Perancangan Tim Siap Tanggap Insiden Siber-CSIRT: Studi Kualitatif Berdasarkan *Business Impact Analysis* di Bank XYZ

Hendra Yada Putra[1)], M. Izman Herdiansyah[2)], Tata Sutabri[3)]

[1)2)3)] Program Studi Magister Teknik Informatika, Universitas Bina Darma
[*)]Correspondence Author: hendra.yp@gmail.com, Palembang, Indonesia
DOI: https://doi.org/10.37012/jtik.v10i1.1903

Abstrak

Dalam operasional perbankan salah satu risiko yang berpotensi meningkat seiring dengan pemanfaatan TI pada skala yang lebih besar adalah risiko yang ditimbulkan oleh ancaman dan insiden siber karena pemanfaatan TI sudah sebagian besar melalui media siber. Pada Bank XYZ semua insiden keamanan siber dikelola oleh Divisi Teknologi Informasi dan belum ada batasan secara spesifik menangani insiden siber khusus skala besar. Insiden siber khusus skala besar terkait dengan pembentukan Tim kerja dengan fungsi yang tidak hanya melakukan pemulihan insiden secara teknis saja, melainkan juga secara berkolaboratif dari sisi non teknis. Mengingat reputasi bank dipertaruhkan saat pemulihan insiden keamanan berlangsung. Selain itu perlu adanya pengaturan secara spesifik mengenai alur kerja, lingkup layanan dan limit dampak yang akan menjadi trigger kapan tim ini akan mulai bekerja. Diperlukan penelitan dengan tujuan untuk mengembangkan pengelolaan insiden keamanan siber yang lebih efektif dan efisien dalam bentuk perencanaan Tim Siap Tanggap Insiden Siber (TTIS), atau lebih dikenal dengan *Computer Security Incident response Team* (CSIRT) yang mengacu pada tingkat kritikalitas pada analisis *Business Impact Analysis* (BIA). Penelitian mengacu pada standard ISO/TS 22317:2021 sebagai panduan analisis BIA dan ISO/IEC 27035:2023 dalam penyusunan kerja Tim TTIS. Hasil BIA memberikan gambaran yang jelas mengenai tingkat kritikalitas proses bisnis yang dimiliki Bank. Penentuan tingkat kritikalitas sangat membantu dalam penyusunan tim TTIS/CSIRT yang efektif dan efisien dalam upaya penangan insiden keamanan informasi skala besar.

Kata Kunci: *Business Impact Analysis*, *Computer Security Incident response Team*, Kritikalitas

Abstract

In banking operations, one of the risks that has the potential to increase with the use of IT on a larger scale is the risk posed by cyber threats and incidents because the majority of IT use is through cyber media. At Bank XYZ all cyber security incidents are managed by the Information Technology Division and there are no specific restrictions on handling specific large-scale cyber incidents. Specific large-scale cyber incidents are related to the formation of a work team with a function that not only carries out incident recovery technically, but also collaboratively from a non-technical side. Considering the bank's reputation is at stake when security incident recovery takes place. Apart from that, there needs to be specific arrangements regarding work flow, scope of services and impact limits which will trigger when this team will start working. Research is needed with the aim of developing more effective and efficient cyber security incident management in the form of planning a Cyber Incident Ready Response Team (TTIS), or better known as a Computer Security Incident Response Team (CSIRT) which refers to the level of criticality in the Business Impact Analysis analysis (BIA). The research refers to the ISO/TS 22317:2021 standard as a guide for BIA analysis and ISO/IEC 27035:2023 in preparing the work of the TTIS Team. The BIA results provide a clear picture of the level of criticality of the Bank's business processes. Determining the level of criticality is very helpful in forming an effective and efficient TTIS/CSIRT team in efforts to handle large-scale information security incidents.

Keywords: *Business Impact Analysis, Computer Security Incident response Team, Criticality*

PENDAHULUAN

Dalam operasional perbankan salah satu risiko yang berpotensi meningkat seiring dengan pemanfaatan TI pada skala yang lebih besar adalah risiko yang ditimbulkan oleh ancaman dan insiden siber karena pemanfaatan TI sudah sebagian besar melalui media siber. Namun demikian, peningkatan pemanfaatan TI juga berpotensi meningkatkan risiko operasional bagi industri perbankan (POJK 11/OJK.03, 2022). Bank tidak hanya dituntut untuk dapat menjaga keamanan Sistem Elektronik yang dimiliki dari serangan siber, namun juga perlu untuk memiliki kemampuan dalam mendeteksi dan memulihkan keadaan pasca terjadinya insiden siber, sehingga bank diharapkan mampu menerapkan tata kelola serta manajemen risiko yang baik untuk tetap dapat beroperasi dengan memanfaatkan TI sebagaimana mestinya dengan menjaga ketahanan dan keamanan siber (SEOJK 29/OJK.03/2022, 2022).

