LAMPIRAN I

ANALISIS RISIKO

No	Nama Aset	Nilai Confidentiality	Nilai Availability	Nilai Integrity
1	Database Myportal (ITSM)			
2	Database Aplikasi Internal			
3	Laptop			
4	*Personal Computer* (PC)			
5	Server On-Premise			
6	Server On-Cloud			
7	Windows Server 2012 R2			
8	Windows 10			
9	Microsoft Office 2013			
10	Microsoft Office 365 (E3 & E1)			
11	*Air Conditioner* (AC) Ruang Server			
12	*Uninterruptible Power Supply (UPS)* Ruang Server			
13	*Fiber Optic*			
14	Kabel UTP (*Un-Twisted Pair*)			
15	CCTV			
16	*Switch*			
17	*Router Firewall*			
18	*Access Point*			
19	Aplikasi ITSM			
20	SQL Server Management Studio (SSMS)			
21	Trendmicro Antivirus			

22	*Server Storage*			
23	Rak Server			
24	*Access Door*			
25	*Access Door Management*			

LAMPIRAN II

ANALISIS RISIKO

Aset Kritis	Ancaman	Keterangan	Probabilitas			Dampak		
			Rendah	Sedang	Tinggi	Reputasi	keuangan	Produktifitas
Sistem Manajemen *Service*	Pencurian kode program	Perlindungan terhadap *malicious code and mobile code*	✓	-	-	-	S	-
	Penyalahgunaan akses	Manajemen keamanan jaringan	-	✓	-	-	-	S
	Pengguna salah memberikan biodata saat pembuatan *Active Directory*	Manajemen akses pengguna	-	✓	-	-	-	S
	Password sistem diketahui oleh pihak yang tidak berwenang sehingga hak akses spesial dapat digunakan	Manajemen akses pengguna	✓	-	-	S	-	R
	Sharing password	Manajemen akses pengguna	-	✓	-	-	-	R
Jaringan	Kesalahan mengakses perangkat	Klasifikasi informasi	-	✓	-	-	-	R
	Penyalahgunaan akses jaringan	Manajemen keamanan jaringan	-	✓	-	-	-	S
	Kesalahan mengakses *port* pada perangkat	Klasifikasi informasi	✓	-	-	R	-	R

	Rusaknya komponen fisik jaringan seperti switch, router, dll	Manajemen keamanan jaringan	-	✓	-	-	R	R
	Pencurian komponen fisik jaringan seperti switch, router, dll	Klasifikasi informasi	-	✓	-	-	R	S
	Kesalahan penempatan perangkat jaringan tidak pada tempatnya (*rack server*)	Klasifikasi informasi	-	✓	-	S	-	S
	Perubahan konfigurasi perangkat jaringan oleh pihak yang tidak berwenang	Klasifikasi informasi	✓	-	-	S	-	R
	Kabel putus	Keamanan Peralatan	✓	-	-	-	R	S
	Penempatan kabel tidak rapi	Keamanan Peralatan	✓	-	-	-	-	R
	Penyadapan informasi melalui jaringan	Manajemen keamanan jaringan	-	✓	-	S	-	R
	Konfigurasi komponen fisik jaringan oleh pihak yang tidak berkepentingan	Manajemen keamanan jaringan	✓	-	-	R	-	R
	Rusaknya modem karena kelebihan beban kerja	Manajemen keamanan jaringan	-	✓	-	-	R	S
	Kesalahan dalam konfigurasi perangkat jaringan (*human error*)	Manajemen keamanan jaringan	✓	-	-	-	-	R

	Ketidakstabilan jaringan area lokal	Pengendalian akses jaringan	✓	-	-	-	-	R
	Beban jaringan VPN terlalu besar	Mobile computing dan kerja jarak jauh (teleworking)	✓	-	-	-	-	R
Perangkat Komputer	Kehilangan aset	Tanggung Jawab terhadap Aset	-	✓	-	-	S	R
	Kerusakan aset	Tanggung Jawab terhadap Aset	✓	-	-	-	R	S
	Kabel putus	Keamanan Peralatan	✓	-	-	R	R	S
	Penempatan kabel tidak rapi	Keamanan Peralatan	✓	-	-	R	-	R
	Masuknya virus/malware	Perlindungan terhadap malicious and mobile code	✓	-	-	R	-	S
Server	Penempatan kabel tidak rapi	Keamanan Peralatan	✓	-	-	R	-	R
	Masuknya virus/malware	Perlindungan terhadap malicious and mobile code	✓	-	-	S	-	S
	Konfigurasi komponen fisik jaringan oleh pihak yang tidak berkepentingan	Manajemen keamanan jaringan	✓	-	-	R	-	R
	Pencurian Server dan atau komponennya	Keamanan Peralatan	-	✓	-	S	R	S
	Kebakaran pada ruang server	Perlindungan terhadap ancaman eksternal dan lingkungan	-	-	✓	S	S	T

