enterprise Architecture* secara sinergis untuk meningkatkan keamanan data dan informasi statistik, sehingga tujuan bisnis pada objek penelitian dapat tercapai. Implementasi dari Enterprise Architecture menggunakan The Open Group Architecture *Framework* (TOGAF) Versi 9.1, sedangkan untuk arsitektur keamanan informasi akan menggunakan *framework* dari SABSA (Sherwood Applied Business Security Architecture). Hasil dari penelitian yaitu blueprint antara artefak keamanan informasi SABSA dengan arsitektur TOGAF.

Integrasi TOGAF (The Open Group Architecture *Framework*) dan SABSA (Sherwood Applied Business Security Architecture) dapat memberikan beberapa kelebihan dalam mendukung sistem keamanan data yang mendukung aksesibilitas dan fleksibilitas dalam perusahaan. Dengan menggunakan kedua *framework* ini, perusahaan dapat mengembangkan strategi keamanan yang sejalan dengan strategi bisnis yang lebih luas. Selain itu, Integrasi *framework* ini dapat memungkinkan perencanaan yang holistik dan konsisten dalam membangun sistem keamanan yang mendukung tujuan bisnis dan memenuhi kebutuhan aksesibilitas dan fleksibilitas.

Integrasi kedua *framework* ini juga membantu mengidentifikasi dan mengatasi ancaman keamanan yang spesifik dan memprioritaskan tindakan mitigasi berdasarkan dampak dan probabilitas risiko. Integrasi TOGAF dan SABSA mencakup pengaturan struktur organisasi, tanggung jawab, kebijakan, dan proses yang terkait dengan pengelolaan keamanan data. Dengan demikian, perusahaan dapat mengadopsi pendekatan yang terstruktur dan terkelola dengan baik dalam memastikan keamanan yang efektif. Integrasi ini memungkinkan perusahaan untuk mengantisipasi dan merespons perubahan dan pertumbuhan bisnis dengan mempertimbangkan aspek keamanan data karena TOGAF memiliki pendekatan *life cycle* yang mencakup perencanaan, desain, implementasi, dan pemantauan. Sedangkan, SABSA memperkaya *life cycle* tersebut dengan perspektif keamanan yang kuat.

Dalam penelitian ini *framework* SABSA dan TOGAF 9.1 diintegrasikan untuk menyediakan solusi keamanan yang komprehensif dan terintegrasi dalam

enterprise security architecture (ESA) Scaleout Creative Agency. Kombinasi SABSA dan TOGAF 9.1 dapat digunakan untuk mengevaluasi risiko keamanan dari arsitektur keamanan dan mengembangkan arsitektur keamanan termasuk mengenai masalah yang diangkat, yaitu aksesibilitas dan fleksibilitas bagi karyawan yang bekerja secara jarak jauh atau *remote*. SABSA menyediakan pendekatan yang diperlukan untuk mengelola risiko keamanan, sementara TOGAF menyediakan kerangka kerja untuk mengelola arsitektur enterprise secara keseluruhan.

1.2. Rumusan Masalah

Berdasarkan latar belakang diatas, masalah yang diangkat pada penelitian ini adalah:

a. Bagaimana mengukur tingkat validitas sistem keamanan untuk Scaleout Creative Agency dengan menggunakan *framework* SABSA?
b. Apa rekomendasi rancangan sistem keamanan untuk Scaleout Creative Agency dengan mengintegrasikan SABSA dan TOGAF 9.1?

1.3. Batasan Masalah

Bagian ini membahas tentang batasan yang digunakan untuk penelitian agar terfokus pada aspek yang diangkat, adapun batasanya sebagai berikut:

a. Kerangka blueprint menggunakan *framework* yang digunakan adalah integrasi SABSA dan TOGAF 9.1.
b. Menganalisa dan meningkatkan sistem keamanan yang berfokus pada aksesibilitas dan fleksibilitas karyawan yang bekerja secara jarak jauh pada Scaleout Creative Agency

1.4. Tujuan Penelitian

Berdasarkan latar belakang yang diangkat, maka dibuat tujuan yang akan diselesaikan pada penelitian ini, antara lain:

a. Menganalisa dan merancang *blueprint* sistem keamanan pada Scaleout Creative Agency menggunakan *framework* SABSA dan TOGAF 9.1.

1.5. Manfaat Penelitian

Manfaat dari penelitian ini, diantaranya:

a. Penelitian ini bermanfaat untuk menambah wawasan penulis tentang bagaimana penerapan integrasi *framework* SABSA dan TOGAF pada sistem keamanan agensi kreatif.
b. Penelitian ini dapat dijadikan bahan pertimbangan kepada stakeholder Scaleout Creative Agency untuk mengaplikasikan blueprint dari usulan yang ada.
c. Hasil penelitian ini dapat dijadikan sebagai acuan dan/atau referensi pada penelitian berikutnya yang membahas tentang penerapan *framework* SABSA dan TOGAF pada sistem pendukung keputusan.

BAB II

TINJAUAN PUSTAKA

2.1. Tinjauan Pustaka

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

Penelitian yang dilakukan oleh Sheerwood, J. et al,. (2009), meneliti 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.

Selain itu, penelitian yang dilakukan oleh Khreishah A. dan Gaber J., (2015), meneliti tentang pentingnya keamanan dalam lingkungan virtualisasi yang digunakan dalam teknologi *cloud computing*. penggunaan *cloud computing* semakin populer dan memungkinkan pengguna untuk mengakses data ataupun aplikasi dari mana saja dan kapan saja dengan menggunakan perangkat apapun. Namun, keamanan menjadi perhatian utama dalam lingkungan virtualisasi dan *cloud computing* karena penggunaan virtualisasi dapat meningkatkan risiko keamanan dan privasi data. Maka, pentingnya audit dan monitoring untuk memantau aktivitas pengguna dalam lingkungan virtualisasi dan *cloud computing*. Dengan audit dan *monitoring* yang tepat, masalah keamanan dapat terdeteksi dan diatasi sebelum menyebabkan kerusakan yang lebih besar.

Secara keseluruhan, penelitian tersebut menekankan bahwa keamanan adalah faktor kunci dalam aksesibilitas dan fleksibilitas di era digital, terutama dalam lingkungan virtualisasi dan *cloud computing*. Oleh karena itu, diperlukan teknologi dan praktik keamanan yang tepat untuk memastikan bahwa data dan informasi pengguna tetap aman dan terlindungi.

Penelitian lainnya dilakukan oleh A. L. A. dos Santos dan V. D. P. Lopes (2019), menjelaskan tentang integrasi kerangka kerja SABSA dengan TOGAF untuk pengembangan arsitektur keamanan perusahaan. Penulis menjelaskan bahwa SABSA dan TOGAF digunakan untuk membangun arsitektur keamanan yang komprehensif dan terintegrasi dalam organisasi. Integrasi kedua kerangka kerja ini memberikan keuntungan yang signifikan, karena SABSA memfokuskan pada identifikasi risiko dan strategi mitigasi yang sesuai, sedangkan TOGAF memfokuskan pada pengembangan arsitektur bisnis dan teknologi yang terpadu.

Penelitian berikutnya dilakukan oleh Maketas D. and Zisopoulos I., (2013), yang 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.

Penelitian yang dilakukan F. Farhana, M. M. H. Khan, M. A. R. Ahad, dan M. M. Alam. (2018), membahas tentang aksesibilitas, keamanan, dan fleksibilitas pada tiga layanan penyimpanan cloud populer: Google Drive, OneDrive, dan Dropbox.

Penelitian ini mengidentifikasi dan mengevaluasi beberapa fitur keamanan dan privasi pada layanan tersebut, seperti autentikasi, enkripsi data, dan kontrol akses. Hasil penelitian menunjukkan bahwa ketiga layanan memiliki tingkat keamanan yang baik dalam hal autentikasi dan enkripsi data, tetapi Dropbox memberikan lebih banyak opsi pengaturan keamanan daripada Google Drive dan OneDrive. Selain itu, Google Drive dan OneDrive memberikan fleksibilitas dan aksesibilitas yang lebih baik dalam hal dukungan multi-platform dan integrasi dengan aplikasi lain. Secara keseluruhan, penelitian ini menunjukkan bahwa ada hubungan antara keamanan, aksesibilitas, dan fleksibilitas pada layanan penyimpanan cloud, dan perlu dipertimbangkan secara bersamaan dalam memilih layanan yang tepat untuk kebutuhan bisnis.

Penelitian yang dilakukan oleh Najib W. et. al,. (2018), perkembangan 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.

2.2. Keaslian Penelitian

Tabel 2. 1 Matriks literatur review dan posisi penelitian

Perancangan Enterprise Security Architecture Menggunakan Integrasi *Framework* SABSA dan TOGAF 9.1 di Scaleout Creative Agency

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
1	Enterprise Security Architecture	John Sherwood, Andrew Clark & David Lynas, 2009.	Penelitian tersebut bertujuan menjelaskan tentang *framework* SABSA dalam konteks Arsitektur, daripada hanya berfokus pada solusi titik jangka bisnis.	Arsitektur keamanan dapat mengatasi berbagai persyaratan operasional dan memberikan dukungan dan pemberdayaan bisnis yang nyata pendek, maka kemungkinan akan gagal untuk memberikan apa yang diharapkan dalam bisnis.	Penelitian ini tidak ada contoh implementasi sistem keamanan pada perusahaan bisnis terkait.	Penelitian ini menjelaskan konsep dasar tentang *framework* SABSA, sedangkan penelitian ini menjelaskan penerapan *framework* SABSA pada sistem keamanan digital agensi
2	Securing Virtualized Environments in *Cloud computing*	Khreishah A. dan Gaber J., IEEE Security & Privacy Magazine, 2015.	Penelitian ini bertujuan untuk mengidentifikasi masalah keamanan dalam lingkungan virtualisasi pada	Kesimpulannya adalah keamanan virtualisasi dapat dipenuhi dengan teknologi dan praktik keamanan yang tepat. Artikel tersebut	Saran: perusahaan harus melakukan evaluasi risiko terhadap sistem virtualisasi yang mereka gunakan untuk	Penelitian ini menjelaskan tentang *cloud computing*, sedangkan penelitian ini meliputi beberapa aspek keamanan yang harus dilakukan perusahaan dalam

Tabel 2.1. (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
			sistem *cloud computing* dan menawarkan solusi untuk mengatasi masalah tersebut. Penelitian ini menyoroti pentingnya keamanan dalam lingkungan virtualisasi pada *cloud computing* dan memperkenalkan beberapa teknik untuk mengamankan lingkungan virtualisasi seperti enkripsi, pengelolaan hak akses, dan pemantauan keamanan. Penelitian ini bertujuan untuk membantu meningkatkan keamanan sistem	menekankan perlunya memperhatikan faktor-faktor keamanan selama fase perencanaan dan desain, serta pelaksanaan dan pengoperasian lingkungan virtualisasi cloud. Artikel tersebut juga mengidentifikasi beberapa tantangan keamanan yang harus diatasi, seperti ancaman virtualisasi dan rentang kendali, serta memberikan saran praktis untuk memperbaiki keamanan virtualisasi cloud. Oleh karena itu, perusahaan perlu mengambil tindakan proaktif untuk memastikan bahwa sistem virtualisasi cloud mereka aman dan terlindungi dari serangan.	menentukan kebijakan keamanan yang tepat. Kelemahan: Penelitian hanya memberikan gambaran umum tentang strategi pengamanan, dan tidak membahas secara detail mengenai implementasinya di lingkungan *cloud computing*.	mengontrol aksesibilitas dan fleksibilitas terhadap karyawan.

Tabel 2.1. (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
			cloud computing dan melindungi data dan informasi yang disimpan di dalamnya.			
3	Integrating SABSA with TOGAF for Enterprise Security Architecture Development	A. L. A. dos Santos dan V. D. P. Lopes, Jurnal Procedia Computer Science, 2019.	Penelitian ini bertujuan untuk memberikan solusi yang lebih baik untuk mengelola keamanan informasi dalam organisasi dengan mengintegrasikan kerangka kerja SABSA yang fokus pada keamanan dan kerangka kerja TOGAF yang fokus pada pengembangan arsitektur perusahaan. Dalam penelitian ini, penulis mengusulkan suatu model yang mengintegrasikan konsep dari kedua	Dalam jurnal tersebut dijelaskan bahwa integrasi kedua kerangka kerja ini dapat membantu organisasi dalam mengidentifikasi, menganalisis, dan menyelesaikan masalah keamanan pada tingkat yang lebih strategis. Integrasi SABSA dengan TOGAF juga dapat membantu organisasi dalam membuat keputusan yang lebih baik tentang investasi keamanan dan memastikan bahwa implementasi keamanan dilakukan secara efektif. Jurnal ini memberikan kesimpulan bahwa integrasi SABSA	Saran: Jurnal ini memberikan pandangan yang jelas dan komprehensif tentang bagaimana integrasi antara SABSA dan TOGAF dapat meningkatkan keamanan perusahaan. Kelemahan: Meskipun jurnal ini memberikan pandangan yang baik tentang integrasi SABSA dan TOGAF, namun tidak terdapat perbandingan dengan metode integrasi keamanan lainnya yang dapat digunakan dalam perusahaan.	Jurnal ini menjelaskan konsep dasar integrasi *framework* SABSA dan TOGAF tanpa adanya objek studi, sedangkan penelitian ini menggunakan Scaleout Creative Agency sebagai objek studi penelitian.

Tabel 2.1. (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
			kerangka kerja untuk mengembangkan arsitektur keamanan perusahaan yang holistik dan terintegrasi. Tujuannya adalah untuk membantu organisasi dalam mengembangkan strategi keamanan informasi yang lebih baik dan mengurangi risiko keamanan informasi secara signifikan.	dengan TOGAF dapat membantu organisasi dalam mengembangkan arsitektur keamanan yang holistik dan terintegrasi dengan bisnis.		
4	Integration of TOGAF and SABSA on the Increased Effectiveness and Security of a Software Development Life Cycle, in the Context of a Spinoff Company	Dimitrios Maketas dan Ioannis Zisopoulos, Lulea University of Technology, 2013	Tujuan dari penelitian ini adalah mengevaluasi pengaruh adopsi kerangka kerja terintegrasi yang menggabungkan TOGAF dan SABSA pada SDLC dalam konteks perusahaan spin-off	Hasil penelitian yang didapatkan dari wawancara dan interaksi dengan tim pengembangan perangkat lunak menunjukkan bahwa *framework* yang digunakan menghasilkan feedback yang positif.	Keterbatasan dari penelitian ini adalah blueprint yang diusulkan tidak dapat diuji di kehidupan nyata, karena membutuhkan penelitian ekstra untuk mengkonfirmasi hasil positif untuk pengembangan perangkat lunak.	Penelitian ini dilakukan dengan objek yang telah memiliki sistem keamanan dan tujuan dari penelitian ini adalah meningkatkan sistem yang sudah diterapkan dalam bentuk blueprint.

Tabel 2.1. (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
			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	Accessibility and Security in the Cloud: A Comparative Study of Google Drive, OneDrive and Dropbox.	F. Farhana, M. M. H. Khan, M. A. R. Ahad, dan M. M. Alam., 2018.	Tujuannya adalah melakukan analisis perbandingan terhadap tiga layanan penyimpanan cloud populer (Google Drive, OneDrive, dan Dropbox) dari sudut pandang aksesibilitas dan keamanan data. Penelitian ini bertujuan untuk	Setiap layanan memiliki kelebihan dan kekurangan masing-masing dalam hal aksesibilitas dan keamanan, dan penting bagi perusahaan untuk mempertimbangkan faktor-faktor ini saat memilih layanan penyimpanan awan yang sesuai untuk kebutuhan mereka.	Saran: perlunya melibatkan lebih banyak subjek pengguna dalam penelitian selanjutnya, serta mempertimbangkan faktor keamanan lainnya selain aksesibilitas. Kelemahan: Penelitian tidak mempertimbangkan berbagai keamanan seperti enkripsi data end-to-end, autentikasi dua	Penelitian yang dilakukan tanpa melibatkan pengguna yang ada, sedangkan penelitian ini melibatkan pengguna atau sumber daya manusia di dalam lingkup kerja Scaleout Creative Agency.

Tabel 2.1. (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
			memberikan wawasan yang berguna bagi pengguna layanan cloud dalam memilih layanan yang sesuai dengan kebutuhan aksesibilitas dan keamanan data mereka.		faktor, dan keamanan fisik data center.	
6	Development of Enterprise Security *Framework* in SKK Migas Based on Integration of ISO 27000 and SABSA Model	Warsun Najib, Sujoko Sumaryono, Lukito Edi Nugroho, Guntur Dharma Putra, IEEE, 2018	Penelitian ini bertujuan untuk mengembangkan kerangka kerja keamanan yang dapat membantu SKK Migas, sebuah perusahaan energi di Indonesia, dalam mengelola risiko keamanan informasi. Penelitian tersebut mencoba mengintegrasikan standar ISO 27000 dengan model SABSA untuk	Integrasi antara ISO 27000 dan SABSA Model dapat membantu SKK Migas untuk mencapai kepatuhan terhadap standar keamanan internasional dan memperkuat posisi mereka sebagai perusahaan yang aman dan andal.	Saran: Implementasi SABSA dan ISO 27000 sangat penting dalam pengembangan kerangka keamanan perusahaan. Kelemahan: Kurangnya penjelasan mengenai proses integrasi antara SABSA dan ISO 27000, sehingga pembaca sulit memahami bagaimana kedua model digunakan secara bersama-sama.	Integrasi yang dilakukan menggunakan *framework* yang berbeda, penelitian ini berfokus pada integrasi SABSA dan TOGAF 9.1.

Tabel 2.1. (Lanjutan)

No	Judul	Peneliti, Media Publikasi, dan Tahun	Tujuan Penelitian	Kesimpulan	Saran atau Kelemahan	Perbandingan
			menciptakan pendekatan yang holistik dan terpadu dalam mengelola risiko keamanan informasi. Tujuan akhir dari penelitian adalah untuk meningkatkan keamanan informasi di SKK Migas dan memastikan keberlangsungan bisnis perusahaan.			

2.3. Landasan Teori

SABSA adalah metodologi untuk mengembangkan arsitektur keamanan informasi dan jaminan informasi perusahaan yang digerakkan oleh risiko dan untuk memberikan solusi infrastruktur keamanan yang mendukung inisiatif bisnis penting. Ini adalah standar terbuka, terdiri dari sejumlah kerangka kerja, model, metode dan proses, gratis untuk digunakan oleh semua, tanpa lisensi yang diperlukan untuk organisasi pengguna akhir yang menggunakan standar dalam mengembangkan dan mengimplementasikan arsitektur dan solusi. SABSA bisa dibilang unik karena memenuhi SEMUA kriteria berikut:

a. SABSA adalah standar terbuka, yang terdiri dari kerangka kerja, model, metode dan proses, gratis untuk digunakan oleh semua, tanpa lisensi yang diperlukan untuk organisasi pengguna akhir yang menggunakan standar dalam mengembangkan dan mengimplementasikan arsitektur dan solusi;
b. Kerangka kerja SABSA tidak terkait dengan pemasok solusi TI mana pun dan sepenuhnya netral terhadap vendor,
c. Kerangka kerja SABSA dapat diskalakan, yaitu dapat diperkenalkan di area dan sistem berikutnya dan diimplementasikan secara bertahap,
d. Kerangka kerja SABSA dapat digunakan di sektor industri apa pun dan di organisasi mana pun baik milik swasta maupun publik, termasuk organisasi komersial, industri, pemerintah, militer, atau amal;
e. Kerangka kerja SABSA dapat digunakan untuk pengembangan arsitektur dan solusi pada tingkat granularitas cakupan apa pun, dari proyek dengan cakupan terbatas hingga kerangka kerja arsitektur keseluruhan perusahaan;

f. SABSA tidak menggantikan atau bersaing dengan risiko informasi atau standar keamanan informasi lainnya – melainkan menyediakan kerangka kerja menyeluruh yang memungkinkan semua standar lain yang ada untuk diintegrasikan di bawah kerangka kerja SABSA tunggal, memungkinkan solusi arsitektur ujung-ke-ujung yang digabungkan.

g. SABSA mengisi celah untuk 'arsitektur keamanan' dan 'manajemen layanan keamanan' dengan mengintegrasikan secara mulus dengan standar lain seperti TOGAF® dan ITIL®.

h. Kerangka kerja SABSA terus dipelihara dan dikembangkan dan versi terbaru diterbitkan dari waktu ke waktu,

i. Pengetahuan tentang SABSA dan bagaimana menerapkannya dapat diperoleh dan dikonfirmasikan melalui program pendidikan dan sertifikasi yang diakui di seluruh dunia, materi pelatihan, ujian dan sertifikat yang dikeluarkan oleh Institut SABSA;

j. Pendidikan, pelatihan, dan sertifikasi SABSA dapat diperoleh melalui salah satu jaringan di seluruh dunia dari Mitra Pendidikan Terakreditasi (AEP) dari SABSA Institute, dengan mendaftar dan menghadiri kursus SABSA Institute yang ditawarkan melalui AEP tersebut dan dengan mengikuti ujian yang sesuai juga ditawarkan melalui jaringan AEP,

k. SABSA dapat digabungkan ke dalam perangkat lunak komputer yang sesuai oleh vendor perangkat lunak yang ingin menawarkan alat tersebut ke pasar terbuka. Namun, untuk menjamin dukungan dari SABSA Limited dalam memvalidasi dan mengakreditasi alat tersebut, vendor hanya perlu

mendekati SABSA Limited untuk mengatur perjanjian komersial di mana dukungan tersebut akan ditawarkan;

Model SABSA

1. Model Arsitektur Berlapis

Untuk menetapkan model berlapis tentang bagaimana arsitektur keamanan dibuat, akan berguna untuk sejenak kembali ke penggunaan kata dalam pengertian konvensionalnya: konstruksi bangunan. Model SABSA terdiri dari enam lapisan, ringkasannya ada di Tabel 2.2. Ini mengikuti secara dekat pekerjaan yang dilakukan oleh John A. Zachman dalam mengembangkan model untuk arsitektur perusahaan, meskipun telah sedikit disesuaikan dengan pandangan keamanan dunia. Setiap lapisan mewakili pandangan pemain yang berbeda dalam proses menentukan, merancang, membangun, dan menggunakan bangunan.

Ada konfigurasi lain dari enam lapisan ini yang mungkin lebih membantu, ditunjukkan pada Gambar 2.1. Dalam diagram ini arsitektur manajemen layanan keamanan' telah ditempatkan secara vertikal di lima lapisan lainnya. Ini karena masalah manajemen layanan keamanan muncul di masing-masing dan setiap dari lima lapisan lainnya. Manajemen layanan keamanan memiliki arti dalam konteks masing-masing lapisan lainnya.

Tabel 2. 2 Tampilan Arsitektur Berlapis

Pandangan Bisnis	Arsitektur Keamanan Kontekstual
Pandangan Arsitek	Arsitektur Keamanan Konseptual
Pandangan Perancang	Arsitektur Keamanan Logis
Pandangan Pembangun	Arsitektur Keamanan Fisik
Pandangan Pedagang	Arsitektur Keamanan Komponen
Pandangan Manajer Layanan	Arsitektur Manajemen Layanan Keamanan

Gambar 2. 1 Model SABSA untuk Arsitektur Keamanan

Adapun beberapa aspek yang dinilai melalui beberapa sudut pandang pada arsitektur yang digunakan dalam metode SABSA, diantaranya;

2. Sudut pandang Bisnis (*Business*)

Ketika sebuah bangunan baru ditugaskan, pemilik memiliki serangkaian persyaratan bisnis yang harus dipenuhi oleh arsitektur. Pada tingkat tertinggi ini dinyatakan dengan nama deskriptif bangunan, misalnya; rumah tangga; pabrik; kantor; pusat olahraga; sekolah; Rumah Sakit; gudang; Bioskop; Pusat perbelanjaan; terminal bandara; stasiun kereta api; dan sebagainya. Masing-masing penggunaan bisnis ini menyiratkan arsitektur yang akan berbeda dari yang lain,

arsitektur yang akan memenuhi harapan fungsi bangunan dalam istilah bisnis. Saat merancang sistem bisnis yang aman, hal yang sama berlaku. Ada banyak kemungkinan pendekatan arsitektur yang dapat Anda ambil, tetapi yang paling cocok akan didorong dari pemahaman yang jelas tentang persyaratan bisnis untuk sistem.

a. Apa jenis sistem itu dan untuk apa itu akan digunakan?
b. Mengapa sistem itu akan digunakan?
c. Bagaimana sistem itu akan digunakan?
d. Siapa yang akan menggunakannya?
e. Di mana sistem itu akan digunakan?
f. Kapan sistem itu akan digunakan?

Dalam Model SABSA, pandangan bisnis ini disebut *arsitektur keamanan kontekstual*. Ini adalah deskripsi konteks bisnis di mana sistem keamanan harus dirancang, dibangun, dan dioperasikan. Dalam model yang disajikan di sini, arsitektur kontekstual berkaitan dengan:

a. Apa? Bisnis, asetnya untuk dilindungi (merek, reputasi, dll.) dan kebutuhan bisnis untuk keamanan informasi (keamanan sebagai enabler bisnis, bisnis elektronik yang aman, kelangsungan dan stabilitas operasional, kepatuhan terhadap hukum, dll.). Dalam hal arsitektur informasi tingkat tertinggi ini dinyatakan sebagai 'keputusan bisnis', bersama dengan tujuan dan sasaran bisnis.
b. Mengapa? Risiko bisnis dinyatakan dalam bentuk peluang bisnis dan ancaman terhadap aset bisnis. Risiko bisnis ini mendorong kebutuhan akan keamanan bisnis (memungkinkan bisnis, peningkatan dan perlindungan

merek, pencegahan penipuan, pencegahan kerugian, pemenuhan kewajiban hukum, pencapaian kelangsungan bisnis, dll.).

c. Bagaimana? Proses bisnis yang membutuhkan keamanan (interaksi bisnis dan transaksi, komunikasi bisnis, dll).

d. WHO? Aspek organisasi keamanan bisnis (struktur tata kelola dan manajemen, struktur rantai pasokan, hubungan outsourcing, kemitraan strategis), termasuk definisi 'perusahaan yang diperluas', yang mencakup semua mitra bisnis dan hubungan eksternal.

e. Di mana? Geografi bisnis dan aspek keamanan bisnis terkait lokasi (pasar desa global, situs perusahaan terdistribusi, kerja jarak jauh, yurisdiksi, dll.).

f. Kapan? Ketergantungan waktu bisnis dan aspek keamanan bisnis terkait waktu dalam hal kinerja dan urutan (proses transaksi bisnis, masa pakai dan tenggat waktu, operasi tepat waktu, waktu ke pasar, dll.).

3. Sudut pandang Arsitek (*Architect*)

Pandangan arsitek adalah keseluruhan konsep dimana persyaratan bisnis perusahaan dapat dipenuhi. Dengan demikian, lapisan Model SABSA ini disebut sebagai arsitektur keamanan konseptual. Ini mendefinisikan prinsip dan konsep dasar yang memandu pemilihan dan pengorganisasian elemen logis dan fisik pada lapisan abstraksi yang lebih rendah. Saat menjelaskan arsitektur keamanan perusahaan, ini adalah tempat untuk menggambarkan konsep dan prinsip keamanan yang akan digunakan. Hal tersebut termasuk:

a. Apa yang ingin dilindungi?, dinyatakan dalam kerangka SABSA dalam hal Atribut Bisnis.

SABSA *Business Attributes Profiling*, Profil ini menyediakan alat 'rekayasa persyaratan' utama yang dengannya persyaratan bisnis dapat ditangkap dalam bentuk standar yang dinormalisasi. Profil Atribut Bisnis SABSA kemudian digunakan sebagai kumpulan aset proksi untuk penilaian risiko SABSA.

b. Mengapa perlindungan tersebut penting?, dalam hal tujuan pengendalian dan pemberdayaan.

Tujuan pengendalian dan pemberdayaan diturunkan langsung dari analisis risiko operasional bisnis (penilaian risiko ini dilakukan terhadap Profil Atribut Bisnis) dan merupakan konseptualisasi motivasi bisnis untuk keamanan.

c. Bagaimana cara supaya ingin mencapai perlindungan tersebut?, dalam hal strategi keamanan manajemen dan teknis tingkat tinggi serta kerangka kerja pemetaan proses yang digunakan untuk menggambarkan proses bisnis.

Strategi-strategi ini menetapkan kerangka kerja berlapis konseptual untuk mengintegrasikan elemen taktis individu di tingkat yang lebih rendah, memastikan bahwa ini cocok dengan cara untuk memenuhi tujuan strategis keseluruhan bisnis. Strategi tersebut dapat mencakup: strategi untuk keamanan aplikasi; strategi keamanan jaringan; strategi *public key infrastructure* (PKI); *role-based access control* (RBAC); dan seterusnya. Untuk setiap area utama dari kebutuhan bisnis yang diidentifikasi dalam arsitektur keamanan kontekstual, akan ada strategi keamanan (kelompok strategi) yang mendukungnya.

d. Siapa yang terlibat dalam manajemen keamanan?, dalam hal peran dan tanggung jawab dan jenis kepercayaan bisnis yang ada di antara para pihak,

termasuk pemilik aset, penjaga dan pengguna, dan penyedia layanan dan pelanggan layanan.

e. Konsep kepercayaan penting berkaitan dengan berbagai otoritas kebijakan yang mengatur kepercayaan dalam suatu domain, kebijakan yang mereka tetapkan untuk mengatur perilaku entitas di masing-masing domain tersebut, dan hubungan kepercayaan antardomain.

f. Di mana ingin mencapai perlindungan yang dikonseptualisasikan dalam kerangka *domain* keamanan? Konsep penting di sini adalah *domain* keamanan (baik logis dan fisik), batas domain dan asosiasi keamanan.

g. Kapankah perlindungan yang relevan? dinyatakan dalam kerangka kerja manajemen waktu bisnis.

4. Sudut pandang Perancang (*Designer*)

Dalam dunia komputasi bisnis dan komunikasi data, proses desain ini sering disebut rekayasa sistem. Ini melibatkan identifikasi dan spesifikasi elemen arsitektur logis dari sistem secara keseluruhan. Pandangan ini memodelkan bisnis sebagai sistem, dengan komponen sistem tersebut, diri mereka sendiri merupakan sub-sistem. Ini menunjukkan elemen keamanan arsitektur utama dalam hal logika layanan keamanan, dan menjelaskan aliran kontrol logis dan hubungan antara elemen-elemen logis ini. Oleh karena itu juga dikenal sebagai arsitektur keamanan logis.

Arsitektur keamanan logis berkaitan dengan:

a. *What*? Informasi bisnis adalah representasi logis dari bisnis nyata. Informasi bisnis inilah yang perlu diamankan.

b. *Why*? Menentukan persyaratan kebijakan keamanan dan manajemen risiko (kebijakan keamanan tingkat tinggi, kebijakan otoritas pendaftaran, kebijakan otoritas sertifikasi, kebijakan domain fisik, kebijakan domain logis, dll.) untuk mengamankan informasi bisnis.

c. *How*? Menentukan layanan keamanan logis (otentikasi entitas, perlindungan kerahasiaan, perlindungan integritas, non- repudiation, jaminan sistem, dll.) dan bagaimana mereka cocok bersama sebagai blok bangunan umum yang dapat digunakan kembali ke dalam sistem keamanan kompleks yang memenuhi persyaratan bisnis secara keseluruhan. Aliran logis dari layanan keamanan juga ditentukan dalam hal peta proses dan spesifikasi fungsional menjelaskan fungsionalitas yang diperlukan.

d. *Who*? Menentukan entitas (pengguna, administrator keamanan, auditor, dll.) dan hubungan timbal balik mereka, atribut, peran resmi dan profil hak istimewa dalam bentuk 'skema', dan kepercayaan yang ada di antara mereka dalam bentuk kerangka kepercayaan .

e. *Where*? Menentukan domain keamanan dan hubungan antar-domain (domain keamanan logis, domain keamanan fisik, asosiasi keamanan).

f. *When*? Menentukan kalender dan jadwal terkait keamanan dalam hal waktu mulai, tenggat waktu, dan masa pakai (seperti untuk pendaftaran, sertifikasi, login, manajemen sesi, dll.).

5. Sudut pandang Pembangun (*Builder*)

Dalam dunia sistem informasi bisnis, perancang menghasilkan sekumpulan abstraksi logis yang menggambarkan sistem yang akan dibangun. Ini perlu diubah menjadi model arsitektur keamanan fisik yang menggambarkan model

teknologi aktual dan menentukan desain rinci dari berbagai komponen sistem. Layanan keamanan logis sekarang dinyatakan dalam mekanisme keamanan fisik dan server yang akan digunakan untuk memberikan layanan ini. Secara total, arsitektur keamanan fisik berkaitan dengan:

a. Apa? Menentukan model data bisnis dan struktur data terkait keamanan (tabel, pesan, pointer, sertifikat, tanda tangan, dll.)
b. Mengapa? Menentukan aturan yang mendorong pengambilan keputusan logis dalam sistem (kondisi, praktik, prosedur, dan tindakan).
c. Bagaimana? Menentukan mekanisme keamanan (enkripsi, kontrol akses, tanda tangan digital, pemindaian virus, dll.) dan aplikasi fisik, middleware, dan server tempat mekanisme ini akan dihosting.
d. Siapa? Menentukan ketergantungan orang dalam bentuk antarmuka manusia (format layar dan interaksi pengguna) dan sistem kontrol akses.
e. Dimana? Menentukan infrastruktur teknologi keamanan dalam bentuk platform host dan jaringan (tata letak fisik perangkat keras, perangkat lunak, dan jalur komunikasi).
f. Kapan? Menentukan manajemen waktu fisik dalam hal waktu dan urutan proses dan sesi (urutan, peristiwa, masa hidup dan interval waktu).

6. Sudut pandang Pedagang (*Tradesman*)

Ketika pembangun merencanakan proses konstruksi, ia perlu mengumpulkan tim ahli di setiap perdagangan bangunan yang akan dibutuhkan: tukang batu, tukang plester, tukang listrik, tukang ledeng, tukang kayu, dan sebagainya. Masing-masing membawa beberapa keterampilan produksi yang

sangat spesifik dan beberapa produk yang sangat spesifik untuk proses konstruksi secara keseluruhan.

Setiap pemasang dan integrator setara dengan seorang pedagang, bekerja dengan produk spesialis dan komponen sistem yang setara dengan bahan dan komponen bangunan. Beberapa dari 'perdagangan' ini terkait dengan perangkat keras, beberapa terkait dengan perangkat lunak, dan beberapa berorientasi pada layanan. 'Pedagang' bekerja dengan serangkaian komponen yang merupakan item perangkat keras, item perangkat lunak, dan spesifikasi serta standar antarmuka. Oleh karena itu lapisan model arsitektur ini juga disebutarsitektur keamanan komponen. Arsitektur komponen berkaitan dengan:

a. Apa? Komponen TIK seperti produk TIK, termasuk tempat penyimpanan dan pengolah data.
b. Mengapa? Alat dan produk terkait manajemen risiko seperti alat analisis risiko, register risiko, pemantauan risiko, dan alat pelaporan.
c. Bagaimana? Alat dan standar proses (alat dan protokol untuk pengiriman proses - baik perangkat keras maupun perangkat lunak).
d. Siapa? Alat dan produk manajemen personalia (identitas, deskripsi pekerjaan, peran, fungsi, tindakan, dan daftar kontrol akses).
e. Dimana? Alat dan standar locator (node, alamat, dan locator lainnya).
f. Kapan? Pengaturan waktu langkah dan alat pengurutan (jadwal waktu, jam, timer, dan interupsi).

7. Sudut pandang Manajer Layanan (*Service Manager*)

Ketika bangunan itu selesai, mereka yang merancang, merancang, dan membangunnya pindah, tetapi seseorang harus menjalankan bangunan itu

selama masa pakainya. Orang seperti ini sering disebut manajer fasilitas atau manajer layanan. Tugas manajer layanan adalah menangani pengoperasian gedung dan berbagai layanannya, memeliharanya agar berfungsi dengan baik, dan memantau seberapa baik kinerjanya dalam memenuhi persyaratan. Kerangka kerja untuk melakukan ini disebutarsitektur keamanan manajemen layanan.

Dalam ranah sistem informasi bisnis, arsitektur manajemen layanan berkaitan dengan operasi sistem klasik dan pekerjaan manajemen layanan. Di sini fokus perhatian hanya pada bagian yang berhubungan dengan keamanan dari pekerjaan itu. Arsitektur manajemen layanan keamanan memperhatikan hal-hal berikut:

a. Apa? Manajemen penyampaian layanan (jaminan kelangsungan operasional dan keunggulan sistem bisnis dan pemrosesan informasi, serta menjaga keamanan data dan informasi bisnis operasional).
b. Mengapa? Manajemen risiko operasional (penilaian risiko, pemantauan dan pelaporan risiko, serta perlakuan risiko untuk meminimalkan kegagalan dan gangguan operasional).
c. Bagaimana? Manajemen pengiriman proses (manajemen dan dukungan sistem, aplikasi dan layanan, melakukan operasi terkait keamanan khusus seperti administrasi keamanan pengguna, administrasi keamanan sistem, pencadangan data, pemantauan keamanan, prosedur tanggap darurat, dll.).
d. Siapa? Manajemen personalia (penyediaan akun dan manajemen dukungan pengguna untuk kebutuhan terkait keamanan semua pengguna dan aplikasi mereka, termasuk pengguna bisnis, operator, administrator, dll.).

e. Dimana? Pengelolaan lingkungan (manajemen bangunan, situs, platform dan jaringan).

f. Kapan? Jadwal manajemen (mengelola kalender dan jadwal terkait keamanan).