Divisi Teknologi dan Sistem Informasi Bank XYZ merupakan divisi yang bertugas dalam mengelola semua aset berbasis TI yang menunjang produk dan layanan digital Bank, termasuk didalamnya terkait pengelolaan Insiden Keamanan Informasi di area siber. Dalam pelaksanaan pengelolaan Insiden Keamanan Informasi ini sendiri tidak mengatur terkait pengeloaan insiden Keamanan Informasi untuk dampak skala besar. Saat insiden Keamanan Informasi tersebut terjadi, dibutuhkan kolaborasi antar unit kerja khususnya yang bersifat non teknis seperti informasi publik, pelaporan ke pihak berwajib, koordinasi mitra bisnis, evaluasi kopetensi SDM dan lainnya. Hal tersebut tidak mungkin di kerjakan oleh Divisi Teknologi dan Sistem Informasi sendiri saja, mengingat divisi ini hanya akan fokus kepada pemulihan layanan secara teknis saja saat terjadi insiden keamanan siber. Dibutuhkan kolaborasi lintas unit kerja yang memang berkompeten dalam mengelola dampak non teknis dari insiden keamanan yang berdampak besar ini, agar pemulihan dapat berlangsung dengan efektif dan efisien. Untuk mewujudkan hal tersebut, maka dalam penelitian ini peneliti bermaksud untuk mengembangkan pengeloaan insiden keamanan yang ada di Bank XYZ khusus untuk insiden dengan dampak skala besar, melalui pembentukan Tim Tanggap Insiden Siber (TTIS)/ CSIRT (*Computer Security Incident Response Team*) (CSIRT Starter Kit v1.0, BSSN, 2021) dengan menggunakan standar ISO 27035:2023 (ISO/IEC 27035-1, 2023) untuk mendesain alur kerja, batasan ruang lingkup layanannya dan limit dampak sebagai triger untuk pengaktifan tim ini. Kesemuanya beranjak dari hasil analisis BIA

(*Business Impact Analysis*) menggunakan standard ISO 22317:2021 (ISO 22317, 2021) untuk menganalisa terkait kritikalitas proses bisnis dari layanan bank beserta interdepensinya.

METODE

Dalam penelitian ini digunakan pendekatan kualitatif, dengan tujuan untuk menganalisa kebutuhan dalam membuat strategi dan langkah tepat sasaran untuk mempersiapkan tim TTIS/CSIRT, terkait dengan upaya pengelolaan dan pemulihan secara efektif dan efisien terhadap ancaman dan insiden siber khususnya yang memiliki dampak sekala besar bagi operasional Bank, dalam hal ini pada PT Bank XYZ sebagai objek studi. Adapun tahapan yang digunakan secara garis besar meliputi:

1. Analisa faktor-faktor yang dibutuhkan terkait pengukuran tingkat kritikalitas terhadap proses bisnis Bank melalui BIA yang mengacu pada ISO/TS 22317:2021 (ISO 22317, 2021). Untuk kemudian dituangkan ke dalam kertas kerja.

Table 1. Kertas Kerja BIA

No	Proses Bisnis	AREA DAMPAK (IMPACT OVER TIME)									Maximum Toleranble Downtime (MTD)	NILAI AREA DAMPAK			Total Nilai Area Dampak	Nilai MTD	%Nilai Kritikalitas	Kategori Kritikalitas
		Tipe area dampak A			Tipe area dampak B			Tipe area dampak ..				Tipe area dampak A	Tipe area dampak B	Tipe area dampak ..				
		Waktu 1	...	Waktu n	Waktu 1	...	Waktu n	Waktu 1	...	Waktu n								
1	Proses Bisnis A	SR	R	T	SR	R	T	SR	R	T	1,1 hari - 7 hari	X	Y	Z	X+Y+Z	C	N%	Rendah
2	Proses Bisnis B	T	T	ST	T	ST	ST	SR	ST	ST	0 jam - 4 jam	X	Y	Z	X+Y+Z	C	N%	Tinggi