	Server gagal *backup*	*Back-up*	-	✓	-	S	-	R
	Password server diketahui oleh orang lain	Manajemen akses pengguna	-	✓	-	R	-	S
	Matinya aliran listrik	Keamanan Peralatan	-	✓	-	S	R	T
	Sharing password	Manajemen akses pengguna	✓	-	-	R	-	R
	Pengguna belum memiliki akses	Manajemen akses pengguna	✓	-	-	-	-	R
	Kesalahan dalam konfigurasi server (*human error*)	Manajemen keamanan jaringan	✓	-	-	R	-	S
	Kesalahan pengetikan biodata pengguna saat pembuatan *Active Directory*	Manajemen akses pengguna	✓	-	-	-	-	R
	Serangan dari luar (*brute force,* DoS*)*	Manajemen akses pengguna	-	✓	-	S	-	S

Berikut adalah penjelasan mengenai sistem penilaian Analisis Risiko, yaitu :

R (Rendah) artinya dampak yang ditimbulkan dari sebuah ancaman tidak terlalu berpengaruh besar terhadap sebuah perusahaan, namun perusahaan tetap mengalami kerugian dari segi produktifitas, reputasi, ataupun keuangan.

S (Sedang) artinya dampak yang ditimbulkan dari sebuah ancaman cukup berpengaruh terhadap sebuah perusahaan dan kerugian yang ditimbulkan menyebabkan perusahaan membuat sebuah upaya pencegahan yang lebih dari penilaian tingkat Rendah untuk meminimalisir ancaman/insiden terjadi kembali. Insiden yang terjadi

pada tingkat ini dilakukan pencatatan supaya tetap dapat dilihat riwayat terjadinya insiden dan cara penanggulangannya.

T (Tinggi) artinya dampak yang ditimbulkan dari sebuah ancaman berpengaruh besar terhadap sebuah perusahaan dan kerugian yang ditimbulkan sangat berpengaruh terhadap produktifitas, reputasi, dan keuangan perusahaan, maka dari itu ancaman tingkat ini menjadi perhatian lebih bagi perusahaan agar dapat tetap dicegah sebelum menimbulkan dampak yang lebih parah. Insiden yang terjadi pada tingkat ini dilakukan pencatatan supaya tetap dapat dilihat riwayat terjadinya insiden dan cara penanggulangannya.

LAMPIRAN III
LEMBAR KUESIONER

Kepada,
Kepala Dept. IT Technical & Service
PT Asuransi Jiwa BCA
Di tempat

Responden yang terhormat,

Saya Ari Setiawan (20170801240) adalah Mahasiswa Program Studi Teknik Informatika Universitas Esa Unggul Jakarta yang sedang melakukan penelitian tentang Perancangan Implementasi Jaringan Dengan Berbasis ISO 27001 Pada PT Asuransi Jiwa BCA. Penelitian ini adalah bagian dari Tugas Akhir sebagai salah satu syarat untuk mendapatkan gelar Sarjana Komputer bagi peneliti. Demi tercapainya hasil yang diinginkan, peneliti mohon kesediaan Bapak/Ibu untuk berpartisipasi mengisi kuesioner ini secara lengkap dan benar.

Kuesioner ini bertujuan untuk mendapatkan data dan opini Bapak/Ibu mengenai proses pengelolaan keamanan teknologi informasi di PT Asuransi Jiwa BCA. Informasi yang diterima dari kuesioner ini bersifat rahasia dan hanya digunkana untuk kepentingan akademis. Tidak ada jawaban yang salah dalam menjawab kuesioner ini. Atas bantuannya saya ucapkan terima kasih.

Jakarta, Januari 2021

Ari Setiawan

Petunjuk Pengisian

Bacalah pernyataan kriteria dari tingkat kematangan dengan seksama. Masing-masing pernyataan memiliki 5 (lima) pilihan jawaban yang menunjukkan tingkat kematangan terhadap atribut tertentu pada proses pengelolaan keamanan jaringan komputer. Pilihan-pilihan jawaban tersebut dari

1 sampai 5 secara berturut-turut mempresentasikan tingkat kapabilitas yang semakin meningkat terhadap suatu atribut pada proses pengelolaan keamanan teknologi informasi. Dimana (1) performed informaslly, (2) planned and tracked, (3) well defined, (4) quantitatively controlled, dan (5) continously improving.

Pada kolom "Jawaban", responden dapat memilih salah satu jawaban yang dianggap bisa mewakili kondisi kapabilitas saat ini, terkait dengan atribut kapabilitas tertentu dalam proses pengelolaan keamanan jaringan komputer dengan memberikan tanda ceklis (✓) pada tempat yang tersedia. Dengan mengetahui posisi kapabilitas saat ini selanjutnya akan dilakukan analisis yang dapat menjadi dasar pendefinisian rancangan solusi untuk perbaikan dalam proses pengelolaan keamanan jaringan komputer.