Namun, merujuk kembali ke Gambar 2.1, ada dimensi lain pada arsitektur manajemen layanan keamanan hubungan vertikalnya dengan lima lapisan model lainnya. Dengan demikian arsitektur manajemen layanan keamanan perlu diinterpretasikan secara rinci pada masing-masing dan setiap satu dari lima lapisan lainnya. Hal ini ditunjukkan pada Tabel 2.3, dengan beberapa contoh jenis kegiatan operasional yang tersirat berkaitan dengan masing-masing lapisan.

Tabel 2. 3 Arsitektur Manajemen Layanan Keamanan

Kontekstual	Pengembangan penggerak bisnis, penilaian risiko bisnis, manajemen layanan, manajemen hubungan, manajemen titik pasokan, dan manajemen kinerja.
Konseptual	Mengembangkan Profil Atribut Bisnis, mengembangkan tujuan manajemen risiko operasional melalui penilaian risiko, perencanaan pemberian layanan, menentukan peran manajemen layanan, tanggung jawab, kewajiban dan nilai budaya, manajemen portofolio layanan, perencanaan dan pemeliharaan katalog layanan dan pengelolaan kriteria dan target kinerja layanan (layanan definisi tingkat)

Tabel 2.3. (Lanjutan)

Logis	Manajemen aset, manajemen kebijakan, manajemen pengiriman layanan, dukungan pelanggan layanan, manajemen katalog layanan, dan manajemen evaluasi layanan
Fisik	Keamanan dan perlindungan aset, pengumpulan data risiko operasional, manajemen operasi, dukungan pengguna, perlindungan sumber daya layanan, dan pengumpulan data kinerja layanan.
Komponen	Perlindungan alat, alat manajemen risiko operasional, penyebaran alat, penyebaran personel, alat manajemen keamanan, dan alat pemantauan layanan

8. Sudut pandang Inspektur (*Inspector*)

Ada pandangan lain dari keamanan dalam sistem informasi bisnis, Pandangan Inspektur, yang berkaitan dengan memberikan jaminan bahwa arsitektur lengkap, konsisten, kuat dan 'cocok untuk tujuan' dalam segala hal. Di bidang keamanan sistem informasi, ini adalah proses 'audit keamanan' yang dilakukan oleh 'auditor komputer' atau personel 'penjaminan kualitas sistem'. Namun, kerangka SABSA tidak mengenali ini sebagai tampilan arsitektur yang terpisah. Pendekatan SABSA untuk audit dan jaminan adalah bahwa model arsitektur secara keseluruhan mendukung kebutuhan ini. Keberadaan arsitektur tersebut merupakan salah satu cara auditor akan menetapkan bahwa keamanan diterapkan secara sistematis dan tepat. Kerangka kerja itu sendiri dapat menyediakan sarana untuk menyusun proses audit. Selain itu, audit dan tinjauan keamanan ditujukan sebagai salah satu program

strategis utama dalam arsitektur manajemen layanan keamanan yang terkait dengan lapisan konseptual.

9. Sudut pandang Pemerintahan (*Governor*)

Pandangan lain dari manajemen keamanan informasi adalah Pandangan Gubernur. Ini memiliki kesamaan dengan Pandangan Inspektur karena menyebar ke seluruh kerangka SABSA, yang semuanya perlu diatur. Namun, ada dua titik fokus untuk pandangan ini yang akan menjadi jelas saat Anda membaca lebih lanjut dan menemukan lebih banyak tentang kolom detail yang merupakan potongan vertikal Matriks SABSA. Ini adalah kolom 'orang', yang berhubungan langsung dengan tata kelola dan manajemen, dan kolom 'motivasi' yang secara khusus menangani manajemen risiko, pembuatan kebijakan dan pemantauan serta pelaporan kepatuhan terhadap kebijakan. Kedua bidang Matriks SABSA ini merupakan pendorong utama pengaruh Gubernur terhadap program manajemen keamanan informasi secara keseluruhan.

Matriks SABSA

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:

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

Gambar 2. 2 Lapisan dan matriks Kelengkapan (*Completeness*)

b. 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. 3 Lapisan dan matriks Justifikasi Bisnis (*Business Justification*)

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

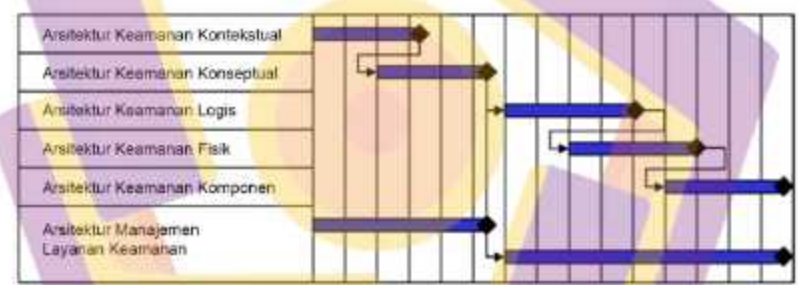
Gambar 2. 4 Matriks SABSA

	ASET (Apa)	MOTIVASI (Mengapa)	PROSES (Cara)	Orang yang)	LOKASI (Dimana)	WAKTU (Kapan)
	[illegible] Pengelolaan	[illegible] Pengelolaan	Proses Pengiriman Pengelolaan	Personil Pengelolaan	Manajemen dari Lingkungan	Waktu & Performa Pengelolaan
	Baris di atas adalah pengulangan Layer 6 dari Matriks SABSA utama. [illegible]					
KONTEKSTUAL ARSITEKTUR	[illegible]	Resiko bisnis Penilaian	[illegible] Pengelolaan	Hubungan Pengelolaan	Titik Pasokan Pengelolaan	Pertunjukan Pengelolaan
	Bisnis Tolok Ukur & Identifikasi Penggerak Bisnis	Analisis Internal & Risiko Eksternal Faktor	[illegible] pelanggan	Mengelola Penyedia Jasa & Pelanggan Layanan; Manajemen Kontrak	[illegible]	Mendefinisikan Bisnis Kinerja yang Didorong Target
KONSEPTUAL ARSITEKTUR	Aset Proksi Pengembangan	[illegible] Tujuan	[illegible]	[illegible] Peran Manajemen	[illegible]	[illegible] Definisi
	Mendefinisikan Bisnis Profil Atribut dengan Kinerja Kriteria, KPI & KRI	[illegible] Atribut Bisnis Aset Proksi	Perencanaan SLA, BCP, Perencanaan keuangan & ROI; Transisi [illegible]	[illegible] tanggung jawab, Kewajiban & Budaya Nilai	[illegible] Katalog Layanan	Layanan Pengelolaan Kriteria kinerja dan Target
LOGIS ARSITEKTUR	Manajemen aset	Manajemen Kebijakan	Pengiriman Layanan Pengelolaan	Layanan Pelanggan [illegible]	Katalog Layanan Pengelolaan	Evaluasi Pengelolaan
	Pengetahuan Pengelolaan; [illegible] & Penyebaran Pengelolaan; Uji & Validasi Pengelolaan	Pengembangan Kebijakan Kesadaran Kebijakan audit	Manajemen SLA; [illegible] Pengelolaan; SM; Manajemen Biaya; Transisi Pengelolaan	[illegible] Administrasi & Penyediaan	Konfigurasi Pengelolaan; [illegible] Pengelolaan	Pemantauan & Pelaporan Performa melawan KPI dan KRI
FISIK ARSITEKTUR	Keamanan Aset & [illegible]	[illegible]	Operasi Pengelolaan	[illegible]	[illegible]	[illegible] Data kinerja Koleksi
	[illegible] Pengelolaan; [illegible]	Resiko operasional Pengelolaan Arsitektur	[illegible] Pengelolaan; Pemulihan bencana	Meja pelayanan; Manajemen Masalah; [illegible]	Fisik & Lingkungan Keamanan Pengelolaan	Sistem dan Pemantauan Layanan Arsitektur
KOMPONEN ARSITEKTUR	[illegible] Alat	Alat ORM	Penyebaran Alat	Personil Penyebaran	Keamanan Alat Manajemen	[illegible]
	Produk & Alat [illegible] Produk & Alat Pemeliharaan	Analisis ORM, Pemantauan dan Alat Pelaporan & Sistem Tampilan	Produk & Alat Seleksi dan Pengadaan; Manajemen proyek	Proses Rekrutmen Proses Disiplin Pelatihan & Alat Kesadaran	Produk & Alat untuk Mengelola Fisik & Keamanan Logis dan Instalasi	Analisis Layanan, Pemantauan dan Alat Pelaporan & Sistem Tampilan

Gambar 2. 5 Matriks manajemen layanan sabsa (sejajar dengan ITIL v3)

Proses Pembangunan SABSA

Model SABSA memberikan dasar untuk proses pengembangan arsitektur, karena jelas bahwa melalui pemahaman kebutuhan bisnis, arsitek dapat membuat visi awal. Ini digunakan oleh desainer untuk membuat desain detail, yang pada gilirannya digunakan oleh pembangun untuk membangun sistem, dengan berbagai macam komponen yang disediakan oleh spesialis. Akhirnya, manajer fasilitas mengoperasikan sistem yang sudah jadi, tetapi kecuali fase sebelumnya memperhitungkan kebutuhan manajemen operasional dan layanan, fase ini dalam masa pakai sistem akan penuh dengan kesulitan. Proses pengembangan itu sendiri ditunjukkan, pada tingkat tinggi, pada gambar 2.6.



Gambar 2. 6 Proses Pengembangan SABSA

Proses pengembangan tingkat tinggi pada Gambar 4 menunjukkan bahwa ada jeda alami setelah dua fase pertama. Setelah Arsitektur Keamanan Kontekstual dan Arsitektur Keamanan Konseptual disetujui dan ditandatangani, maka pekerjaan pada fase selanjutnya dapat dimulai, dengan kerja paralel yang cukup besar. Namun, sulit untuk membuat kemajuan yang berguna pada tahap selanjutnya sampai dua tahap pertama ini cukup jelas. Godaan untuk langsung ke implementasi produk dan alat tertentu harus dihindari, karena ini adalah sumber dari begitu

banyak masalah parah selama fase operasional. Pengembangan sub-proses Arsitektur Manajemen Layanan Keamanan perlu dimulai tepat di awal proses, karena aspek ini diperlukan untuk pengembangan Arsitektur Keamanan Kontekstual dan Konseptual. Sekali lagi, ada jeda alami saat dua fase pertama di tandatangani, setelah itu pengembangan Arsitektur Manajemen Layanan Keamanan dapat dilanjutkan.

Siklus Hidup SABSA

Proses Pengembangan SABSA dapat dilihat dalam konteks Siklus Hidup SABSA secara keseluruhan untuk arsitektur keamanan, yang ditunjukkan pada Gambar 2.7. Dalam Siklus Hidup SABSA ini, dua fase pertama dari proses dikelompokkan ke dalam aktivitas yang disebut 'Strategi dan Perencanaan'. Ini diikuti oleh aktivitas yang disebut 'Desain', yang mencakup desain arsitektur manajemen logis, fisik, komponen, dan layanan. Kegiatan ketiga adalah *'Implement'*, dilanjutkan dengan *'Manage and Measure'*.

Pentingnya aktivitas *"Strategi dan Planning"* adalah bahwa di awal proses Anda menetapkan metrik kinerja target (lihat pembahasan Profil Atribut Bisnis SABSA di bawah). Setelah sistem beroperasi, penting untuk mengukur kinerja aktual terhadap target, dan untuk mengelola setiap penyimpangan yang diamati. Manajemen tersebut mungkin hanya melibatkan manipulasi parameter operasional, tetapi juga dapat memberikan umpan balik ke siklus pengembangan baru. Kegagalan untuk memenuhi tujuan kinerja adalah peristiwa risiko. Jadi sasaran kinerja (atau indikator kinerja utama – KPI) juga mampu dilihat dari perspektif yang berlawanan sebagai indikator risiko utama (KRI). Biasanya dalam kerangka SABSA untuk menetapkan dua indikator kinerja atau risiko. Indikator

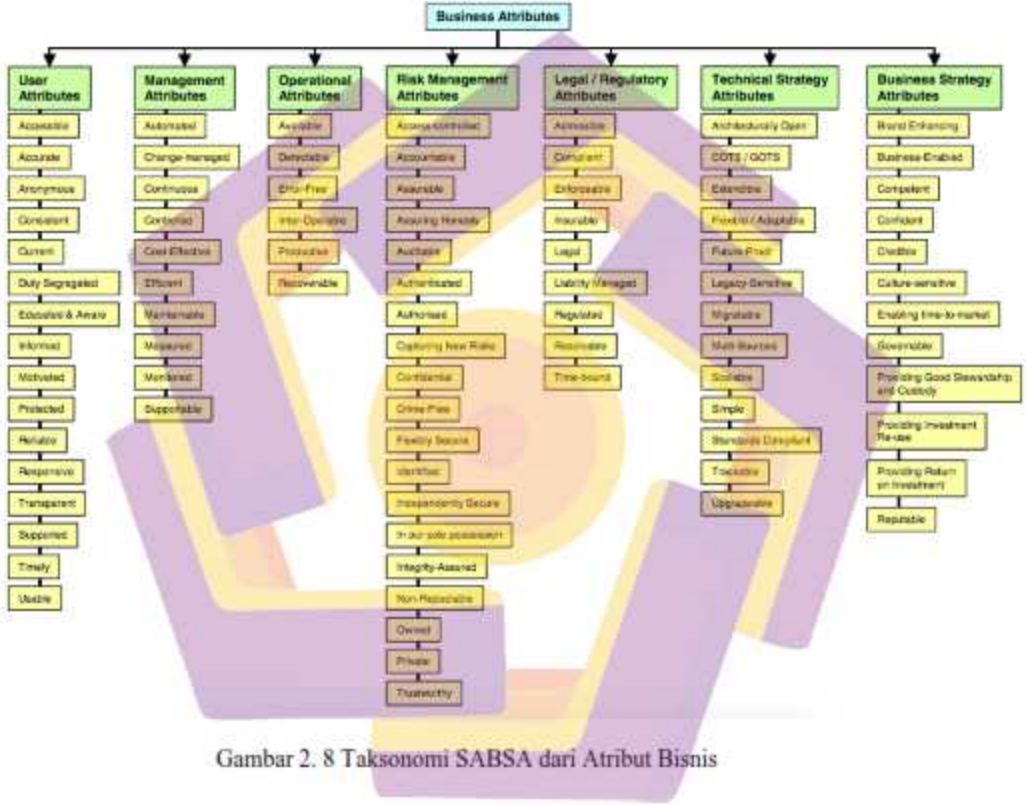
utama adalah ambang batas target aktual yang mewakili batas kinerja yang dapat diterima (juga merupakan ekspresi dari selera risiko), tetapi indikator sekunder lainnya dapat digunakan sebagai mekanisme peringatan dini untuk memberikan kesempatan untuk mengelola risiko kembali dalam zona nyaman. organisasi sebelum selera risiko ini terlampaui. Ini cocok untuk 'pelaporan lampu lalu lintas' pada kartu skor dan dasbor, menggunakan kode warna hijau, kuning dan merah.

Gambar 2. 7 SABSA *Lifecycle*

Profil Atribut Bisnis SABSA adalah inti dari metodologi SABSA. Teknik "*requirements engineering*" inilah yang membuat SABSA benar-benar unik dan menyediakan hubungan antara kebutuhan bisnis dan desain teknologi/proses.

Business Attributes Profiling adalah alat yang sangat kuat yang memungkinkan setiap kebutuhan bisnis yang unik untuk diterjemahkan, distandarisasi dan 'dinormalisasi' ke dalam format SABSA. Setiap profil hanya memilih Atribut Bisnis SABSA yang berlaku untuk bisnis spesifik organisasi (membuat atribut baru jika ditemukan celah). Taksonomi menyediakan daftar periksa atribut yang mungkin dan analis bisnis dapat memutuskan apakah atribut yang diberikan harus dimasukkan dalam profil khusus ini atau tidak.

Profil Atribut Bisnis SABSA adalah konseptualisasi penting dari bisnis nyata, dan membentuk bagian inti dari 'Arsitektur Keamanan Konseptual'. Dapat dilihat pada baris 2, kolom 1 dari Matriks SABSA pada Tabel 3. Ini juga memungkinkan pemilihan metrik yang digunakan untuk menetapkan target kinerja sebagai bagian integral dari Profil Atribut Bisnis SABSA yang nantinya dapat diukur (apakah Anda mencapai target?). Ini juga merupakan pilihan analis bisnis, baik menggunakan metrik yang disarankan dalam definisi rinci atribut, atau membuat metrik baru jika tampaknya lebih sesuai. Jadi aktivitas 'Kelola & Ukur' dalam Siklus Hidup SABSA didasarkan pada Profil Atribut Bisnis SABSA yang ditetapkan selama aktivitas 'Strategi & Perencanaan', dan yang telah disesuaikan secara khusus untuk membuat konsep bisnis organisasi unik ini.



Gambar 2. 8 Taksonomi SABSA dari Atribut Bisnis

Gambar 2. 9 Taksonomi SABSA dari Atribut Bisnis ICT

Manajemen Resiko SABSA

Dalam kerangka SABSA ada penekanan besar pada dualitas risiko-keseimbangan antara peluang dan ancaman. Banyak definisi 'risiko operasional' melewatkan poin penting ini dan hanya fokus pada risiko penurunan atau potensi kerugian. Hal ini sangat disayangkan, karena manajemen risiko operasional memberikan banyak peluang untuk mengembangkan keunggulan operasional dan meningkatkan layanan dan pengiriman produk kepada pelanggan. Ini juga dapat berkontribusi secara signifikan untuk memenuhi tujuan kinerja perusahaan dan membantu manajer lini individu untuk mencapai KPI target pribadi mereka. SABSA sepenuhnya mencakup aspek 'peluang' ini dari manajemen risiko operasional pada umumnya dan manajemen risiko informasi pada khususnya. Gambar 2.10 menunjukkan ini dalam format diagram.

Gambar 2. 10 Model Risiko Operasional SABSA

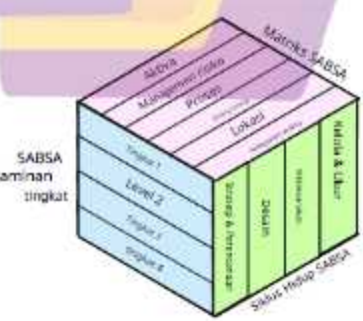
Gambar 2. 11 Proses Manajemen Risiko SABSA

Berdasarkan Model Risiko Operasional SABSA dengan mengenali peluang dan ancaman, kerangka kerja SABSA juga menyediakan Proses Manajemen Risiko SABSA ujung ke ujung yang mencakup setiap tahap Siklus Hidup SABSA secara rinci. Gambar 2.11 memberikan dan ringkasan ikhtisar dari proses manajemen risiko ini dan Gambar 2.12 menunjukkan tingkat detail berikutnya. Rincian lengkap dari proses ini dijelaskan dalam standar SABSA.

Gambar 2. 12 Rincian Proses Manajemen Risiko SABSA

Jaminan SABSA

Komponen 'Assure' dari proses Manajemen Risiko SABSA juga memiliki SABSA Assurance *Framework*-nya sendiri yang ditunjukkan pada Gambar 2.13, menawarkan kemungkinan tingkat jaminan yang berbeda untuk kebutuhan bisnis yang berbeda. Ini juga dapat diterapkan pada setiap kolom Matriks SABSA dan untuk setiap tahapan Siklus Hidup SABSA. Rincian lengkap tentang bagaimana model ini digunakan dijelaskan dalam standar SABSA.



Gambar 2. 13 Kerangka Jaminan SABSA

Tata Kelola SABSA

Gambar 2.14 menunjukkan ikhtisar Proses Tata Kelola SABSA, yang sekali lagi dipetakan ke dalam empat tahap Siklus Hidup SABSA.

Gambar 2. 14 Proses Tata Kelola SABSA

Sherwood Applied Business Security Architecture (SABSA) merupakan metodologi pengembangan arsitektur enterprise information security dan information assurance yang berdasarkan risk-driven dan bertujuan untuk menghasilkan solusi infrastruktur yang aman. Ini merupakan standar terbuka, yang terdiri dari sejumlah kerangka, model, metode dan proses. SABSA bersifat gratis untuk digunakan oleh semua pihak, tanpa lisensi yang diperlukan untuk organisasi pengguna akhir yang memanfaatkan standar dalam mengembangkan dan melaksanakan arsitektur dan solusi enterprise. Karakteristik SABSA dapat dijelaskan sebagai berikut (Sherwood, J., Clark, A. dan Lynas D.: 2009):

a. Merupakan suatu *open standard*, berisi *framework*, model, metode dan proses yang bersifat *free-licensing*;

b. Tidak terkait dengan solusi TI tertentu yang dikeluarkan oleh suatu vendor;
c. Bersifat *scalable* yang artinya dapat diimplementasikan sedikit demi sedikit secara *incremental*;
d. Dapat diterapkan di berbagai sektor industri dan jenis organisasi;
e. Dapat diterapkan untuk arsitektur organisasi yang kecil ataupun berskala *enterprise*;
f. Tidak menggantikan atau menyaingi *framework* yang ada seperti information risk atau information security. SABSA lebih bersifat melingkupi atau mengintegrasikan *framework* yang telah ada;
g. Mengisi gap antara security architecture dan security service management dengan cara mengintegrasikan standar yang telah ada seperti TOGAF dan ITIL;
h. *Framework* selalu diperbaiki dan dikembangkan secara terus menerus;
i. Pengetahuan mengenai SABSA dapat diberikan melalui training dan sertifikasi yang diatur oleh SABSA Institute; dan
j. SABSA dapat diintegrasikan dengan suatu software tool yang telah memiliki akreditasi dari SABSA.

Enterprise Architecture (EA) adalah sebuah cara untuk membuat tampilan abstrak dari sebuah perusahaan (*enterprise*) atau organisasi yang membantu dalam membuat perencanaan dan keputusan yang lebih baik. Menurut IBM, ruang lingkup dari EA itu tidak hanya terpaku pada perencanaan strategis bisnis perusahaan saja, melainkan bagaimana menyelaraskan strategi bisnis dengan IT perusahaan tersebut.

Lingkup EA tidak hanya sebatas pada perencanaan teknologi saja, melainkan mencakup perencanaan strategis sebagai pendorong utama bagi perusahaan dan perencanaan bisnis kebutuhan sumber daya perusahaan. Berdasarkan definisi tersebut, maka dapat dihasilkan formula sederhana dari EA, yang melibatkan Strategi (S), Bisnis (B) dan Teknologi (T) :

EA = S + B + T

TOGAF (*The Open Group's Architecture Framework*) merupakan sebuah *framework* EA yang dikembangkan oleh *The Open Group* sejak tahun 1995 sampai sekarang [12]. TOGAF ini digunakan untuk mengembangkan Arsitektur Enterprise, dimana terdapat metode dan tools yang detail untuk mengimplementasikannya, hal ini lah yang membedakan dengan *framework* Arsitektur Enterprise lainnya misalnya *Zachman*. Salah satu kelebihan menggunakan *framework* TOGAF ini adalah karena sifatnya yang fleksibel dan bersifat open source. TOGAF ini menyediakan metode dan tools yang digunakan untuk membangun, mengelola dan mengimplementasikan serta pengembangan dan pemeliharaan *Enterprise Architecture*. TOGAF memberikan metode yang detail bagaimana membangun, mengelola serta mengimplementasikan Enterprise Architecture dengan menggunakan *Architecture Development Method* (ADM). Metode ADM ini digunakan sebagai panduan untuk merencanakan, merancang, mengembangkan dan mengimplementasikan EA.

Integrasi SABSA dan TOGAF

1. Aturan Integrasi

SABSA dan TOGAF sama-sama berfokus kepada bisnis, serta memiliki visi arsitektur sebagai sebuah *blueprint architecture* untuk perusahaan. Pada penelitian ini, proses integrasi kedua *framework* ini dibatasi pada beberapa aturan sebagai berikut:

1. Ketika artefak yang sama muncul pada level arsitektur yang berbeda, level abstraksi yang digunakan untuk pemetaan (*mapping*) adalah level arsitektur yang tertinggi. Melalui cara ini, proses integrasi akan terus fokus pada level perusahaan (*enterprise*) sehingga dapat sejalan dengan arsitektur SABSA.

2. Proses pemetaan dibuat secara praktis dan terstruktur dalam bentuk matriks tabel, sehingga hasilnya dapat dipahami secara jelas oleh perusahaan yang akan menggunakan *blueprint* tersebut.

3. Ruang lingkup integrasi terbatas pada elemen dan konsep artefak yang paling penting dan berguna.

2. Pilar Integrasi TOGAF dan SABSA

Integrasi TOGAF-SABSA didasarkan pada tiga pilar, diantaranya;

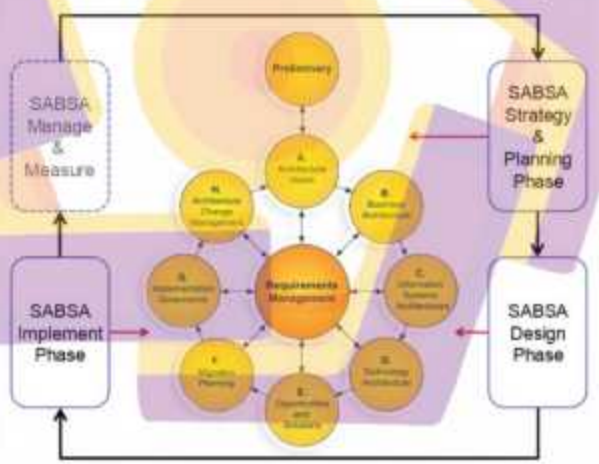
1. *Security Measures* (Pemilihan langkah-langkah keamanan) didasarkan pada manajemen resiko dimana pendekatan SABSA dalam implementasi manajemen resiko didasarkan pada perspektif kebutuhan bisnis.

2. *Requirement Management* memegang peran sentral dalam pengembangan arsitektur TOGAF. TOGAF tersebut mengintegrasikan pendekatan kebutuhan atribut bisnis SABSA untuk menyediakan teknik yang kuat dalam membangun arsitektur security.

3. *Integration Process* dalam penelitian ini adalah dengan melakukan proses pemetaan (*mapping*) dan permodelan artefak arsitektur keamanan SABSA yang relevan dengan setiap fase dari TOGAF-ADM.

3. Integrasi SABSA *Lifecycle* dengan TOGAF-ADM

Gambar 2.15 memperlihatkan ilustrasi integrasi SABSA *Lifecycle* kedalam TOGAF-ADM, dimana masing-masing fase pada ADM dikelompokkan ke setiap tahapan *Lifecycle* pada SABSA. ADM mencakup komponen-komponen artefak (*block dan buliding*) yang dihasilkan pada setiap fase, sedangkan SABSA mencakup artefak security yang secara relevan akan dipetakan (mapping) sesuai dengan fase-fase ADM tersebut.



Gambar 2. 15 Integrasi SABSA *Lifecycle* kedalam TOGAF-ADM

Integrasi SABSA *Lifecycle* dengan TOGAF-ADM dapat dilakukan dengan mengaitkan tahap-tahap dari SABSA *Lifecycle* dengan tahap-tahap dari TOGAF-ADM *(The Open Group Architecture Development Method).*

1. SABSA Analisis Bisnis dapat digabungkan dengan TOGAF-ADM tahap 1, yaitu "*Architecture Vision*".
2. SABSA Analisis Risiko dapat digabungkan dengan TOGAF-ADM tahap 2, yaitu "Business Architecture"
3. SABSA Arsitektur dapat digabungkan dengan TOGAF-ADM tahap 3 dan 4, yaitu "*Information Systems Architecture*" dan "*Technology Architecture*".
4. SABSA Desain dapat digabungkan dengan TOGAF-ADM tahap 5, yaitu *"Operations Architecture"*
5. SABSA Implementasi dapat digabungkan dengan TOGAF-ADM tahap 6, yaitu *"Migrating to Target Architecture"*
6. SABSA Pemeliharaan dapat digabungkan dengan TOGAF-ADM tahap 7, yaitu "*Implementing Governance*"
7. Integrasi arsitektur keamanan yang dikembangkan dengan arsitektur bisnis, teknologi, dan informasi yang dikembangkan dengan menggunakan metode TOGAF.
8. Penyesuaian arsitektur keamanan yang dikembangkan selama proses integrasi dengan arsitektur bisnis, teknologi, dan informasi yang dikembangkan dengan menggunakan metode TOGAF.
9. Validasi arsitektur keamanan yang dikembangkan selama proses integrasi dengan arsitektur bisnis, teknologi, dan informasi yang dikembangkan dengan menggunakan metode TOGAF.

10. Implementasi arsitektur keamanan yang dikembangkan selama proses integrasi dengan arsitektur bisnis, teknologi, dan informasi yang dikembangkan dengan menggunakan metode TOGAF.

Selain itu dalam pengintegrasian SABSA *Lifecycle* dengan TOGAF, terdapat empat fase utama yang perlu diperhatikan:

1. Fase Strategi dan Perencanaan: Fase ini melibatkan pemahaman dan dokumentasi bisnis, tujuan, dan kebutuhan organisasi. Selain itu, pada fase ini juga melibatkan analisis risiko dan pengembangan arsitektur keamanan yang sesuai dengan bisnis dan risiko yang diidentifikasi. Pada fase ini SABSA *Lifecycle* digabungkan dengan tahap *Business Architecture, Information Systems Architecture, dan Technology Architecture* dari TOGAF-ADM.
2. Fase Desain : Fase ini melibatkan pengembangan desain solusi keamanan yang sesuai dengan arsitektur yang telah dikembangkan pada tahap sebelumnya. Tujuan dari fase desain adalah untuk mengembangkan rencana keamanan yang dapat diimplementasikan dengan sukses dan digunakan dengan efektif untuk melindungi aset bisnis yang relevan. Fase desain ini sangat penting karena dalam fase ini arsitektur keamanan yang akan diterapkan dalam organisasi sudah ditetapkan dan dirancang, sehingga dapat memberikan gambaran yang jelas tentang solusi keamanan yang akan diterapkan dan dapat mempercepat proses implementasi.

3. Fase Implementasi: Fase di mana rencana keamanan yang telah dikembangkan dalam fase analisis dan desain diterapkan dalam sistem operasi atau lingkungan yang sebenarnya. Dalam fase ini, perangkat lunak dan perangkat keras keamanan diterapkan, konfigurasi diatur, prosedur operasi ditetapkan, dan pelatihan diberikan kepada staf yang terkait. Tujuan dari fase implementasi adalah untuk memastikan bahwa solusi keamanan yang ditentukan dapat diimplementasikan dengan sukses dan digunakan dengan efektif untuk melindungi aset bisnis yang relevan. Pada fase ini SABSA *Lifecycle* digabungkan dengan tahap *Operations Architecture dan Migrating to Target Architecture* dari TOGAF-ADM
4. Fase Manajemen dan Pemeliharaan: Fase ini melibatkan pemeliharaan dan peningkatan solusi keamanan yang telah diimplementasikan. Pada fase ini SABSA *Lifecycle* digabungkan dengan tahap *Implementing Governance* dari TOGAF-ADM.

Pada setiap fase ini, perlu diperhatikan kompatibilitas dan integrasi antara arsitektur keamanan yang dikembangkan dengan arsitektur bisnis, teknologi, dan informasi yang dikembangkan dengan menggunakan metode TOGAF.

BAB III

METODE PENELITIAN

3.1. Jenis, Sifat, dan Pendekatan Penelitian

Penelitian ini merupakan penelitian kualitatif yang menggunakan metode *action research*. Penelitian kualitatif berakar pada latar belakang ilmiah sebagai kebutuhan, mengarahkan sasaran penelitiannya pada usaha menemukan teori dari dasar yang bersifat deskriptif, mengandalkan analisis data secara induktif, lebih mementingkan proses dan hasil, membatasi studi dengan fokus memiliki seperangkat kriteria untuk memeriksa keabsahan data, dan rancangan penelitiannya bersifat sementara, serta hasil penelitiannya disepakati oleh kedua belah pihak antara peneliti dan objek penelitian (Moleong, L.J., 2005). Berdasarkan pendapat-pendapat tersebut, penelitian kualitatif berfokus kepada kejadian atau fenomena alamiah pada peristiwa yang dialami oleh objek penelitian.

Metode *action research* merupakan penelitian yang berfokus langsung pada tindakan sosial. *action research* ini didasarkan pada tindakan masyarakat yang dilakukan di suatu tempat yang terdapat manajemen di lingkungan tersebut seperti instansi rumah sakit, sekolah, pabrik, agensi, dan lain sebagainya (Hasibuan., 2007). *Action research* juga merupakan langkah-langkah nyata dalam mencari yang paling cocok untuk memperbaiki keadaan di lingkungan tersebut (Taggart, M., 1991). *Action research* terdiri dari satu, dua, tiga, atau empat siklus, yang mana masing-masing siklus terdiri dari; *look*, *think*, and *act*. *Look* merupakan fase mengumpulkan data atau informasi yang relevan. *Think* yaitu menggali dan

menganalisis apa yang terjadi pada objek penelitian, dan *Act* terdiri dari perencanaan tindakan dan implementasi serta meng-evaluasi.

Studi kasus yang dilakukan pada penelitian ini adalah Scaleout Creative Agency, merupakan sebuah perusahaan yang bergerak di bidang rumah produksi dan marketing, fungsi dan peran sebagai layanan jasa marketing untuk UKM atau *brand owner*. Scaleout Creative Agency ini berperan sebagai penyedia layanan dalam industri kreatif, seperti desain grafis, pengembangan web, atau produksi konten (video dan foto).

Yogyakarta dipilih sebagai lokasi agensi kreatif karena kota ini dikenal sebagai pusat seni dan budaya di Indonesia, dengan banyaknya komunitas seni dan perguruan tinggi yang memiliki jurusan terkait seni dan kreativitas. Hal ini menciptakan lingkungan yang mendukung perkembangan industri kreatif di Yogyakarta. Scaleout juga memiliki spesialisasi dalam melayani klien dari luar kota, yang mencakup klien individu, perusahaan, atau organisasi yang ingin memanfaatkan keahlian kreatif agensi untuk memenuhi kebutuhan mereka. Preferensi klien yang berbeda dapat mencakup preferensi gaya desain, target audiens, atau tujuan komunikasi yang ingin dicapai melalui proyek kreatif, tergantung juga pada penyesuaian jenis konten mengenai preferensi target iklan di daerah tersebut.

Salah satu tantangan yang dihadapi oleh agensi kreatif di Yogyakarta adalah adanya banyak pendatang di kota tersebut dengan preferensi yang berbeda-beda. Dengan keberagaman pendatang yang datang ke Yogyakarta, agensi kreatif harus memiliki pemahaman yang mendalam tentang preferensi masing-masing

pendatang. Setiap individu memiliki latar belakang, budaya, dan preferensi yang unik, sehingga Scaleout Creative Agency harus mampu memahami kebutuhan dan harapan dari setiap klien.

Agensi kreatif dapat mengatasi tantangan ini dengan melakukan penelitian dan analisis pasar yang mendalam. Hal ini dapat dilakukan melalui observasi terhadap pendatang yang ada di Yogyakarta secara langsung atau dari sosial media. Dengan memahami preferensi dan kebutuhan mereka, Scaleout dapat mengembangkan strategi pemasaran yang tepat untuk menarik perhatian dan memenuhi harapan klien. Selain itu, Scaleout juga dapat memanfaatkan teknologi dan media sosial untuk mencapai target pasar yang lebih luas. Dengan menggunakan platform digital, agensi kreatif dapat menjangkau pendatang yang lebih banyak dan memperkenalkan layanan mereka secara efektif.

Selain memahami preferensi klien, Scaleout beradaptasi dengan keberagaman budaya dan nilai-nilai yang ada di Yogyakarta. Hal ini penting agar Scaleout dapat menciptakan konten dan desain yang relevan dan sensitif terhadap kebutuhan dan nilai-nilai lokal. Dalam menghadapi preferensi klien yang berbeda, Scaleout Creative Agency memiliki pendekatan yang fleksibel dan adaptif. Mereka memahami pentingnya memahami kebutuhan dan preferensi klien dengan baik sebelum memulai proyek.

Tim Scaleout akan melakukan pertemuan awal dengan klien untuk mendapatkan pemahaman yang mendalam tentang visi dan tujuan proyek, serta preferensi klien dalam hal estetika, gaya, dan pesan yang secara komunikasi jarak jauh atau dekat, seperti pertemuan melalui video conference, atau pertemuan di

kantor. Setelah memahami preferensi klien, Scaleout Creative Agency akan mengembangkan konsep dan desain yang sesuai dengan preferensi tersebut. Mereka akan bekerja secara kolaboratif dengan klien, memberikan kesempatan untuk memberikan masukan dan melakukan revisi hingga hasil akhir sesuai dengan harapan klien.

Scaleout juga menyadari pentingnya mengelola ekspektasi klien yang berbeda. Mereka berkomunikasi secara terbuka dan memberikan edukasi dengan klien mengenai batasan dan kemungkinan dalam proyek. Dalam menjalankan operasionalnya, Scaleout juga memastikan keamanan data klien yang dipercayakan kepada mereka. Namun sayangnya, penerapan kebijakan keamanan informasi yang memastikan kerahasiaan dan integritas data klien, serta melindungi dari ancaman keamanan seperti kebocoran data atau akses tidak sah belum sepenuhnya optimal.