2. Melakukan identifikasi semua proses bisnis beserta interdepensinya yang khususnya berhubungan dengan unit kerja dan asset mana saja yang terlibat berdasarkan tingkat kritikalitasnya.
3. Menentukan unit kerja yang terlibat nantinya untuk menjadi bagian dalam Tim TTIS/CSIRT. Penyusunan Tim ini mengacu pada ISO/IEC 27035-2:2023 (ISO/IEC 27035-2, 2023), dan hasil interdepedensi BIA.
4. Melakukan analisa terkait kebutuhan Operasional Tim TTIS/CSIRT, berupa pengembangan dari alur kerja pengelolaan insiden siber yang ada di Bank, serta menentukan faktor apa saja yang menjadi *trigger* bagi tim ini untuk mulai bekerja dengan mengacu ISO/IEC 27035-1:2023 (ISO/IEC 27035-1, 2023)

Teknik atau Metode Pengumpulan Data yang digunakan adalah observasi, wawancara dan studi pustaka. Untuk pelaksanaan metode observasi peneliti berkoordinasi dengan pihak bank terkait. Data proses bisnis bank yang menjadi kegiatan rutin, dan hal-hal

terkait tata kelola pengelolaan insiden keamanan informasi, untuk kemudian dianalisa berdasarkan studi pustaka yang dilakukan. Adapun wawancara kepada pihak bank adalah pada responden yang kompeten di unit kerja yang membidangi pengelolaan teknologi Informasi, keamanan, infrasturktur, operasional dukungan dan layanan bisnis, dan PR (*Public Relations*).

HASIL DAN PEMBAHASAN

Dalam melakukan analisis BIA ditentukan terlebih dahulu faktor-faktor yang dibutuhkan dalam menyusun parameternya, mengacu pada Standard (ISO/TS 22317, 2021) (ISO 22317, 2021) parameter dan metode pengukurannya sendiri disesuaikan dengan kondisi organisasi, berikut hasil analisis peneliti:

1. Penentuan Tipe Area Dampak dan Kriteria Tingkat Area Dampak

   Mengacu pada faktor penyusunan Rencana Pemulihan Bencana (POJK No.21/POJK.03/2017, 2017) (POJK 21/OJK.03, 2017) maka tipe area dampak yang digunakan terdiri dari *Finansial, Operasional bisnis, Kepatuhan, Reputasi*. Selanjutnya ditentukan parameter nilai tingkat dampak berdasarkan kriteria tingkat dampak (ISO/TS 22317, 2021) (ISO 22317, 2021), sebagai berikut:

Tabel 2. Parameter Kriteria Tingkat Dampak

No.	Kriteria Tingkat Dampak	Nilai Tingkat Dampak
1.	Sangat Rendah (SR)	1
2.	Rendah (R)	2
3.	Sedang (S)	3
4.	Tinggi (T)	4
5.	Sangat Tinggi (ST)	5

   Parameter diatas dikorelasikan dengan tipe area dampak dengan parameter kriteria tingkat dampak, dengan variabel mengacu pada data historikal bank dan aturan internal tingkat layanan bank, sehingga diperoleh:

Ta el 3. Parameter Kriteria tingkat dampak berdasarkan Area Dampak

Area Dampak	Pengisian Parameter dan Penjelasan
Finansial	1 (SR) : Tidak memiliki dampak. 2 (R) : Nilai kerugian finansial < 25% rata-rata Transaksi per layanan per 1 Hari. 3 (S) : Nilai kerugian finansial > 25%-50% rata-rata Transaksi per layanan per 1 Hari. 4 (T) : Nilai kerugian finansial > 50%-100% rata-rata Transaksi per layanan per 1 Hari. 5 (ST) : Nilai kerugian finansial > 100% rata-rata Transaksi per Layanan per 1 Hari.
Operasional Bisnis	1 (SR) : Berdampak kecil, operasional kantor terhenti < 1 Jam 2 (R) : Berdampak kecil, operasional kantor terhenti 1 - 2 Jam 3 (S) : Berdampak sedang, operasional kantor terhenti 2 - 4 Jam 4 (T) : Berdampak besar, operasional kantor terhenti 4 - 8 Jam 5 (ST) : Berdampak sangat besar, operasional kantor terhenti > 8 Jam
Kepatuhan	1 (SR) : Tidak berdampak 2 (R) : Mendapatkan peringatan/teguran tertulis dari regulator. 3 (S) : Mendapatkan sanksi dari regulator berupa denda < Rp 5.000.000,-. 4 (T) : Mendapatkan sanksi dari regulator berupa denda > Rp 5.000.000,-. 5 (ST) : Pembatasan sebagian atau seluruh kegiatan usaha Perusahaan (freeze)
Reputasi	1 (SR) : Tidak berdampak. 2 (R) : Nasabah / Stakeholders menyampaikan keluhan lisan maupun tertulis kepada Bank. 3 (S) : Nasabah / Stakeholders menyampaikan surat keluhan ke media cetak lokal. 4 (T) : Nasabah / Stakeholders menyampaikan surat keluhan ke media cetak nasional. 5 (ST) : Nasabah / Stakeholders menyampaikan surat keluhan / komplain ke media cetak nasional dan media elektronik.