Untuk kebutuhan diatas mohon kiranya Bapak/Ibu sebagai responden dapat memberikan jawaban atas pernyataan-pernyataan yang diberikan dalam kuesioner ini untuk kemudian dapat saya olah dalam penelitian tugas akhir ini.

Nama Responden :
Jabatan Responden :

Berikut penjelasan mengenai sistem penilaian kemampuan berdasarkan *System Security Engineering Capability Maturity Model* (SSE-CMM) adalah :

Level 1 ***Performed*** **(Dilakukan informal)** artinya kinerja belum sepenuhnya direncanakan dan dilacak, kinerja tergantung pada pengetahuan individu dan organisasi. Serta tidak ada peraturan tertulis untuk melaksanakan tindakan, perintah pelaksanaan dilakukan hanya melalui lisan.

Level 2 ***Managed*** **(Dikelola)** artinya kinerja sesuai prosedur yang sudah diverifikasi. Hasil kerja sesuai dengan persyaratan. Perbedaan dengan proses level 1 adalah bahwa proses kinerja pada level 2 telah direncanakan dan dikelola.

Level 3	***Well Defined* (Didefinisikan dengan Baik)** artinya kinerja pada level ini dilakukan sesuai dengan persetujuan, sesuai dengan standar yang telah ada, dan proses telah didokumentasikan. Perbedaan dengan proses level 2 adalah bahwa proses kinerja pada level ini direncanakan dan dikelola dengan menggunakan standar yang ditetapkan organisasi.
Level 4	***Quantitatively Managed* (Dikelola secara Kuantitatif)** artinya langkah-langkah detail pada proses kinerja dikumpulkan dan dianalisis. Ini mengarah ke pemahaman kuantitatif terhadap kemampuan proses dan kemampuan untuk meningkatkan kinerja. Perbedaan dengan level 3 adalah bahwa proses kinerja pada level ini didefinisikan, dipahami, dan dikendalikan secara kuantitatif. Perbedaan dengan level 3 adalah bahwa proses kinerja pada level ini didefinisikan, dipahami, dan dikendalikan secara kuantitatif.
Level 5	**Optimizing (Mengoptimalkan)** perbedaan dengan proses level 4 adalah bahwa proses pada level ini didefinisikan dan proses telah sesuai dengan standar dan dilakukan perbaikan dan peningkatan secara terus-menerus. Proses kinerja ini didasarkan pada pemahaman kuantitatif dari dampak akibat perubahan proses.

8	**Pengelolaan Aset**					
8.1	**Tanggung Jawab Terhadap Aset**					
8.1.1	**Inventaris Aset**					
Sasaran: Untuk mengenali aset organisasi dan menetapkan tanggung jawab perlindungan yang sesuai.						
No	**Pernyataan**	**1**	**2**	**3**	**4**	**5**
1	Aset yang terkait dengan informasi dan fasilitas pemrosesan informasi harus diidentifikasi dan inventarisasi aset harus dibuat dan dipelihara.					
2	Semua inventaris dari aset penting dicatat dan dipelihara.					
3	Aset yang relevan dalam siklus hidup informasi (pembuatan, pemrosesan, penyimpanan, transmisi, penghapusan, dan					

	penghancuran) harus diidentifikasi dan dokumentasinya dibuat dan disimpan dalam inventaris khusus.					

8	**Pengelolaan Aset**					
8.1	**Tanggung Jawab Terhadap Aset**					
8.1.2	**Kepemilikan Aset**					
Sasaran: Untuk mengenali aset organisasi dan menetapkan tanggung jawab perlindungan yang sesuai.						
No	**Pernyataan**	**1**	**2**	**3**	**4**	**5**
1	Organisasi dapat menentukan aset yang diinventariskan					
2	Penanganan yang tepat ibla aset dihapus atau dihancurkan					
3	Organisasi dapat menentukan pengklasifikasian aset dan perlindungan yang tepat					

8	**Pengelolaan Aset**					
8.2	**Klasifikasi Informasi**					
8.2.2	**Pelabelan Informasi**					
Sasaran: Untuk memastikan bahwa informasi mendapatkan tingkat perlindungan yang layak berdasarkan kepentingannya di dalam organisasi.						
No	**Pernyataan**	**1**	**2**	**3**	**4**	**5**
1	Terdapat skema klasifikasi informasi, yang digunakan untuk klasifikasi dan kriteria informasi untuk meninjau klasifikasi dari waktu ke waktu.					
2	Skema klasifikasi informasi harus berdasarkan kerahasiaan, integritas, dan ketersediaan.					
3	Skema klasifikasi informasi bersifat konsisten di dalam organisasi.					
4	Hasil klasifikasi informasi harus menunjukkan nilai aset.					
5	Hasil klasifikasi informasi diperbaharui sesuai dengan perubahan nilai aset dan kekritisan aset.					