3.2. Metode Pengumpulan Data

Pengumpulan data dilakukan untuk memperoleh informasi yang dibutuhkan dalam mencapai tujuan penelitian. Tujuan yang diungkpakan dalam bentuk hipotesis merupakan jawaban sementara terhadap pertanyaan penelitian. Metode pengumpulan data bisa dilakukan dengan cara:

1. Data Primer

Data Primer adalah data yang diambil langsung dari objek penelitian atau merupakan data yang berasal dari narasumber asli atau pertama (Zainal, 2007). Data Primer pada penelitian ini diperoleh dari;

a. Wawancara

Wawancara merupakan teknik pengumpulan data yang dilakukan melalui tatap muka dan tanya jawab langsung antara pengumpul data maupun peneliti terhadap narasumber atau sumber data. Penelitian ini dilakukan wawancara kepada Administrator TI atau yang berwenang pada sistem keamanan pada objek penelitian.

b. Observasi

Observasi merupakan salah satu teknik pengumpulan data yang juga dapat digunakan untuk merekam berbagai fenomena yang terjadi (situasi dan kondisi). Teknik ini digunakan bila penelitian ditujukkan untuk mempelajari perilaku manusia, proses kerja, sistem pada suatu instansi dan gejala-gejala pada suatu lingkup atau komunitas.

2. Data Sekunder

Pengolahan data mencakup beberapa tahapan, diantaranya; meng-edit data (*editing*) dan meng-kode data (*code*) (Zainal, 2007). Mengedit data adalah tahap memeriksa data yang terkumpul atau menyempurnakan dengan melakukan pengumpulan data ulang ke sumber-sumber tersebut (Zainal, 2007). Pengkodean data pada penelitian ini yaitu dengan memberikan kategori berdasarkan pengelompokkan arsitektur keamanan sesuai dengan *framework* yang digunakan. Data sekunder diperoleh melalui dua cara, yaitu:

a. Studi dokumentasi digunakan untuk mencari data-data sekunder yang dibutuhkan dalam melakukan tata kelola TI yang ada.

b. Akses Internet digunakan untuk mencari data pendukung dari berbagai buku, *e-book* maupun jurnal-jurnal yang relevan.

3.3. Metode Analisis Data

Metode analisis data yang digunakan dalam penelitian ini adalah *framework* SABSA. Adapun tahapan yang digunakan dalam menganalisis data pada penelitian ini, diantaranya;

a. Tahap 1: Pengumpulan data

Tahap ini merupakan pengumpulan data yang diperlukan sesuai dengan artefak *security* yang ada pada *framework* SABSA untuk digunakan sebagai pendefinisian scope permasalahan dan mengumpulkan data yang dibutuhkan.

b. Tahap 2: *Processing* data dengan *framework* SABSA dengan mengintegrasikan ke *framework* TOGAF.

Model bisnis pada objek penelitian di tahap ini adalah pengolahan data sistem keamanan yang diperoleh dari objek penelitian dan mengintegrasikan *framework* SABSA dengan TOGAF, berikut ini langkah-langkah (steps) yang dilakukan untuk mengintegrasikan SABSA kedalam TOGAF-ADM :

a. Step 1: Mendefinisikan artefak security SABSA yang diintegrasikan ke fase ADM.
b. Step 2 : Melakukan pemetaan (mapping) SABSA *Lifecycle* dengan TOGAF ADM untuk setiap artefak security SABSA terhadap setiap fase ADM.
c. Step 3 : Mendefinisikan detail output mapping dari artefak security yang dibutuhkan oleh setiap fase ADM.

d. Step 4 : Mengintegrasikan hasil mapping kedalam model format EA.

e. Step 5: Membuat model integrasi ISMS (Information Security Management System) ke dalam EA.

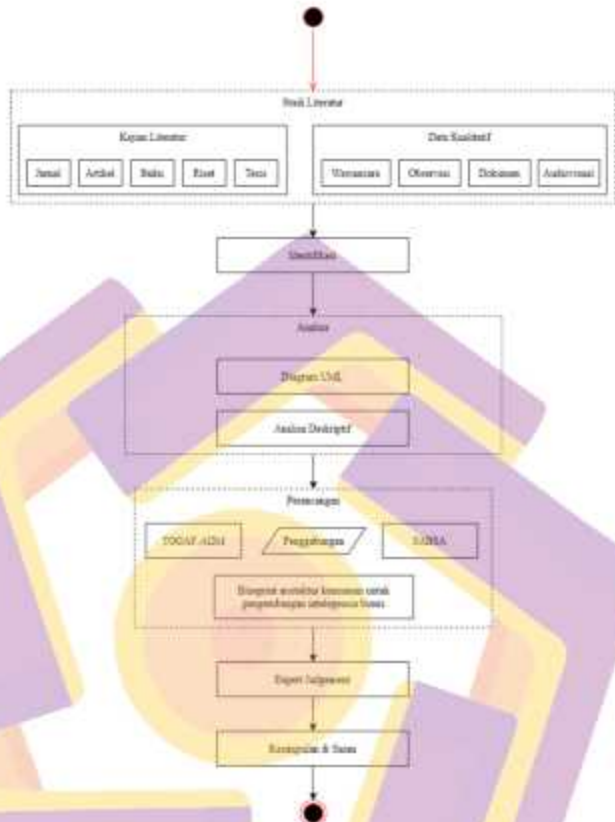
f. Step 6 : Membuat model dari proses integrasi akhir ISMS.

c. Tahap 3: validasi sistem keamanan

Mengacu pada penelitian yang dilakukan oleh Syamsuddin, A (2015), tahap ini digunakan untuk me-validasi rancangan blueprint sistem keamanan yang sudah jadi. Tahap validasi dilakukan dengan metode *expert judgement* yang mana validasi dilakukan dengan dipresentasikan kepada ahli *external* perusahaan dan stakeholder *internal* dari pihak Scaleout Creative Agency dalam skenario FGD (Focus Group Discussion) dengan mempresentasikan hasil integrasi (*blueprint*) SABSA dengan TOGAF pada proses sebelumnya.

3.4. Alur Penelitian

Dari uraian diatas tentang metode penelitian yang digunakan, maka dapat dilihat alur penelitian seperti pada gambar 3.1 berikut.



Gambar 3. 1 Alur penelitian

Berdasarkan alur penelitian diatas, terdapat tahapan dalam penelitian ini. Adapun tahapan dalam penelitian ini dijelaskan sebagai berikut; Dikarenakan metode penelitian ini menggunakan metode *action research* maka alur penelitian ini di awali dengan tahapan.

A. Tahap Perencanaan (*planning*)

Tahapan yang diawali dengan perumusan masalah bagaimana gambaran sistem pelayanan dan keamanan data klien yang terjadi saat ini seperti alur

pelayanan klien, aplikasi yang digunakan, dan infrastruktur TI yang digunakan terutama pada sistem keamanan.

B. Tahap *Observation*

Tahap ini merupakan tahapan pengumpulan data dan studi pustaka dengan metode pengumpulan data. Hal tersebut dilakukan dengan cara observasi dan wawancara terhadap pihak terkait di Scaleout Creative Agency.

C. Tahap *action*

Tahapan ini merupakan proses analisis atau *processing* data untuk menentukan alur proses bisnis dengan menggunakan diagram UML (*Unified Modelling Language*). Setelah mendapatkan hasil dari proses analisis tersebut maka didapatkan aktivitas utama dan aktivitas pendukung pada alur sistem keamanan pada Scaleout Creative Agency. Langkah berikutnya adalah melakukan perencanaan *enterprise architecture* sistem keamanan menggunakan *framework* SABSA yang mana alur pengerjaan penelitiannya dibagi menjadi enam fase utama, diantaranya;

1. Fase I: pengumpulan data.

Fase I adalah proses awal penelitian yang bertujuan untuk mengumpulkan seluruh data obyek penelitian/studi kasus dan literatur yang terkait sebagai dasar pemikiran. Data tersebut terdiri atas data kualitatif, dokumen inteligensia bisnis, dokumen keamanan informasi dan literatur yang terkait.

2. Fase II: Identifikasi (*Identification*).

Fase ini adalah proses identifikasi terhadap data yang telah dikumpulkan pada fase I.

3. Fase III: Analisis.

Fase III adalah proses analisis data yang sudah diidentifikasi di fase II. Analisis dijelaskan secara deskriptif.

4. Fase IV: Perancangan.

Fase ini adalah proses pengembangan rancangan arsitektur keamanan untuk pengembangan inteligensia bisnis sesuai dengan *framework* SABSA.

5. Fase V: Validasi (*Validation*).

Fase ini merupakan proses validasi rancangan yang telah dihasilkan pada tahap perancangan. Metode yang digunakan adalah *expert judgement* dengan mempresentasikan proses pada fase IV kepada manajer dan/atau stakeholder pada objek penelitian. *Expert judgement* adalah istilah yang merujuk secara khusus pada teknik penilaian yang dibuat berdasarkan seperangkat kriteria dan/atau keahlian tertentu yang telah diperoleh di area pengetahuan tertentu, atau bidang produk, disiplin tertentu, industri, dll.

6. Fase VI: Penutup.

Fase VI adalah fase terakhir yang bertujuan untuk memberikan kesimpulan dan saran terhadap hasil penelitian yang telah dilakukan mulai dari tahap awal hingga akhir (tahap V).

BAB IV

HASIL PENELITIAN DAN PEMBAHASAN

4.1. Studi Kasus

Studi kasus yang dilakukan pada penulisan penelitian ini adalah Scaleout Creative Agency, sebuah agensi kreatif dan rumah produksi yang bergerak di bidang pemasaran digital berbasis audiovisual dan digital dengan tujuan *branding* dan *selling*. Scaleout Creative Agency terletak di Jl. Sidodadi II, Corongan, Maguwoharjo, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta. Scaleout menerima klien dari luar kota dengan preferensi klien yang berbeda daerah menjadikan tantangan tersendiri dalam menangani kebutuhan klien dengan karakteristik yang berbeda-beda.

Untuk mengatasi tantangan tersebut, Scaleout Creative Agency harus mampu memahami karakteristik klien dari daerah yang berbeda dan memiliki kemampuan untuk beradaptasi dengan preferensi klien tersebut. Selain itu, agensi kreatif juga harus mampu mengikuti perkembangan teknologi terkini dalam industri kreatif, terutama pada sistem keamanan yang diterapkan. Dalam menghadapi tantangan ini, agensi kreatif dapat mengembangkan strategi pemasaran yang efektif dan berorientasi pada klien.

Misalnya, agensi kreatif dapat mengembangkan program pelatihan dan *workshop* untuk karyawan agar dapat mengembangkan keterampilan dan edukasi tentang sistem keamanan yang dibutuhkan untuk menghadapi tantangan tersebut. Selain itu, Scaleout Creative Agency juga mengembangkan kerjasama dengan mitra

dan *supplier* yang memiliki jaringan yang luas, sehingga dapat membantu untuk menjangkau klien dari daerah yang berbeda dengan lebih mudah.

Secara keseluruhan, agensi kreatif di Yogyakarta yang menerima klien dari luar kota dengan preferensi klien yang berbeda daerah dapat mengembangkan strategi bisnis yang efektif dengan memahami karakteristik klien dan mengikuti perkembangan teknologi terkini. Dengan demikian, agensi kreatif dapat memberikan nilai tambah bagi klien dan dapat memperluas jangkauan bisnis mereka.

Namun, dengan banyakanya klien dari luar kota dan karyawan yang ada, tentunya perlu sistem keamanan yang sangat diperlukan untuk melindungi aset digital yang ada, seperti data klien, karya, dan kekayaan intelektual. Maka penelitian ini di rancang untuk meningkatkan kualitas keamanan di Scaleout Creative Agency dari segi bisnis.

4.2. Hasil Pengumpulan Data

a. Wawancara

Pada tahap awal penelitian dilakukan pengumpulan data yang sudah dipilah dalam di Scaleout Creative Agency ketika wawancara langsung kepada narasumber, berikut dijelaskan pada tabel 4.1. Adapun data lengkap mengenai pengumpulan data, tersaji dalam lampiran di penelitian ini.

Tabel 4. 1 Data Quesioner

No	Pertanyaan	Jawaban
1	Apa arsitektur teknologi informasi yang sedang digunakan oleh Scaleout Creative Agency	Sistem manajemen konten (CMS), Sistem manajemen proyek untuk mengelola proyek dan kolaborasi, Sistem manajemen relasi pelanggan (CRM), Sistem manajemen sumber daya manusia (HR)
2	Apa aset penting yang harus dilindungi dari ancaman keamanan?	Data Klien, Kekayaan Intelektual, Aset digital
3	Apa risiko keamanan yang paling mungkin terjadi pada aset tersebut?	a. Kehilangan data atau pencurian data b. Ancaman virus atau malware c. Serangan siber d. Kesalahan manusia e. Kebocoran data atau pelanggaran privasi f. Ketidakpatuhan terhadap regulasi dan peraturan
4	Apa tingkat keparahan risiko keamanan dan dampak potensialnya pada Scaleout Creative Agency?	a. Kerugian Finansial b. Hilangnya reputasi c. Kerugian waktu dan produktivitas d. Sanksi hukum

Tabel 4.1. (Lanjutan)

No	Pertanyaan	Jawaban
5	Bagaimana risiko keamanan diidentifikasi, dievaluasi, dan dikelola dalam perusahaan?	Identifikasi Risiko, Evaluasi Risiko, Prioritasi Risiko
6	Apa langkah-langkah konkret yang diambil untuk mengurangi risiko keamanan pada aset	a. Kebijakan keamanan jarak jauh b. Perangkat lunak keamanan c. Penggunaan jaringan VPN d. Membatasi akses e. Pelatihan karyawan
7	Apa kriteria penilaian risiko keamanan yang digunakan dalam Scaleout Creative Agency?	Nilai aset, ancaman, kerentanan, dampak, kemungkinan, kepekaan, kepatuhan
8	Apa batasan akses yang diperlukan oleh pengguna?	a. Batasan akses ke data sensitif b. Batasan akses ke sistem informasi c. Batasan akses jaringan d. Batasan akses perangkat mobile e. Batasan akses lokasi
9	Apa sistem atau aplikasi yang akan/sedang diimplementasikan?	• Aplikasi Produktivitas: Adobe Premiere Pro 2020, Adobe, After Effects 2020, Adobe Photoshop 2022, Adobe Illustrator 2020,

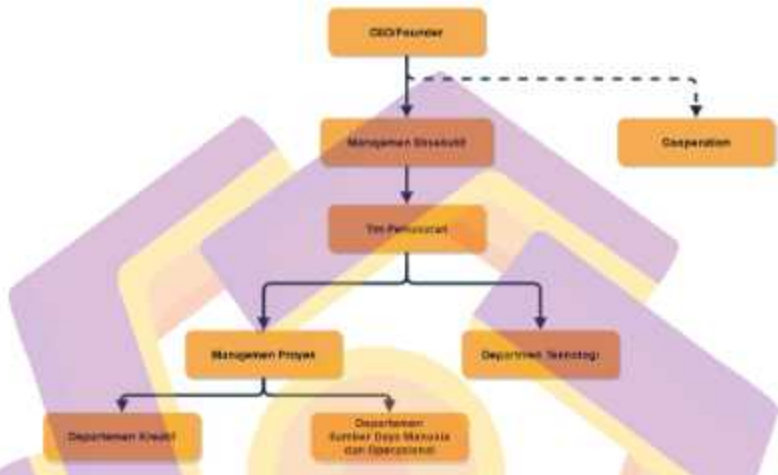
Tabel 4.1. (Lanjutan)

No	Pertanyaan	Jawaban
		Adobe, Lightroom Classic, Adobe Audition 2020, Canva online • Aplikasi bisnis: Meta Ads, Facebook, Google drive, Telegram, WhatsApp, Microsoft Office 2019, Google Chrome Browser, Firefox Browser, Zoom, Figma, Google Ads, Notes, Tiktok
10	Pengalaman dan pemahaman tentang ancaman keamanan dan risiko yang berpotensi terjadi terkait dengan fleksibilitas dan aksesibilitas	Ancaman keamanan jaringan, Kehilangan data, Ancaman phishing, Risiko keamanan vendor

b. Struktur Organisasi

Dalam suatu organisasi bisnis pasti terdapat jabatan tertinggi di suatu perusahaan yaitu CEO yang bertanggung jawab atas eksekutif jalannya perusahaan, lalu dibawahnya terdapat manajemen dan kooperasi yang membantu CEO dalam melaksanakan fungsionalitasnya sebagai eksekutif, dan di bawahnya ada tim marketing/pemasaran dimana sebagai ujung tombak perusahaan dalam menjual jasa pada agensi, di dalam tim pemasaran terdapat manajemen proyek untuk mengatur jalannya proyek bisnis agensi, menaungi departemen kreatif dan SDM, lalu terdapat

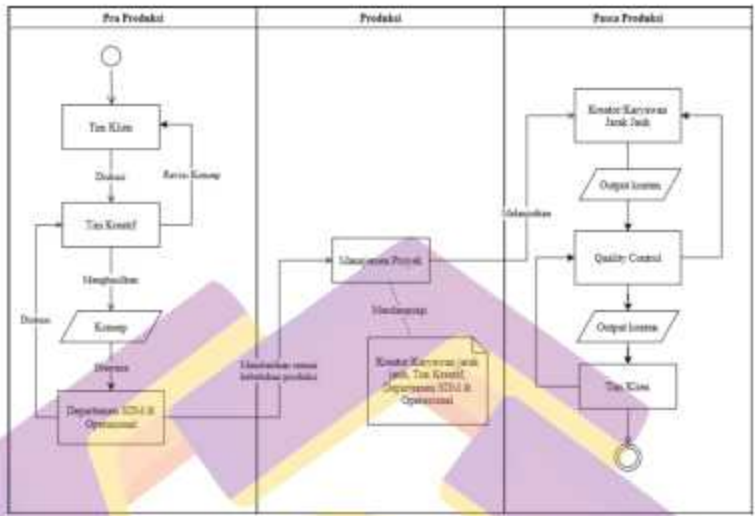
departmen teknologi yang mempunyai tanggung jawab terhadap aksesibilitas dan fleksibilitas serta data privasi perusahaan. Scaleout Creative Agency memiliki struktur organisasi seperti pada gambar 4.1.



Gambar 4. 1 Struktur Organisasi

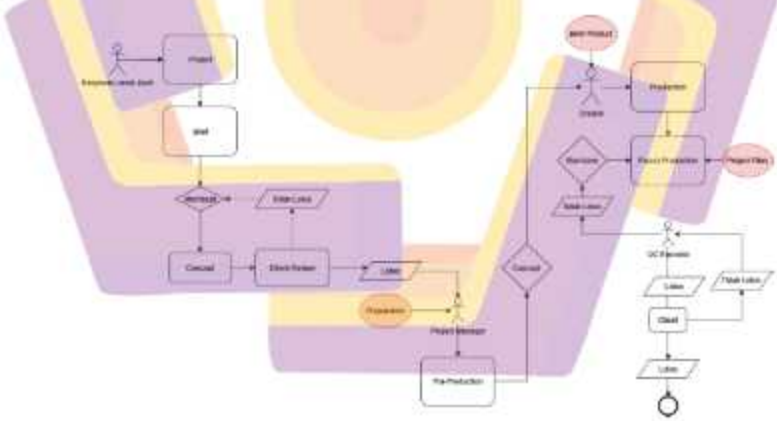
c. Bisnis Proses

Dalam suatu perusahaan diperlukannya alur produksi seperti pada gambar 4.2 yang di bagi menjadi 3 segmen yaitu pra-produksi, produksi dan pasca produksi, disetiap segmen memiliki proses dan fungsi tersendiri dan alur yang sistematis agar terciptanya aksesibilitas dan fleksibilitas dalam perusahaan.



Gambar 4. 2 Alur Produksi

d. Sistem keamanan yang diterapkan



Gambar 4. 3 Alur Kerja yang diterapkan

Scaleout Creative Agency menerapkan sistem keamanan yang masih terdapat banyak risiko yang mungkin terjadi (Gambar 4.3), khususnya mengenai sistem *sharing* data yang untuk mendukung fleksibilitas dan aksesibilitas karyawan

jarak jauh. Berikut kelemahan sistem keamanan yang diterapkan oleh Scaleout Creative Agency;

a. Penggunaan perangkat pribadi tanpa kebijakan yang jelas: Karyawan jarak jauh menggunakan perangkat pribadi mereka untuk mengakses data Scaleout tanpa adanya kebijakan yang jelas terkait penggunaan perangkat tersebut. Hal tersebut mengakibatkan risiko keamanan yang tinggi, karena perangkat pribadi tersebut mungkin tidak memenuhi standar keamanan yang sama dengan perangkat perusahaan.
b. Tidak adanya enkripsi data: Data yang dikirim dan diterima oleh karyawan jarak jauh tidak dienkripsi, sehingga rentan terhadap serangan dan pengintaian oleh pihak yang tidak berwenang. Ini meningkatkan risiko kebocoran data dan pelanggaran keamanan.
c. Tidak ada pemantauan dan pembaruan sistem yang teratur: Tidak ada pemantauan dan pembaruan sistem secara teratur untuk memastikan keamanan yang berkelanjutan. Kelemahan keamanan yang muncul tidak terdeteksi dengan cepat, dan tidak ada tindakan perbaikan yang diambil untuk mengatasi masalah tersebut.
d. Kurangnya pelatihan keamanan bagi karyawan: Karyawan jarak jauh tidak diberikan pelatihan keamanan yang memadai terkait penggunaan jaringan, perangkat, dan praktik keamanan yang baik. Ini meningkatkan risiko serangan sosial, kebocoran data akibat kelalaian, dan kerentanan sistem.

e. Kurangnya pemisahan hak akses: Tidak ada pemisahan yang jelas antara hak akses karyawan jarak jauh terhadap data dan sistem perusahaan. Hal ini meningkatkan risiko penyebaran data yang tidak sah atau penggunaan data yang tidak diizinkan.

Kelemahan-kelemahan ini menyebabkan risiko tinggi terkait keamanan data dalam konteks aksesibilitas dan fleksibilitas karyawan jarak jauh. Mada diperlukan perbaikan dan peningkatan dalam sistem keamanan di Scaleout Creative Agency untuk mengurangi risiko ini dan melindungi data perusahaan secara efektif.

4.3. Identifikasi Resiko

Masuk pada tahap selanjutnya yaitu identifikasi, identifikasi disini meliputi keamanan dan risiko, baik dari eksternal maupun internal perusahaan. Adapun data quesioner dari data perusaan mengenai aplikasi, data dan infrastruktur di Scaleout Creative Agency, telah tersaji dalam lampiran.

Tabel 4. 2 Quesioner data perusahaan

No.	Jenis Risiko	Kode	Kejadian Risiko	Frekuensi Risiko yang terjadi					Pengaruh risiko terhadap sistem keamanan				
				1	2	3	4	5	1	2	3	4	5
1	Internal	A1	Kehilangan data klien atau kebocoran data rahasia klien	X						X			
		A2	Serangan malware atau virus pada sistem			X						X	
		A3	Kebocoran informasi rahasia atau kekayaan intelektual		X					X			

Tabel 4.2. (Lanjutan)

No.	Jenis Risiko	Kode	Kejadian Risiko	Frekuensi Risiko yang terjadi					Pengaruh risiko terhadap sistem keamanan				
				1	2	3	4	5	1	2	3	4	5
		A4	Kerusakan atau kehilangan peralatan komputer dan teknologi				X				X		
		A5	Pelanggaran privasi data karyawan atau pelanggaran regulasi privasi data	X						X			
		A6	Kecelakaan atau kejadian tak terduga yang dapat merusak fasilitas atau aset kreatif agensi				X				X		
		A7	Ketergantungan terhadap layanan pihak ketiga atau vendor				X					X	
		A8	Kesalahan manusia atau kesalahan dalam proses bisnis yang dapat mengakibatkan kerugian.			X					X		
2	Eksternal	B1	Risiko kehilangan data karena penggunaan perangkat yang tidak aman saat bekerja dari jarak jauh.		X						X		

Tabel 4.2. (Lanjutan)

No.	Jenis Risiko	Kode	Kejadian Risiko	Frekuensi Risiko yang terjadi					Pengaruh risiko terhadap sistem keamanan				
				1	2	3	4	5	1	2	3	4	5
		B2	Risiko penyebaran malware melalui jaringan yang tidak aman saat mengakses data atau sistem dari luar jaringan agensi.			X						X	
		B3	Risiko kebocoran informasi rahasia karena penggunaan komunikasi yang tidak aman, seperti email atau pesan instan.	X						X			
		B4	Risiko penipuan dan phising karena penggunaan identitas palsu atau lemah untuk mengakses data dan sistem agensi.	X						X			
		B5	Risiko keamanan jaringan yang rentan karena koneksi yang tidak aman atau lemah saat mengakses jaringan	X						X			

Tabel 4.2. (Lanjutan)

No.	Jenis Risiko	Kode	Kejadian Risiko	Frekuensi Risiko yang terjadi					Pengaruh risiko terhadap sistem keamanan				
				1	2	3	4	5	1	2	3	4	5
			agensi dari luar.										
		B6	Risiko keamanan perangkat karena penggunaan perangkat yang tidak aman atau perangkat pribadi yang rentan saat mengakses data dan sistem agensi dari jarak jauh.		X							X	
		B7	Risiko akses tidak sah ke data dan sistem karena tidak adanya kontrol akses yang tepat saat bekerja dari jarak jauh.			X					X		
		B8	Risiko kehilangan data karena ketidakmampuan backup data yang tepat saat bekerja dari jarak jauh.		X						X		
		B9	Risiko ketidakpatuhan terhadap kebijakan dan standar keamanan	X					X				

Tabel 4.2. (Lanjutan)

No.	Jenis Risiko	Kode	Kejadian Risiko	Frekuensi Risiko yang terjadi					Pengaruh risiko terhadap sistem keamanan				
				1	2	3	4	5	1	2	3	4	5
			karena kurangnya pemahaman dan kesadaran tentang kebijakan dan standar keamanan yang berlaku di agensi.										
		B10	Risiko serangan DDoS atau hacking yang dapat mengakibatkan kerusakan pada data dan sistem agensi.	X								X	

Keterangan Penilaian:

1. Sangat Jarang (SJ) = Jarang (hampir tidak mungkin) terjadi pada kondisi tertentu (dalam kurun 1 kali terjadi selama 2 tahun)
2. Jarang (J) = Kemungkinan kecil terjadi pada setiap kondisi (1x dalam 2 tahun)
3. Terkadang (T) = Mungkin terjadi pada kondisi tertentu (1-2 kali dalam 2 tahun)
4. Sering (S) = Kemungkinan besar terjadi pada setiap kondisi (2x dalam 2 tahun)
5. Sangat Sering (SS) = Hampir pasti terjadi pada setiap kondisi (lebih dari 3x dalam 2 tahun).

Maka, adapun hasil dari matriks risiko penilaian K3 sebagai bentuk cara mengukur tingkat validitas sistem keamanan untuk Scaleout Creative Agency dengan menggunakan *framework* SABSA, data survey diatas telah di isi oleh kepala IT di Scaleout Creative Agency seperti pada tabel 4.3 dan 4.4, sebagai berikut;

Tabel 4. 3 Tingkat risiko

		Dampak				
		1	2	3	4	5
Frekuensi	5					
	4			A4, A6	A7	
	3		B7	A8	A2, B2	
	2		A3	B1, B6, B8		
	1	B3, B4, B5, B9	A1, A5		B10	

Tabel 4. 4 Evaluasi Risiko

Faktor	Frekuensi	Dampak	Risk Level	Tipe Risiko	Kontrol Tambahan
A1	1	2	2	Rendah	Perlu Aturan/Prosedur/Rambu
A2	3	4	12	Tinggi	Perlu Perencanaan Pengendalian
A3	2	2	4	Rendah	Perlu Aturan/Prosedur/Rambu
A4	4	3	12	Tinggi	Perlu Perencanaan Pengendalian
A5	1	2	2	Rendah	Perlu Aturan/Prosedur/Rambu
A6	4	3	12	Tinggi	Perlu Perencanaan Pengendalian
A7	4	4	16	Tinggi	Perlu Perencanaan Pengendalian
A8	3	3	9	Sedang	Perlu Tindakan Langsung
B1	2	3	6	Sedang	Perlu Tindakan Langsung
B2	3	4	12	Tinggi	Perlu Perencanaan Pengendalian
B3	1	1	1	Rendah	Perlu Aturan/Prosedur/Rambu
B4	1	1	1	Rendah	Perlu Aturan/Prosedur/Rambu
B5	1	1	1	Rendah	Perlu Aturan/Prosedur/Rambu
B6	2	3	6	Sedang	Perlu Tindakan Langsung
B7	3	2	6	Sedang	Perlu Tindakan Langsung
B8	2	3	6	Sedang	Perlu Tindakan Langsung
B9	1	1	1	Rendah	Perlu Aturan/Prosedur/Rambu
B10	1	4	4	Sedang	Perlu Tindakan Langsung

4.4. Tahapan Pengintegrasian

Berikut ini langkah-langkah (steps) yang dilakukan untuk mengintegrasikan SABSA kedalam TOGAF-ADM:

• Step 1: Mendefinisikan artefak *security* SABSA yang diintegrasikan ke fase ADM.

• Step 2: Melakukan pemetaan (*mapping*) SABSA *Lifecycle* dengan TOGAF ADM untuk setiap artefak security SABSA terhadap setiap fase ADM (Tabel 4.5).

• Step 3: Mendefinisikan detail output mapping dari artefak *security* yang dibutuhkan oleh setiap fase ADM (Tabel 4.6, Tabel 4.7, Tabel 4.8. dan Tabel 4.9).

• Step 4: Mengintegrasikan hasil mapping kedalam model format *Enterprise Security Architecture* (Gambar 4.4).

• Step 5: Membuat model integrasi ISMS (*Information Security Management System*) ke dalam EA (Gambar 4).

• Step 6: Membuat model akhir *Enterprise Security Architecture*: integrasi proses ISMS (Gambar 5).

Tabel 4. 5 Matriks Mapping SABSA Lifecycle dengan TOGAF ADM

SABSA *Lifecycle*		Fase TOGAF-ADM	Artefak *Security* SABSA
	Strategy & Planning Phase (P1) (P1=P+A)	*Preliminary (Pr) (Pr1+Pr2+Pr3+Pr4+Pr5)*	*Pr1. Business Drivers*
			Pr2. Security Principles
			Pr3. Key Risk Areas
			Pr4. Risk Appetite
			Pr5. Security Resource Plan
		A. Architecture Vision (A1)	*A1. Security Stakeholders*
	Design Phase(P2)		*B1. Business Risk Model*
			B2. Law and Regulation

Tabel 4.5. (Lanjutan)

	(P2= B+C+D)	*B. Business Architecture (B1+B2+B3+B4+B5+B6 +B7+B8)*	*B3. Control Frameworks*
			B4. Security Domain Model
			B5. Trust Framework
			B6. Security Organization
			B7. Security Policy Architecture
		C. Information System Architecture (C1+C2+C3)	*C1. Security Services Catalog*
			C2. Classification of Services
			C3. Security Rules, Practices and Procedures
		D. Technology Architecture (D1+D2)	*D1. Security Rules, Practices and Procedures*
			D2. Security Standards
	Implement Phase (P3) (P3 = E+F+G)	*E. Opportunities and Solutions*	*E1. Treatment Risk Assestments*
		F. Migration Planning	*F1. Security Risk Assestments*
		G. Implementation Governance (G1+G2+G3)	*G1. Security Managements*
			G2. Security Audits
			G3. Security Awareness
	Manage & Measure Phase (P4) (P4 = H)	*H. Architecture Change Development (H1+H2)*	*H1. Risk Managements*
			H2. Security Architecture Governances

Tabel 4. 6 Output Hasil Mapping pada Fase Strategy & Planning (P1)

	Artefak	Output hasil *mapping*
Strategy and planning (P1)	Pr1	1. *Taxonomy of Business Assets* (Visi, Misi, Strategi dan Scaleout Creative Agency). 2. *Inventory of Operational Processes* (SOP Kegiatan Scaleout Creative Agency). 3. *Organisational Structure* (Struktur Scaleout Creative Agency).

Tabel 4.6. (Lanjutan)

		4. *Business Dependences* (Tujuan Bisnis dan Relasinya Scaleout Creative Agency dengan vendor atau karyawan lainnya). 5. *Inventory of Building, Sites and Territories* (Bangunan, ruangan dan peta lokasi perusahaan)
	Pr2	1. Prinsip-prinsip security diimplementasikan ke dalam *Enterprise Architecture* dengan menggunakan ISO 27001 ISMS (*Information Security Management System*). 2. Menggunakan standar *information security: control based standards* (ISO 17779)
	Pr3	1. *Opportunities and Threats Inventory* (Daftar ancaman dan resiko keamanan). 2. Arsitektur manajemen resiko keamanan di masing-masing unit divisi (Diseminasi).
	Pr4	*Control Objectives and Policy Architecture* (Kebijakan strategis dalam mengantisipasi resiko keamanan pada arsitektur perusahaan).
	Pr5	Daftar sumber daya keamanan (*security-resources*) yang diperlukan untuk memberikan unsur keamanan terhadap arsitektur perusahaan.
	A1	Daftar semua stakeholder (termasuk yang berhubungan dengan keamanan) untuk menyetujui arsitektur keamanan

Tabel 4.6. (Lanjutan)

		(CEO, tim internal, admin Scaleout Creative Agency, pemberi otoritas regulasi).

Tabel 4. 7 Output Hasil Mapping pada Fase Design (P2)

	Artefak	Output hasil *mapping*
Design (P2)	B1	Model Resiko Bisnis Perusahaan: memperlihatkan daftar resiko keamanan informasi yang selaras dengan resiko bisnis perusahaan (*enterprise*).
	B2	1. *Risk Management Rules and Procedures* (SOP dan aturan dalam manajemen resiko). 2. Peraturan CEO Scaleout Creative Agency mengenai arsitektur bisnis perusahaan.
	B3	1. *Process Mapping Framework* (Pemetaan proses monitoring dan evaluasi kegiatan). 2. *Enablement & Control Objectives* (Teknologi informasi dan sistem informasi mendukung serta sesuai dengan persyaratan regulasi).
	B4	1. Kerangka dan konsep dari *Security Domain*. 2. *Domain Maps* (Definisi domain security untuk internal dan eksternal perusahaan).
	B5	*Entity & Trust Framework* (Kerangka model *security* yang dipercaya dengan skema entitas).

Tabel 4.7. (Lanjutan)

	B6	Struktur organisasi keamanan perusahaan yang bertanggung jawab dalam menangani manajemen resiko keamanan dan information security (*security risks*).
	B7	Mencakup beberapa aspek *security* : *physical & information security* serta *business continuity*.
	B8	Daftar katalog layanan business yang berelasi dengan keamanan arsitektur perusahaan.
	C1	Daftar katalog layanan arsitektur SI yang berelasi dengan keamanan arsitektur (ICT).
	C2	*Information Assets & Services, Host Platforms, Layout & Networks, dan Access Control System.*
	C3	Dokumentasi panduan dan petunjuk mengenai prosedur (SOP) dan peraturan keamanan.
	D1	Dokumentasi panduan dan petunjuk mengenai prosedur (SOP) dan peraturan keamanan, khususnya yang berkaitan dengan arsitektur teknologi
	D2	Standar keamanan umum (*general*), TLS dan SAML.

Tabel 4. 8 Output Hasil Mapping pada Fase Implement (P3)

	Artefak	Output hasil *mapping*
Implement (P3)	E1	STAT-QAF: kerangka jaminan kualitas implementasi desain arsitektur melalui tools statistik.
	F1	SIX SIGMA : kerangka jaminan kualitas implementasi desain *security architecture*.
	G1	1. Implementasi tata kelola keamanan (*security roles and responsibilities*). 2. Penetapan indikator kinerja keamanan dan manajemen resiko (*security key performance and risk indicators*).
	G2	1. Review konfigurasi sistem keamanan untuk melihat keselarasan dengan desain perencanaan. 2. Laporan hasil pemeriksaan (audit) desain, pengembangan, dan pelaksanaan arsitektur keamanan terhadap tujuan bisnis, kebijakan keamanan, dan tujuan pengendalian. 3. *Functional & non-functional testing*, termasuk testing keamanan, kinerja, dan pemeliharaan.
	G3	Pelatihan (*trainning*) kepada para karyawan di Scaleout Creative Agency mengenai kesadaran dan pemahaman terhadap komponen dan subsistem arsitektur keamanan yang akan diterapkan.

Tabel 4. 9 Output Hasil Mapping pada Fase Manage and Measure (P4)

	Artefak	Output hasil *mapping*
Manage and measure (P4)	H1	1. *Risk Management Tools & Standards*, meliputi tool analisis resiko, daftar resiko yang telah didaftar, monitoring resiko dan tools laporan manajemen resiko. 2. *Operational Risk Management*, meliputi jaminan antisipasi resiko, monitoring antisipasi resiko dan manajemen resiko serta laporan kegiatan perlakuan (treatment) terhadap resiko yang dihadapi oleh Scaleout Creative Agency.
	H2	1. Keputusan mengenai perubahan-perubahan yang harus dilakukan dalam lingkup arsitektur perusahaan/organisasi sekarang sebagai akibat dari implementasi arsitektur keamanan. 2. Perubahan kebutuhan organisasi (requirement) untuk memenuhi standar keamanan yang diintegrasikan kedalam arsitektur enterprise (EA).

4.5. Permodelan *Enterprise Security Architecture* (ESA)

Langkah selanjutnya adalah membuat model format arsitektur keamanan Scaleout Creative Agency berdasarkan poin-poin (*output*) hasil mapping antara artefak security SABSA dengan komponen-komponen dalam TOGAF-ADM. Dalam penelitian ini, penulis membatasi model format Enterprise Security Architecture (ESA) tersebut hanya dalam tiga *layer* teratas, yaitu *Contextual Layer, Conceptual Layer dan Logical Layer* (Tabel 4.10, Tabel 4.11 dan Tabel 4.12).