2. Penentuan parameter frame waktu

   Frame waktu dibuat sebanyak 7 (Tujuh) kelompok dengan urutan waktu insiden disusun mengacu pada pengembangan aturan internal tingkat layanan penanganan insiden Bank, berupa:

Tabel 4. Parameter frame waktu

Kode	Waktu	Penjelasan
Waktu 1	0-2 Jam	Nilai dampak SR, R, S, T, atau ST pada kurun waktu 0 - 2 Jam
Waktu 2	2,1-4 Jam	Besaran nilai dampak (SR, R, S, T, atau ST) pada kurun waktu 2,1 - 4 Jam
Waktu 3	4,1-24 Jam	Besaran nilai dampak (SR, R, S, T, atau ST) pada kurun waktu 4,1 - 24 Jam
Waktu 4	1,1-7 Hari	Besaran nilai dampak (SR, R, S, T, atau ST) pada kurun waktu 1,1 - 7 Hari
Waktu 5	7,1-14 Hari	Besaran nilai dampak (SR, R, S, T, atau ST) pada kurun waktu 7,1 - 14 Hari
Waktu 6	14,1- 30 Hari	Besaran nilai dampak (SR, R, S, T, atau ST) pada kurun waktu 14,1 - 30 Hari
Waktu 7	> 30 Hari	Besaran nilai dampak (SR, R, S, T, atau ST) pada kurun waktu > 30 Hari

3. Penentuan Kriteria MTD (*maximum Tolerable Downtime*)

Informasi MTD pada masing-masing proses bisnis mengacu kepada pemilik layanan berdasakan data historikal, dimana terkait dengan RTO (*Recovery Time Object*) (ISO 22317, 2021) dan WRT (*Work Recovery Time*) terhadap toleransi waktu pemulihan suatu insiden, hasil dari observasi dan wawancara didapati parameter sebagai berikut:

Tabel 5. Parameter MTD

Waktu MTD	Nilai MTD
0 jam - 4 jam	5
4,1 jam - 24 jam	4
1,1 hari - 7 hari	3
7,1 hari - 14 hari	2
14,1 hari - 30 hari	1

4. Kertas Kerja

Semua parameter yang telah ditentukan akan menjadi acuan bagi penilaian bisnis proses saat dimasukkan kedalam kertas kerja sebagai mana disampaikan pada Tabel 1, untuk kemudian dinilai dengan formulasi:

1) Perhitungan inputan pada kolom area dampak dan waktu MTD akan dinilai sesuai dengan parameter yang sudah ditentukan.
2) Untuk Nilai area dampak per tipe area dampak pada setiap proses bisnis diperoleh dari total inputan tingkat dampak disetiap frame waktu pada per area dampak (nilai tingkat dampak dari parameter Tabel 2) dibagi dengan 30 (tiga puluh). Sehingga:
   a. Nilai area dampak Finansial = (waktu1+ … +waktu7)/30
   b. Nilai area dampak Operasional Bisnis = (waktu1 + … + waktu7)/30
   c. Nilai area dampak Kepatuhan = (waktu1 + … + waktu7)/30
   d. Nilai area dampak Reputasi = (waktu1 + … + waktu7)/30
3) Total nilai area dampak pada masing-masing bisnis proses diperoleh :

   Total Nilai Area Dampak = Nilai area dampak Finansial + Nilai area dampak Operasional Bisnis + Nilai area dampak Kepatuhan + Nilai area dampak Reputasi
4) Untuk nilai pada kolom area dampak jika diisi semua dengan nilai maksimum (ST), maka didapat Total Nilai Area dampak = 4.667, sedang nilai maksimum MTD ada

pada nilai 5, sehingga Nilai Pembagi Maksimum didapat sebesar = 4.667 x 5 = 23,333