9	Kendali Akses					
9.2	Manajemen Akses Pengguna					
9.2.1	Registrasi dan Pembatalan Registrasi					
Sasaran: Untuk mencegah akses fisik oleh pihak yang tidak berwenang, kerusakan dan interferensi terhadap lokasi dan informasi organisasi.						
No	**Pernyataan**	**1**	**2**	**3**	**4**	**5**
1	Adanya prosedur terkait dengan tata cara pendafataran atau pembatalan pendaftaran pengguna atau karyawan pada sistem perusahaan.					
2	Adanya manajemen kerentanan terhadap pengguna pada sistem.					
3	Adanya kebijakan pemberian dan pembatasan hak ases terhadap pengguna pada sistem perusahaan					
4	Adanya peninjauan kembali hak akses secara berkala dan penghapusan hak akses apabila tidak sesuai.					
5	Pemilik aset menentukan aturan akses kontrol yang tepat, hak akses dan pembatasan aturan pengguna terhadap aset mereka.					

9	Kendali Akses					
9.2	Manajemen Akses Pengguna					
9.2.6	Penghapusan Atau Penyesuaian Hak Akses					
Sasaran: Untuk memastikan akses pengguna yang berwenang dan untuk mencegah akses oleh pihak yang tidak berwenang ke sistem dan layanan.						
No	**Pernyataan**	**1**	**2**	**3**	**4**	**5**
1	Adanya manajemen kerentanan terhadap *password* pengguna pada sistem.					
2	Adanya pengendalian manajemen terkait alokasi *password* pengguna					
3	Adanya pembatasan kesalahan masukan *password*.					
4	Konsistensi antara hak - hak akses dan informasi klasifikasi kebijakan sistem dan jaringan					
5	Aturan khusus yang dibutuhkan terkait sebelum berlakunya persetujuan dan tidak disetujui					

11	Keamanan Fisik dan Lingkungan					
11.1	Area Aman					
11.1.2	Kendali masuk fisik					
Sasaran: Untuk mencegah akses fisik yang tidak sah, kerusakan dan interferensi terhadap informasi dan fasilitas pengolahan informasi organisasi.						
No	**Pernyataan**	**1**	**2**	**3**	**4**	**5**
1	Ruang Lingkup keamanan harus didefinisikan dan penempatan serta kekuatan lain pada lingkup berdasarkan kebutuhan keamanan aset dan hasil dari penilaian risiko.					
2	Tersedianya area penerima tamu untuk mengontrol akses fisik (seperti membatasi otorisasi, hanya untuk pegawai)					
3	Lingkup lokasi yang termasuk fasilitas pemrosesan informasi harus memiliki bunyi dan terkunci (seperti *access door*)					

11	Keamanan Fisik dan Lingkungan					
11.1	Area Aman					
11.1.3	Mengamankan Kantor, Ruangan dan Fasilitas					
Sasaran: Untuk mencegah akses fisik yang tidak sah, kerusakan dan interferensi terhadap informasi dan fasilitas pengolahan informasi organisasi.						
No	**Pernyataan**	**1**	**2**	**3**	**4**	**5**
1	Tersedianya dokumen pencatatan aktifitas keluar masuk ruangan atau fasilitas pemrosesan informasi sebagai pencegahan terhadap pegawai yang tidak memiliki akses.					
2	Lingkup lokasi yang termasuk fasilitas pemrosesan informasi harus memiliki bunyi dan selalu tertutup atau terkunci.					

12	Keamanan Operasi					
12.2	Perlindungan Dari Malware					
12.2.1	Kendali Terhadap Malware					
Sasaran: Untuk memastikan informasi dan fasilitas pengolahan informasi terlindungi dari malware.						
No	**Pernyataan**	**1**	**2**	**3**	**4**	**5**

1	Terdapat kebijakan mengenai penggunaan perangkat lunak yang resmi beserta pengontrolannya.					
2	Adanya kontrol untuk mencegah dan mendeteksi perangkat lunak yang tidak sah serta penggunaan situs berbahaya yang dicurigai.					
3	Adanya kebijakan terkait degan sumber yang digunakan untuk mendapatkan file dan software untuk mencegah risiko.					
4	Adanya manajemen kerentanan terhadap malicious code atau malware.					
5	Tinjauan rutin perangkat lunak dan konten data sistem yang mendukung proses bisnis yang penting.					

12	**Keamanan Operasi**					
12.3	**Cadangan (*Backup*)**					
12.3.1	**Cadangan Informasi**					
Sasaran: Untuk melindungi dari kehilangan data						
No	**Pernyataan**	**1**	**2**	**3**	**4**	**5**
1	Kebijakan backup informasi yang mencakup pertahanan dan perlindungan informasi.					
2	Tersedianya fasilitas backup informasi yang memadai untuk memastikan informasi penting dapat dipulihkan setelah terjadi insiden atau kegagalan media.					
3	Pencatatan backup informasi yang akurat dan lengkap serta dokumentasi prosedur perbaikan.					
4	Penyimpanan backup di tempat yang aman dan jarak yang cukup.					
5	Tingkat perlindungan fisik dan ligkungan backup informasi yang konsisten sesuai dengan standar yang diterapkan pada lokasi utama organisasi.					
6	Adanya pengujian media backup secara berkala.					
7	Penggunaan enkripsi pada backup.					