Struktur layout rancangan model format enterprise security architecture adalah sebagai berikut:

- *Contextual Layer => Viewpoints AND Business Driver*
- *Conceptual Layer => Business Attribute AND Control Objectives*
- *Logical Layer => Measures*
- *Conceptual AND Logical Layer => [People, Data, Application, Network, Platform, Physical & Organization].*

Gambar 4. 4 Format Enterprise Security Architecture Scaleout Creative Agency

Berikut ini penjelasan ringkas mengenai artefak security, komponen dan deskripsi aktifitas pada format Enterprise Security Architecture Scaleout Creative Agency untuk setiap layer tersebut (Tabel 4.10, Tabel 4.11 dan Tabel 4.12).

1. *Contextual Layer*

Tabel 4. 10 Deskripsi Aktifitas untuk Komponen Artefak Security (*Contextual Layer*)

Artefak Security	Komponen Artefak	Deskripsi Aktifitas
Business Viewpoint	*Business Assets (=>Security Requirement)*	1. Identifikasi kebutuhan bisnis untuk keamanan informasi. 2. Memanfaatkan aset bisnis sebagai value untuk mendukung kebutuhan bisnis terhadap keamanan informasi. 3. Identifikasi persyaratan keamanan untuk menjamin kontinuitas operasional bisnis. 4. Identifikasi persyaratan keamanan untuk *system assurance*.
Business Driver	*Business Risk Model (=>Risk Assessment)*	Penilaian risiko harus dilakukan oleh organisasi saat menghadapi resiko bisnis dan memiliki respon keamanan terhadap berbagai kemungkinan resiko keamanan yang ditemui, meliputi beberapa area: *brand protection, fraud*

Tabel 4.10. (Lanjutan)

Artefak Security	Komponen Artefak	Deskripsi Aktifitas
		protection, loss prevention, business continuity, confidence of stakeholders dan operational risk.
	Business Process Analysis (=>Security for business process)	Melakukan analisis dan identifikasi terhadap persyaratan keamanan yang didorong (driven) oleh business process, meliputi : 1. Interaksi business, memerlukan identifikasi dan otentikasi entitas dari business process. 2. Komunikasi business antar process.

2. Conceptual Layer

Tabel 4. 11 Deskripsi Aktifitas untuk Komponen Artefak Security (*Conceptual Layer*)

Artefak Security	Komponen Artefak	Deskripsi Aktifitas
Business Attribut Profile	Atribut security yang harus diimplementasikan (BAP) kedalam business assets	1. Identifikasi business assets yang membutuhkan proteksi keamanan. 2. Mapping atribut security (SABSA) kedalam business drivers, meliputi: • Access-control • Availability • Authenticated • Confidential • Integrity • Trustworthy

Tabel 4.11. (Lanjutan)

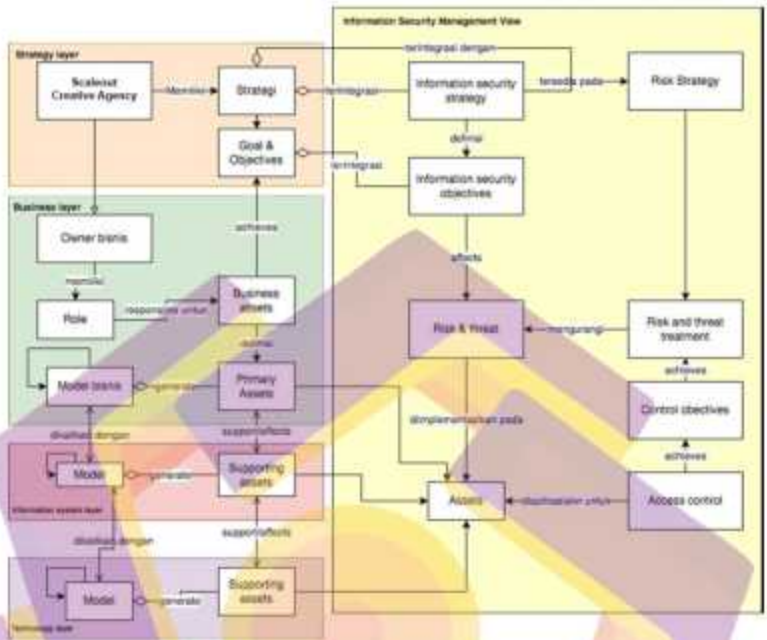
Artefak Security	Komponen Artefak	Deskripsi Aktifitas
		• Maintainability • Usability • Authorised • Measured • Flexible Secure • Auditable
Control Objectives	Security Audits dan Assurance Level (=>Information Security Assurance)	Menggunakan tujuan pengendalian (control objectives) untuk mengkonseptualkan strategi mitigasi dalam upaya mengatasi resiko business yang muncul. Control objectives yang didefinisikan disini adalah: • Data Quality • Risk Management • Information Security • Policy • High Trust

3. Logical Layer

Tabel 4. 12 Deskripsi Aktifitas untuk Komponen Artefak Security (*Logical Layer*)

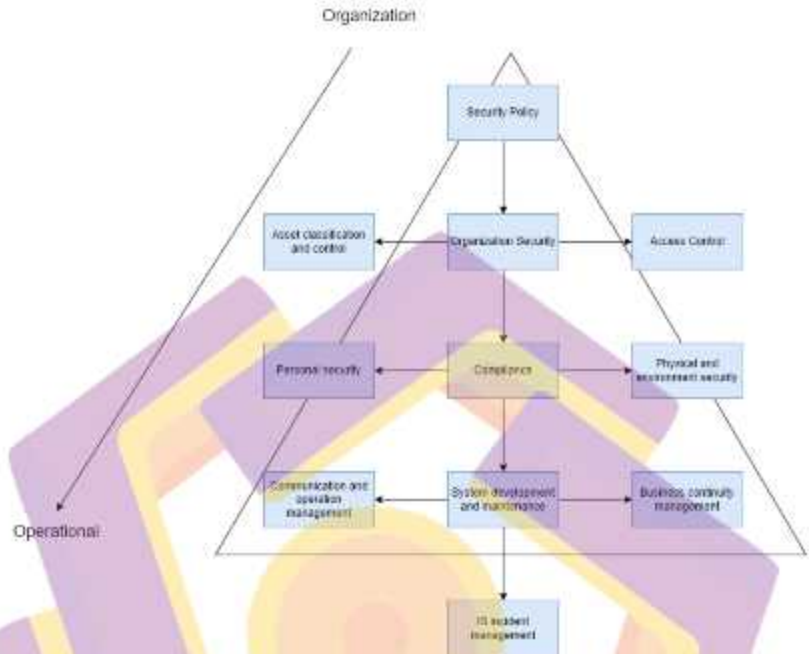
Artefak Security	Komponen Artefak	Deskripsi Aktifitas
Measures	• Security Strategies • Security Standards • Security Patterns • Security Services • Security Products & Tools	1. Identifikasi strategi untuk kebijakan keamanan dan arsitekturnya. 2. Identifikasi pengukuran standar keamanan arsitektur dengan melihat tingkat kematangan arsitektur. 3. Identifikasi pengukuran layanan security pada seluruh entitas yang terlibat pada arsitektur keamanan organisasi

Langkah selanjutnya (Step 5) adalah membuat model konseptual integrasi *Information Security Management System* (ISMS) kedalam ADM TOGAF (Gambar 4.5) berdasarkan artefak-artefak hasil identifikasi yang dilakukan pada step sebelumnya. Pada tahapan ini, penulis membatasi integrasi tersebut hanya pada 4 (empat) fase ADM, yaitu *Strategy, Business, Information System* dan *Technology*.



Gambar 4. 5 Model Integrasi ISMS dengan *Enterprise Architecture* di Scaleout Creative Agency

Langkah terakhir (*Step* 6) adalah membuat model konseptual akhir dari integrasi proses ISMS kedalam EA sebagai satu kesatuan proses bisnis yang saling mendukung (Gambar 4.6). Pada tahapan ini, penulis mengintegrasikan artefak security (ISMS) sebagai core business didalam EA digital agensi.



Gambar 4. 6 Model Akhir Integrasi Proses ISMS Scaleout Creative Agency

Pada gambar 4.6 menggambarkan flow blueprint arsitektur dari integrasi proses ISMS. Dimulai dari atas terdapat *Security Policy*, lalu di *breakdown* hingga menjadi *organization security* yang terdapat 2 bagian yaitu *asset classification* dan *access control*. Lalu di dalam *organization security* terdapat *compliance* ini berfungsi unruk kepatuhan terhadap keamanan yang meliputi 2 hal yaitu *personal security*, *physical and environtment security*, lalu flow selanjutnya dilakukan *system development and maintenance* berguna untuk mengembangkan dan memonitoring *business continuity management*, dan *communiation and operation management* dan di akhir terdapat *IS incident management* untuk menhandle atau mengatasi suatu permasalahan management. Flow dari atas hingga bawah

menunjukkan bagaimana sebuah organisasi hingga operational perusahaan berjalan, dimulai dari security policy yang memuat peraturan-peraturan organisasi hingga IS incident management.

Fase terakhir adalah *expert judgement* yang dilakukan dengan dua tahap, diantaranya; presentasi kepada ahli keamanan IT diluar perusahaan dan presentasikan kepada stakeholder dan/atau manajer Scaleout, adapun yang dilakukan adalah; Memilih dan mengonfirmasikan aktivitas yang akan dianalisis; Membuat daftar pernyataan dan/atau pertanyaan; 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.

4.6. Tahapan Prelimenary

Sebelum memasuki tahap terakhir, yaitu *Expert Judgement*, terdapat tahap prelimenary. Tahapan ini merupakan bagian perancangan *Enterprise Architecture* dimana menjelaskan proses rancangan dalam fungsionalitas dan operasional yang dibuat. Proses ini akan menghasilkan artefak yaitu *principle katalog* yaitu menjelaskan prinsip-prinip sesuai dengan kebutuhan bisnis.

Tabel 4. 13 Tahapan *Prelimenary Enterprise Architecture* Scaleout Creative Agency

No	Arsitektur	Prinsip	Deskripsi
1.	Arsitektur Bisnis	*Eco friendly*	Bisnis yang berulang dan ramah lingkungan baik dari segi teknologi maupun operasional

Tabel 4.13. (Lanjutan)

No	Arsitektur	Prinsip	Deskripsi
		Kualitas karyawan yang terlatih dan bermutu	Mengadakan pelatihan dan expertise dalam perusahaan
		Perbaikan terus menerus dalam area kegiatan utama	Melakukan monitoring terhadap kegiatan usaha terutama dalam kegiatan yanng penting atau kritikal
		Kepatuhan hukum	Memastikan karyawan berjalan sesuai SOP dan kepatuhan hukum yang ada
2.	Data	Kemudahan Dalam pengolahan data	Terdapat kemudahan akses data terhadap entitias-entitas perusahaan
		Pembagian data	Data harus dapat dibagikan kepada seluruh pengguna yang membutuhkan sesuai dengan tingkatan otoritasnya yang telah ditentukan
		Aset Data	Data merupakan aset yang memiliki nilai untuk perusahaan dan harus dijaga serta dirawat dengan baik
		Transparansi Data	Data harus transaparan dengan berbasis teknologi informasi

Tabel 4.13. (Lanjutan)

No	Arsitektur	Prinsip	Deskripsi
		Keamanan data	Data yang harus dimiliki perusahaan harus dijaga dan dilindungi dari eksploitasi data oleh pengguna tanpa otoritas yang sesuai.
3.	Aplikasi	Otoritas Aplikasi	User diberikan hak akses aplikasi berdasarkan jabatan dan fungsi kerja masingmasing
		Integrasi Aplikasi	Aplikasi yang digunakan harus terintegrasi dengan aplikasi lainnya yang ada pada perusahaan
4.	Arsitektur Teknologi	Keamanan teknologi	Teknologi yang digunakan didalam perusahaan diharapkan sudah dapat menutupi celah keamanan perusahaan baik dari serangan malware maupun serangan lainnya.
		Penggunaan teknologi *realtime*	Teknologi yang digunakan dapat diakses kapan saja.
		Kontrol infrastruktur teknologi	Adanya maintenance berkala yang dilakukan perusahaan untuk menjaga aset fisik dan non fisik pada performa yang baik.

4.7. Architecture Vision

Architecture vision adalah fase pertama dalam *enterprise architecture*, fase ini menggambarkan value bisnis yang dilakukan oleh top manajerial perusahaan, gambar 4.7 adalah value chain menggambarkan aktivitas utama sedangkan tabel 4.14 menggambarkan *solution concept* untuk menciptakan solusi berupa konsep *office* untuk mencapai target *architecture*.

Gambar 4. 7 Value Chain di Scaleout Creative Agency

Pada gambar 4.7. menjelaskan bahwa terdapat segmen dari *value chain* atau visi arsitektur, yang pertama ada infrastruktur perusahaan, infrastruktur perusahaan adalah semua struktur dan fasilitas yang diperlukan dalam menjelaskan kegiatan usaha atau operasional perusahaan, maka sangat penting sebuah perusahaan memiliki value chain dari infrastruktur perusahaan, agar meningkatkan nilai dari sebuah perushaan. Selanjutnya terdapat manajemen SDM, untuk terciptanya karyawan yang memiliki value tinggi maka perusahaan harus memiliki system manejemen SDM (Sumber Daya Manusia) untuk mengatur dan mengembangkan

karyawan baik dari segi *hardskill* maupun *softskill*. Selanjutnya yang ketiga adalah pengembangan teknologi informasi, hal ini sangat penting guna mengubah atau transformasi perusahaan yang sebelumnya masih manual atau tradisional menjadi semakin maju dan canggih sehingga mempermudah dan meningkatkan efisiensi perusahaan dalam menjalankan keguatan usaha. Di tahap akhir ada marketing, marketing disini meliputi digital marketing, pemasaran produk, dan pengelolaan produk, yang dapat meningkatkan value dari perusahaan dan meningkatkan margin keuntungan untuk perusahaan, ketiga hal tersebut menjadi point penting di marketing guna meningkatkan awareness pengguna dan mendapatkan pelanggan baru. Untuk margin sendiri adalah tujuan akhir dari membuat semua segmen tersebut yaitu return atau revenue yang sustainability dalam menghadapi pangsa pasar, dimana basic atau pondasi segmen harus kuat dan saling bersinergi.

Tabel 4. 14 *Solution Concept* Scaleout Creative Agency

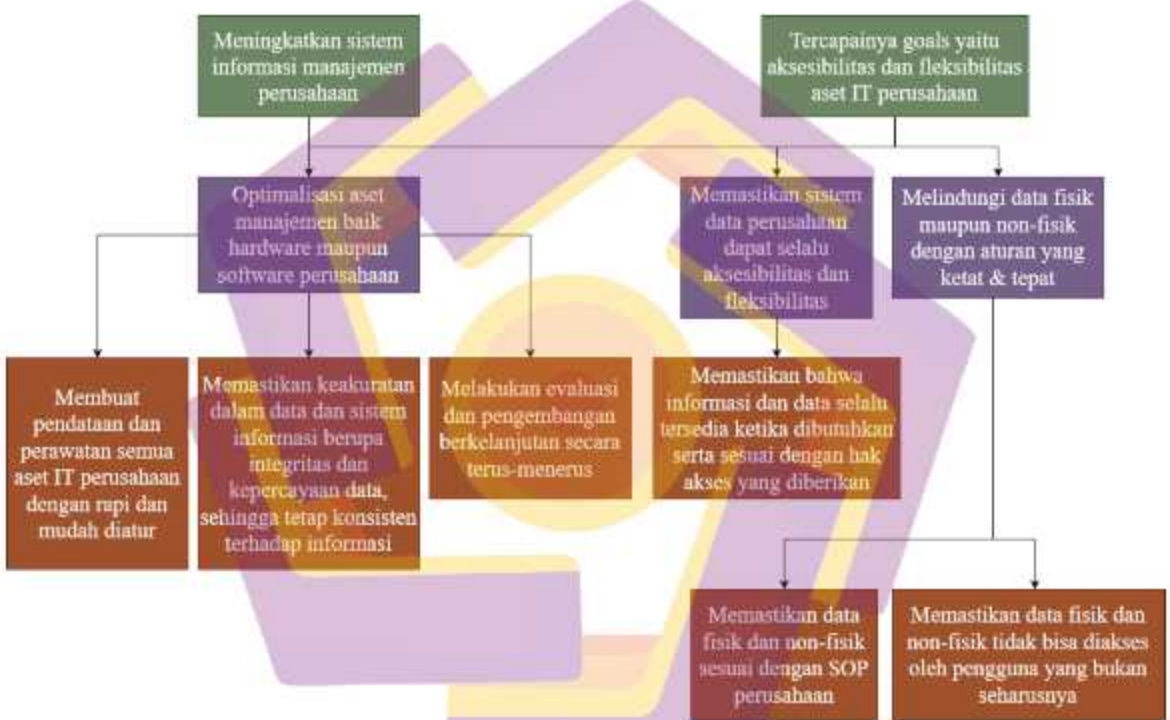
Channel	Internet		VPN
Front Office	Pengelola operasional Scaleout Creative Agency		
Middle Office	User Management	Antivirus	Distribution Management System (DMS)
Back Office	Pelaporan	Survey	Audit

Pada tabel 4.14 terdapat solution concept yang menggambarkan bagaimana relasi antara front, midle dan back office terhubung dan menjalani kegiatan operasional

terutama di office perusahaan. Pada front office terdapat pengelolaan operasional perusahaan yang berhubungan dengan *customer* atau cs, selanjutnya terdapat *middle office* adalah pengelolaan user management baik dari sisi pengguna ataupun office itu sendiri dimana untuk menjembatani antara keduanya, dengan menggunakan antivirus untuk keamanan, service desk untuk operational dengan DMS(*Data Management System*) untuk kegiatan operasional sperti survey, audit dll. Lalu terdapat back office yaitu pelaporan, survey, dan audit, digunakan untuk keperluan data dan evaluasi serta crosscheck seluruh kegiatan operasional office, dan terdapat channel yaitu fasilitas yang digunakan untuk menghubungkan ketiga hal tersebut dengan internet dan VPN, dimana internet berguna untuk menghubungkan semua segmen office, sedangkan VPN digunakan untuk menjaga privasi jaringan antar segmen apabila ada data atau hal yang mencurigakan atau krusial.

4.8. Business Architecture

Business architecture adalah tahapan yang mendeskripsikan tentang kebutuhan bisnis proses *enterprise* dalam menjalankan operasional bisnis demi mencapai tujuan yang di inginkan. Perancangan business architecture juga merupakan landasan perancangan arsitektur lainnya seperti *business goals, business function, obective,* dan *business driven.* Dalam konteks penelitian ini, *business architecture* akan membantu mengidentifikasi dan memetakan proses bisnis yang terkait dengan keamanan, aksesibilitas, dan fleksibilitas data di Scaleout Creative Agency. Gambar 4.8 merupakan bagan penjelasan mengenai komponen penting dalam business architecture.



Gambar 4. 8 Business Architecture Scaleout Creative Agency

Business architecture mencakup pengorganisasian bisnis dan proses bisnis yang digunakan untuk mencapai tujuan bisnis tertentu. Dalam penelitian ini, business architecture akan menjadi dasar untuk merancang dan mengelola sistem keamanan data yang mencakup kebutuhan aksesibilitas dan fleksibilitas untuk karyawan jarak jauh. Proses pengembangan business architecture dimulai dengan memahami tujuan bisnis agensi kreatif dan proses bisnis yang ada. Langkah selanjutnya adalah mengidentifikasi area yang perlu ditingkatkan dalam pengelolaan keamanan data dan membuat blueprint yang baru untuk sistem keamanan yang lebih baik. *Business architecture* juga melibatkan analisis risiko dan pemilihan solusi teknologi informasi yang sesuai dengan kebutuhan agensi kreatif.

4.9.Information System Architecture

Pada fase atau tahapan ini bertujuan untuk mengembangkan arsitektur target yang mencakup ruang lingkup aplikasi dan data. Namun sebelumnya terdapat matriks fungsi bisnis dan entitas sebagai penilaian (Tabel 4.15).

Tabel 4. 15 Tabel *Information System Architecture* Scaleout Creative Agency

Data	*Application*
Data Architecture	Logical Application
Google Analytics	Physical Application
Meta Data	Non Physical Application
Master Class	Information System
Data Warehouse	
Data Integration	

Pada tabel 4.15 menjelaskan tentang arsitektur system informasi yang terdiri dari dua bagian yaitu data dan aplikasi, pada segmen data terdapat data arsitektur, google analitik, *metadata, master class, data warehouse* dan *data integration*. Data arsitektur adalah serangkaian struktur dan fasilitas data yang dibuat atau digunakan dalam suatu organisasi, selanjutnya google analitik adalah tools yang digunakan untuk mengolah data, mendapatkan insight dan mendapatkan informasi baru berdasarkan Analisa dengan begitu memudahkan perusahaan dalam mengambil keputusan, selanjutnya meta data adalah data mentah atau data yang belum di olah/diproses dan biasanya merupakan data-data yang detail atau mendasar untuk diproses lebih lanjut, selanjutnya ada master class adalah penggunaan kelas yang

handal atau ahli dalam suatu bidang terutama data, selanjutnya terdapat data warehouse adalah tempat penyimpanan data mentah yang belum di proses misalnya transaksi keuangan, asuransi dll. Selanjutnya terdapat data integration adalah proses kombinasi atau menyatukan data dari berbagai sumber data yang nanti nya akan di olah atau di proses, prosesnya meliputi cleansing dan pemetaan sebelum dilakukan ETL, dan diakhir akan di proses melalui data transform atau proses ETL dilakukan. Selanjutnya pada layer atau segmen aplikasi terdapat *logical application* dimana hal-hal logic seperti *flowchart, flow* bisnis dibuat dan di analisis dalam pembuatannya, selanjutnya ada *physical application* yaitu layer fisik yang terdapat di dunia nyata seperti internet hub, router, switch yang digunakan untuk menghubungkan konektivitas antar segmen, lalu ada non physical application berfungsi sebagai aplikasi yang tidak terlihat dalam dunia nyata seperti data server, aliran data, konektivitas jaringan dll, diperlukan dalam setiap membangun information system architecture yang memiliki system tersendiri.

Gambar 4. 9 Blueprint Enterprise Information Architecture di Scaleout Creative Agency

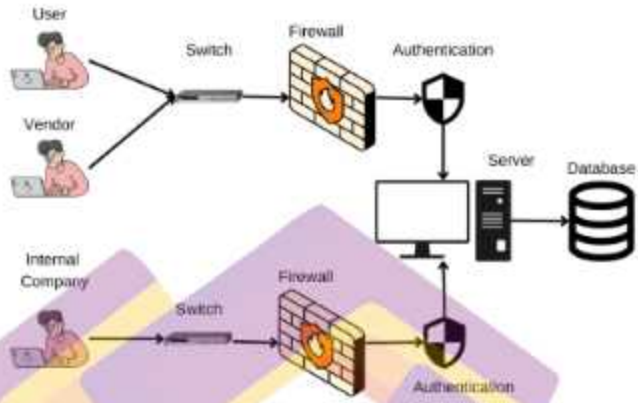
Dalam dunia bisnis pasti terdapat Blueprint tentang informasi arsitektur yaitu terdiri dari berbagai macam divisi atau organisasi yang saling terhubung satu sama lain, tetapi harus melewati serangkaian pengecekan seperti antivirus, hak akses, firewall, baru bisa terkoneksi dengan baik dengan divisi lain, hal ini berguna untuk kelancaran pertukaran data atau informasi yang dibutuhkan antar divisi seperti pada gambar 4.9.

4.10. Technology Architecture

Pada tahapan atau fase ini menjelaskan tentang teknologi arsitektur yang telah dirancang berupa tabel 4.16 dan gambar 4.10.

Tabel 4. 16 Penggunaan Teknologi Arsitektur Scaleout Creative Agency

Tipe	Prinsip	Klasifikasi
Hardware	Komputer	Critical
	Hp	Critical
	Router	Critical
	Lan	Critical
	Mouse	Support
	Keyboard	Support
	Hardisk	Critical
Software	Whatsapp	Critical
	Zoom	Critical
	Google	Critical
	Adobe package	Support
	Ms Office	Critical
	Tiktok	Support
	M-Banking	Critical
	Instagram	Support
	Notes	Support



Gambar 4. 10 *Blueprint Technology Architecture* Scaleout Creative Agency

Penggunaan teknologi arsitektur pasti memiliki perangkat atau klasifikasi di dalamnya, perangkat yang digunakan biasanya adalah komputer, handphone, dll guna menunjang operasional bisnis, klasifikasi perangkat memiliki dasar parameter seperti, seberapa sering digunakan, seberapa penting digunakan, dan seberapa mahal perangkat tersbut maka akan menjadi critical, namun apabila ada salah satu parameter yang tidak terpenuhi yaitu menjadi support saja seperti harganya murah, atau jarang digunakan.

Pada gambar 4.10 menggambarkan skema teknis bagaimana system arsitektur blueprint di implementasi, seperti pegawai internal mengakses switch lalu ada firewall tersendiri dan ada authentications untuk mengecek keaslian anggota dan tipe anggota seperti apa, lalu baru bisa terhubung ke server dan menggunakan data.

4.11. Blueprint Enterprise Architecture

Dalam pengembangan enterprise architecture diperlukan roadmap atau gambaran besar suatu sistem keamanan yang disebut blueprint dimana isinya adalah rancangan serta penjelasan bisnis proses. Penulis telah membuat sebuah rancangan *blueprint* seperti pada gambar 4.11.

ENTERPRISE ARCHITECTURE SCALEOUT CREATIVE AGENCY					
RENCANA STRATEGIS					
Scope: Internal dan Eksternal	GOALS 1: Security Awareness	GOALS 2: Menjaga Privasi Data	GOALS 3: Aksesibilitas data	GOALS 4: Fleksibilitas Data	GOALS 5: Evaluasi Berkelanjutan
IT Program: 1. Pelatihan karyawan 2. User management 3. Menggunakan Antivirus 4. Menggunakan DMS	Monitoring sistem	Perlindungan software	Business Architecture	Penanganan Insiden	Pembagian Hak Akses
	1. Aplikasi 2. User 3. Admin 4. Hak Akses	1. User 2. Pelatihan 3. Pengembangan berkelanjutan	Data Architecture	1. Aplikasi 2. User Aplikasi 3. Login 4. Role 5. Hak Akses 6. Report Insiden	1. User 2. Koordinasi 3. Peninjauan evalitasi 4. Kebijakan
	Antivirus	User management	Application Architecture	Perlindungan data	Service Operation

Gambar 4. 11 *Blueprint Enterprise Architecture* Scaleout Creative Agency

Pada gambar 4.11 dalam rencana strategis enterprise architecture terdapat hal teknis yang perlu di kaji dan di implementasi sesuai dengan goals 1 hingga goals 5 yang menjadi output atau standar keberhasilan suatu rencana. Dalam mendefinisikan rencana kita perlu scope baik internal maupun eksternal, dengan membuat program-program pengembangan SDM seperti pelatihan karyawan, manajemen user, menggunakan antivirus dan DMS yang berguna untuk keamanan dan efisiensi dari segi document dan data. Di dalam rencana strategis terdapat 3 segmen arsitektur, yaitu; bisnis arsitektur, data arsitektur dan aplikasi arsitektur. Dalam business arsitektur hal yang perlu di implementasi adalah penanganan insiden apabila terjadi sesuatu hal yang diluar dugaan, lalu membagi hak akses ke

setiap user agar tidak sembarangan atau ceroboh dalam menggunakan atau mengakses data untuk bisnis, selanjutnya terdapat monitoring system berguna untuk memantau dan mengecek apakah system berjalan dengan baik atau tidak, apa ada masalah atau tidaknya, maka dari itu perlu adanya perlindungan software dimana semua software berjalan dengan semestinya tidak ada bug atau virus di dalam nya, ataupun diserang oleh hacker dari luar jaringan yang dapat mencuri data critical. Segmen ke 2 (data architecture) adalah implementasi arsitektur data, terdapat 5 hal pada layer pertama untuk di implementasi seperti install aplikasi, penggunaan aplikasi untuk user, login dengan membedakan hak akses dan role yang digunakan serta report insien bila ada hal diluar dugaan atau masalah lain, layer selanjutnya terdapat 4 yang harus di perhatikan yaitu user, koordinasi, evaluasi penjualan dan kebijakan dalam pengelolaan perusahaan, selanjutnya terdapat 4 hal yang diperhatikan seperti aplikasi, role user, admin dan hak akses untuk kedua role tersebut harus di bedakan fungsionalitas dan kegunaan akun tersebut, sehingga pada layer akhir terdapat pelatihan user dengan pengembangan berkelanjutan agar menerima ouput goals yang sesuai. Pada segmen terakhir terdapat application architecture yang berguna untuk memetakan arsitektur dari aplikasi baik physical ataupun non physical, untuk pertama-tama implementasi perlindungan data diperlukan seperti install antivirus, privacy data, hak akses dll, berguna untuk membatasi dan memantau siapa saja user yang menggunakan data tersebut, lalu service operation digunakan untuk pelayanan operasional dalam menjalani kegiatan bisnis, perlu adanya service operasional baik dari sisi customer ataupun after sales, selanjutnya penggunaan antivirus yang harus digunakan berbagaimacam antivirus

seperti windows defender ataupun software pihak ketiga, bisa juga dengan menggunakann document security, dan yang terakhir terdapat user management berguna untuk mengatur role ataupun hak akses dari pengguna dengan begitu user pun tidak akan asal-asalan dalam menggunakan data terutama data critical perusahaan yang tidak bisa diakses oleh sembarangan user, harus memiliki hak akses dan role yang sesuai.

Adapun ancaman yang dialami perusahaan jika terdapat hal diluar policy atau dugaan. Tabel 4.17 menjelaskan solusi yang direkomendasikan.

Tabel 4. 17 Ancaman dan rekomendasi tindakan di Scaleout Creative Agency

No.	Ancaman	Klasifikasi	Solusi tindakan mencegah	Solusi tindakan apabila terkena resiko
1.	Social Engineering	Critical	1.Mengabaikan pesan, atau email yang mencurigakan 2.Menghubungi It Scurity 3.Jangan mengklik apapun didalam pesan/email 4.Hapus email/pesan bila terbukti terdapat malware	1.Segera putus koneksi internet LAN 2.Segera lakukan Tindakan scan antivirus 3.Backup secara berkala data critical

Tabel 4.17. (Lanjutan)

No.	Ancaman	Klasifikasi	Solusi tindakan mencegah	Solusi tindakan apabila terkena resiko
				4.Ketahui jenis malware dan solusinya
2.	Data leaked	Critical	1.Menutup/memperbaiki port data yang rentan 2.Memeriksa data yang berpotensi bocor seperti data critical 3.Menggunakan antivirus 4.Lakukan scan seminggu sekali atau setiap hari	1.Segera menutup atau memperbaiki port data 2.Kenali malware yang menyerang dan solusinya 3.Lakukan Risk asesmen 4.Backup data secara berkala terutama data critical
3.	SQL Injection	Critical	1.Analisa celah keamanan yang rentan/tidak terdapat validasi query	1.Analisa field/data yang ter inject

Tabel 4.17. (Lanjutan)

No.	Ancaman	Klasifikasi	Solusi tindakan mencegah	Solusi tindakan apabila terkena resiko
			2.Analisa field atau data yang memiliki rentan di inject 3.Berikan validasi pada front end dan backend agar tidak sembarangan data masuk	2.Hapus atau rewrite data yang ter inject 3.Lalu lakukan backup data yang di hapus tersebut 4.Lakukan monitoring data secara berkala apabila terdapat data aneh/mencurigakan
4.	Aksesibilitas Data	Critical	1. Memastikan kepatuhan terhadap standar keamanan, seperti mengikuti praktik pengamanan data yang direkomendasikan dan	1.Membagikan hak akses kepada karyawan yang membutuhkan 2.Authorisasi karyawan

Tabel 4.17. (Lanjutan)

No.	Ancaman	Klasifikasi	Solusi tindakan mencegah	Solusi tindakan apabila terkena resiko
			mengadopsi teknologi keamanan yang tepat 2. Menggunakan akses kontrol yang ketat dengan menerapkan autentikasi pengguna dan izin akses yang tepat. 3. Menggunakan perangkat lunak atau alat konversi format data yang dapat mengubah data menjadi format yang kompatibel. 4. Menyediakan dokumentasi lengkap dan terperinci tentang data, termasuk instruksi	3.Pastikan data aksesible atau tersedia untuk karyawan yang membutuhkan 4.membatasi koneksi dengan orang yang tidak berkepentingan dan membuka koneksi data kepada orang yang berkepentingan 5.Memastikan kompatibilitas format data yang dapat dan mudah diakses olah yang berkepentingan

Tabel 4.17. (Lanjutan)

No.	Ancaman	Klasifikasi	Solusi tindakan mencegah	Solusi tindakan apabila terkena resiko
			penggunaan, format data, definisi atribut, dll	
5.	Kecurangan Karyawan Internal/Nepotisme	Critical	1. Batasi akses karyawan yang tidak berkepentingan 2. Kurangi hal-hal yang tidak diperlukan dalam bisnis yang nantinya berpotensi membuat kecurangan 3. Tingkatkan dan perketat sistem audit	1.Periksa pihak yang terlibat seluruhnya 2.Lakukan audit ke semua karyawan yang terlibat 3.Lakukan pemeriksaan terhadap data ataupun cashflow perusahaan
6.	Struktur data yang kaku (Fleksibilitas)	Critical	1. Menerapkan strategi manajemen metadata yang baik untuk memudahkan pemahaman struktur	1. Mengadopsi pendekatan desain yang lebih fleksibel, seperti penggunaan

Tabel 4.17. (Lanjutan)

No.	Ancaman	Klasifikasi	Solusi tindakan mencegah	Solusi tindakan apabila terkena resiko
			data dan memungkinkan adaptasi lebih lanjut 2. Mengadopsi praktik manajemen data yang baik, termasuk pemodelan data yang konsisten dan penggunaan standar domain yang diterima secara luas 3. Memperkuat praktik pengelolaan data yang baik, seperti penerapan aturan validasi dan pembaruan rutin untuk menjaga integritas data.	skema data terbuka (open schema) atau skema data semantik
7.	Slow Growth Business	Major	1.Lakukan pengembangan bisnis secara continuity	1.Lakukan brainstorming dengan mencari referensi saat ini

Tabel 4.17. (Lanjutan)

No.	Ancaman	Klasifikasi	Solusi tindakan mencegah	Solusi tindakan apabila terkena resiko
			mengikuti perkembangan jaman 2.Analisa competitor 3.Fokus pada produk dan marketing	2.Lakukan diskusi dan survey dengan user/pengguna 3.Lakukan system ATM(Amati Tiru Modifikasi) 4.Adopsi cara kerja terbaru guna menunjang produktivitas kinerja karyawan

4.12. Expert Judgement

Tahap terakhir dari penelitian ini yaitu melakukan presentasi *expert judgement* dari ahli yang mengacu pada tanggapan yang diberikan oleh ahli di bidang akademisi yang memiliki pengetahuan dan pengalaman yang relevan dalam bidang keamanan IT dalam perusahaan. *Expert Judgement* digunakan untuk memperoleh wawasan mendalam dan pemahaman tentang isu-isu yang kompleks

dan teknis, serta memberikan rekomendasi berdasarkan pengetahuan dan pengalaman ahli.

Selain itu, pada tahap akhir ini juga dilakukan *Focused Group Discussion* (FGD) yang melibatkan para stakeholder dari Scaleout Creative Agency yang mewakili berbagai sudut pandang atau kepentingan yang berbeda. FGD bertujuan untuk mendapatkan perspektif dan pemahaman yang lebih luas mengenai topik dalam penelitian ini dengan mengadakan diskusi terfokus dan terstruktur terkait hasil penelitian sistem keamanan yang berfokus pada aspek aksesibilitas dan fleksibilitas di Scaleout Creative Agency. Para stakeholder yang terlibat dalam presentasi ini adalah perwakilan manajemen agensi kreatif, diantaranya; CEO, tim keamanan TI, dan manajer proyek.

Dalam presentasi tersebut, stakeholder menyampaikan tanggapan dari hasil *blueprint* penelitian yang meliputi analisis mendalam terhadap kebijakan keamanan yang telah ada, prosedur pengelolaan risiko, dan identifikasi ancaman keamanan yang spesifik terkait dengan lingkungan kerja jarak jauh. Selain itu, presentasi ini juga mencakup evaluasi terhadap infrastruktur teknologi yang ada, termasuk rancangan/blueprint untuk meningkatkan sistem keamanan terkait aksesibilitas dan fleksibilitas pekerjaan karyawan jarak jauh. Hasil penelitian menyoroti kelemahan potensial dalam infrastruktur tersebut dan rekomendasi perbaikan untuk meningkatkan tingkat keamanan. Adapun pertanyaan yang diajukan oleh ahli external dan para stakeholder dari presentasi rancangan blueprint beserta jawaban dari penulis terkait pertanyan-pertanyaan tersebut, diantaranya;

A. Ahli IT

a) Dalam konteks goals dalam rencana strategis, mana prioritasnya yang terlebih dahulu?

b) Dalam kolom IT program apakah sudah urut?