Sehingga rumusan untuk Nilai kritikalitas untuk setiap bisnis proses didapat adalah:

$$\%Nilai\ Kritikalitas = \frac{(Total\ Area\ Dampak \times Nilai\ MTD)}{23{,}33}$$

5. Penentuan kelompok Tingkat Kritikalitas

Pengelompokan tingkat kritikalitas untuk mempermudah dalam melihat tingkat kritikalitas pada semua proses bisnis yang dianalisa sehingga dapat secara cepat dalam membantu manajemen menentukan prioritas, pengelompokan ini sendiri juga melalui keputusan yang diambil oleh manajemen terkait tingkat risiko appetite Bank.

Tabel 6. Tabel Tingkat Kritikalitas

No.	Kategori tingkat kritikalitas	Persentasi Kritikalitas
1.	Tinggi	100%-60%
2.	Sedang	33%-59%
3.	Rendah	0-33%

6. Hasil Analisis

Hasil analisis BIA tertuang dalam kertas kerja (Tabel 7) berupa seberapa besar tingkat Nilai Kritikalitas dari masing-masing proses bisnis berdasarkan faktor-faktor yang dianalisis berdasarkan formulasi yang disusun sebelumnya, semakin besar persentasi kritikaliasnya, maka akan semakin memiliki dampak besar bagi Bank sehingga tentunya dalam operasional bisnis harus mendapat proritas lebih tinggi.