13	Keamanan Komunikasi					
13.1	Manajemen Keamanan Jaringan					
13.1.1	Kendali Jaringan					
Sasaran: Untuk menjamin perlindungan informasi dalam jaringan dan fasilitas pendukung pengolahan informasi.						
No	**Pernyataan**	**1**	**2**	**3**	**4**	**5**
1	Penetapan tanggung jawab dan prosedur untuk pengelolaan peralatan jaringan.					
2	Adanya pemisahan tanggung jawab operasional untuk jaringan dengan operasional yang lain.					
3	Adanya pemantauan dan tindakan memutus akses sesuai untuk mendeteksi tindakan yang dapat berpengaruh terhadap keamanan informasi.					
4	Adanya autentikasi sistem di jaringan.					
5	Pembatasan koneksi sistem ke jaringan.					
6	Adanya koordinasi manajemen untuk mengoptimalkan layanan kepada organisasi.					
7	Adanya kebijakan yang mengatur jaringan dan layanan jaringan mana yang diizinkan untuk diakses.					

LAMPIRAN IV

LEMBAR PENILAIAN BIA

Nama Responden : Vincent Darmawan, S. Kom, M. Mkom

Jabatan Responden : Kepala Dept. IT *Infrastructure*

No	Nama Aset	Nilai BIA	Keterangan
1	Database Myportal (ITSM)		
2	Database Aplikasi Internal		
3	Laptop		
4	*Personal Computer* (PC)		
5	Server On-Premise		
6	Server On-Cloud		
7	Windows Server 2012 R2		
8	Windows 10		
9	Microsoft Office 2013		
10	Microsoft Office 365 (E3 & E1)		
11	*Air Conditioner* (AC) Ruang Server		
12	*Uninterruptible Power Supply (UPS)* Ruang Server		
13	*Fiber Optic*		
14	Kabel UTP (*Un-Twisted Pair*)		
15	CCTV		
16	*Switch*		
17	*Router Firewall*		
18	*Access Point*		
19	Aplikasi ITSM		
20	SQL Server Management Studio (SSMS)		
21	Trendmicro Antivirus		
22	*Server Storage*		
23	Rak Server		
24	*Access Door*		
25	*Access Door Management*		

LAMPIRAN V

LEMBAR WAWANCARA

Responden : Vincent Darmawan, S. Kom, M. Mkom

Jabatan : Kepala Dept. IT *Infrastructure*

Pewawancara : Ari Setiawan

Tanggal : 18 Desember 2020

Tempat : *Online* melalui telepon

1	**P:**	**Apakah tugas dari Departemen IT *Technical & Services* ?**
	N:	Mengawasi, menyediakan informasi dan melayani kebutuhan teknologi informasi para pegawai pada PT Asuransi Jiwa BCA yang bersifat teknis maupun non-teknis
2	**P:**	**Apa saja contoh data yang dikelola oleh Departemen IT *Technical & Services* ?**
	N:	Ada beberapa data yang dikelola pada Dept. IT *Technical & Services* salah beberapa diantaranya yaitu keamanan dan kehandalan infrastruktur komputer serta perangkat pendukungnya
3	**P:**	**Apakah ada SOP tertulis untuk manajemen keamanan jaringan dan informasi ?**
	N:	Iya ada
4	**P:**	**Pernahkan terjadi ancaman atau insiden terkait dengan keamanan jaringan dan informasi ? Jika ada insidennya seperti apa ?**
	N:	Pernah sempat ada, contohnya beberapa melalui *email* spam yang isinya ancaman kepada karyawan atau menghimbau karyawan untuk mengganti *password*-nya dengan *password* baru melalui link yang mereka berikan. Ada beberapa dari karyawan yang terkecoh dan melakukan klik pada link yang diberikan
5	**P:**	**Apakah ada dampak/kerugian yang ditimbulkan dari ancaman/insiden yang pernah terjadi ?**
	N:	Dampak yang terjadi akibat masalah dari *spamming email* yang kita dapat yaitu *hacker* yang mengirimi pesan tersebut mendapatkan beberapa informasi dari karyawan seperti username, jabatan, dan password lama
6	**P:**	**Apakah ada langkah yang dilakukan untuk memperbaiki akibat dari insiden yang terjadi? Dan apakah memerlukan biaya untuk memperbaikinya ?**
	N:	Ada tergantung dari insiden yang terjadi, kita mengambil contoh insiden *spamming email* dan langkah yang kita lakukan yaitu memberitahu karyawan agar langsung mengganti seluruh *password* yang digunakan baik itu *password login* windows, *password email* ataupun *password* aplikasi