Jawab:

a) Untuk urutan dari blueprint EA (Enterprise Architecture) dari integrasi TOGAF dan SABSA dapat ditentukan berdasarkan langkah-langkah berikut:

i. Security Awareness (Kesadaran Keamanan) merupakan langkah pertama untuk memastikan bahwa semua karyawan memiliki kesadaran atau pengetahuan yang cukup tentang keamanan informasi dan praktik keamanan yang tepat. Ini melibatkan pelatihan dan penyuluhan mengenai ancaman keamanan, kebijakan keamanan, dan tindakan pencegahan yang harus diikuti.

ii. Menjaga Privasi Data, setelah kesadaran keamanan tercipta, langkah selanjutnya adalah menjaga privasi data. Hal ini melibatkan penerapan kebijakan dan prosedur yang memastikan perlindungan data sensitif dari akses yang tidak sah. Upaya ini meliputi enkripsi data, pengaturan akses yang tepat, dan pengelolaan identitas pengguna.

iii. Aksesibilitas Data, penting untuk memastikan aksesibilitas data yang tepat bagi karyawan jarak jauh. Hal ini melibatkan implementasi solusi teknologi yang memungkinkan karyawan untuk mengakses data dan aplikasi yang diperlukan dengan aman dari jarak jauh. Penggunaan *Virtual Private Network* (VPN), kebijakan akses yang tepat, dan

perlindungan perangkat mobile menjadi beberapa aspek yang perlu dipertimbangkan.

iv. Fleksibilitas Data. Fleksibilitas data juga penting untuk mendukung kebutuhan karyawan jarak jauh. Hal ini melibatkan penggunaan teknologi dan sistem yang memungkinkan *sharing* dan kolaborasi data secara efektif. Solusi seperti *cloud computing, file sharing* yang aman, dan kolaborasi *real-time* menjadi penting untuk meningkatkan fleksibilitas data.

v. Evaluasi Berkelanjutan. Langkah terakhir adalah melakukan evaluasi berkelanjutan terhadap sistem keamanan yang diterapkan. Ini melibatkan pemantauan, pengukuran, dan penilaian secara rutin terhadap efektivitas kebijakan, solusi teknologi, dan tindakan keamanan yang telah diimplementasikan. Evaluasi ini membantu dalam mengidentifikasi kelemahan atau celah keamanan yang mungkin terjadi dan memungkinkan untuk perbaikan yang diperlukan.

Dalam konteks integrasi SABSA dan TOGAF, langkah-langkah tersebut dapat diterapkan dengan menggunakan kerangka kerja TOGAF untuk perancangan arsitektur yang terintegrasi dan mempertimbangkan aspek keamanan dari SABSA dalam setiap tahap pengembangan arsitektur.

b) Berikut urutan penerapan blueprint pada kolom Program IT:

i. Pelatihan Karyawan : Langkah pertama adalah memberikan pelatihan keamanan kepada karyawan. Pelatihan ini mencakup pemahaman tentang kebijakan keamanan, praktik terbaik dalam penggunaan sistem,

dan tindakan pencegahan yang harus diikuti. Pelatihan ini penting untuk meningkatkan kesadaran karyawan tentang ancaman keamanan dan bagaimana mereka dapat berkontribusi dalam melindungi sistem.

ii. User Management. Langkah selanjutnya adalah mengelola akses pengguna dengan baik. Ini melibatkan penerapan kebijakan dan prosedur yang jelas untuk manajemen pengguna, termasuk pemberian hak akses yang tepat berdasarkan kebutuhan pekerjaan. Hal ini membantu memastikan bahwa setiap karyawan memiliki akses yang sesuai dengan tanggung jawab mereka dan mengurangi risiko akses yang tidak sah.

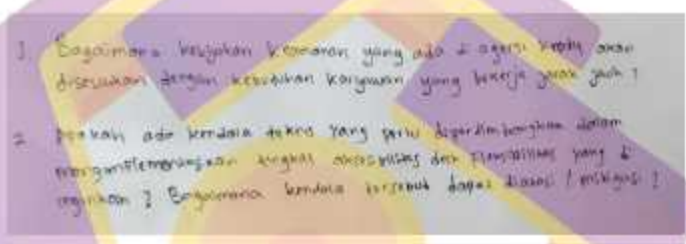
iii. Menggunakan Antivirus merupakan salah satu langkah penting dalam melindungi sistem adalah menggunakan perangkat lunak antivirus yang kuat dan terbaru. Antivirus membantu mendeteksi dan menghapus malware serta melindungi sistem dari ancaman keamanan yang mungkin muncul melalui email, unduhan, atau sumber lainnya. Perangkat lunak antivirus harus diperbarui secara teratur untuk memastikan perlindungan yang efektif.

iv. Menggunakan DMS (Document Management System) Implementasikan sistem manajemen dokumen (DMS) yang aman untuk menyimpan dan mengelola dokumen penting. DMS dapat memberikan keamanan tambahan dengan mengendalikan akses ke dokumen yang sensitif dan melacak versi dan riwayat perubahan dokumen. Hal ini

memastikan bahwa data yang disimpan dalam sistem DMS dilindungi dengan baik dan dapat diakses dengan aman oleh karyawan jarak jauh.

Urutan tersebut dapat bervariasi, tergantung pada kebutuhan dan konteks spesifik agensi kreatif. Oleh karena itu, urutan ini telah di modifikasi dan disesuaikan dengan implementasi integrasi TOGAF dan SABSA pada penelitian ini.

B. Tim Keamanan IT Scaleout Creative Agency



Gambar 4. 12 Tanggapan dari IT Scaleout Creative Agency

a) Bagaimana kebijakan keamanan yang ada di agensi kreatif akan disesuaikan dengan kebutuhan karyawan yang bekerja jarak jauh?

Jawab:

Untuk menyelaraskan kebijakan keamanan dengan kebutuhan karyawan yang bekerja jarak jauh, Scaleout Creative Agency dapat mengadopsi beberapa langkah berikut:

i) Evaluasi kebutuhan karyawan jarak jauh: perlunya pemahaman mengenai kebutuhan karyawan yang bekerja jarak jauh secara mendalam. Hal ini meliputi aksesibilitas ke sistem, aplikasi, dan data yang diperlukan untuk menjalankan tugas mereka dengan efektif. Evaluasi ini dapat dilakukan dengan survey yang lebih

mendalam melalui survei, wawancara, atau diskusi dengan karyawan yang terlibat dengan kerja jarak jauh.

ii) Penyesuaian kebijakan keamanan: Setelah memahami kebutuhan karyawan jarak jauh, perlunya penyesuaian kebijakan keamanan yang ada. Hal ini dapat meliputi pengaturan tingkat akses, kebijakan penggunaan perangkat pribadi, enkripsi data, dan langkah-langkah keamanan lainnya yang relevan dengan kegiatan karyawan jarak jauh.

iii) Penyediaan akses yang aman: Scaleout Creative Agency juga harus memastikan bahwa karyawan jarak jauh memiliki akses yang aman ke sistem dan data yang diperlukan. Hal ini dapat melibatkan penggunaan teknologi seperti VPN (*Virtual Private Network*) untuk mengamankan koneksi jaringan, autentikasi multi-faktor untuk memastikan keaslian pengguna, dan enkripsi *end-to-end* untuk melindungi data yang dikirim melalui jaringan.

iv) Pelatihan keamanan: perlu adanya pelatihan keamanan kepada karyawan jarak jauh untuk meningkatkan kesadaran mereka tentang ancaman keamanan dan praktik yang aman. Pelatihan ini dapat mencakup penggunaan yang aman perangkat dan aplikasi, deteksi *phishing*, manajemen kata sandi yang kuat, dan praktik keamanan umum lainnya.

v) Monitoring dan pemantauan: Scaleout harus memiliki sistem pemantauan dan pemantauan yang efektif untuk mengawasi

aktivitas dan akses karyawan jarak jauh. Ini memungkinkan deteksi dini terhadap perilaku mencurigakan atau aktivitas yang tidak diotorisasi dan memungkinkan tindakan respons yang cepat.

vi) Tinjauan dan pembaruan berkala: Kebijakan keamanan perlu diperbarui secara berkala sesuai dengan perubahan kebutuhan dan ancaman keamanan yang muncul. Tinjauan rutin harus dilakukan untuk memastikan kebijakan tetap relevan, efektif, dan sesuai dengan praktik keamanan terbaik.

Dengan mengikuti langkah-langkah di atas, Scaleout Creative Agency dapat memastikan bahwa kebijakan keamanan mereka disesuaikan dengan kebutuhan karyawan yang bekerja jarak jauh, menjaga data dan sistem mereka tetap aman, serta memberikan lingkungan kerja yang aman bagi karyawan mereka.

b) Apakah ada kendala teknis yang perlu dipertimbangkan dalam mengimplementasikan tingkat aksesibilitas dan fleksibilitas yang diinginkan? Bagaimana kendala tersebut dapat diatasi atau mitigasi?

Jawab:

Ya, ada beberapa kendala teknis yang perlu dipertimbangkan dalam mengimplementasikan tingkat aksesibilitas dan fleksibilitas yang diinginkan pada sistem TI agensi kreatif, terutama terkait dengan keamanan dan ketersediaan data.

i) Keamanan: Perusahaan perlu memastikan bahwa data sensitif tidak mudah diakses oleh orang yang tidak berwenang. Hal ini dapat diatasi dengan memastikan bahwa hanya karyawan yang

telah terverifikasi dan diotorisasi yang memiliki akses ke data sensitif. Solusi seperti sistem otorisasi dan autentikasi yang kuat dan multifaktor dapat membantu mengurangi risiko keamanan.

ii) Ketersediaan: Dalam lingkungan kerja jarak jauh, ketersediaan data menjadi sangat penting untuk memastikan kelancaran proses bisnis. Untuk memastikan ketersediaan, perusahaan perlu memastikan bahwa sistem TI dan jaringan dapat diakses dengan mudah oleh karyawan jarak jauh. Solusi seperti teknologi *load balancing* dan sistem pemantauan jaringan dapat membantu memastikan ketersediaan yang optimal.

iii) Kompatibilitas: Karyawan jarak jauh mungkin menggunakan berbagai perangkat dan sistem operasi yang berbeda. Untuk memastikan aksesibilitas dan fleksibilitas, perusahaan perlu memastikan bahwa sistem TI dan aplikasi dapat berjalan dengan lancar pada berbagai platform dan perangkat.

iv) Skalabilitas: Dalam perkembangan zaman yang pesat, perusahaan perlu memastikan bahwa sistem TI dan infrastruktur dapat dengan mudah disesuaikan dengan pertumbuhan dan kebutuhan bisnis yang berkembang. Solusi seperti menggunakan teknologi cloud dan infrastruktur yang dapat diskalakan dapat membantu perusahaan untuk meningkatkan fleksibilitas dan skabilitas sistem TI.

v) Kecepatan koneksi: Koneksi internet yang lambat dapat menghambat produktivitas karyawan jarak jauh. Oleh karena itu, perusahaan perlu memastikan bahwa karyawan memiliki akses ke koneksi internet yang cepat dan andal. Solusi seperti menyediakan karyawan dengan akses ke jaringan VPN (Virtual Private Network) yang aman dan cepat dapat membantu memastikan koneksi yang optimal.

Untuk mengatasi kendala-kendala tersebut, perusahaan perlu mengadopsi pendekatan yang holistik dalam mengembangkan arsitektur TI dan kebijakan keamanan yang mempertimbangkan berbagai aspek teknis, operasional, dan bisnis secara menyeluruh. Perusahaan juga harus secara teratur melakukan evaluasi dan pemantauan terhadap sistem dan infrastruktur TI yang ada untuk memastikan bahwa kebutuhan karyawan yang bekerja jarak jauh terpenuhi secara optimal.

C. CEO Scaleout Creative Agency

Gambar 4. 13 Tanggapan dari CEO Scaleout Creative Agency

a) Apakah ada biaya atau investasi tambahan yang diperlukan untuk mengimplementasikan blueprint ini?

Jawab:

Dari survey yang dilakukan pada Scaleout Creative Agency, terdapat beberapa biaya yang harus dikeluarkan terkait dengan implementasi blueprint ini antara lain:

i) Perangkat dan Infrastruktur: Diperlukan perangkat tambahan seperti Antivirus, VPN, atau perangkat jaringan tambahan (Switch, server, penyimpanan cloud, dsb). Perlunya investasi dalam perangkat keras dan perangkat lunak yang sesuai dengan kebutuhan keamanan dalam mendukung aksesibilitas dan fleksibilitas.

ii) Pelatihan dan Pendidikan: Untuk memastikan pemahaman dan kepatuhan terhadap kebijakan dan prosedur keamanan yang baru, pelatihan dan pendidikan kepada karyawan diperlukan. Ini dapat mencakup pelatihan tentang penggunaan perangkat keamanan, praktik keamanan, dan kesadaran akan ancaman keamanan. Biaya yang terkait dengan pelatihan ini perlu diperhitungkan.

iii) Pemantauan dan Audit: Setelah implementasi kebijakan keamanan dan fleksibilitas, penting untuk melakukan pemantauan dan audit secara berkala untuk memastikan kepatuhan dan efektivitas kebijakan tersebut. Biaya yang terkait dengan pemantauan dan audit ini perlu diperhitungkan.

b) Bagaimana blueprint ini dapat memberikan nilai tambah bagi agensi kreatif secara keseluruhan?

Seperti yang sudah dijelaskan pada presentasi, *blueprint* yang sudah dibuat dapat untuk mengoptimalkan sistem keamanan dan fleksibilitas di Scaleout serta dapat memberikan nilai tambah bagi Scaleout secara keseluruhan dalam beberapa cara, diantaranya;

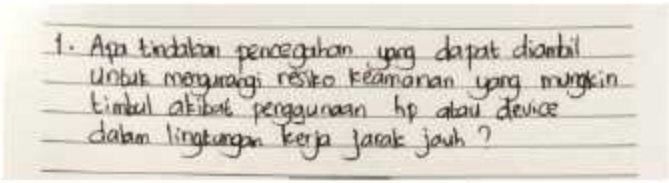
i) Meningkatkan efisiensi dan produktivitas: Dengan sistem keamanan yang lebih kuat dan fleksibilitas yang lebih besar, karyawan dapat bekerja dengan lebih efisien dan produktif tanpa harus khawatir tentang ancaman keamanan atau kendala teknis lainnya. Hal ini dapat menghemat waktu dan biaya operasional yang signifikan bagi agensi.

ii) Meningkatkan reputasi dan kepercayaan pelanggan: Dengan sistem keamanan yang lebih kuat, Scaleout dapat menjamin keamanan data dan informasi klien. Hal ini dapat meningkatkan kepercayaan pelanggan dan reputasi secara keseluruhan.

iii) Mengurangi risiko keamanan dan pengeluaran biaya: Dengan sistem keamanan yang lebih kuat, agensi dapat mengurangi risiko keamanan dan biaya terkait pelanggaran data atau serangan siber.

Secara keseluruhan, blueprint ini dapat memberikan nilai tambah yang signifikan bagi Scaleout Creative Agency dengan meningkatkan keamanan, fleksibilitas, efisiensi, reputasi, daya saing, dan mengurangi risiko dan pengeluaran biaya.

D. Manajer Proyek Scaleout Creative Agency


1. Apa tindakan pencegahan yang dapat diambil untuk mengurangi resiko keamanan yang mungkin timbul akibat penggunaan hp atau device dalam lingkungan kerja jarak jauh ?

Gambar 4. 14 Tanggapan dari CEO Scaleout Creative Agency

a) Apa tindakan pencegahan yang dapat diambil untuk mengurangi risiko keamanan yang mungkin timbul akibat penggunaan hp atau device dalam lingkungan kerja jarak jauh?

Jawab:

Berikut adalah beberapa tindakan pencegahan yang dapat diambil:

i) Menerapkan kebijakan keamanan perangkat mobile: Buat kebijakan yang jelas mengenai penggunaan perangkat mobile dalam lingkungan kerja jarak jauh. Kebijakan ini harus mencakup langkah-langkah seperti penggunaan kata sandi yang kuat, enkripsi data, pengaturan instalasi aplikasi, dsb.

ii) Menggunakan solusi MDM (*Mobile Device Management*): Solusi MDM dapat membantu mengelola dan mengamankan perangkat mobile yang digunakan dalam lingkungan kerja jarak jauh. Dengan solusi MDM, agensi dapat melakukan pemantauan, pengaturan kebijakan, penghapusan data jarak jauh, dan pembaruan perangkat secara terpusat.

iii) Menggunakan VPN (*Virtual Private Network*): Mendorong penggunaan VPN saat karyawan mengakses jaringan perusahaan dari perangkat mobile mereka. VPN membantu melindungi

komunikasi dan data dengan mengenkripsi lalu lintas internet, sehingga menjaga keamanan saat mengakses sumber daya perusahaan secara jarak jauh.

iv) Memberikan pelatihan keamanan kepada karyawan: Berikan pelatihan keamanan yang terkait dengan penggunaan perangkat mobile kepada karyawan, contohnya kesadaran akan ancaman keamanan, praktik terbaik dalam mengamankan perangkat dan data, serta tindakan pencegahan lainnya yang harus diikuti saat bekerja jarak jauh.

v) Melakukan kebijakan cadangan dan pemulihan data: Memastikan ada kebijakan cadangan data yang teratur dan pemulihan data dalam kasus kehilangan atau kerusakan perangkat mobile. Hal ini penting untuk memastikan bahwa data yang penting tetap aman dan dapat dipulihkan jika terjadi insiden.

Dengan mengambil tindakan pencegahan ini, Scaleout Creative Agency menyetujui untuk penerapan blueprint yang telah dibuat, namun tidak dalam jangka waktu terdekat. Pihak Scaleout Creative Agency menyadari bahwa blueprint tersebut dapat mengurangi risiko keamanan yang terkait dengan penggunaan perangkat mobile dalam lingkungan kerja jarak jauh, dan menjaga kerahasiaan dan integritas data perusahaan.

Hasil presentasi expert judgement ini diharapkan dapat memberikan pemahaman yang lebih baik tentang kebutuhan keamanan dalam konteks

aksesibilitas dan fleksibilitas di agensi kreatif. Selain itu, informasi yang disampaikan oleh stakeholder dalam presentasi ini dapat menjadi landasan untuk merancang kebijakan, prosedur, dan tindakan mitigasi yang lebih efektif dalam menghadapi risiko keamanan yang terkait dengan karyawan jarak jauh pada agensi kreatif.

BAB V

PENUTUP

5.1. Kesimpulan

Hasil dari penelitian ini merupakan penggabungan dan penyempurnaan sistem yang sudah ada agar dapat mengembangkan dan memajukan sistem keamanan perusahaan. Keunggulan yang telah diperoleh dari penelitian ini adalah melengkapi dan membuat rancangan sistem keamanan dalam bentuk blueprint, dengan tujuan untuk meningkatkan sistem keamanan di Scaleout Creative Agency, terutama mengenai fleksibilitas dan aksesibilitas data.

Pengintegrasian kedua framework ini dengan tujuan supaya perusahaan dapat menghasilkan solusi keamanan yang lebih kuat, terintegrasi dengan baik dalam konteks arsitektur perusahaan, dan mendukung aksesibilitas dan fleksibilitas data untuk karyawan jarak jauh. Karena, framework SABSA membantu dalam memahami risiko bisnis yang spesifik dan mendefinisikan pengukuran kinerja di aspek keamanan yang relevan. Sedangkan, TOGAF menyediakan *framework* yang luas untuk perencanaan dan manajemen di bagian *enterprise architecture*.

Integrasi *framework* SABSA dan TOGAF ini sistematis, fleksibel dan aksesibel dalam hal sistem keamanan data, namun tidak menutup kemungkinan terdapat fraud serta human error dalam penggunaannya. Untuk meminimalisir resiko tersebut penelitian ini memberikan solusi seperti audit, evaluasi berlanjut, membagi hak akses serta menggunakan antivirus dan firewall agar terhindar dari ancaman keamanan.

Maka dari itu perlunya diterapkan beberapa peraturan yang mendukung penerapan blueprint ini, seperti; SOP, audit, verifikasi identitas, pengendalian akses, kebijakan keamanan yang ketat, dan monitoring. Dengan menggabungkan pendekatan tersebut, perusahaan dapat mengurangi risiko human fraud pada bagian social engineering dan meningkatkan keamanan. Penting untuk memastikan bahwa langkah-langkah ini diimplementasikan secara konsisten dan diperbarui sesuai dengan perkembangan ancaman keamanan yang baru muncul.

Penelitian sejalan dengan penelitian tentang "Perancangan enterprise security architecture melalui integrasi arsitektur keamanan informasi dengan *Enterprise Architecture* (SABSA dan TOGAF 9.1)" yang dilakukan oleh Kurniawan, Novianto Budi (2013) dengan studi kasus-nya adalah Direktorat Diseminasi Statistik BPS yaitu unit kerja BPS yang berperan sebagai "pintu gerbang" keluar masuknya data dan informasi statistik. Dari penelitian tersebut, arsitektur keamanan SABSA dapat diintegrasikan secara sinergis dengan arsitektur organisasi (EA TOGAF) untuk menghasilkan sebuah *Enterprise Security Architecture* yang baik.

Pada penelitian ini *framework* SABSA dan TOGAF memiliki keunggulan dalam menjawab permasalahan aksesibilitas dan fleksibilitas data yang aman di akses oleh karyawan jarak jauh, dalam membangun arsitektur keamanan data, dengan mengintegrasikan *framework* SABSA dan TOGAF maka akan menghasilkan *framework* arsitektur yang unggul dalam sistem keamanan.

5.2. Saran

Hasil penelitian menemukan kekurangan dan celah keamanan apabila data dan sistem keamanan di salah gunakan oleh pihak internal itu sendiri, sulitnya *tracking system* untuk mencari bukti insiden apabila ditemukan kasus yang ada pada internal perusahaan Scaleout walaupun sudah diberikan hak akses masing-masing, autentikasi dan *firewall* disetiap divisi harus melewati semua arsitektur sistem keamanan.

Sistem keamanan sudah diperketat dan lebih sistematis dengan SABSA dan TOGAF, untuk implementasinya kemungkinan akan sulit karena membutuhkan biaya banyak dan waktu yang tidak singkat, namun hal ini bertujuan meningkatkan fleksibilitas, aksesiblitas, dan sistem keamanan data.

Untuk saran kedepannaya pelatihan internal dan integritas karyawan yang paling berpengaruh jalannya sistem keamanan serta manajemen perusahaan yang unggul agar terciptanya objektif tujuan perusahaan kedepannya.

DAFTAR PUSTAKA

PUSTAKA MAJALAH, JURNAL ILMIAH ATAU PROSIDING

Khreishah A. dan Gaber J., "Securing Virtualized Environments in *Cloud computing*". IEEE Security & Privacy Magazine. 2015.

A. L. A. dos Santos dan V. D. P. Lopes., "Integrating SABSA with TOGAF for Enterprise Security Architecture Development". Jurnal Procedia Computer Science, Volume 164, halaman 491-498, 2019.

F. Farhana, M. M. H. Khan, M. A. R. Ahad, dan M. M. Alam., "Accessibility and Security in the Cloud: A Comparative Study of Google Drive, OneDrive and Dropbox". Journal of *Cloud computing*. 2018.

Sherwood, J., Clark, A. and Lynas, D. "Enterprise Security Architecture". SABSA White Penelitian, 6, 43-54. 2009.

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.

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.

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

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

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

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.

PUSTAKA ELEKTRONIK

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

LAMPIRAN

1. Quesioner Data Perusahaan (diisi oleh IT Scaleout Creative Agency)

1. Faktor-faktor yang berpengaruh terhadap keamanan aksesibilitas dan fleksibilitas pada Scaleout Creative Agency

No.	Jenis Risiko	Kode	Kejadian Risiko	Frekuensi Risiko yang terjadi					Pengaruh risiko terhadap sistem keamanan				
				1	2	3	4	5	1	2	3	4	5
1	Internal	A1	Kehilangan data klien atau kebocoran data rahasia klien	X						X			
		A2	Serangan malware atau virus pada sistem			X						X	
		A3	Kebocoran informasi rahasia atau kekayaan intelektual		X					X			
		A4	Kerusakan atau kehilangan peralatan komputer dan teknologi				X				X		
		A5	Pelanggaran privasi data karyawan atau pelanggaran regulasi privasi data	X						X			
		A6	Kecelakaan atau kejadian tak terduga yang dapat merusak fasilitas atau aset kreatif agensi				X				X		
		A7	Ketergantungan terhadap layanan pihak ketiga atau vendor				X					X	
		A8	Kesalahan manusia atau kesalahan dalam proses bisnis yang dapat mengakibatkan kerugian.			X					X		
2	Eksternal	B1	Risiko kehilangan data karena penggunaan perangkat yang tidak aman saat bekerja dari jarak jauh.		X						X		
		B2	Risiko penyeberan malware melalui jaringan yang tidak aman saat mengakses data atau sistem dari luar jaringan agensi.			X						X	
		B3	Risiko kebocoran informasi rahasia karena penggunaan komunikasi yang tidak aman, seperti email atau pesan instan.	X					X				
		B4	Risiko penipuan dan phising karena penggunaan identitas palsu atau lemah untuk mengakses data dan sistem agensi.	X					X				
		B5	Risiko keamanan jaringan yang rentan karena koneksi yang tidak aman atau lemah saat mengakses jaringan agensi dari luar.	X					X				
		B6	Risiko keamanan perangkat karena penggunaan perangkat yang tidak aman atau perangkat pribadi yang rentan saat mengakses data dan sistem agensi dari jarak jauh.		X						X		
		B7	Risiko akses tidak sah ke data dan sistem karena tidak adanya kontrol akses yang tepat saat bekerja dari jarak jauh.			X				X			

	B8	Risiko kehilangan data karena ketidakmampuan backup data yang tepat saat bekerja dari jarak jauh.	✓			X	
	B9	Risiko ketidakpatuhan terhadap kebijakan dan standar keamanan karena kurangnya pemahaman dan kesadaran tentang kebijakan dan standar keamanan yang berlaku di agensi.	X		✓		
	B10	Risiko serangan DDoS atau hacking yang dapat mengakibatkan kerusakan pada data dan sistem agensi.	X				✓

A. Petunjuk Pengisian Kuesioner:

a. Jawaban merupakan persepsi Bapak/Ibu terhadap frekuensi yang terjadi, dan pengaruh risiko terhadap sistem keamanan

b. Pengisian kuesioner dilakukan dengan memberi tanda ☑ atau X pada kolom yang telah disediakan

B. Keterangan Penilaian

1. Sangat Jarang (SJ) = Jarang (hampir tidak mungkin) terjadi pada kondisi tertentu (dalam kurun 1 kali terjadi selama 2 tahun)
2. Jarang (J) = Kemungkinan kecil terjadi pada setiap kondisi (1x dalam 2 tahun)
3. Terkadang (T) = Mungkin terjadi pada kondisi tertentu (1-2 kali dalam 2 tahun)
4. Sering (S) = Kemungkinan besar terjadi pada setiap kondisi (2x dalam 2 tahun)
5. Sangat Sering (SS) = Hampir pasti terjadi pada setiap kondisi (lebih dari 2x dalam 2 tahun)

C. Keterangan untuk penilaian

Dampak kerugian meliputi Reputasi dan Finansial pada perusahaan.

1. Tidak ada pengaruh = Tidak ada kerugian
2. Rendah = Kerugian <5%
3. Sedang = Kerugian 5% - 10%
4. Tinggi = Kerugian 10% - 20%
5. Sangat tinggi = Kerugian >20%

1. Faktor-faktor yang berpengaruh terhadap risiko keamanan aksesibilitas dan fleksibilitas pada Scaleout Creative Agency

No.	Jenis Risiko	Kode	Kejadian Risiko	Frekuensi Risiko yang terjadi					Pengaruh risiko terhadap sistem keamanan				
				1	2	3	4	5	1	2	3	4	5
1	Aplikasi	A1	Adobe Premiere Pro 2020			✓			✓				
		A2	Adobe After Effects 2020	✓					✓				
		A3	Adobe Photoshop 2022	✓					✓				
		A4	Adobe Illustrator 2020	✓					✓				
		A5	Adobe Lightroom Classic	✓					✓				
		A6	Adobe Audition 2020	✓					✓				
		A7	Canva online	✓							✓		
		A8	Capcut	✓						✓			
		A9	Microsoft Office 2019	✓							✓		
		A10	Google Chrome Browser		✓							✓	
		A11	Firefox Browser	✓								✓	
		A12	Telegram	✓								✓	
		A13	WhatsApp	✓								✓	
		A14	Media Player Classic	✓					✓				
		A15	Zoom	✓					✓	✓			
		A16	Corel Draw	✓					✓				
		A17	Internet Download Manager		✓							✓	
		A18	Format Factory	✓					✓				
		A19	Celtx Scriptwriter	✓					✓				
		A20	Meta Ads										
		A21	Facebook		✓								
		A22	Google drive										
		A23	Telegram										
		A24	WhatsApp										
		A25	Microsoft Office 2019										
		A26	Google Chrome Browser										
		A27	Firefox Browser										
		A28	Zoom										
		A29	Figma										
		A30	Google Ads										
		A31	Notes										
		A32	Tiktok										
		A33	Instagram										
		A34	Youtube										
		A35	M-Banking										
2	Data	B1	Data klien	✓						✓			
		B2	Data proyek			✓					✓		
		B3	Data kreatif			✓					✓		
		B4	Data keuangan		✓					✓	✓		
		B5	Data karyawan	✓							✓		
		B6	Data operasional		✓					✓	✓		
		B7	Data teknologi		✓	✓					✓		
3.	Infrastruktur	C1	Jaringan komputer			✓						✓	

		C2	Server	✓							✓	
		C3	Perangkat penyimpanan			✓					✓	
		C4	Perangkat keras			✓				✓		
		C5	Perangkat lunak		✓	●				✓		
		C6	Cloud computing	✓							✓	

A. Petunjuk Pengisian Kuesioner.

a. Jawaban merupakan persepsi Bapak/Ibu terhadap frekuensi yang terjadi, dan pengaruh risiko terhadap sistem keamanan

b. Pengisian kuesioner dilakukan dengan memberi tanda ☑ atau X pada kolom yang telah disediakan

B. Keterangan Penilaian

1. Sangat Jarang (SJ) = Jarang (hampir tidak mungkin) terjadi pada kondisi tertentu (dalam kurun 1 kali terjadi selama 2 tahun)
2. Jarang (J) = Kemungkinan kecil terjadi pada setiap kondisi (1x dalam 2 tahun)
3. Terkadang (T) = Mungkin terjadi pada kondisi tertentu (1-2 kali dalam 2 tahun)
4. Sering (S) = Kemungkinan besar terjadi pada setiap kondisi (2x dalam 2 tahun)
5. Sangat Sering (SS) = Hampir pasti terjadi pada setiap kondisi (lebih dari 3x dalam 2 tahun)

C. Keterangan untuk penilaian

Dampak kerugian meliputi Reputasi dan Finansial pada perusahaan.

1. Tidak ada pengaruh = Tidak ada kerugian
2. Rendah = Kerugian <5%
3. Sedang = Kerugian 5% - 10%
4. Tinggi = Kerugian 10% - 20%
5. Sangat tinggi = Kerugian >20%

2. Data Quesioner Keseluruhan

1. Apa Visi dan Misi Scaleout Creative Agency

   a. Visi: Menjadi top 5 agensi kreatif terbaik di Indonesia.

   b. Misi: Membantu 50 merek untuk menjadi market top pemimpin.

2. Apa strategi bisnis perusahaan?

Scaleout Creative Agency membangun personal branding (produk atau orang) yang kuat dengan menunjukkan karya-karya yang kreatif dan inovatif serta memberikan pengalaman terbaik bagi klien serta membangun hubungan jangka panjang dengan klien mereka dengan memberikan layanan berkualitas tinggi dan terus mengembangkan solusi kreatif yang sesuai dengan kebutuhan bisnis klien.

3. Apa saja kendala bisnis yang harus dipertimbangkan dalam mengembangkan solusi teknologi informasi?

   a. Anggaran

   b. Keterbatasan sumber daya

   c. Kompleksitas teknologi

d. Kesesuaian dengan kebutuhan bisnis

e. Kepatuhan peraturan dan keamanan

4. Apa arsitektur bisnis yang sedang digunakan oleh Scaleout Creative Agency?

Scaleout Creative Agency memadukan kedua model arsitektur bisnis, dengan menawarkan paket layanan jasa berlangganan yang mana klien membayar biaya berlangganan bulanan sesuai dengan paket yang ditawarkan di website dan proyek berbasis bisnis yang mana setiap proyeknya akan dihargai secara terpisah dan disesuaikan dengan kebutuhan klien. Model bisnis ini memungkinkan agensi kreatif untuk menghasilkan pendapatan yang stabil dan fleksibel dalam jangka pendek dan panjang.

5. Apa arsitektur teknologi informasi yang sedang digunakan oleh Scaleout Creative Agency

   a. Sistem manajemen konten (CMS) untuk mengelola dan mempublikasikan konten seperti gambar, video, dan teks.

   b. Sistem manajemen proyek untuk mengelola proyek dan kolaborasi dengan klien dan tim internal.

   c. Sistem manajemen sumber daya manusia (HR) untuk mengelola informasi karyawan dan administrasi kepegawaian.

   d. Sistem manajemen relasi pelanggan (CRM) untuk mengelola interaksi dan komunikasi dengan klien dan pelanggan.

6. Bagaimana infrastruktur teknologi informasi disusun dan dikelola dalam arsitektur teknologi informasi?

   a. Perencanaan: Perencanaan infrastruktur teknologi informasi yang dapat dilakukan adalah menyusun rencana strategis TI dan anggaran untuk implementasi infrastruktur TI.

   b. Desain: Desain infrastruktur teknologi informasi yang dapat dilakukan adalah memilih jenis server dan penyimpanan data yang cocok untuk kebutuhan bisnis.

   c. Implementasi: Implementasi infrastruktur teknologi informasi yang dapat dilakukan adalah memasang jaringan untuk memudahkan akses data dan berbagi sumber daya.

d. Operasi dan pemeliharaan: Operasi dan pemeliharaan infrastruktur teknologi informasi yang dapat dilakukan adalah melakukan backup data secara berkala untuk mencegah kehilangan data.

e. Replace: Infrastruktur teknologi informasi yang dapat dilakukan adalah mengganti server yang sudah usang dengan yang baru dan meninggalkan aplikasi yang tidak lagi digunakan.

7. Apa standar keamanan yang diterapkan dalam arsitektur bisnis dan teknologi informasi?

a. Enkripsi: Data sensitif dan informasi rahasia dienkripsi baik dalam penyimpanan maupun pengiriman data seperti yang Scaleout lakukan dengan penyimpanan clouds (google drive) dan komunikasi ter-enkripsi (WhatsApp dan Telegram).

b. Autentikasi: Sistem keamanan dalam pengaksesan data dan informasi memiliki mekanisme otentikasi untuk memastikan hanya pengguna yang memiliki hak akses yang benar yang dapat mengakses data.

c. Firewall: Sistem firewall melindungi jaringan pada perusahaan dari serangan jaringan dan perangkat lunak berbahaya yang sudah ada di sistem operasi.

d. Anti-malware dan Antivirus: Setiap perangkat dan sistem di Scaleout Creative Agency telah menggunakan anti-malware dan antivirus yang diperbarui secara berkala dari sistem operasi.

e. Backup dan pemulihan: Sistem backup dan pemulihan di Scaleout Creative Agency yaitu menduplikat data ke hard disk atau penyimpanan clouds untuk memastikan bahwa data dapat dipulihkan jika terjadi kehilangan data. Apabila projek sudah selesai kami akan menghapus data-data yang sudah tidak dibutuhkan.

8. Apa aset penting yang harus dilindungi dari ancaman keamanan?

a. Data Klien: Data klien seperti informasi pribadi, informasi keuangan, dan informasi bisnis harus

b. dilindungi dengan ketat karena kebocoran data dapat menyebabkan kerusakan reputasi dan potensi

c. tuntutan hukum.

d. Kekayaan Intelektual: Scaleout Creative Agency menghasilkan karya intelektual seperti video, audio,
e. desain, dan kampanye iklan. Aset ini harus dilindungi agar tidak dicuri atau disalahgunakan oleh pihak
f. lain.
g. Aset Digital: Scaleout Creative Agency mengelola sejumlah besar aset digital seperti file desain,
h. audiovisual, database klien, dan media sosial. Aset digital ini harus dilindungi dari serangan seperti
i. malware dan hacking.
j. Aplikasi: Scaleout Creative Agency menggunakan berbagai macam aplikasi seperti perangkat lunak
k. desain grafis, perangkat lunak manajemen proyek, dan perangkat lunak keuangan. Aplikasi ini harus
l. dilindungi dari serangan yang dapat menyebabkan kerusakan atau kehilangan data.
m. Infrastruktur IT: Agensi kreatif juga harus melindungi infrastruktur IT seperti jaringan, server, dan
n. sistem penyimpanan data dari ancaman keamanan. Infrastruktur IT yang rentan dapat menyebabkan
o. penurunan kinerja atau bahkan downtime yang dapat merugikan bisnis.

9. Apa risiko keamanan yang paling mungkin terjadi pada aset tersebut?
    a. Kehilangan data atau pencurian data
    b. Ancaman virus atau malware
    c. Serangan siber
    d. Kesalahan manusia
    e. Kebocoran data atau pelanggaran privasi
    f. Ketidakpatuhan terhadap regulasi dan peraturan

10. Apa tingkat keparahan risiko keamanan dan dampak potensialnya pada Scaleout Creative Agency?
    a. Kerugian Finansial
    b. Hilangnya reputasi
    c. Kerugian waktu dan produktivitas
    d. Sanksi hukum
11. Siapa yang bertanggung jawab untuk mengelola risiko keamanan pada aset tersebut?

Tim keamanan informasi, Manajer, Admin dan CEO.