		internal yang mereka gunakan dan mengharuskan karyawan untuk mengganti passwordnya secara berkala 3 bulan sekali. Untuk masalah *spamming email* ini tidak memerlukan biaya, namun sebagai tindak pencegahan lebih lanjut dari sisi IT *Technical & Services* langsung melakukan uji coba *penetration testing* internal maupun eksternal dengan menggunakan pihak ketiga untuk menguji apakah ada celah lain yang terbuka akibat masalah tersebut dan untuk sisi eksternal tentu saja membutuhkan biaya.
7	**P:**	**Apakah sampai saat ini, perusahaan ini pernah di evaluasi tata kelola dengan framework-framework yang ada ? (Contoh menggunakan ISO, COBIT, ITIL)**
	N:	Belum ada, hanya audit internal maupun audit eksternal saja, untuk audit eksternalnya dari BCA yang masih dalam satu group dan melalui vendor.
8	**P:**	**Apakah ada pencatatan terhadap aset yang dimiliki oleh PT Asuransi Jiwa BCA ?**
	N:	Ada, pencatatan aset dilakukan oleh departemen lain yang dibantu pihak IT
9	**P:**	**Apa saja aset-aset yang terdapat pada perusahaan ini ?**
	N:	Komputer, Laptop, Meja, Kursi, Telepon, TV, Kulkas, Microwave, Server, Switch, Router, Firewall, Rack server, kartu akses
10	**P:**	**Menurut bapak, perlukah dilakukan audit terhadap sistem manajemen keamanan informasi pada perusahaan ini ?**
	N:	Perlu, supaya dapat meningkatkan kebutuhan sistem jaringan dan informasi yang ada pada perusahaan ini

Responden : Royman Naibaho, S. Kom

Jabatan : Pimpinan IT *Helpdesk*

Pewawancara : Ari Setiawan

Tanggal : 16 Desember 2020

Tempat : Ruang Meeting Balendra PT Asuransi Jiwa BCA

1	**P:**	**Dari hasil wawancara pertama yang telah saya lakukan, didapatkan fakta bahwa PT Asuransi Jiwa BCA memiliki fungsi untuk menyediakan informasi dan melayani kebutuhan teknologi informasi para pegawai, bagaimana cara IT Helpdesk & Service melayani kebutuhan teknologi informasi para pegawai ?**
	N:	Menggunakan sistem ticketing yang disebut ITSM
2	**P:**	**Apakah sistem ticketing tersebut dibuat oleh pihak PT Asuransi Jiwa BCA atau oleh pihak ketiga ? Jika menggunakan pihak ketiga apakah ada perjanjian khusus dengan pihak ketiga untuk melakukan perbaikan secara berkala ?**
	N:	Iya, terdapat perjanjian dengan pihak ketiga
3	**P:**	**Apakah sistem tersebut hanya dapat digunakan oleh pihak IT saja atau pegawai lain dapat menggunakannya juga ? Jika iya, apakah ada sosialisasi cara penggunaan, dan adakah keluhan dari para pegawai?**
	N:	Iya seluruh pegawai dapat menggunakan sistem tersebut dan saat pertama kali pihak departemen lain akan memberitahukan cara menggunakan sistem tersebut dan untuk mengingatkan kembali dari pihak IT akan membantu jika pegawai lainnya kesulitan dalam menggunakan sistem tersebut
4	**P:**	**Apakah ada laporan bulanan mengenai masalah keamanan jaringan dan informasi ?**
	N:	Ada, seluruh pencatatan dikumpulkan dalam satu *bundle* dan dilakukan *review* bulanan untuk melihat apakah ada yang harus diperbaiki atau ditingkatkan lagi dari setiap masalah yang ada kedepannya
5	**P:**	**Apakah di PT Asuransi Jiwa BCA memiliki ruangan dengan akses yang terbatas atau hanya diperbolehkan beberapa pegawai saja yang dapat masuk ?**
	N:	Ada, contohnya salah satu ruangan khusus untuk melakukan akses ke server dan juga ruangan antar departemen dipisahkan oleh pintu yang memiliki akses, jadi pegawai tidak bisa sembarangan asal masuk saja antar departemen satu dengan lainnya
6	**P:**	**Apakah hanya pegawai dari departemen IT *Technical* & *Services* saja yang dapat masuk ke ruang server ?**
	N:	Iya hanya pegawai IT *Technical* & *Services* saja
7	**P:**	**Apakah ada laporan terkait waktu pegawai PT Asuransi Jiwa BCA keluar-masuk ruangan server ?**
	N:	Ada, laporan tersebut masih berbentuk kertas yang ditulis secara manual jika ada pegawai keluar-masuk ke ruang server lalu dimasukkan kedalam satu dokumen