12. Bagaimana risiko keamanan diidentifikasi, dievaluasi, dan dikelola dalam perusahaan?
    a. Identifikasi Risiko: Mengevaluasi risiko keamanan pada sistem, aplikasi, dan data yang ada di perusahaan.
    b. 2. Evaluasi Risiko: Mengevaluasi setiap risiko untuk menentukan tingkat keparahan dan dampak potensialnya pada aset penting.
    c. 3. Prioritasi Risiko: Risiko harus diprioritaskan berdasarkan tingkat keparahan dan dampaknya pada aset penting.
    d. 4. Mengelola Risiko: Langkah terakhir adalah mengelola risiko melalui pengembangan strategi mitigasi dan rencana tindakan untuk mengurangi atau menghilangkan risiko.
13. Apa langkah-langkah konkret yang diambil untuk mengurangi risiko keamanan pada aset tersebut?
    a. Kebijakan keamanan jarak jauh: Agensi kreatif harus memiliki kebijakan keamanan jarak jauh yang jelas dan diterapkan dengan ketat. Kebijakan ini harus mencakup masalah seperti password, enkripsi, dan penggunaan perangkat lunak keamanan. Semua karyawan yang bekerja dari jarak jauh harus diberikan pelatihan tentang kebijakan ini.
    b. Perangkat lunak keamanan: Agensi kreatif harus menginstal perangkat lunak keamanan di semua perangkat karyawan jarak jauh, seperti antivirus dan firewall.

Perangkat lunak ini harus diperbarui secara teratur untuk memastikan perlindungan terhadap ancaman keamanan terbaru.

c. Penggunaan jaringan VPN: Agensi kreatif harus memastikan bahwa karyawan yang bekerja dari jarak jauh menggunakan jaringan VPN yang aman saat mengakses data perusahaan. Ini akan memastikan bahwa data yang diakses oleh karyawan dienkripsi dan aman dari ancaman keamanan.

d. Enkripsi data: Agensi kreatif harus mengenkripsi semua data penting yang diakses oleh karyawan jarak jauh. Hal ini akan memastikan bahwa data tetap aman saat ditransmisikan melalui jaringan.

e. Membatasi akses: Agensi kreatif harus membatasi akses karyawan jarak jauh ke data yang mereka butuhkan untuk bekerja. Ini akan meminimalkan risiko akses yang tidak sah dan membantu melindungi data penting dari ancaman keamanan.

f. Pemantauan akses: Agensi kreatif harus memantau akses karyawan jarak jauh ke data perusahaan dan mengambil tindakan jika ada aktivitas yang mencurigakan.

g. Pembaruan perangkat: Agensi kreatif harus memastikan bahwa semua perangkat yang digunakan oleh karyawan jarak jauh diperbarui secara teratur. Ini akan memastikan bahwa perangkat tersebut dilindungi dari ancaman keamanan terbaru.

h. Pengujian keamanan: Agensi kreatif harus melakukan pengujian keamanan secara teratur untuk mengidentifikasi dan mengurangi risiko keamanan. Pengujian ini harus mencakup pengujian penetrasi dan audit keamanan.

i. Pelatihan karyawan: Agensi kreatif harus memberikan pelatihan keamanan yang cukup kepada karyawan jarak jauh. Hal ini akan membantu meningkatkan kesadaran keamanan dan membantu karyawan menghindari ancaman keamanan.

14. Apa kriteria penilaian risiko keamanan yang digunakan dalam Scaleout Creative Agency?

a. Nilai aset: Aset yang bernilai tinggi memiliki risiko keamanan yang lebih tinggi. Oleh karena itu, nilai aset harus dipertimbangkan saat menilai risiko keamanan.

b. Ancaman: Ancaman yang datang dari dalam atau luar organisasi harus dievaluasi dan dianalisis untuk menilai risiko keamanan.

c. Kerentanan: Kerentanan atau kelemahan dalam sistem atau infrastruktur dapat menyebabkan risiko keamanan yang signifikan. Kerentanan harus diidentifikasi dan diperbaiki.

d. Dampak: Dampak yang ditimbulkan akibat terjadinya risiko keamanan harus dinilai, baik dari segi keuangan maupun reputasi perusahaan.

e. Kemungkinan: Kemungkinan terjadinya risiko keamanan juga harus dinilai, dengan mempertimbangkan faktor seperti seberapa sering risiko dapat terjadi dan seberapa besar kemungkinan terjadinya.

f. Kepekaan: Beberapa aset atau informasi mungkin lebih sensitif daripada yang lain, sehingga perlu diberikan perhatian khusus dalam penilaian risiko keamanan.

g. Kepatuhan: Ada persyaratan dan regulasi tertentu yang harus dipatuhi oleh agensi kreatif, dan risiko keamanan harus dinilai dalam konteks kepatuhan terhadap regulasi tersebut.

15. Bagaimana risiko keamanan dapat diukur dan dipantau dalam jangka waktu tertentu?

Selama ini kami belum melakukan pengukuran dan memantau risiko keamanan, kami segera memperbaiki risiko keamanan dengan cara yang bisa dilakukan, seperti contoh pada tahun 2022, salah satu komputer terkena serangan Ransomware, maka kami segera menghubungi beberapa pelayanan terkait hal tersebut namun sangat disayangkan, hasilnya nihil, dan kami hanya bisa format data dan mengalami kerugian yang cukup signifikan.

16. Apa upaya yang dilakukan untuk meningkatkan kesadaran keamanan di seluruh Scaleout Creative Agency?

Beberapa upaya yang dapat dilakukan untuk meningkatkan kesadaran keamanan kepada semua unit di dalam sebuah perusahaan agensi kreatif antara lain:

a. Pelatihan Keamanan: Memberikan pelatihan keamanan kepada seluruh karyawan tentang praktik terbaik dalam menjaga keamanan dan privasi data, serta memberikan pemahaman tentang ancaman keamanan yang mungkin timbul dan bagaimana cara mengatasinya.
b. Kebijakan Keamanan: Memiliki kebijakan keamanan tertulis yang jelas dan mudah dipahami oleh seluruh karyawan. Kebijakan ini harus mencakup semua aspek keamanan, termasuk penggunaan perangkat mobile, kebijakan akses, dan password.
c. Komunikasi: Mengadakan rapat rutin dengan semua karyawan untuk membahas keamanan, termasuk menginformasikan mereka tentang ancaman keamanan terbaru dan cara menghindarinya.
d. Pengujian Keamanan: Melakukan pengujian keamanan secara teratur untuk menemukan celah keamanan di sistem dan aplikasi, dan memperbaikinya secepat mungkin.
e. Pemantauan Keamanan: Memantau aktivitas jaringan dan sistem untuk mendeteksi aktivitas mencurigakan dan tindakan yang tidak sah, sehingga dapat segera ditangani dan mencegah kerugian yang lebih besar.

Dengan melakukan upaya-upaya tersebut, diharapkan kesadaran keamanan dapat ditingkatkan dan risiko keamanan dapat ditekan seminimal mungkin.

17. Siapa pengguna utama sistem atau aplikasi yang akan diimplementasikan?

Semua karyawan baik di kantor atau kerja jarak jauh.

18. Apa kebutuhan pengguna untuk mengakses aplikasi atau sistem?
    a. Akses ke aplikasi bisnis
    b. Akses ke data dan informasi
    c. Koneksi internet
    d. Perangkat yang sesuai
    e. Hak akses yang sesuai
19. Apa jenis akses yang diperlukan oleh pengguna (seperti akses jarak jauh atau akses di dalam jaringan)?

Akses jarak jauh ke berbagai aplikasi dan sistem, termasuk aplikasi kreatif seperti Adobe Creative Suite, sistem manajemen konten, aplikasi kolaborasi seperti Microsoft Teams, dan layanan cloud seperti Dropbox atau Google Drive. Akses jarak jauh ini memungkinkan karyawan untuk bekerja dari mana saja dengan koneksi internet yang stabil. Namun, akses jarak jauh dapat meningkatkan risiko keamanan jika tidak diatur dengan baik, sehingga perlu diterapkan kebijakan keamanan yang tepat untuk meminimalkan risiko tersebut.

20. Bagaimana pengguna akan berinteraksi dengan aplikasi atau sistem?

Jaringan yang diperlukan oleh karyawan jarak jauh, yaitu jaringan pribadi virtual (VPN) untuk terhubung dengan jaringan internal agensi kreatif. Setelah terhubung ke jaringan, pengguna dapat berinteraksi dengan aplikasi atau sistem seperti layaknya bekerja dari kantor. Tapi, untuk saat ini karyawan jarak jauh terhubung dengan jaringan umum tanpa VPN, yang memungkinkan risiko tinggi dalam keamanan aset.

21. Apa batasan akses yang diperlukan oleh pengguna?

a. Batasan akses ke data sensitif
b. Batasan akses ke sistem informasi
c. Batasan akses jaringan
d. Batasan akses perangkat mobile
e. Batasan akses lokasi

22. Bagaimana penggunaan aplikasi atau sistem akan dipantau dan dilaporkan?

Pemantauan saat ini menggunakan aplikasi media sosial berupa Telegram dengan manual laporan progress dan update informasi.

23. Apa kebijakan keamanan yang harus dipatuhi oleh pengguna?

Kebijakan hak akses yang ketat untuk memastikan hanya orang yang berwenang yang dapat mengakses data dan sistem informasi penting sesuai dengan pekerjaan tiap departemen, untuk karyawan jarak jauh saat ini menggunakan intruksi manual seperti intruksi penghapusan aset bila sudah tidak diperlukan.

24. Bagaimana penggunaan aplikasi atau sistem diukur dan dinilai?

Sejauh ini kami mengukur dan menilai penggunaan aplikasi dari umpan balik karyawan jarak jauh secara berkala dan mengevaluasinya.

25. Bagaimana penggunaan aplikasi atau sistem dapat ditingkatkan dan disesuaikan dengan kebutuhan pengguna?

Dalam peningkatan dan penyesuaian sistem atau aplikasi, kami berfokus pada evaluasi, dukungan teknis dan pemantauan secara berkala terkait penyesuaian sistem atau aplikasi yang dibutuhkan pasar sesuai perkembangan zaman.

26. Apa sistem atau aplikasi yang akan/sedang diimplementasikan?

Sistem atau aplikasi yang akan/sedang diimplementasikan?

a. Perangkat Lunak (Produktivitas Konten)

No.	Nama Aplikasi
1.	Adobe Premiere Pro 2020
2.	Adobe After Effects 2020
3.	Adobe Photoshop 2022
4.	Adobe Illustrator 2020
5.	Adobe Lightroom Classic
6.	Adobe Audition 2020
7.	Canva online
8.	Capcut
9.	Microsoft Office 2019
10.	Google Chrome Browser
11.	Firefox Browser
12.	Telegram
13.	WhatsApp
14.	Media Player Classic
15.	Zoom
16.	Corel Draw
17.	Internet Download Manager
18.	Format Factory
19.	Celtx Scriptwriter

b. Aplikasi Bisnis

No.	Nama Aplikasi	No.	Nama Aplikasi
1.	Meta Ads	9.	Zoom
2.	Facebook	10.	Figma
3.	Google drive	11.	Google Ads
4.	Telegram	12.	Notes
5.	WhatsApp	13.	Tiktok
6.	Microsoft Office 2019	14.	Instagram
7.	Google Chrome Browser	15.	Youtube
8.	Firefox Browser	16.	M-Banking

c. Database

Scaleout Creative Agency memiliki 2 bentuk database untuk menyimpan data klien, karyawan, proyek, karyawan, dan aset kreatif, diantaranya;

1. Google drive sebagai penyimpanan data online
2. Hard disk memory sebagai penyimpanan data offline

27. Apa kebutuhan teknologi yang diperlukan untuk mendukung aplikasi atau sistem?

Sistem keamanan yang lebih aware tentang serangan DDoS atau malware, Aksesibilitas yang mudah dan aman melalui VPN.

28. Bagaimana aplikasi atau sistem akan diinstal dan dikonfigurasi?

Scaleout Creative Agency melakukan pemasangan perangkat produksi seperti pada umumnya (Adobe, Celtx, dsb), untuk aplikasi bisnis diperlukan pendaftaran akun seperti Google suites, Microsoft Office, dsb.

29. Apa jaringan dan infrastruktur teknologi yang diperlukan untuk mendukung aplikasi atau sistem?

Jaringan dan infrastruktur teknologi yang diperlukan untuk mendukung aplikasi atau sistem

a. Jaringan komunikasi : Dibutuhkan jaringan komunikasi yang aman dan dapat mendukung transfer data dalam jumlah besar dan tingkat kecepatan yang tinggi antara pengguna dan server.
b. Keamanan jaringan: Untuk melindungi jaringan dari ancaman keamanan, seperti serangan hacker atau malware. Beberapa tindakan yang selama ini dilakukan adalah penggunaan firewall, enkripsi data, dan tindakan pengelolaan hak akses.
c. Infrastruktur backup dan pemulihan: Diperlukan sistem backup dan pemulihan data dalam menanggapi situasi darurat untuk memastikan bahwa data tidak hilang atau rusak akibat kegagalan perangkat keras atau perangkat lunak.

30. Bagaimana aplikasi atau sistem akan dikelola dan dioperasikan?

Operasional aplikasi dan sistem yang berjalan di Scaleout yaitu pengelolaan infrastruktur jaringan, server, dan perangkat keras serta perangkat lunak lainnya termasuk pembaharuan pemeliharaan secara teratur untuk menjaga kinerja dan keamanannya.

31. Apa standar keamanan yang harus dipenuhi oleh teknologi yang digunakan?

Standar keamanan yang digunakan Scaleout selama ini yaitu melalui enkripsi data yang ada pada platform Google suites, Telegram, dan WhatsApp.

32. Bagaimana keamanan teknologi akan di pantau dan dievaluasi?

Scaleout Creative Agency selama ini hanya melakukan pembaruan sistem dan aplikasi secara teratur untuk memastikan bahwa kelemahan keamanan yang diketahui telah diperbaiki.

33. Apa jaringan dan infrastruktur teknologi yang diperlukan untuk mendukung aplikasi atau sistem?

Informasi tentang model bisnis agensi kreatif, termasuk tujuan dan sasaran bisnis, pelanggan, produk atau layanan yang ditawarkan, dan pasar yang dilayani.

a. Deskripsi bisnis

Scaleout Creative Agency adalah agensi kreatif dan rumah produksi yang berfokus dan berspesialisasi dalam komunikasi pemasaran dan branding seperti video dan desain. tidak hanya membuat video yang enak dipandang, tentunya juga tepat sasaran. Scaleout Creative Agency telah berdiri sejak tahun 2019 dan telah menghasilkan ribuan konten video pemasaran. Target pelanggan kami yaitu UMKM di seluruh Indonesia, yang membutuhkan video digital untuk pemasaran produknya, baik secara branding maupun konversi. Kedepannya Scaleout Creative Agency akan selalu mengikuti perkembangan zaman, seperti era digitalisasi yang sangat dibutuhkan pada zaman ini. Produk yang kami tawarkan juga akan selalu berinovasi dengan kebutuhan klien di masa mendatang.

b. Pelanggan

Scaleout Creative Agency bergerak sebagai agensi kreatif untuk memproduksi konten-konten di platform sosial media dengan target pelanggannya adalah UMKM, namun tak jarang juga mendapat klien dalam bentuk usaha mengenah keatas. Persona buyer Scaleout Creative Agency, sebagai berikut;

Persona Buyer		
No.	Jenis	Keterangan
1	Usia	24 – 45 Tahun
2	Pekerjaan	Business Owner
3	Domisili	Indonesia
4	Tempat tinggal	Kota
5	Medsos Buyer	Tiktok, Instagram, & Facebook
6	Berita/Informasi Favorit	Perkembangan bisnis
7	Hobi/Minat	Berdagang
8	Tujuan	Branding dan/atau konversi
9	Bahasa	Indonesia, Inggris
10	Penghasilan	Rp30.000.000 – Rp50.000.000

c. Meningkatkan Brand Awareness: Agensi kreatif dapat membantu klien untuk meningkatkan kesadaran merek mereka melalui strategi pemasaran yang efektif, kreatif dan terukur. Sasaran bisnis dalam hal ini adalah meningkatkan kesadaran merek dan citra positif di mata pelanggan dan konsumen.

d. Meningkatkan Penjualan: Agensi kreatif dapat membantu klien dalam mengembangkan strategi pemasaran dan kampanye promosi yang bertujuan meningkatkan penjualan dan profitabilitas bisnis. Sasaran bisnis dalam hal ini adalah meningkatkan omset dan keuntungan perusahaan klien.

e. Menjalin Hubungan Baik dengan Klien: Agensi kreatif harus memiliki hubungan kerja yang baik dengan klien untuk memastikan kepuasan pelanggan dan keberlanjutan bisnis jangka

panjang. Sasaran bisnis dalam hal ini adalah mempertahankan hubungan baik dengan klien dan meningkatkan loyalitas mereka terhadap agensi.

f. Memperluas Jangkauan Pasar: Agensi kreatif dapat membantu klien dalam memasuki pasar baru atau mengembangkan pasar yang sudah ada melalui kampanye pemasaran yang tepat sasaran. Sasaran bisnis dalam hal ini adalah memperluas jangkauan pasar dan mengembangkan basis pelanggan yang lebih luas.

g. Menjaga Reputasi Positif: Agensi kreatif harus menjaga reputasi positif mereka di mata klien dan konsumen untuk memastikan keberlanjutan bisnis jangka panjang. Sasaran bisnis dalam hal ini adalah menjaga dan meningkatkan reputasi agensi di mata klien, konsumen, dan industri.

34. Data tentang lingkungan bisnis, termasuk tren industri, persaingan, dan faktor eksternal lain yang dapat mempengaruhi strategi bisnis.

    a. Tren Industri:

        i. Digitalisasi: Semakin banyak agensi kreatif yang beralih ke platform digital dan solusi teknologi informasi untuk meningkatkan efisiensi dan memperluas jangkauan pasar mereka.

        ii. Perkembangan teknologi: Teknologi terus berkembang dan semakin banyak inovasi yang muncul di industri ini, seperti teknologi virtual dan augmented reality yang dapat digunakan untuk membuat pengalaman kreatif yang lebih menarik dan interaktif.

        iii. Fokus pada data dan analitik: Semakin banyak agensi kreatif yang mengambil pendekatan berbasis data untuk kreativitas dan desain, menggunakan data untuk memahami pelanggan mereka dan memperoleh wawasan berharga tentang perilaku konsumen.

        iv. Penggunaan media sosial: Media sosial terus menjadi platform yang sangat penting bagi agensi kreatif untuk mempromosikan merek dan mengembangkan kreativitas yang lebih menarik.

v. Kepedulian terhadap keberlanjutan: Banyak agensi kreatif yang semakin memperhatikan dampak lingkungan dan sosial dari praktik bisnis mereka, dengan mengambil tindakan untuk mengurangi limbah dan emisi karbon mereka, dan menggunakan bahan-bahan yang lebih ramah lingkungan.

vi. Inklusivitas dan keberagaman: Semakin banyak agensi kreatif yang menempatkan inklusivitas dan keberagaman sebagai prioritas utama dalam desain dan pemasaran mereka, menciptakan kampanye yang merangkul berbagai latar belakang dan perspektif.

b. Persaingan:

i. Agensi kreatif besar seperti WPP, Omnicom, Publicis Groupe, dan Interpublic Group (IPG) yang memiliki cabang di seluruh dunia dan menawarkan berbagai layanan kreatif, seperti periklanan, branding, digital marketing, dan lain-lain.

ii. Perusahaan teknologi seperti Google, Facebook, dan Amazon yang memiliki layanan pemasaran digital dan menyediakan platform untuk menjangkau audiens secara online.

iii. Agensi kreatif kecil yang fokus pada layanan kreatif tertentu, seperti desain grafis, fotografi, atau video produksi.

iv. Persaingan lokal yang melibatkan agensi kreatif yang lebih kecil dan lebih spesifik dalam pelayanan lokal.

Persaingan yang semakin ketat ini dapat mempengaruhi strategi bisnis agensi kreatif dalam mempertahankan klien yang sudah ada dan menarik klien baru. Oleh karena itu, agensi kreatif perlu berinovasi dalam menciptakan nilai tambah bagi klien dan mempertahankan kualitas layanan mereka.

c. Faktor Ekonomi:

i. Kondisi perekonomian makro: Kondisi perekonomian makro seperti pertumbuhan ekonomi, inflasi, suku bunga, dan nilai tukar dapat

mempengaruhi daya beli konsumen dan ketersediaan dana untuk investasi dalam industri kreatif.

ii. Perubahan pasar: Perubahan dalam perilaku konsumen, preferensi dan tren pasar dapat mempengaruhi permintaan produk atau layanan yang ditawarkan oleh agensi kreatif. Jika agensi kreatif tidak dapat mengantisipasi perubahan ini dengan cepat, mereka mungkin kehilangan pangsa pasar.

iii. Persaingan: Persaingan yang ketat dalam industri kreatif dapat mempengaruhi harga produk atau layanan, serta mempengaruhi keuntungan dan pangsa pasar. Agensi kreatif harus mampu bersaing secara efektif dalam pasar yang kompetitif ini.

iv. Perubahan teknologi: Perubahan teknologi dapat mempengaruhi cara agensi kreatif menghasilkan dan menyebarkan produk atau layanan. Agensi kreatif harus mampu menyesuaikan dengan cepat untuk tetap relevan dan bersaing di pasar yang semakin berkembang ini.

v. Ketersediaan sumber daya: Ketersediaan sumber daya seperti tenaga kerja terampil dan peralatan teknologi juga dapat mempengaruhi kemampuan agensi kreatif untuk memproduksi produk atau layanan berkualitas tinggi dan menghadapi persaingan.

d. Perubahan Teknologi:

i. Perkembangan Teknologi Cloud Computing: Cloud computing memungkinkan agensi kreatif untuk mengakses sumber daya teknologi secara fleksibel dan hemat biaya, tanpa perlu melakukan investasi besar dalam infrastruktur TI.

ii. Perkembangan Teknologi Mobile: Penggunaan smartphone dan tablet semakin berkembang dan memberikan kemudahan akses untuk konsumen ke produk dan layanan agensi kreatif.

iii. Perkembangan Teknologi Virtual dan Augmented Reality: Teknologi ini dapat digunakan oleh agensi kreatif untuk meningkatkan pengalaman pengguna dengan produk dan layanan yang ditawarkan.

iv. Perkembangan Teknologi Artificial Intelligence (AI) dan Machine Learning: AI dan Machine Learning dapat digunakan oleh agensi kreatif untuk mempercepat dan memperbaiki proses produksi serta meningkatkan efisiensi dan efektivitas bisnis.

v. Perkembangan Teknologi Blockchain: Teknologi ini dapat digunakan oleh agensi kreatif untuk mengamankan transaksi keuangan dan transparansi dalam pembayaran royalti kepada kreator.

vi. Perkembangan Teknologi Big Data dan Analitik: Teknologi ini dapat digunakan oleh agensi kreatif untuk menganalisis data pelanggan dan memahami preferensi mereka sehingga dapat menawarkan produk dan layanan yang lebih tepat sasaran.

c. Regulasi Pemerintah:

i. Hak Cipta dan Kekayaan Intelektual: Regulasi hak cipta dan kekayaan intelektual dapat mempengaruhi strategi bisnis di agensi kreatif karena bisnis ini sangat bergantung pada hak kekayaan intelektual yang dimiliki oleh perusahaan. Perusahaan harus memastikan bahwa karyawannya memahami hak cipta dan kekayaan intelektual dan mematuhi semua aturan terkait dalam pembuatan karya.

ii. Regulasi Pajak: Pajak adalah faktor penting dalam strategi bisnis di agensi kreatif. Perusahaan harus memperhatikan regulasi pajak yang berlaku di negara atau wilayah tempat mereka beroperasi dan memastikan kepatuhan terhadap aturan tersebut.

iii. Regulasi Industri: Regulasi industri seperti aturan tentang periklanan dan promosi, serta standar kualitas produk, dapat mempengaruhi strategi bisnis

di agensi kreatif. Perusahaan harus memahami semua aturan dan regulasi terkait dan memastikan kepatuhan terhadap mereka dalam bisnis mereka.

iv. Regulasi Privasi Data: Regulasi privasi data seperti GDPR (General Data Protection Regulation) dapat mempengaruhi strategi bisnis di agensi kreatif yang mengumpulkan, menyimpan, atau memproses data pribadi. Perusahaan harus memastikan bahwa mereka mematuhi semua regulasi privasi data yang berlaku dan melindungi data pribadi pelanggan mereka.

v. Regulasi Perlindungan Konsumen: Regulasi perlindungan konsumen dapat mempengaruhi strategi bisnis di agensi kreatif karena perusahaan harus memastikan bahwa produk atau layanan yang mereka tawarkan sesuai dengan standar yang ditetapkan dan tidak mengecewakan pelanggan. Perusahaan harus memahami regulasi perlindungan konsumen yang berlaku dan memastikan kepatuhan terhadap aturan tersebut.

35. Informasi tentang teknologi yang digunakan oleh agensi kreatif, termasuk infrastruktur TI, aplikasi, sistem manajemen konten, dan alat kolaborasi.

a. Infrastruktur TI

i. Jaringan: Biznet

ii. Server: FTP Server

iii. Sistem penyimpanan:

b. Offline: Hard disk internal/eksternal

c. Online: Google Drive, penyimpanan cloud medsos (Telegram, WhatsApp)

d. Perangkat keras jaringan: Huawei EG8145V5 dan TP-Link Wireless USB Adapter

e. Perangkat lunak pengelolaan jaringan: TP-LINK

f. Aplikasi produktivitas

No.	Nama Aplikasi
1.	Adobe Premiere Pro 2020
2.	Adobe After Effects 2020
3.	Adobe Photoshop 2022
4.	Adobe Illustrator 2020
5.	Adobe Lightroom Classic
6.	Adobe Audition 2020
7.	Canva online
8.	Capcut
9.	Microsoft Office 2019
10.	Google Chrome Browser
11.	Firefox Browser
12.	Telegram
13.	WhatsApp
14.	Media Player Classic
15.	Zoom
16.	Corel Draw
17.	Internet Download Manager
18.	Format Factory
19.	Celtx Scriptwriter

g. Sistem manajemen konten: WordPress, Instagram, Tiktok, Youtube, Facebook.

h. Alat kolaborasi: Zoom, Telegram, Google Meet.

36. Informasi tentang peraturan dan persyaratan hukum yang berlaku untuk agensi kreatif dan industri kreatif secara umum, termasuk undang-undang tentang privasi data, keamanan informasi, dan hak cipta.

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik di Indonesia

37. Data tentang staf dan struktur organisasi agensi kreatif, termasuk jumlah karyawan, peran dan tanggung jawab, dan keahlian teknis.

a. Jumlah karyawan internal : 8 Orang

b. CEO/Founder: Pemilik atau manajemen agensi kreatif memiliki peran penting dalam memastikan bahwa keterlibatan stakeholder terkait dengan keamanan informasi dan privasi data karyawan jarak jauh dikelola dengan baik.

c. Tim Pemasaran: Bertanggung jawab atas analisis pasar, riset klien, dan pengembangan strategi untuk kampanye pemasaran dan promosi.

d. Manajemen Proyek: Bertanggung jawab atas hubungan dengan klien dan memastikan bahwa proyek-proyek dipenuhi dengan baik dan tepat waktu.

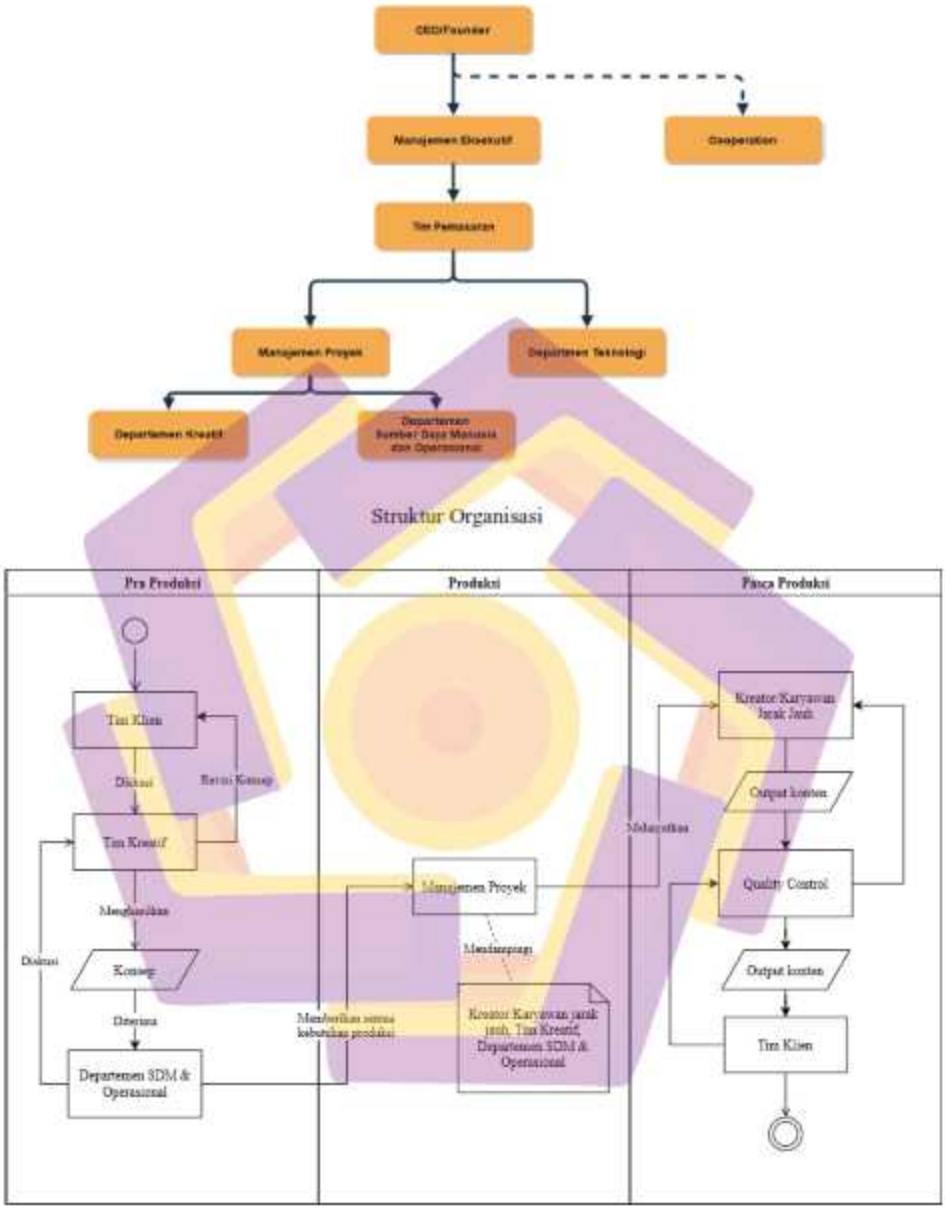
e. Manajemen Eksekutif: Terdiri dari eksekutif senior seperti Presiden, CFO, dan CMO, yang bertanggung jawab atas operasi dan keuangan perusahaan termasuk akuntansi, penggajian, dan pengelolaan kas.

f. Departemen Kreatif: Terdiri dari tim desain grafis, tim kreatif, tim penulis konten, dan lain-lain, yang bertanggung jawab atas pembuatan konten termasuk materi konten.

g. Departemen Teknologi: Bertanggung jawab atas pengembangan dan pemeliharaan situs web, aplikasi, dan sistem informasi lainnya yang diperlukan untuk kampanye pemasaran dan promosi.

h. Departemen Sumber Daya Manusia dan Operasional: Bertanggung jawab atas perekrutan, pelatihan, dan pengembangan karyawan, serta manajemen kinerja dan kebijakan karyawan serta bertanggung jawab atas manajemen fasilitas dan sumber daya yang diperlukan untuk menjalankan operasi sehari-hari agensi kreatif.

i. Quality Control: Bertanggung jawab memeriksa hasil pekerjaan dari kreator/karyawan jarak jauh sebelum diberikan ke klien, sekaligus menjembatani komunikasi antara klien dengan kreator/karyawan jarak jauh.



Alur Produksi

38. Informasi tentang tujuan dan sasaran organisasi, termasuk strategi bisnis jangka panjang dan pendek, dan tantangan atau peluang yang dihadapi organisasi.

39. Informasi tentang tujuan dan sasaran, termasuk strategi bisnis jangka panjang dan pendek, dan tantangan atau peluang yang dihadapi Scaleout Creative Agency, diantaranya;

a. Tujuan

Memperoleh keuntungan, meningkatkan pangsa pasar, dan mempertahankan keunggulan kompetitif. Sasaran yang terkait dengan tujuan ini dapat mencakup pertumbuhan pendapatan, ekspansi ke pasar baru, dan pengembangan keterampilan dan keahlian dalam tim.

b. Strategi bisnis

Strategi bisnis jangka panjang dan pendek Scaleout Creative Agency berkaitan dengan mengidentifikasi kebutuhan klien dan menciptakan solusi kreatif yang inovatif untuk memenuhi kebutuhan tersebut. Scaleout Creative Agency juga memilih untuk fokus pada pengembangan merek atau kampanye pemasaran untuk klien mereka. Dalam hal ini, strategi bisnis Scaleout Creative Agency dapat terdiri dari peningkatan pelayanan kreatif, peningkatan efisiensi operasional, atau pengembangan keterampilan dan keahlian karyawan.

c. Tantangan dan peluang

Tantangan dan peluang yang dihadapi Scaleout Creative Agency tergantung pada situasi industri yang berkembang. Beberapa tantangan dapat meliputi perubahan tren atau permintaan pasar, perubahan dalam regulasi atau kebijakan industri, dan persaingan dengan Scaleout Creative Agency lainnya. Sementara itu, peluang dapat terdiri dari pertumbuhan pasar yang meningkat atau permintaan yang berkembang untuk layanan kreatif yang baru dan inovatif.

40. Kebijakan keamanan perusahaan terkait dengan penggunaan perangkat dan akses jaringan dari jarak jauh.

Kebijakan hak akses yang ketat untuk memastikan hanya orang yang berwenang yang dapat mengakses data dan sistem informasi penting sesuai dengan pekerjaan tiap departemen, untuk karyawan jarak jauh saat ini menggunakan intruksi manual seperti intruksi penghapusan aset bila sudah tidak diperlukan.

41. Jenis data sensitif atau kritis yang diakses oleh karyawan jarak jauh dan cara mengelola dan membatasi akses ke data tersebut.

Jenis data sensitif atau kritis yang diakses oleh karyawan jarak jauh dan cara mengelola dan membatasi akses ke data tersebut. Scaleout Creative Agency memiliki beberapa jenis data sensitif atau kritis yang diakses oleh karyawan jarak jauh, termasuk:

a. Informasi pribadi pelanggan
b. Data klien dan proyek
c. Karya seni asli dan kreatif

Selama ini untuk mengelola dan membatasi akses ke data sensitif atau kritis ini, Scaleout Creative Agency memberlakukan instruksi untuk menghapus data sensitif atau kritis dari perangkat mereka secara

aman saat data tersebut tidak lagi diperlukan dan pelatihan karyawan untuk memastikan bahwa mereka memahami pentingnya menjaga kerahasiaan data sensitif atau kritis dan bagaimana melindunginya dari ancaman keamanan.

42. Proses identifikasi dan autentikasi yang digunakan untuk mengakses sistem dan aplikasi dari jarak jauh, termasuk penggunaan multi-factor authentication (MFA).

Scaleout Creative Agency menggunakan sistem autentikasi dari sistem keamanan yang disediakan oleh platform yang digunakan, seperti otentikasi data dari google drive, autentikasi platform media sosial yang digunakan seperti gmail, telegram dan WhatsApp.

43. Pemantauan dan audit aktivitas penggunaan sistem dan akses jarak jauh untuk mendeteksi potensi ancaman dan pelanggaran keamanan.

Scaleout Creative Agency menggunakan sistem pemantauan secara otomatis dari notifikasi yang muncul ketika ada aktivitas login atau izin akses data dari google drive.

44. Penggunaan teknologi enkripsi untuk melindungi data saat transit dan saat disimpan di perangkat karyawan jarak jauh.

Scaleout belum memberlakukan teknologi enkripsi pada data yang dibagikan ke karyawan jarak jauh, terkecuali enkripsi data yang sudah tersedia dari platform komunikasi.

45. Rencana keamanan darurat dan pemulihan bisnis dalam skenario keamanan jarak jauh yang mengancam operasi perusahaan.

Rencana keamanan darurat dan pemulihan bisnis dalam skenario keamanan jarak jauh yang mengancam operasi perusahaan.

a. Identifikasi ancaman keamanan yang mungkin terjadi, seperti serangan siber, kebocoran data, atau kehilangan peralatan.
b. Penilaian risiko dan dampak potensial dari setiap ancaman keamanan yang teridentifikasi.
c. Penetapan prioritas keamanan untuk data dan sistem informasi yang sensitif atau penting, serta penerapan kebijakan dan prosedur untuk membatasi akses ke data tersebut.
d. Pengembangan strategi pemulihan bisnis yang mencakup pemulihan data dan sistem, serta prosedur untuk mengembalikan operasi normal setelah bencana keamanan terjadi.
e. Pelatihan karyawan dan staf tentang prosedur keamanan dan rencana darurat.
f. Uji coba dan evaluasi rencana darurat secara berkala untuk memastikan efektivitasnya dan melakukan perubahan jika diperlukan.
g. Pemantauan dan penilaian risiko keamanan secara terus-menerus untuk mengidentifikasi ancaman baru atau perubahan dalam lingkungan keamanan.

46. Informasi mengenai jenis pekerjaan yang dilakukan oleh karyawan jarak jauh, termasuk aktivitas dan lingkungan kerja yang mungkin berbeda dengan karyawan yang bekerja di kantor.

Beberapa karyawan yang bekerja secara remote dan/atau freelance yang bekerja dengan Scaleout merupakan seorang videografer, editor video, konseptor, pengisi suara, yang memiliki pengalaman atau aktivitas yang kurang lebih sama dengan yang bekerja di kantor.

47. Data mengenai jenis data dan informasi yang diakses oleh karyawan jarak jauh serta cara mereka mengakses data tersebut.

a. Konsep konten (dalam bentuk dokumen)

b. Data klien (Berupa brief produk)

c. Aset digital (Berupa footages, grafis, audio dan aset lainnya) Cara karyawan jarak jauh mengakses data ini biasanya melalui koneksi internet dengan akses berbasis cloud (Google Drive), namun tidak jarang juga dengan cara offline (Hard Disk).

48. Informasi mengenai teknologi yang digunakan oleh karyawan jarak jauh, termasuk jenis perangkat keras dan lunak, serta cara mereka terhubung ke jaringan perusahaan.

Selama ini karyawan jarak jauh bekerja menggunakan laptop atau komputer pada umumnya, dengan cara terhubung ke Scaleout Creative Agency melalui aplikasi Telegram, WhatsApp atau akses data via Google Drive.

49. Data mengenai kebijakan dan prosedur keamanan perusahaan yang telah diimplementasikan dan diikuti oleh karyawan jarak jauh.

Data mengenai kebijakan dan prosedur keamanan perusahaan yang telah diimplementasikan dan diikuti oleh karyawan jarak jauh. Scaleout Creative Agency selama ini bekerja dengan karyawan jarak jauh dengan komunikasi yang terenkripsi di Platform Telegeram dan WhatsApp dan sharing data dengan sistem keamanan di Google Drive, namun masih sering menggunakan offline sharing (Hard Disk), maka prosedur keamanan yang diimplementasikan, diantaranya;

a. Prosedur pemantauan akses jarak jauh : Secara komunikasi manual di platform media social

b. Kebijakan keamanan perangkat lunak : Ada kalanya kami mengingatkan kepada Karyawan untuk selalu melakukan pembaruan perangkat, terutama untuk sistem keamanannya.

c. Kebijakan privasi dan pengamanan data : Mengontrol data yang sensitif dengan cara meminta kepada karyawan jarak jauh untuk menghapus data tersebut.

d. Prosedur pelaporan insiden keamanan : Insiden yang terjadi akan dianalisa dan didiskusikan untuk dicarikan solusinya.

50. Informasi tentang regulasi dan persyaratan hukum yang berlaku terkait keamanan data dan privasi karyawan jarak jauh.
    a. Undang-Undang Nomor 19 Tahun 2016 tentang Informasi dan Transaksi Elektronik, yang mengatur tentang perlindungan informasi dan data yang ditransmisikan melalui jaringan elektronik.
    b. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang mengatur tentang tata cara penyimpanan, pengolahan, dan pengamanan data elektronik.
    c. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Standar Keamanan Sistem Informasi, yang mengatur tentang persyaratan keamanan informasi dan sistem informasi.
    d. General Data Protection Regulation (GDPR) yang berlaku di Uni Eropa, yang memberikan perlindungan data dan privasi bagi warga negara Uni Eropa, termasuk dalam konteks pekerjaan jarak jauh.
    e. Undang-Undang Nomor 13 Tahun 2003 tentang Ketenagakerjaan, yang mengatur tentang hak-hak dan perlindungan karyawan, termasuk hak atas privasi dan keamanan dalam konteks pekerjaan jarak jauh.
    f. Peraturan perusahaan atau kebijakan internal yang menetapkan persyaratan keamanan dan privasi data karyawan, serta prosedur pengelolaan dan perlindungan aset perusahaan, termasuk untuk karyawan jarak jauh.
51. Data tentang insiden keamanan yang pernah terjadi pada perusahaan, khususnya yang berkaitan dengan karyawan jarak jauh, sehingga dapat digunakan sebagai acuan untuk memperbaiki kebijakan dan prosedur keamanan yang ada.
    a. Februari-Mei 2022, terjadi kesalahan sumber daya manusia yaitu penyimpanan offline pada hard disk internal ter-format, dan dibawa ke pihak ketiga bagian restorasi, namun data tidak selamat seutuhnya. (Kejadian tidak terdokumentasi)
    b. Ransonware

Mei 2022, Salah satu komputer terkena malware berupa ransomware yang langsung menginfeksi semua data di komputer tersebut. Kami langsung mencari teknisi yang bisa menangani hal tersebut, namun sayangnya jenis ransomware yang menginfeksi merupakan versi terbaru dan belum bisa menyelamatkan data-data di penyimpanan komputer, alhasil kami lakukan format pada penyimpanan.

52. Bagaimana keterlibatan stakeholder Scalcout Creative Agency dan pemangku kepentingan lainnya dikelola?

    a. CEO/Founder: Pemilik atau manajemen agensi kreatif memiliki peran penting dalam memastikan bahwa keterlibatan stakeholder terkait dengan keamanan informasi dan privasi data karyawan jarak jauh dikelola dengan baik.

    b. Tim Pemasaran: Bertanggung jawab atas analisis pasar, riset klien, dan pengembangan strategi untuk kampanye pemasaran dan promosi.

    c. Manajemen Proyek: Bertanggung jawab atas hubungan dengan klien dan memastikan bahwa proyek-proyek dipenuhi dengan baik dan tepat waktu.

    d. Manajemen Eksekutif: Terdiri dari eksekutif senior seperti Presiden, CFO, dan CMO, yang bertanggung jawab atas operasi dan keuangan perusahaan termasuk akuntansi, penggajian, dan pengelolaan kas.

    e. Departemen Kreatif: Terdiri dari tim desain grafis, tim kreatif, tim penulis konten, dan lain-lain, yang bertanggung jawab atas pembuatan konten termasuk materi konten.

    f. Departemen Teknologi: Bertanggung jawab atas pengembangan dan pemeliharaan situs web, aplikasi, dan sistem informasi lainnya yang diperlukan untuk kampanye pemasaran dan promosi.

g. Departemen Sumber Daya Manusia dan Operasional: Bertanggung jawab atas perekrutan, pelatihan, dan pengembangan karyawan, serta manajemen kinerja dan kebijakan karyawan serta bertanggung jawab atas manajemen fasilitas dan sumber daya yang diperlukan untuk menjalankan operasi sehari-hari agensi kreatif.

h. Quality Control: Bertanggung jawab memeriksa hasil pekerjaan dari kreator/karyawan jarak jauh sebelum diberikan ke klien, sekaligus menjembatani komunikasi antara klien dengan kreator/karyawan jarak jauh.

53. Daftar aplikasi dan sistem yang digunakan oleh karyawan jarak jauh, beserta tingkat sensitivitas data yang diakses dan perlindungan yang dibutuhkan.

No.	Jenis Aplikasi	Tingkat Sensitivitas
1.	Google Drive	70%
2.	Telegram & WhatsApp	85%
3.	Adobe Suites	50%
4.	Capcut	25%

54. Informasi mengenai infrastruktur teknologi yang digunakan untuk mendukung karyawan jarak jauh, seperti server, jaringan, dan perangkat lunak yang digunakan untuk memantau keamanan.

Scaleout Creative Agency tidak menggunakan infrastruktur apapun untuk memantau keamanan karyawan jarak jauh.

55. Informasi mengenai kebijakan keamanan yang ada dan tingkat kepatuhan karyawan jarak jauh terhadap kebijakan tersebut.

a. Kebijakan Akses: Scaleout Creative Agency memiliki kebijakan yang membatasi akses karyawan jarak jauh hanya pada aplikasi dan data yang diperlukan untuk pekerjaan mereka. Setiap permintaan akses tambahan harus melalui proses otorisasi yang ketat. Data menunjukkan bahwa 95% permintaan akses tambahan disetujui setelah melalui proses otorisasi yang benar.

b. Kebijakan Perangkat Keras: Scaleout Creative Agency memberikan fasilitas berupa perangkat keras yang hanya bisa digunakan di area kantor sedangkan untuk karyawan jarak jauh menggunakan perangkat keras sendiri. Data menunjukkan bahwa 70% karyawan jarak jauh menggunakan perangkat keras sendiri.

56. Identitas stakeholders keamanan

Tidak ada stakeholders keamanan di Scaleout Creative Agency.

57. Kebutuhan keamanan

a. Keamanan Sistem: Agensi kreatif perlu memastikan bahwa sistem teknologi mereka aman dari ancaman siber seperti virus, malware, serangan phishing, dan hacking.
b. Keamanan Data: Perusahaan dapat mengadopsi kebijakan keamanan data dan mengenkripsi data sensitif untuk melindunginya dari ancaman siber.
c. Keamanan Akses: Perlu memiliki kebijakan akses yang ketat dan mengelola identitas dan akses pengguna dengan hati-hati.
d. Kebijakan Password yang Kuat: Perusahaan dapat mengadopsi kebijakan password yang kuat dan memperkuat penggunaannya melalui pelatihan dan kesadaran karyawan.
e. Pengawasan Aktivitas Pengguna: Perusahaan dapat menggunakan solusi pemantauan aktivitas pengguna dan alat pemantauan keamanan lainnya untuk memantau aktivitas pengguna.
f. Penyimpanan Data Cadangan: Perusahaan perlu menggunakan solusi penyimpanan cadangan dan pemulihan bencana untuk memastikan bahwa data mereka selalu tersedia dan aman.

58. Kebijakan keamanan

Belum, masih perlunya peninjauan dan revisi terkait hal tersebut.

59. Ketergantungan stakeholder

a. Karyawan: Scaleout Creative Agency bergantung pada karyawan untuk menghasilkan karya kreatif dan memberikan layanan kepada klien. Karyawan juga bertanggung jawab untuk menjaga keamanan informasi dan aset perusahaan.

b. Klien: Scaleout Creative Agency sangat bergantung pada klien untuk mendapatkan proyek dan pendapatan. Klien juga dapat memberikan akses ke informasi rahasia dan rincian proyek yang perlu dilindungi.

c. Vendor: Scaleout Creative Agency juga bergantung pada vendor untuk menyediakan layanan teknologi, perangkat keras, perangkat lunak, dan infrastruktur yang mendukung operasi bisnis.

d. Mitra: Scaleout Creative Agency dapat memiliki mitra yang membantu memasarkan dan mendistribusikan produk atau layanan. Ketergantungan pada mitra dapat meningkatkan risiko keamanan jika akses diberikan ke data sensitif.

60. Rencana manajemen keamanan

Belum, masih perlunya peninjauan dan revisi terkait hal tersebut.

61. Data mengenai jenis pekerjaan yang dilakukan oleh karyawan jarak jauh

a. Freelance Editor

b. Konseptor

62. Data mengenai teknologi dan infrastruktur yang digunakan oleh karyawan jarak jauh

a. Komputer dan Laptop Jaringan Handphone berbasis android dan iPhone

b. Data mengenai kebijakan dan prosedur yang telah ditetapkan oleh perusahaan terkait karyawan jarak jauh

63. Data mengenai kebijakan dan prosedur yang telah ditetapkan oleh perusahaan terkait karyawan jarak jauh.

a. Kebijakan keamanan informasi: Belum ada

b. Kebijakan privasi data: Data karyawan yang bekerja jarak jauh sudah terkumpul dalam database gmail

c. Perangkat lunak keamanan: dalam hal keamanan, perangkat lunak selalu melakukan update

d. Komunikasi: Komunikasi yang dilakukan hanya dengan aplikasi Telegram yang ter-enkripsi.

e. Penjadwalan dan pemantauan: hal ini dilakukan dengan laporan progress di tiap harinya via aplikasi Telegram dan google drive

f. Pelatihan: Pelatihan mengenai kebijakan dan prosedur hanya sebatas teknikal pra-produksi hingga pasca produksi

g. Pengaturan kantor di rumah: Scaleout Creative Agency memberikan fasilitas seperti google drive, zoom meeting, baik untuk komunikasi dan produksi.

64. Data mengenai tingkat keamanan teknologi yang diterapkan pada sistem yang digunakan karyawan jarak jauh

a. Sistem otentikasi multi-faktor: Google account menggunakan kode otentikasi yang dikirimkan melalui smartphone admin.

b. Enkripsi data: Transfer data menggunakan aplikasi Google Drive, Telegram, WhatsApp yang terenkripsi.

c. Anti virus dan anti malware: Menggunakan sistem keamanan dari sistem operasi tiap komputer (Windows 10).

65. Data mengenai tingkat kesiapan karyawan dalam menghadapi risiko keamanan saat bekerja jarak jauh

Tidak ada

66. Data mengenai histori dan trend terkait risiko keamanan pada karyawan jarak jauh pada periode sebelumnya.

Tidak ada

67. Data mengenai jenis aset yang dimiliki oleh agensi kreatif, termasuk aset digital dan non-digital.

a. Inventarisasi aset digital:

i. Domain website : www.scaleout.id

ii. Akun media sosial

1. https://web.facebook.com/scaleout.id

2. https://www.instagram.com/scaleout.id/

3. https://www.youtube.com/channel/UCaQ3bBqIn0S5hCU0Mk6yXlw

iii. Konten website (artikel, foto, video, dll.)

Semua konten ada di akun media sosial.

iv. Desain grafis (logo, brosur, kartu nama, dll.)

v. Perangkat lunak

No.	Nama Aplikasi
1.	Adobe Premiere Pro 2020
2.	Adobe After Effects 2020
3.	Adobe Photoshop 2022
4.	Adobe Illustrator 2020
5.	Adobe Lightroom Classic
6.	Adobe Audition 2020
7.	Canva online
8.	Capcut
9.	Microsoft Office 2019
10.	Google Chrome Browser
11.	Firefox Browser
12.	Telegram
13.	WhatsApp
14.	Media Player Classic
15.	Zoom
16.	Corel Draw
17.	Internet Download Manager
18.	Format Factory
19.	Celtx Scriptwriter

vi. Aplikasi bisnis

No.	Nama Aplikasi
1.	Meta Ads
2.	Facebook
3.	Google drive
4.	Telegram
5.	WhatsApp
6.	Microsoft Office 2019
7.	Google Chrome Browser
8.	Firefox Browser
9.	Zoom
10.	Figma
11.	Google Ads
13.	Tiktok
14.	Instagram
15.	Youtube
16.	M-Banking

b. Inventaris Non-Digital

No.	Model	Spesifikasi
1.	Komputer 1 (Internal)	Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz 2.90 GHz RAM : 16,0 GB Intel® UHD Graphics 630 Monitor LED MSI
2.	Komputer 2 (Internal)	Intel(R) Core(TM) i7-4970 CPU @ 3.60GHz(CPUs), ~3.6 GHz RAM : 8,0 GB NVIDIA GeForce GT 730 Monitor LED MSI
3.	Komputer 3 (Karyawan Jarak Jauh)	Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz 2.19 GHz RAM 16,0 GB Monitor LED Asus
4.	Printer	Brother DCP-T420W
5.	Hard disk Eksternal (3)	WD Blue (1 TB) Seagate Barracuda (1 TB) (2)
6.	Router (3)	TP-Link Wireless USB Adapter

68. Data mengenai nilai aset dan potensi dampak kerugian jika aset tersebut terancam atau terjadi kebocoran data.

- Nilai aset: Pengelolaan proyek bernilai mulai dari 4.750 jt – 10 jt. Basis data pelanggan dengan 1000 data pelanggan.
- Potensi dampak kerugian:
    - Kebocoran data pada aset digital dan non-digital pengelolaan proyek dapat menyebabkan hilangnya informasi penting dan kerugian finansial hingga Rp 7 sampai 12 Juta karena keterlambatan proyek dan biaya pemulihan data.
    - Potensi dampak kerugian: Kebocoran data pada basis data pelanggan dapat menyebabkan kehilangan kepercayaan pelanggan, kerugian finansial karena serangan siber atau kesalahan sdm, dan hilangnya reputasi perusahaan yang dapat berdampak pada penurunan omset dan keuntungan perusahaan.
    - Potensi dampak kerugian: Kebocoran desain produk rahasia dapat menyebabkan kehilangan keunggulan kompetitif, hilangnya hak kekayaan intelektual, dan kerugian finansial hingga jutaan dolar karena biaya pemulihan hak kekayaan intelektual dan kerugian pasar.

69. Data mengenai lokasi aset, termasuk apakah aset tersebut terdapat di dalam atau di luar jaringan perusahaan.
    a. Aset digital disimpan di penyimpanan cloud (Google Drive)
    b. Aset non-digital disimpan di kantor Scaleout.id yang berlokasi di Jl. Sidodadi II, Corongan, Maguwoharjo, Kec. Depok, Kabupaten Sleman, Daerah Istimewa Yogyakarta 55282. (Google Maps: https://goo.gl/maps/83R3usZ8aJSHgtjd7)
    c. Aset mobile: beberapa karyawan menggunakan handphone bermacam-macam, dominan menggunakan sistem operasi Android namun tidak jarang juga beberapa karyawan menggunakan handphone dengan sistem operasi iOS.

70. Data mengenai pihak-pihak yang memiliki akses terhadap aset tersebut, baik dari dalam maupun dari luar perusahaan.

Semua karyawan yang memiliki hak akses dan klien yang bersangkutan atau yang sedang dalam kerja sama proyek.

71. Data mengenai kebijakan-kebijakan yang sudah ada mengenai penggunaan dan perlindungan aset, termasuk apakah kebijakan tersebut sudah disesuaikan dengan kondisi karyawan jarak jauh.

Tidak ada data mengenai kebijakan-kebijakan yang tertulis di Scaleout Creative Agency.

72. Data mengenai prosedur-prosedur yang sudah ditetapkan untuk mengelola aset, termasuk prosedur backup dan restore data.
    a. Prosedur backup data: Setiap selesai produksi konten, aset digital (footage video dan foto) penting disimpan pada hard disk komputer internal Scaleout Creative Agency. Backup data diawasi oleh staf SDM perusahaan.
    b. Prosedur restore data: Jika terjadi kehilangan data atau kegagalan server, kami biasanya menghubungi pihak ketiga untuk menyelesaikan masalah tersebut. Prosedur ini dilakukan untuk memastikan bahwa data perusahaan dapat dipulihkan dengan cepat dan bisnis dapat berjalan normal kembali.
    c. Prosedur pengelolaan kata sandi: Setiap karyawan diberikan kata sandi unik untuk mengakses sistem perusahaan, dan selama ini kata sandi telah di ubah pada awal tahun 2023.
    d. Prosedur akses data: Karyawan internal diberikan hak akses hanya pada data dan sistem yang dibutuhkan untuk pekerjaannya, dan selama tidak ada kontrol akses, hanya saja diperlukan verifikasi ketika login. Karyawan eksternal seperti freelance hanya diberikan hak akses untuk mengupload konten yang sudah di-edit ke link google drive yang diberikan.
    e. Prosedur penanganan insiden keamanan: Selama ini Scaleout Creative Agency hanya menggantungkan keamanan aset dari serangan siber dari antivirus/proteksi malware dari sistem operasi yang selalu update.
73. Aplikasi dan sistem yang digunakan untuk bekerja dari jarak jauh, termasuk platform kolaborasi, perangkat lunak produktivitas, dan perangkat keras yang digunakan.

Aplikasi dan sistem yang digunakan untuk bekerja dari jarak jauh, termasuk platform kolaborasi, perangkat lunak produktivitas, dan perangkat keras yang digunakan.

a. Platform kolaborasi:
    i. Zoom
    ii. WhatsApp
    iii. Google suites
    iv. Telegram
    v. Meta Ads
b. Perangkat lunak produktivitas:
    i. Microsoft Office
    ii. Google Suite
c. Perangkat keras:
    i. Komputer/Laptop
    ii. Perangkat mobile

74. Penggunaan data dan informasi penting oleh karyawan yang bekerja dari jarak jauh, termasuk jenis data yang diakses, cara data diakses, dan lokasi data.

Penggunaan data dan informasi penting oleh karyawan yang bekerja dari jarak jauh

a. Data klien: Karyawan/freelance dapat mengakses data klien seperti informasi kontak, dan rencana proyek melalui meeting bersama klien dan atas persetujuan Manajemen Proyek.
b. Kekayaan intelektual: Karyawan khusus dari departemen kreatif memiliki akses ke informasi rahasia perusahaan seperti paten, merek dagang, dan hak cipta untuk pembuatan konsep melalui zoom meeting atau dokumen yang dibagikan melalui platform media sosial atau google suite.
c. Sistem informasi: Karyawan dan/atau freelance dapat mengakses sistem informasi seperti database klien, platform kolaborasi, dan aplikasi kreatif melalui persetujuan Manajemen Proyek.

75. Ketersediaan dan keandalan koneksi internet untuk karyawan jarak jauh, termasuk kecepatan koneksi dan penggunaan jaringan pribadi virtual (VPN).

Jaringan dari pekerja jarak jauh menggunakan provider milik pribadi, sedangkan kami sendiri belum menyediakan VPN, karena transfering data masih sering menggunakan cara yang manual (hard disk).

76. Kebijakan keamanan dan privasi yang diterapkan pada perangkat dan koneksi yang digunakan oleh karyawan jarak jauh, termasuk penggunaan kata sandi, autentikasi dua faktor, dan enkripsi data.

Kebijakan keamanan dan privasi yang diterapkan kepada pekerja jarak jauh menggunakan sistem enkripsi data untuk mengakses data yang dibutuhkan (mengunduh/mengunggah data/konten), atau dilakukan secara manual, yaitu melalui salin data dari hard disk.

77. Pelatihan dan kesadaran keamanan karyawan jarak jauh tentang kebijakan dan prosedur keamanan yang diterapkan oleh perusahaan.

Belum ada pelatihan secara khusus kepada karyawan/freelance jarak jauh, namun kami hanya reminder mengenai cara akses data yang dibutuhkan.

78. Data tentang karyawan yang melakukan pekerjaan jarak jauh, termasuk data tentang lokasi dan jarak antara karyawan dan kantor, teknologi yang digunakan, dan jenis pekerjaan yang dilakukan.

79.

No.	Nama	Lokasi	Jarak	Perangkat yang digunakan	Jenis pekerjaan
1	Asrul	Brebes, Jawa Barat	308 Km	Smartphone	CEO & Marketing
2	Ara	Jl. Imogiri Timur, Bantul	14,5 Km	Smartphone Laptop	Divisi Kreatif
3	Oji	Banguntapan, Bantul	6,5 Km	Smartphone Laptop	Freelancer
4	Alvian	Maguwo, Sleman	5,5 Km	Smartphone Laptop	Freelancer
5	Arfan	Sewon, Bantul	14,5 Km	Smartphone Laptop	Freelancer
6	Hanif	Godean, Sleman	19,3 Km	Smartphone Laptop	Freelancer
7	Ilham	Tempel, Sleman	20 Km	Smartphone Laptop	Freelancer

80. Data tentang jenis dan jumlah data yang diakses dan digunakan oleh karyawan jarak jauh, termasuk data sensitif dan data yang harus dijaga kerahasiaannya.

No.	Jenis Data	Tingkat Sensitivitas & Kerahasiaan
1.	Footage Video	80%
2.	Aset gambar	60%
3.	Brief klien	85%
4.	Brand Identity Modul	90%

81. Data tentang kemungkinan ancaman keamanan yang dapat mempengaruhi karyawan jarak jauh, seperti serangan malware, kehilangan atau pencurian perangkat, dan akses tidak sah ke sistem atau data.
    a. Serangan phishing
    b. Serangan malware
    c. Serangan DDoS
    d. Pelanggaran data
    e. Serangan jaringan
    f. Kehilangan atau pencurian perangkat
    g. Akses tidak sah ke sistem atau data
82. Data tentang risiko potensial dan dampaknya pada bisnis jika terjadi kebocoran data atau insiden keamanan lainnya yang melibatkan karyawan jarak jauh, termasuk biaya yang terkait dengan pelanggaran data dan dampak pada reputasi perusahaan.
    a. Biaya pelanggaran data
    b. Kehilangan kepercayaan pelanggan
    c. Potensi pencurian kekayaan intelektual
    d. Penyebaran malware atau ransomware
    e. Serangan siber
83. Informasi tentang kebijakan keamanan yang telah ditetapkan oleh perusahaan terkait dengan penggunaan perangkat dan jaringan pribadi karyawan.

Tidak ada kebijakan terkait penggunaan perangkat dan jaringan pribadi milik karyawan.

84. Data tentang tingkat keamanan jaringan dan sistem perusahaan, serta upaya apa yang telah dilakukan untuk memastikan keamanan akses jarak jauh.

Keamanan yang telah diterapkan di Scaleout Creative Agency diantaranya; Pengelolaan hak akses data dan informasi, sistem otentikasi, enkripsi, anti-virus dan anti-malware, firewall, namun belum adanya sistem pemantauan yang jelas, pendidikan dan pelatihan untuk karyawan jarak jauh, dan beberapa poin keamanan yang telah diterapkan belum 100% maksimal karena masih kurang ketatnya sistem

keamanan, seperti belum menerapkan VPN di distribusi sistem informasi kepada karyawan jarak jauh. Upaya yang sudah dilakukan sebatas melalukan update sistem teknologi keamanan di sistem operasi.

85. Informasi tentang risiko keamanan khusus yang terkait dengan penggunaan perangkat mobile oleh karyawan jarak jauh.
    a. Kehilangan perangkat: Jika perangkat mobile karyawan hilang atau dicuri, informasi rahasia dan data sensitif perusahaan dapat jatuh ke tangan orang yang tidak berwenang.
    b. Serangan malware: Perangkat mobile karyawan yang terinfeksi malware atau virus dapat membuka jalan bagi peretas untuk mengakses informasi perusahaan.
    c. Penyadapan data: Koneksi internet yang tidak aman pada perangkat mobile karyawan dapat membuat data perusahaan yang ditransmisikan rentan terhadap penyadapan.
    d. Pemakaian perangkat pribadi: Jika karyawan menggunakan perangkat pribadi untuk bekerja, risiko keamanan dapat meningkat karena perangkat tersebut mungkin tidak dilindungi dengan perangkat lunak keamanan perusahaan atau memenuhi standar keamanan yang sama seperti perangkat yang disediakan oleh perusahaan.
    e. Penggunaan jaringan Wi-Fi publik: Karyawan yang menggunakan perangkat mobile mereka untuk mengakses jaringan Wi-Fi publik dapat meningkatkan risiko peretasan atau pemantauan data.
    f. Kurangnya kepatuhan: Karyawan yang tidak patuh terhadap kebijakan keamanan perusahaan dapat memperburuk risiko keamanan dan membuka celah bagi peretas untuk mengakses sistem perusahaan.
86. Data tentang pengalaman dan pelatihan keamanan karyawan terkait dengan penggunaan akses jarak jauh dan praktik keamanan yang sesuai.

Tidak tersedia

87. Kinerja bisnis
    a. Pertumbuhan pendapatan: Penurunan pendapatan dalam satu tahun terakhir menunjukkan kinerja bisnis yang kurang baik.

b. Tingkat kepuasan klien: Klien merasa puas dengan layanan dan produk yang Scaleout Creative Agency berikan, namun juga ada klien yang merasa kurang puas dikarenakan belum optimalnya kesepakatan diawal. Sebagai perbandingan yaitu 90% : 10% kepuasan klien.

c. Retensi karyawan:

Tahun	Retensi Karyawan	Keterangan
2019	Cukup bagus	80% karyawan merasa senang dalam bekerja
2020	Cukup bagus	80% karyawan merasa senang dalam bekerja
2021	Bagus	50% karyawan merasa cukup senang dalam bekerja
2022	Kurang bagus	30% karyawan merasa cukup senang dalam bekerja, dan beberapa ada yang resign dikarenakan kondisi finansial Scaleout yang kurang baik.

d. Waktu proyek: Selama ini proyek selesai dengan tepat waktu, namun juga ada beberapa kendala yang membuat proyek tidak selesai sesuai dengan timeline. Sebagai perbandingan yaitu 80% : 20%.

e. Inovasi: Pada tahun 2019 Scaleout membuat inovasi produk yang menyesuaikan dengan kebutuhan pasar, yaitu dengan menyesuaikan produk di Tiktok.

f. Branding: Branding yang kami lakukan cukup dapat mendapatkan interaksi dari audiens.

88. Data risiko

    a. Risiko Kehilangan Data: Risiko ini dapat terjadi ketika data yang berharga, seperti karya seni atau dokumen klien, hilang atau rusak. Hal ini dapat terjadi karena kegagalan sistem, kerusakan perangkat keras atau lunak, atau kesalahan manusia.
    b. Risiko Keamanan Jaringan: Risiko ini terjadi ketika jaringan atau sistem komputer disusupi oleh pihak yang tidak berwenang. Penyerang dapat mencuri data, mengubah data, atau bahkan merusak sistem.
    c. Risiko Kepatuhan Hukum: Risiko ini terkait dengan masalah hukum yang terjadi karena pelanggaran hak cipta atau privasi, atau ketidakpatuhan terhadap peraturan dan perundang-undangan yang berlaku.
    d. Risiko Keselamatan Karyawan: Risiko ini terkait dengan keamanan karyawan yang bekerja di lingkungan agensi kreatif. Risiko ini dapat berupa kecelakaan di tempat kerja atau bahaya kesehatan yang terkait dengan pekerjaan, seperti penyakit yang disebabkan oleh zat kimia.
    e. Risiko Teknologi: Risiko ini terkait dengan kegagalan perangkat keras atau lunak, atau dengan adanya kerentanan dalam sistem. Risiko ini dapat menyebabkan kegagalan sistem, kehilangan data, atau ketidakmampuan untuk mengakses sistem atau data yang penting.

89. Undang-undang dan regulasi terkait privasi data seperti GDPR, HIPAA, atau CCPA, pada negara atau wilayah tempat agensi beroperasi?

    a. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) yang mengatur tentang transaksi elektronik dan memberikan perlindungan terhadap informasi pribadi pengguna yang disimpan oleh penyedia layanan.
    b. Peraturan Menteri Komunikasi dan Informatika Nomor 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik yang mengatur tentang panduan pengelolaan data pribadi yang aman dan bertanggung jawab di dalam sistem elektronik.

90. Kebijakan perusahaan terkait dengan privasi data dan keamanan informasi yang telah ditetapkan?

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik di Indonesia

91. Standar keamanan yang diterapkan dalam Scaleout Creative Agency seperti ISO 27001 atau NIST Cybersecurity *Framework*?

Belum menerapkan *framework* tersebut. Sistem keamanan di Scaleout Creative Agency hanya menggunakan platform penyimpanan pihak ketiga.

92. Persyaratan peraturan dan perizinan khusus yang diperlukan untuk menjalankan bisnis di sektor kreatif, seperti lisensi kreatif atau izin hak cipta.
    a. Izin Usaha: Izin usaha diperlukan untuk menjalankan bisnis di Indonesia. Izin usaha ini dapat diperoleh dari Kementerian Hukum dan HAM atau Badan Koordinasi Penanaman Modal (BKPM) untuk investasi asing.
    b. Peraturan Perlindungan Data Pribadi: Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) dan Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Pedoman Pelaksanaan Perlindungan Data Pribadi pada Layanan Aplikasi dan Situs Web (Permenkominfo No. 20/2016) dan Pedoman Perlindungan Data Pribadi pada Pengolahan Data Kependudukan (Permenkominfo No. 5/2018).
93. Pedoman dan regulasi terkait dengan pelaporan insiden keamanan dan penanganan kejadian darurat dalam kasus pelanggaran keamanan.
    a. Keputusan Menteri Komunikasi dan Informatika Nomor 133 Tahun 2019 tentang Pedoman Pelaporan Insiden Keamanan Informasi dan Penanganannya yang menetapkan pedoman pelaporan insiden keamanan informasi yang harus dilakukan oleh penyelenggara sistem.
    b. Panduan Nasional Keamanan Siber (Panduan NAKSI) yang dikeluarkan oleh Badan Siber dan Sandi Negara (BSSN) yang berisi tentang prosedur penanganan insiden keamanan siber.

94. Kebijakan keamanan dan privasi data klien yang harus dipatuhi oleh seluruh pegawai dan mitra bisnis.

1. Pengumpulan dan penggunaan data:

Aset yang diperlukan oleh Scaleout Creative Agency dari kliennya yaitu berupa Aset fisik dan asset digital yang hanya diperlukan untuk kebutuhan produksi konten sesuai dengan kerja sama yang berlangsung tanpa adanya penyelewengan hak aset yang sudah diberikan. Aset fisik merupakan produk dari klien tersebut, sedangkan aset digital berupa gambar (logo produk), footage (opsional), dokumen (brief produk), audio (penyebutan nama produk, atau keperluan tagline). Aset diperlukan untuk mendukung kerja sama antara Scaleout Creative Agency dengan mitra bisnis, terutama untuk kebutuhan output konten. Data diolah dengan memahami brief yang sudah dijabarkan, kemudian

konsep/ide cerita di bangun sesuai dengan brief produk tersebut, lalu kami memproduksi konten sesuai dengan konsep/ide cerita yang sudah disusun dengan pedoman brief produk tersebut, mulai dari pelafalan nama produk, cara penggunaan, "do & don'ts", dsb, kemudian dilanjutkan tahap editing konten dengan asset dan footage yang sudah diberikan. Lalu masuk tahap QC internal dan revisi klien, pada tahap ini ada beberapa request tentang asset data yang perlu dimasukkan di konten atau sebaliknya. Setelah disetujui, tahap terakhir adalah posting konten ke platform media sosial.

2. Penanganan data:

Semua data disimpan dengan melalui penyimpanan offline dan online. Data yang dikirimkan melalui media sosial (di dalam chat) akan diunduh dan di simpan ke dalam hard disk komputer, sedangkan data yang dikirimkan melalui penyimpanan online seperti google drive, tim kreatif akan mengelola dengan cara meminta akses kepada pengirim lalu membaca dan/atau mengunduh (apabila diperlukan) data tersebut untuk kepentingan pembuatan konten. Pengakses data didalam hard disk atau di penyimpanan cloud seperti google drive, merupakan satu orang yang memang berwenang dalam hal tersebut, namun, beberapa kasus data tersebut perlu di berikan kepada karyawan/freelance yang bekerja jarak jauh untuk keperluan editing, disinilah letak kelemahan sistem keamanan, karena data di transfer hanya menggunakan enkripsi dari platform media sosial, dan aturan kebijakan keamanan yang berlaku di perusahaan kreatif.

3. Kepatuhan terhadap peraturan:

Scaleout Cerative Agency merupakan sebuah badan usaha berbentuk CV, maka kami menyesuaikan dengan aturan yang berlaku di Indonesia, yaitu;

1. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE). UU ITE mengatur tentang tata cara penggunaan informasi dan transaksi elektronik, termasuk pengamanan dan perlindungan data pribadi.

2. Peraturan Pemerintah No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Peraturan ini mengatur tentang pengamanan data elektronik dan persyaratan keamanan untuk penyelenggara sistem dan transaksi elektronik.
3. Peraturan Menteri Komunikasi dan Informatika No. 20 Tahun 2016 tentang Perlindungan Data Pribadi dalam Sistem Elektronik. Peraturan ini mengatur tentang perlindungan data pribadi dalam sistem elektronik, termasuk persyaratan pengolahan, penyimpanan, dan penghapusan data pribadi.

4. Pelatihan dan kesadaran:

Selama ini kami masih jarang memberikan edukasi yang kompleks kepada karyawan/freelance dan mitra terkait kebijakan privasi dan keamanan data klien dan menjaga privasi data tersebut.

5. Pelaporan kejadian:

Di Scaleout Creative Agency, kelemahan pada pelaporan kejadian yaitu tidak dilakukan dengan tertulis, jadi hanya beberapa orang yang tahu akan kejadian-kejadian yang pernah terjadi, seperti serangan ransomware di tahun 2022, human error pada tahun 2021, dsb.

6. Peninjauan dan penilaian:

Peninjauan tidak dilakukan secara berkala dan tidak dilakukan dengan tertulis, maka penanganan dilakukan setelah masalah datang.

95. Aplikasi dan sistem yang digunakan untuk memproses, menyimpan, dan mengakses data sensitif klien dan informasi rahasia perusahaan.
    a. Google Drive
    b. Komputer/Hard disk
    c. Media sosial: Telegram & WhatsApp
96. Manajemen aset bisnis yang mencakup inventarisasi aset digital, kekayaan intelektual, dan aplikasi.

a. Inventarisasi aset digital:

i. Domain website : www.scaleout.id

ii. Akun media sosial

1. https://web.facebook.com/scaleout.id

2. https://www.instagram.com/scaleout.id/

3. https://www.youtube.com/channel/UCaQ3bBqIn0S5hCU0Mk6vXlw

iii. Konten website (artikel, foto, video, dll.)

Semua konten ada di akun media sosial.

iv. Desain grafis (logo, brosur, kartu nama, dll.)