8	**P:**	**Untuk aset yang dimiliki oleh PT Asuransi Jiwa BCA seperti server, komputer, router, switch, ups, dll, apakah ada pemeliharaan rutin untuk menjaga aset tersebut optimal kinerjanya ? Atau apakah pemeliharaan tersebut dilakukan apabila terjadi insiden saja ?**
	N:	Ada pemeliharaan rutin yang dilakukan disini dan jika terjadi insiden dilakukan kembali pemeliharaan secara langsung disaat terjadinya insiden tersebut
9	**P:**	**Untuk server PT Asuransi Jiwa BCA, apakah ada backup rutin untuk menjaga apabila suatu saat terjadi kerusakan/insiden pada server ?**
	N:	Dilakukan backup setiap hari
10	**P:**	**Apakah ada prosedur atau SOP untuk melakukan *backup* server tersebut ? Lalu untuk lokasi *backup* data tersebut apakah menurut bapak sudah aman ?**
	N:	Ada, lokasi *backup* sudah aman

Responden : Sandy Arief Permana, S. Kom, M. Kom

Jabatan : Kepala Dept. IT Security & Governance

Pewawancara : Ari Setiawan

Tanggal : 16 Desember 2020

Tempat : Online melalui teams meeting

1	**P:**	**Apakah sebelumnya PT Asuransi Jiwa BCA sudah pernah dilakukan audit dari sisi keamanan informasinya ?**
	N:	Kalau audit sudah pernah dari audit internal dan dari vendor pihak ketiga, itupun masih secara global
2	**P:**	**Mengenai audit tersebut, berarti yang lebih spesifik mengarah ke evaluasi tata kelola dengan menggunakan framework-framework seperti ISO 27001 atau ITIL apakah sudah pernah ada sebelumnya ?**
	N:	Belum ada, hanya dari audit yang telah saya sebutkan tadi
3	**P:**	**Apakah di PT Asuransi Jiwa BCA ini menggunakan sistem pengawasan untuk perangkat lunak yang tidak resmi ataupun situs-situs yang dilarang dan berbahaya ?**
	N:	Iya kita disini menggunakan sistem keamanan berupa *endpoint security, cloud security* dan juga *firewall*, keduanya berfungsi sebagai pencegahan, pengawasan, dan penanganan terhadap kejahatan siber yang dapat terjadi
4	**P:**	**Bagaimana cara kerja dari perangkat *firewall* yang digunakan untuk pencegahan dari kejahatan siber pada PT Asuransi Jiwa BCA ini ?**
	N:	*Simple*-nya sama seperti perangkat *firewall* pada umumnya, kita membuat *policies* atau aturan pada *firewall* guna melakukan pencegahan berupa *blocking*, *dropping*, *monitoring* dan *sandboxing* pada setiap *traffic* data yang melintas
5	**P:**	**Bagaimana perangkat *endpoint security* dapat mendeteksi adanya perangkat lunak yang tidak resmi ?**
	N:	Sebenarnya sama saja cara kerjanya seperti antivirus, namun perangkat ini lebih canggih karena ada sistem *artificial intelligence* didalamnya yang dapat mendeteksi apabila perangkat lunak yang digunakan tidak bersumber dari situs resminya atau sebut saja aplikasi *crack*.
6	**P:**	**Selain perangkat *endpoint security* dan *firewall* apakah terdapat perangkat pencegahan kejahatan siber lainnya ?**
	N:	Iya ada, kita juga menggunakan sistem *backup* yang terenkripsi dan juga peletakannya ditempat yang berbeda, misalkan ada data yang hilang atau rusak dan data tersebut dibutuhkan kembali kita dapat mengambil data (*restore*) yang dibutuhkan tadi melalui data salinannya, dan data yang hilang ini sudah pasti aman karena terenkripsi.
7	**P:**	**Apakah pernah ada kejadian kerusakan atau kehilangan data sebelumnya ?**
	N:	Ada, tetapi kasusnya bukan karena serangan siber dari pihak luar melainkan karena *human error* atau kesalahan pegawai itu sendiri dan juga setiap beberapa hari data yang ada pada folder tertentu di server penyimpanan kita itu akan terhapus guna meminimalisir penuhnya penyimpanan, oleh karena