SCALEOUT.ID

v. Perangkat lunak

No.	Nama Aplikasi
1.	Adobe Premiere Pro 2020
2.	Adobe After Effects 2020
3.	Adobe Photoshop 2022
4.	Adobe Illustrator 2020
5.	Adobe Lightroom Classic
6.	Adobe Audition 2020
7.	Canva online
8.	Capcut
9.	Microsoft Office 2019

10.	Google Chrome Browser
11.	Firefox Browser
12.	Telegram
13.	WhatsApp
14.	Media Player Classic
15.	Zoom
16.	Corel Draw
17.	Internet Download Manager
18.	Format Factory
19.	Celtx Scriptwriter

vi. Aplikasi bisnis

No.	Nama Aplikasi	No.	Nama Aplikasi
1.	Meta Ads	9.	Zoom
2.	Facebook	10.	Figma
3.	Google drive	11.	Google Ads
4.	Telegram	12.	Notes
5.	WhatsApp	13.	Tiktok
6.	Microsoft Office 2019	14.	Instagram
7.	Google Chrome Browser	15.	Youtube
8.	Firefox Browser	16.	M-Banking

b. Data pelanggan dan klien

1. Daikin
2. Lumecolors
3. Hyundai
4. Tugu Jogja
5. LinkAja
6. Milagros
7. Kutus Kutus
8. Nocra
9. Hamzah Batik
10. Kanjeng Heritage
11. Oriflakes
12. Dan lebih banyak lagi

ii. Email dan kontak bisnis

Website: https://scaleout.id/

No. Telp.: 08112634734

iii. Proyek kreatif yang sedang berjalan

1. Oriflakes
2. Hamzah Batik Malioboro
3. Halte Tour

iv. Server dan sistem penyimpanan data

1. Google Drive
2. Hard disk komputer

v. Hak cipta atas karya kreatif yang dihasilkan oleh agensi

97. Manajemen risiko yang mencakup penilaian risiko terhadap inventarisasi data, aplikasi, aset digital, dan kekayaan intelektual.

    a. Idenfitikasi risiko:

        i. Risiko kehilangan data atau kebocoran data yang berharga seperti data klien atau data proyek.

        ii. Risiko keamanan jaringan dan sistem yang rentan terhadap serangan siber, virus, dan malware.

        iii. Risiko kesalahan manusia dalam pengelolaan data atau penggunaan sistem, seperti ketidakhati-hatian dalam membuka lampiran email yang mencurigakan atau penggunaan password yang mudah ditebak.

        iv. Risiko kegagalan peralatan atau sistem seperti server, komputer, atau perangkat lunak.

        v. Risiko pelanggaran kebijakan privasi dan keamanan data, seperti penyalahgunaan data pribadi atau penggunaan data klien tanpa izin.

        vi. Risiko kehilangan atau kerusakan aset fisik seperti peralatan atau perangkat keras.

        vii. Risiko ketidakpatuhan terhadap peraturan atau hukum yang berlaku, seperti pelanggaran hak cipta atau peraturan privasi data.

        viii. Risiko kegagalan dalam menyediakan layanan atau produk yang memenuhi harapan klien atau pelanggan.

        ix. Risiko reputasi dan citra bisnis yang rusak akibat masalah keamanan data atau pelanggaran privasi.

    b. Evaluasi risiko:

        i. Identifikasi ancaman potensial

        ii. Penilaian kerentanan

        iii. Penilaian dampak

        iv. Penetapan tingkat risiko

v. Penetapan strategi mitigasi risiko

vi. Pemantauan dan peninjauan

c. Penanganan risiko:

i. Evaluasi risiko secara berkala

ii. Pemantauan keamanan jaringan

iii. Penggunaan teknologi keamanan

iv. Pelatihan keamanan

v. Back-up dan pemulihan

vi. Pemantauan aktivitas pengguna

vii. Kebijakan keamanan

d. Pemantauan dan evaluasi:

i. Penilaian risiko secara berkala

ii. Pemantauan aktivitas pengguna

iii. Evaluasi keamanan aplikasi

iv. Pelaporan insiden keamanan

v. Pemantauan perubahan regulasi

98. Ketergantungan agensi kreatif dengan layanan lainnya yang dapat memengaruhi keamanan dan fleksibilitas sistem.

Scaleout Creative Agency sangat bergantung pada layanan sistem penyimpanan cloud yang sangat krusial dan sangat mempengaruhi keamanan dan fleksibilitas sistem.

99. Persyaratan bisnis: informasi tentang persyaratan bisnis untuk keamanan informasi, seperti kebutuhan fleksibilitas dan aksesibilitas untuk mendukung operasi bisnis.

a. Ketersediaan akses ke sistem dan aplikasi: Akses data dilakukan via penyimpanan cloud dan menggunakan transfer data offline (Hard disk)

b. Perlindungan kekayaan intelektual: belum ada penerbitan hak cipta yang dilakukan oleh Scaleout Creative Agency

c. Keamanan data klien: Jaminan keamanan data berdasarkan platform penyimpanan cloud yang dipakai dan aplikasi untuk komunikasi.

100. Ancaman keamanan: informasi tentang ancaman keamanan yang mungkin dihadapi oleh agensi kreatif, seperti serangan siber, pencurian data, dan akses tidak sah.

a. Serangan siber: Scaleout melakukan update keamanan pada sistem operasi untuk mengurangi serangan siber.

b. Pencurian data: Karyawan Scaleout mengedepankan kejujuran dan tindakan tegas terkait pencurian data, walaupun belum pernah terjadi, tapi semua karyawan memahami data sensitif klien.

c. Akses tidak sah: Akses di kontrol oleh orang-orang yang berwenang di Scaleout, maka segala akses yang tidak sah akan dibatasi dengan otentikasi dari platform (google).

d. Kekurangan keamanan fisik: Scaleout tidak memiliki sistem keamanan fisik, seperti cctv atau lain sebagainya.

101. Risiko keamanan: informasi tentang risiko keamanan yang muncul dari ancaman keamanan yang teridentifikasi.

a. Kehilangan data

b. Downtime sistem

c. Kerentanan informasi klien

d. Kerentanan infrastruktur TI

e. Pelanggaran regulasi keamanan

102. Kebijakan keamanan: informasi tentang kebijakan keamanan yang diterapkan di agensi kreatif, seperti kebijakan keamanan informasi, kebijakan aksesibilitas, dan kebijakan fleksibilitas.

a. Kebijakan keamanan informasi: kebijakan ini menetapkan standar keamanan yang harus diikuti oleh seluruh karyawan dan mitra bisnis Scaleout Creative Agency, yang terlibat dalam pengolahan data dan informasi di agensi kreatif. Hal ini meliputi

penggunaan kata sandi yang kuat, pembatasan akses berdasarkan hak akses, enkripsi data, dan lain sebagainya.

b. Kebijakan aksesibilitas: kebijakan ini menetapkan aturan tentang akses ke sistem dan data oleh karyawan jarak jauh atau dari luar perusahaan Scaleout yang mana aksesnya menggunakan penyimpanan cloud dan/atau hard disk.

c. Kebijakan fleksibilitas: kebijakan ini menetapkan standar untuk penggunaan perangkat pribadi, seperti laptop atau telepon pintar, di dalam lingkungan Scaleout Creative Agency.

103. Penerapan keamanan: informasi tentang bagaimana kebijakan keamanan diimplementasikan di agensi kreatif, seperti alat keamanan yang digunakan dan proses pengaturan keamanan.

Kebijakan penggunaan alat keamanan menggunakan sistem yang sudah disediakan beberapa vendor, seperti cloud penyimpanan (google) dan media sosial yang dipakai (Telegram, WhatsApp, dsb). Kebijakan hak akses sesuai dengan wewenang tiap departmen

104. Evaluasi keamanan: informasi tentang bagaimana keamanan diukur dan dinilai di agensi kreatif, seperti pengujian keamanan, audit keamanan, dan pemantauan keamanan.

Scaleout Creative Agency belum melakukan audit sistem keamanan.

105. Rencana keamanan: informasi tentang rencana pengembangan keamanan untuk agensi kreatif, seperti perencanaan keamanan jangka pendek dan jangka panjang, dan rencana respons keamanan dalam situasi darurat.

Sejauh ini belum ada rencana penginkatan keamanan, kami hanya akan melakukan backup data secara teratur, memastikan bahwa pemulihan sistem dan data dapat dilakukan dalam waktu yang sesingkat mungkin, dan melakukan updating perangkat seiring perkembangan zaman.

106. Informasi tentang bisnis dan arsitektur sistem informasi agensi kreatif, termasuk aset digital, aplikasi, data, dan infrastruktur yang digunakan.

a. Deskripsi bisnis

Scaleout Creative Agency adalah agensi kreatif dan rumah produksi yang berfokus dan berspesialisasi dalam komunikasi pemasaran dan branding seperti video dan desain. tidak hanya membuat video yang enak dipandang, tentunya juga tepat sasaran. Scaleout Creative Agency telah berdiri sejak tahun 2019 dan telah menghasilkan ribuan konten video pemasaran. Target pelanggan kami yaitu UMKM di seluruh Indonesia, yang membutuhkan video digital untuk pemasaran produknya, baik secara branding maupun konversi. Kedepannya Scaleout Creative Agency akan selalu mengikuti perkembangan zaman, seperti era digitalisasi yang sangat dibutuhkan pada zaman ini. Produk yang kami tawarkan juga akan selalu berinovasi dengan kebutuhan klien di masa mendatang.

b. Proses Bisnis

i. Identifikasi kebutuhan klien: Proses ini dimulai dengan mendengarkan kebutuhan klien dan memahami tujuan dan tujuan bisnis mereka.

ii. Pengembangan konsep: Setelah memahami kebutuhan klien, tim kreatif mengembangkan konsep dan ide untuk memenuhi kebutuhan tersebut.

iii. Penentuan anggaran: Tim akuntansi atau manajemen proyek akan menentukan anggaran yang dibutuhkan untuk proyek dan memastikan bahwa anggaran tersebut sesuai dengan kebutuhan klien.

iv. Penetapan jadwal: Manajemen proyek akan menentukan jadwal proyek dan mengkoordinasikan tugas antara tim kreatif dan manajemen proyek.

v. Produksi: Setelah konsep disetujui, tim kreatif akan memproduksi konten yang dibutuhkan, seperti desain grafis, konten web, atau video.

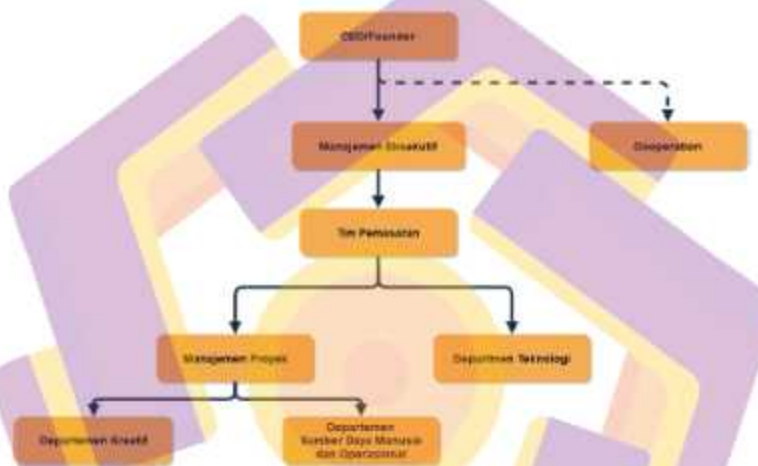
vi. Quality control: Konten yang telah selesai, akan melalui pengecekan oleh tim QC internal untuk memastikan tidak ada kekeliruan pada video sebelum diberikan kepada klien.

vii. Preview: Klien akan memberikan umpan balik pada konten yang diproduksi dan tim kreatif akan melakukan revisi jika diperlukan. Konten juga akan diuji untuk memastikan kualitas dan kesesuaian.

viii. Penyelesaian dan pengiriman: Setelah proyek selesai, konten akan diserahkan kepada klien dalam bentuk yang diminta, seperti file digital atau link google drive yang berisikan file konten.

ix. Evaluasi kinerja: Tim manajemen proyek akan mengevaluasi kinerja tim dan proyek untuk memastikan bahwa proyek berjalan dengan baik dan dalam anggaran dan jadwal yang ditetapkan.

c. Struktur organisasi:



i. CEO/Founder: Bertanggung jawab atas visi dan arah strategis perusahaan, serta memimpin manajemen eksekutif.

ii. Admin Pemasaran: Bertanggung jawab atas analisis pasar, riset klien, dan pengembangan strategi untuk kampanye pemasaran dan promosi.

iii. Manajemen Proyek: Bertanggung jawab atas hubungan dengan klien dan memastikan bahwa proyek-proyek dipenuhi dengan baik dan tepat waktu.

iv. Manajemen Eksekutif: Terdiri dari eksekutif senior seperti Presiden, CFO, dan CMO, yang bertanggung jawab atas operasi dan keuangan perusahaan termasuk akuntansi, penggajian, dan pengelolaan kas.

v. Departemen Kreatif: Terdiri dari tim desain grafis, tim kreatif, tim penulis konten, dan lain-lain, yang bertanggung jawab atas pembuatan konten termasuk materi konten.

vi. Departemen Strategi dan Riset: Departemen Teknologi: Bertanggung jawab atas pengembangan dan pemeliharaan situs web, aplikasi, dan sistem informasi lainnya yang diperlukan untuk kampanye pemasaran dan promosi.

vii. Departemen Sumber Daya Manusia dan Operasional: Bertanggung jawab atas perekrutan, pelatihan, dan pengembangan karyawan, serta manajemen kinerja dan kebijakan karyawan serta bertanggung jawab atas manajemen fasilitas dan sumber daya yang diperlukan untuk menjalankan operasi sehari-hari agensi kreatif.

d. Arsitektur sistem informasi

e. Jaringan: Biznet (Huawei EG8145V5)

f. Perangkat keras

No.	Model	Spesifikasi
1.	Komputer 1 (Internal)	Intel(R) Core(TM) i5-10400 CPU @ 2.90GHz 2.90 GHz RAM : 16,0 GB Intel® UHD Graphics 630 Monitor LED MSI
2.	Komputer 2 (Internal)	Intel(R) Core(TM) i7-4970 CPU @ 3.60GHz(CPUs), ~3.6 GHz RAM : 8,0 GB NVIDIA GeForce GT 730

		Monitor LED MSI
3.	Komputer 3 (Karyawan Jarak Jauh)	Intel(R) Core(TM) i5-6500 CPU @ 3.20GHz 2.19 GHz RAM 16,0 GB Monitor LED Asus
4.	Printer	Brother DCP-T420W
5.	Hard disk Eksternal (3)	WD Blue (1 TB) Seagate Barracuda (1 TB) (2)
6.	Router (3)	TP-Link Wireless USB Adapter

g. Perangkat Lunak (Produktivitas Konten)

No.	Nama Aplikasi
1.	Adobe Premiere Pro 2020
2.	Adobe After Effects 2020
3.	Adobe Photoshop 2022
4.	Adobe Illustrator 2020
5.	Adobe Lightroom Classic
6.	Adobe Audition 2020
7.	Canva online
8.	Capcut
9.	Microsoft Office 2019

10.	Google Chrome Browser
11.	Firefox Browser
12.	Telegram
13.	WhatsApp
14.	Media Player Classic
15.	Zoom
16.	Corel Draw
17.	Internet Download Manager
18.	Format Factory
19.	Celtx Scriptwriter

h. Aplikasi Bisnis

No.	Nama Aplikasi
1.	Meta Ads
2.	Facebook
3.	Google drive
4.	Telegram
5.	WhatsApp
6.	Microsoft Office 2019
7.	Google Chrome Browser
8.	Firefox Browser
9.	Zoom
10.	Figma
11.	Google Ads
12.	Notes
13.	Tiktok
14.	Instagram
15.	Youtube
16.	M-Banking

i. Database

Scaleout Creative Agency memiliki 2 bentuk database untuk menyimpan data klien, karyawan, proyek, karyawan, dan aset kreatif, diantaranya;

i. Google drive sebagai penyimpanan data online

ii. Hard disk memory sebagai penyimpanan data offline

j. Kebijakan keamanan

i. Kebijakan Akses: kebijakan akses yang ketat untuk memastikan hanya orang yang berwenang yang dapat mengakses data dan sistem informasi penting, seperti akses google drive, platform iklan, admin, dsb.

ii. Kebijakan Sandi: Kebijakan ini mencakup pengaturan panjang sandi, kompleksitas sandi, periode penggantian sandi dan peningkatan keamanan dengan autentikasi ganda oleh tiap pihak/divisi yang berwenang.

k. Pelanggan

Scaleout Creative Agency bergerak sebagai agensi kreatif untuk memproduksi konten-konten di platform sosial media dengan target pelanggannya adalah UMKM, namun tak jarang juga mendapat klien dalam bentuk usaha mengenah keatas. Persona buyer Scaleout Creative Agency, sebagai berikut;

Persona Buyer		
No.	Jenis	Keterangan
1	Usia	24 – 45 Tahun
2	Pekerjaan	Business Owner
3	Domisili	Indonesia
4	Tempat tinggal	Kota
5	Medsos Buyer	Tiktok, Instagram, & Facebook
6	Berita/Informasi Favorit	Perkembangan bisnis
7	Hobi/Minat	Berdagang
8	Tujuan	Branding dan/atau konversi
9	Bahasa	Indonesia, Inggris
10	Penghasilan	Rp30.000.000 – Rp50.000.000

107. Persyaratan keamanan dan standar yang diterapkan oleh badan regulasi dan industri yang relevan untuk agensi kreatif.

Scaleout Creative Agency merupakan Commanditaire Vennootschap (CV) yang menggunakan regulasi standar dari pemerintahan, yaitu Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat ("Permenkominfo No. 5/2021").

108. Informasi tentang vendor dan penyedia layanan pihak ketiga yang digunakan oleh agensi kreatif dan evaluasi risiko keamanan yang terkait dengan penggunaan layanan tersebut.

Informasi tentang vendor dan penyedia layanan pihak ketiga yang digunakan oleh agensi kreatif dan evaluasi risiko keamanan yang terkait dengan penggunaan layanan tersebut

a. Vendor Jaringan : Indihome (https://indihome.co.id/) dan Biznet Home (https://biznethome.net/) merupakan 2 layanan jaringan yang kami gunakan selama ini, untuk akses informasi, untuk keamanan jaringan kami kurang begitu paham.
b. Vendor Property : iFrame, Andigital merupakan 2 rentalan property yang kami gunakan untuk memproduksi konten, risiko terdapat pada footage pada memory yang kadang tidak segera dihapus saat menggunakan memory dari vendor, maka untuk mengurangi dampak risiko tersebut kami selalu mengganti dengan memori milik Scaleout.
c. Vendor Sumber Daya Manusia : Freelance Videografer dan Editor, merupakan salah satu pekerja jarak jauh yang kami gunakan. Tingkat risiko pada vendor ini cukup tinggi, karena kurang adanya sistem keamanan yang kuat terkait informasi yang dibagikan dan masih dengan cara manual yaitu meminta menghapus data yang sudah tidak diperlukan.

109. Evaluasi kepatuhan hukum agensi kreatif terhadap persyaratan keamanan dan regulasi yang relevan.

Scaleout Creative Agency merupakan Commanditaire Vennootschap (CV) yang menggunakan regulasi standar dari pemerintahan, yaitu Peraturan Menteri Komunikasi dan Informatika Nomor 5 Tahun 2020 Tentang Penyelenggara Sistem Elektronik Lingkup Privat ("Permenkominfo No. 5/2021").

110. Informasi mengenai aset-aset kunci agensi kreatif, seperti data klien, kekayaan intelektual, dan sistem yang harus dijaga keamanannya?

Scaleout Creative Agency melindungi data klien, kekayaan intelektual, dan sistem informasi dengan memastikan bahwa karyawan hanya memiliki akses yang sesuai dengan tanggung jawab dan pekerjaan mereka seperti penggunaan password yang kuat, sistem keamanan jaringan yang baik, dan penggunaan sistem otentikasi dua faktor pada beberapa platform media sosial.

111. Kebijakan keamanan yang telah ada di agensi kreatif, seperti kebijakan akses, penggunaan perangkat mobile, dan kebijakan password?

Kebijakan Keamanan Scaleout Creative Agency, Kebijakan di bagi menjadi 4 kategori, diantaranya;

a. Hak akses penuh (full access): memberikan pengguna akses penuh ke seluruh data dan informasi dalam sistem. Pada kategori ini yaitu CEO/Founder.
b. Hak akses terbatas (limited access): memberikan pengguna akses terbatas ke data dan informasi tertentu dalam sistem. Pada kategori ini yaitu Admin Pemasaran, Manajemen Eksekutif.
c. Hak akses baca saja (read-only access): memberikan pengguna hak untuk melihat data dan informasi, namun tidak dapat mengubah atau menghapusnya. Pada kategori ini yaitu Departemen Strategi dan Riset, Departemen Sumber Daya Manusia dan Operasional.
d. Hak akses pengelolaan (management access): memberikan pengguna hak untuk mengelola data dan informasi, seperti menambah, mengubah, atau menghapus data. Pada kategori ini yaitu Manajemen Proyek, Departemen Kreatif.
e. Setiap Ketua Departmen memiliki wewenang untuk mengubah password, backup data secara berkala, meng-update software, dan lain sebagainya untuk mengelola keamanan data Scaleout Creative Agency.

112. Informasi tentang lingkungan teknologi yang digunakan oleh agensi kreatif, termasuk sistem operasi, aplikasi, dan infrastruktur jaringan?

Sistem operasi yang digunakan pada perangkat laptop dan komputer rata-rata Windows 10 dan MacOS Mojave, sedangkan pada smartphone yaitu Android dan iPhone.

No.	Nama Aplikasi Produksi
1.	Adobe Premiere Pro 2020
2.	Adobe After Effects 2020
3.	Adobe Photoshop 2022
4.	Adobe Illustrator 2020
5.	Adobe Lightroom Classic
6.	Adobe Audition 2020
7.	Canva online
8.	Capcut
9.	Microsoft Office 2019
10.	Google Chrome Browser
11.	Firefox Browser
12.	Telegram
13.	WhatsApp
14.	Media Player Classic
15.	Zoom
16.	Corel Draw
17.	Internet Download Manager
18.	Format Factory
19.	Celtx Scriptwriter

No.	Nama Aplikasi Bisnis
1.	Meta Ads
2.	Facebook
3.	Google drive
4.	Telegram
5.	WhatsApp
6.	Microsoft Office 2019
7.	Google Chrome Browser
8.	Firefox Browser
9.	Zoom
10.	Figma
11.	Google Ads
12.	Notes
13.	Tiktok
14.	Instagram
15.	Youtube
16.	M-Banking

Infrastruktur jaringan yang kami gunakan yaitu Biznet (Huawei EG8145V5) dengan router TP-Link Wireless USB Adapter.

113. Data mengenai sistem manajemen keamanan yang sudah ada di agensi kreatif, seperti SIEM (Security Information and Event Management), IDS (Intrusion Detection System), dan firewall?

Scaleout Creative Agency menggunakan manajemen keamanan yang sudah disediakan dari beberapa platform atau sistem operasi yang digunakan, seperti firewall atau enkripsi data pada google dan/atau sosial media lain.

114. Informasi mengenai aset perusahaan yang perlu dilindungi, seperti data sensitif, sistem informasi, aplikasi, dan infrastruktur teknologi.

a. Data klien: termasuk informasi pribadi dan rahasia, seperti nama, alamat, nomor telepon, dan informasi keuangan.
b. Kekayaan intelektual: termasuk hak cipta, merek dagang, desain.
c. Sistem informasi: termasuk server, aplikasi, dan database.
d. Aplikasi dan software: termasuk perangkat lunak kreatif seperti Adobe Creative Suite dan perangkat lunak manajemen proyek.
e. Infrastruktur teknologi: termasuk jaringan komputer, firewall, router, dan perangkat lainnya yang digunakan untuk menghubungkan karyawan dan perangkat mereka ke sistem perusahaan.

115. Kebijakan keamanan dan aturan penggunaan sistem yang telah ditetapkan oleh agensi kreatif, termasuk kebijakan untuk karyawan jarak jauh.

Kebijakan yang berlaku tidak dilakukan secara tertulis dan disepakati berdasarkan lisan, masih perlunya peninjauan dan revisi terkait hal tersebut, berikut kebijakan kepada karyawan jarak jauh terhadap penggunaan sistem;

a. Karyawan jarak jauh wajib melakukan backup data setelah selesai produksi konten ke hard disk milik kantor, lalu data bisa di salin ke penyimpanan milik pribadi karyawan untuk bisa dikerjakan dirumah.
b. Karyawan jarak jauh yang memerlukan data dari cloud, pihak kantor akan memberikan akses yang dibutuhkan, seperti link penyimpanan google drive, transfer data via WhatsApp dan Telegram.
c. Selesai proyek karyawan jarak jauh akan meminta ijin kepada bagian kepala Departemen Sumber Daya Manusia dan Operasional untuk melakukan penghapusan data, apabila sudah tidak diperlukan.

116. Informasi tentang sistem deteksi intrusi dan sistem keamanan lain yang digunakan oleh perusahaan untuk melindungi sistem dari ancaman keamanan. Firewall dan Sistem Autentikasi dan Otorisasi

117. Data tentang pelaporan dan manajemen insiden keamanan, termasuk tindakan yang harus diambil dalam hal terjadinya pelanggaran keamanan. Tidak ada pelaporan selama ini, dan tindakan yang dilakukan yaitu menghubungi pihak ketiga sebagai layanan service terkait. Untuk manajemen insiden keamanan kedepannya belum ada tindakan atau rencana.

118. Daftar layanan yang disediakan oleh agensi kreatif kepada karyawan, baik yang dapat diakses secara jarak jauh maupun tidak.
a. Jaringan
b. Akses informasi
c. Perangkat keras
d. Aplikasi editing

119. Kebijakan aksesibilitas dan fleksibilitas: data mengenai kebijakan dan standar aksesibilitas dan fleksibilitas yang diadopsi oleh agensi kreatif.

a. Standar aksesibilitas: Agensi kreatif menerapkan standar aksesibilitas yang ketat untuk memastikan bahwa setiap karyawan dapat mengakses informasi dan sumber daya yang dibutuhkan untuk menyelesaikan tugas mereka. Ini termasuk penggunaan perangkat lunak dan perangkat keras yang dapat diakses oleh orang dengan disabilitas, serta aksesibilitas fisik yang memadai di lokasi kantor.

b. Kebijakan fleksibilitas: Agensi kreatif mendorong fleksibilitas dalam jadwal kerja dan lingkungan kerja yang memungkinkan karyawan untuk bekerja dengan cara yang paling produktif dan efektif bagi mereka. Ini mencakup jadwal kerja yang fleksibel, bekerja dari rumah atau lokasi lain yang jauh, dan dukungan teknologi yang memungkinkan karyawan untuk tetap terhubung dan produktif di luar lingkungan kantor.

120. Keamanan data dan privasi: data tentang jenis data yang disimpan, bagaimana data tersebut diakses, dikelola, dan disimpan serta bagaimana keamanan data dan privasi dijaga.

Keamanan data dan privasi di simpan di gmail dan hanya dapat diakses oleh pihak yang berwenang.

121. Penentuan strategi mitigasi risiko keamanan yang terkait dengan fleksibilitas dan aksesibilitas, seperti peningkatan kontrol keamanan, penerapan teknologi keamanan baru, atau restrukturisasi sistem untuk meminimalkan risiko.

Scaleout belum menentukan strategi mtigasi risiko keamanan selama ini.

122. Penilaian risiko keamanan terkait dengan aplikasi, data, infrastruktur, dan sistem yang digunakan untuk fleksibilitas dan aksesibilitas.

1. Faktor-faktor yang berpengaruh terhadap risiko kearsipan aksesibilitas dan fleksibilitas pada Seaknot Creative Agency

No.	Jenis Risiko	Kode	Kejadian Risiko	Frekuensi Risiko yang terjadi					Pengaruh risiko terhadap sistem kearsipan				
				1	2	3	4	5	1	2	3	4	5
1	Aplikasi	A1	Adobe Premiere Pro 2020			X			X				
		A2	Adobe After Effects 2020	X					X				
		A3	Adobe Photoshop 2022	X					X				
		A4	Adobe Illustrator 2020	X					X				
		A5	Adobe Lightroom Classic	X					X				
		A6	Adobe Audition 2020	X					X				
		A7	Canva online	X							X		
		A8	Capcut	X						X			
		A9	Microsoft Office 2019	X							X		
		A10	Google Chrome Browser		X							X	
		A11	Firefox Browser	X								X	
		A12	Telegram	X								X	
		A13	WhatsApp	X								X	
		A14	Media Player Classic	X					X				
		A15	Zoom	X					X	X			
		A16	Corel Draw	X					X				
		A17	Internet Download Manager		X							X	
		A18	Format Factory	X					X				
		A19	Canva Semprwriter	X					X				
		A20	Meta Ads										
		A21	Facebook		X								
		A22	Google drive										
		A23	Telegram										
		A24	WhatsApp										
		A25	Microsoft Office 2019										
		A26	Google Chrome Browser										
		A27	Firefox Browser										
		A28	Zoom										
		A29	Figma										
		A30	Google Ads										
		A31	Notes										
		A32	Tiktok										
		A33	Instagram										
		A34	Youtube										
		A35	M-Banking										
2	Data	B1	Data klien	X						X			
		B2	Data proyek			X					X		
		B3	Data vendor			X					X		
		B4	Data keuangan		X					X	X		
		B5	Data karyawan	X							X		
		B6	Data confidential		X					X	X		
		B7	Data teknologi		X	X					X		
3	Infrastruktur	C1	Jaringan komputer			X						X	
		C2	Server	X								X	
		C3	Perangkat penyimpanan			X						X	
		C4	Perangkat keras		X						X		
		C5	Perangkat lunak		X	X					X		
		C6	Cloud computing	X								X	

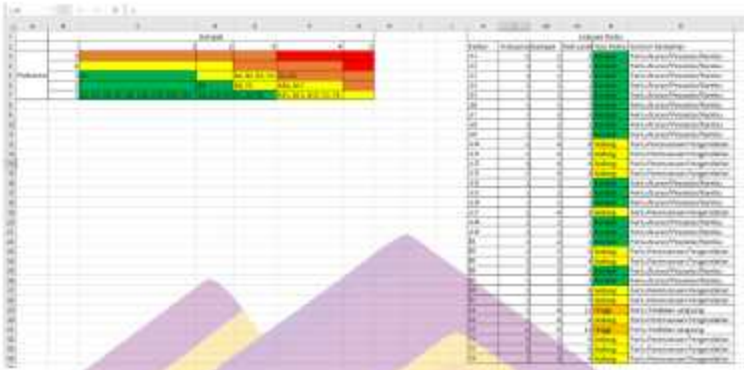
A. **Petunjuk Pengisian Kuesioner.**
   a. Jawaban menyatakan persepsi Bapak/Ibu terhadap (frekuensi) yang terjadi, dan pengaruh risiko terhadap sistem kearsipan.
   b. Pengisian kuesioner dilakukan dengan memberi tanda ☑ atau X pada kolom yang telah disediakan

B. **Keterangan Penilaian**
   1. Sangat Jarang (SJ) = Jarang (hampir tidak mungkin) terjadi pada kondisi tertentu (dalam kurun 1 kali terjadi selama 2 tahun)
   2. Jarang (J) = Kemungkinan kecil terjadi pada setiap kondisi (1x dalam 2 tahun)
   3. Terkadang (T) = Mungkin terjadi pada kondisi tertentu (1-2 kali dalam 2 tahun)
   4. Sering (S) = Kemungkinan besar terjadi pada setiap kondisi (2x dalam 2 tahun)
   5. Sangat Sering (SS) = Hampir pasti terjadi pada setiap kondisi (lebih dari 2x dalam 2 tahun)

C. **Keterangan untuk penilaian**

Tingkat kerugian meliputi Reputasi dan Finansial pada perusahaan.

1. Tidak ada pengaruh = Tidak ada kerugian
2. Rendah = Kerugian <5%
3. Sedang = Kerugian 5% - 10%
4. Tinggi = Kerugian 10% – 20%
5. Sangat tinggi = Kerugian >20%



123. Identifikasi potensi ancaman keamanan pada sistem yang digunakan.

a. Sistem distribusi data kepada karyawan jarak jauh yang dinilai masih belum optimal keamanannya. Menilai dari riwayat kejadian bencana yang terjadi, cukup besar dampak yang ditimbulkan.

124. Rencana pengelolaan risiko.

Dalam rencana pengelolaan risiko selama ini, Scaleout belum memiliki rencana yang terstruktur dari segala macam risiko keamanan.

125. Kebijakan identitas dan akses.

a. Sistem akses jarak jauh: Karyawan yang bekerja dari jarak jauh harus memiliki akses yang terbatas ke sistem dan data, serta hanya melalui koneksi yang aman dan diizinkan.

b. Manajemen hak akses: Manajemen hak akses mencakup pemberian akses hanya pada data yang diperlukan dan memastikan bahwa hak akses tersebut dihapus atau dikurangi ketika karyawan tidak lagi memerlukan akses tersebut.

c. Kebijakan penghapusan: Kebijakan identitas dan akses harus mencakup prosedur penghapusan hak akses akun karyawan yang tidak lagi aktif atau diperlukan.

126. Rencana pemulihan bencana.

Dalam rencana pemulihan bencana selama ini, Scaleout belum memiliki rencana yang terstruktur dari segala macam risiko keamanan.

127. Hasil audit keamanan.

Belum pernah dilakukan audit keamanan di Scaleout Creative Agency

128. Data tentang aset digital yang dimiliki oleh agensi kreatif dan informasi tentang bagaimana aset tersebut dikelola dan dilindungi.

Aset dikelola dan dilindungi dengan enkripsi data yang telah di sediakan oleh pihak ketiga.

a. Inventarisasi aset digital:

i. Domain website : www.scaleout.id

ii. Akun media sosial

1. https://web.facebook.com/scaleout.id/
2. https://www.instagram.com/scaleout.id/
3. https://www.youtube.com/channel/UCaQ3bBqIn0S5hCU0Mk6vXIw

iii. Konten website

Semua konten ada di akun media sosial.

iv. Desain grafis (logo)

SCALEOUT.ID

v. Perangkat lunak

No.	Nama Aplikasi
1.	Adobe Premiere Pro 2020
2.	Adobe After Effects 2020
3.	Adobe Photoshop 2022
4.	Adobe Illustrator 2020
5.	Adobe Lightroom Classic
6.	Adobe Audition 2020
7.	Canva online
8.	Capcut
9.	Microsoft Office 2019

10.	Google Chrome Browser
11.	Firefox Browser
12.	Telegram
13.	WhatsApp
14.	Media Player Classic
15.	Zoom
16.	Corel Draw
17.	Internet Download Manager
18.	Format Factory
19.	Celtx Scriptwriter

vi. Aplikasi bisnis

No.	Nama Aplikasi
1.	Meta Ads
2.	Facebook
3.	Google drive
4.	Telegram
5.	WhatsApp
6.	Microsoft Office 2019
7.	Google Chrome Browser
8.	Firefox Browser

9.	Zoom
10.	Figma
11.	Google Ads
12.	Notes
13.	Tiktok
14.	Instagram
15.	Youtube
16.	M-Banking

vii. Data pelanggan dan klien

1. Daikin
2. Lumecolors
3. Hyundai
4. Tugu Jogja
5. LinkAja
6. Milagros
7. Kutus Kutus
8. Noera
9. Hamzah Batik
10. Kanjeng Heritage
11. Oriflakes
12. Dan lebih banyak lagi

viii. Email dan kontak bisnis

Website: https://scaleout.id/

No. Telp.:

ix. Proyek kreatif yang sedang berjalan

1. Oriflakes
2. Hamzah Batik Malioboro
3. Halte Tour

x. Server dan sistem penyimpanan data

1. Google Drive
2. Hard disk komputer

xi. Hak cipta atas karya kreatif yang dihasilkan oleh agensi

Belum ada hak cipta yang diterbitkan oleh Scaleout Creative Agency

129. Pengalaman dan pemahaman tentang ancaman keamanan dan risiko yang berpotensi terjadi terkait dengan fleksibilitas dan aksesibilitas dalam pengembangan arsitektur TI pada agensi kreatif, termasuk pemahaman tentang praktik terbaik dalam mengurangi risiko tersebut.

a. Ancaman keamanan jaringan: Risiko ini muncul ketika jaringan perusahaan tidak dilindungi dengan baik. Hal ini dapat menyebabkan penipuan, pencurian data, dan serangan jaringan. Oleh karena itu, perusahaan perlu mengimplementasikan sistem keamanan jaringan yang kuat dan mengaktifkan firewall dan sistem deteksi intrusi.

b. Kehilangan data: Risiko ini terjadi ketika data perusahaan hilang karena kegagalan perangkat keras atau perangkat lunak, serangan virus atau malware, atau kesalahan manusia. Untuk menghindari risiko ini, perusahaan perlu mempertahankan sistem backup yang baik dan menguji keandalannya secara teratur.

c. Ancaman phishing: Risiko ini terjadi ketika karyawan agensi kreatif menjadi korban serangan phishing. Dalam serangan phishing, penjahat mencoba untuk mendapatkan informasi pribadi karyawan dengan mengirim email palsu atau pesan instan. Untuk mengurangi risiko ini, perusahaan harus melatih karyawan tentang cara mengidentifikasi dan menghindari serangan phishing.

d. Risiko keamanan perangkat mobile: Dalam lingkungan kerja jarak jauh, karyawan sering menggunakan perangkat mobile untuk bekerja. Namun, risiko keamanan seperti pencurian perangkat, akses tidak sah ke informasi, dan malware dapat mengancam keamanan informasi perusahaan. Untuk mengatasi risiko ini, perusahaan harus memperkuat

keamanan perangkat mobile dan mengimplementasikan perangkat lunak manajemen perangkat mobile (MDM).

e. Risiko keamanan vendor: Risiko ini terjadi ketika agensi kreatif bergantung pada vendor yang kurang memiliki sistem keamanan yang kuat. Hal ini dapat menyebabkan kebocoran informasi dan akses tidak sah ke jaringan perusahaan. Untuk mengurangi risiko ini, perusahaan harus melakukan evaluasi keamanan vendor secara teratur dan menetapkan persyaratan keamanan yang ketat dalam kontrak dengan vendor.

130. Informasi tentang perubahan arsitektur keamanan yang diperlukan untuk meningkatkan fleksibilitas dan aksesibilitas sistem.

Belum ada arsitektur keamanan yang diterapkan di Scaleout Creative Agency, diharapkan dari penelitian yang dilakukan oleh Sdr. Alvian Trias Kurniawan, dapat memberikan perubahan mengenai arsitektur keamanan untuk meningkatkan fleksibilitas dan aksesibilitas.

3. Expert Judgement

Presentasi expert judgement & tanggapan dari para stakeholder