		itu pernah ada pegawai yang lupa untuk memindahkan datanya dan meminta data tersebut kepada tim IT dan kami pun segera melakukan *restore* data pada data yang diminta.
8	**P:**	**Apakah ada dokumentasi terkait tata kelola keamanan informasi yang ada pada PT Asuransi Jiwa BCA ?**
	N:	Jika dokumentasi yang dimaksud itu seperti aturan standar operasional, tata cara penggunaan suatu perangkat atau *software*, iya kita ada dan menyimpannya menjadi satu dokumen pada rak khusus dan juga pada *file server*.
9	**P:**	**Jika dokumen yang tadi dijelaskan disimpan dalam *file server*, berarti dokumen tersebut dapat dilihat oleh pegawai dari lain divisi ? Mengapa ?**
	N:	Tentu saja tidak, karena dalam *file server* kita menggunakan *rules* pada GPO (*Group Policy Object*) Windows Server yang mana hanya pegawai dari divisi yang sama saja atau pegawai yang diberikan akses saja yang dapat melihat isi suatu folder yang ada pada *file server*, jadi tidak bisa dikonsumsi oleh sembarang pegawai.
10	**P:**	**Terkait hak akses, apakah ada aturan yang membatasi pegawai untuk melakukan pekerjaannya dalam kantor selain pada *file servevr* tadi, contohnya seperti menggunakan aplikasi tertentu pada laptop atau komputer, perizinan menggunakan ruangan tertentu, *browsing*, dan menggunakan perangkat tambahan pada laptop seperti *flashdisk* ? Jika ada apakah membutuhkan dokumen khusus untuk membuka akses yang tidak diperbolehkan tadi ?**
	N:	Iya betul kami menggunakan aturan yang membatasi pergerakan pegawai dalam menjalankan operasional menggunakan perangkat kantor, tujuannya kembali lagi guna menjaga keamanan dan kelancaran operasional perusahaan, tetapi jika ada pegawai yang membutuhkan akses khusus untuk membuka aplikasi atau website yang diblokir contohnya seperti yahoo atau google drive atau dapat mencolok *flashdisk* pegawai yang bersangkutan harus membuat sebuah dokumen pengecualian sebagai syaratnya.

LAMPIRAN VI

SURAT PERMOHONAN IZIN PENELITIAN

Universitas Esa Unggul
Fakultas Ilmu Komputer

Jakarta, 12 Agustus 2022

Nomor : 81-053/SP/KAPRODI-IF/FASILKOM/UEU/EXT/VIII/2022
Lampiran : -
Perihal : *Surat Permohonan Izin Untuk Penelitian*

Kepada Head of IT Technical & Services
PT Asuransi Jiwa BCA Chase Plaza,
Jl. Jendral Sudirman, Kuningan, Setiabudi,
Jakarta Selatan, DKI Jakarta 12920

Dengan Hormat,

Sehubungan dengan mata kuliah Tugas Akhir (Skripsi) yang memerlukan data dan informasi bagi mahasiswa Fakultas Ilmu Komputer Program Studi Teknik Informatika, bersama ini kami sampaikan bahwa mahasiswa kami bermaksud untuk mencari beberapa data / informasi. Adapun nama mahasiswa tersebut adalah :

NIM	Nama	No HP	Judul Skripsi
20170801240	Ari Setiawan	085716737556	Perancangan Implementasi Jaringan dengan Berbasis ISO 27001 pada PT Asuransi Jiwa BCA

Kami berharap Bapak/Ibu memberikan izin penelitian untuk Mahasiswa tersebut.

Demikianlah atas perhatian dan kerjasamanya, kami ucapkan terima kasih

Hormat kami,

Universitas Esa Unggul

M.Bahrul Ulum, S.Kom, M.Kom
Kaprodi Teknik Informatika

C.c : 1. Arsip

Note : pada saat pengambilan data bisa mengikuti protokol covid (memakai masker, handsanitizer dan pengecekan suhu tubuh, dan sangat disarankan untuk mengambil data secara online).

Jl. Arjuna Utara 9, Tol Tomang, Kebon Jeruk, Jakarta 11510, Indonesia
(021) 567 4223 ext. 206, 207 (021) 567 4248
www.esaunggul.ac.id

LAMPIRAN VII

SURAT KONFIRMASI PERSETUJUAN PENELITIAN

BCAlife

Jakarta, 15 Agustus 2022

Nomor : **010/ITE/BCAL/VIII/2022**
Perihal : **Konfirmasi Persetujuan Penelitian**

Kepada Yth:
M. Bahrul Ulum, S.Kom, M.Kom
Ketua Program Studi Fakultas Teknik Informatika
Universitas Esa Unggul
Kebon Jeruk, Jakarta Barat

Dengan Hormat,
Berdasarkan surat nomor 81-053/SP/KAPRODI-IF/FASILKOM/UEU/EXT/VIII/2022 perihal permohonan izin penelitian kepada mahasiswa :

Nama	:	Ari Setiawan
NIM	:	20170801240
Program Studi	:	Teknik Informatika
Semester	:	Ganjil 2020/2021

Bersama ini kami menyetujui bahwa mahasiswa tersebut untuk melakukan riset/penelitian pada Divisi IT *Technical & Services* terhitung mulai tanggal 1 Desember 2020 s/d 28 Maret 2021, untuk melakukan wawancara dan pengumpulan data, dengan ketentuan sebagai berikut:

- Semua data yang dipelajari selama riset/penelitian hanya untuk kepentingan akademis dan tidak untuk disebarluaskan.
- Perusahaan tidak memberikan dana selama melaksanakan riset/penelitian.
- Membuat laporan (*softcopy*) hasil riset/penelitian kepada Divisi IT Technical & Services PT Asuransi Jiwa BCA.

Demikian disampaikan, atas perhatian dan kerja sama yang diberikan kami ucapkan terima kasih.

PT Asuransi Jiwa BCA

Aryadi Setiawan
Head of IT Technical & Services