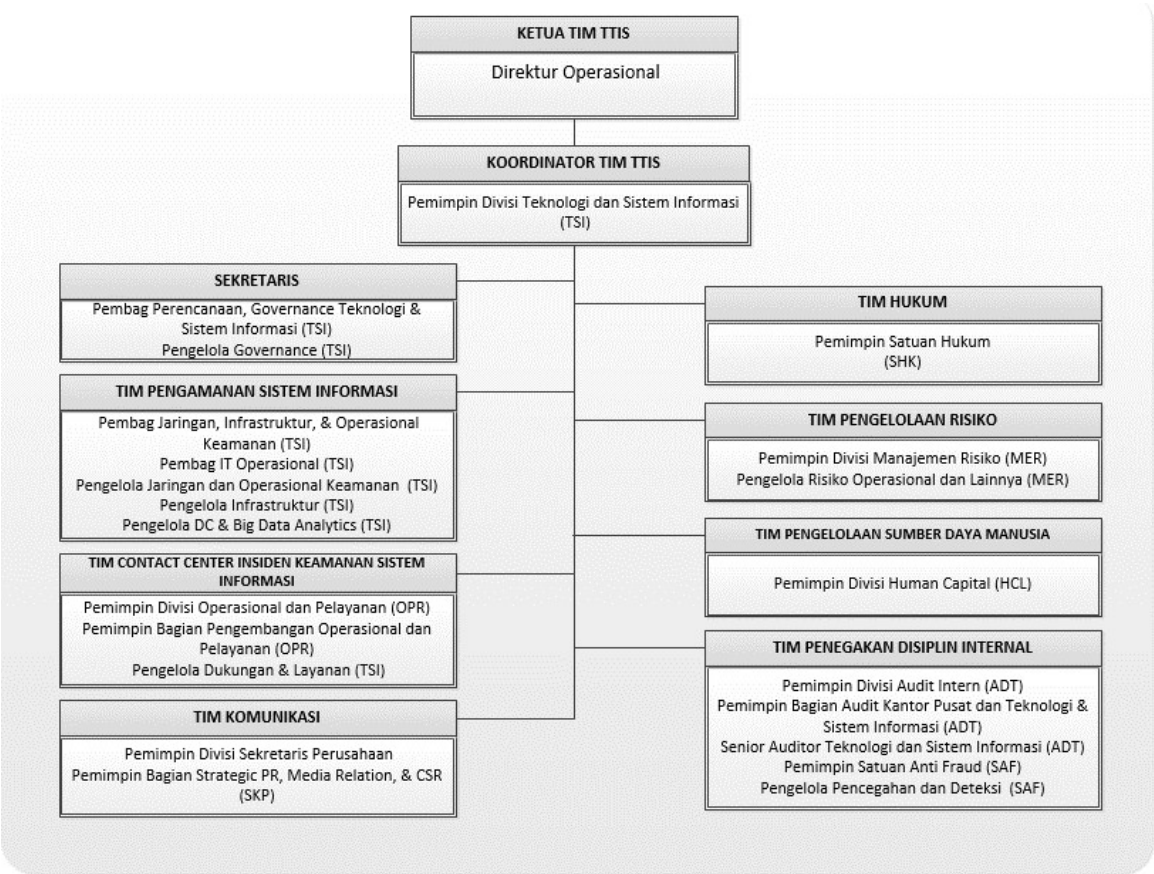
Tabel 7. Tabel Hasil BIA

No	Goup Proses Bisnis	AREA DAMPAK (IMPACT OVER TIME)																										
		Finansial							Operasional Bisnis							Kepatuhan							Reputasi						
		Waktu 1	Waktu 2	Waktu 3	Waktu 4	Waktu 5	Waktu 6	Waktu 7	Waktu 1	Waktu 2	Waktu 3	Waktu 4	Waktu 5	Waktu 6	Waktu 7	Waktu 1	Waktu 2	Waktu 3	Waktu 4	Waktu 5	Waktu 6	Waktu 7	Waktu 1	Waktu 2	Waktu 3	Waktu 4	Waktu 5	Waktu 6	Waktu 7
1	Operasional Channel Transaksi	T	T	ST	ST	ST	ST	ST	R	S	ST	ST	ST	ST	ST	SR	S	T	ST	ST	ST	ST	R	R	T	ST	ST	ST	ST
2	Operasional Core Proses Bank	T	T	ST	ST	ST	ST	ST	R	S	ST	ST	ST	ST	ST	SR	S	T	ST	ST	ST	ST	R	R	T	ST	ST	ST	ST
3	Operasional Core Tresuri	T	T	ST	ST	ST	ST	ST	R	S	ST	ST	ST	ST	ST	SR	S	T	ST	ST	ST	ST	R	R	T	ST	ST	ST	ST
4	Layanan Channel Service Bank	T	T	ST	ST	ST	ST	ST	R	S	ST	ST	ST	ST	ST	SR	S	T	T	ST	ST	ST	R	R	T	ST	ST	ST	ST
5	Operasional Infrasturktur	T	T	ST	ST	ST	ST	ST	R	S	ST	ST	ST	ST	ST	SR	S	T	T	ST	ST	ST	R	R	T	ST	ST	ST	ST
6	Operasional Support	T	T	ST	ST	ST	ST	ST	R	S	ST	ST	ST	ST	ST	SR	SR	T	T	ST	ST	ST	R	R	T	ST	ST	ST	ST
7	Layanan transaksi antar Bank Elektronik	S	T	ST	ST	ST	ST	ST	R	S	ST	ST	ST	ST	ST	SR	SR	T	ST	ST	ST	ST	R	R	T	ST	ST	ST	ST
8	Operasional Payment	S	T	ST	ST	ST	ST	ST	R	S	ST	ST	ST	ST	ST	SR	SR	T	ST	ST	ST	ST	R	R	T	ST	ST	ST	ST
9	Operasional Transaksi Valas	ST	ST	ST	ST	ST	ST	ST	R	R	ST	ST	ST	ST	ST	SR	SR	T	T	T	T	ST	R	R	T	ST	ST	ST	ST
10	Layanan pembukaan service Devisa	S	S	T	ST	ST	ST	ST	R	S	ST	ST	ST	ST	ST	SR	SR	R	T	ST	ST	ST	R	R	T	ST	ST	ST	ST
11	Layanan Dukungan Bisnis Bank	SR	R	ST	ST	ST	ST	ST	R	S	ST	ST	ST	ST	ST	SR	SR	T	T	ST	ST	ST	R	R	S	ST	ST	ST	ST
12	Layanan Pembukaan Deposito	S	T	ST	ST	ST	ST	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	T	ST	ST	ST	R	R	T	ST	ST	ST	ST
13	Layanan Pembukaan Kredit	S	T	ST	ST	ST	ST	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	T	ST	ST	ST	R	R	T	ST	ST	ST	ST
14	Layanan Pembukaan Tabungan	S	T	ST	ST	ST	ST	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	T	ST	ST	ST	R	R	T	ST	ST	ST	ST
15	Layanan Pembayaran Elektronik Bank	S	S	T	ST	ST	ST	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	T	ST	ST	ST	R	R	T	ST	ST	ST	ST
16	Layanan Pembelian Elektronik Bank	S	S	T	ST	ST	ST	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	T	ST	ST	ST	R	R	T	ST	ST	ST	ST
17	Layanan Pembukaan Giro	S	S	T	ST	ST	ST	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	T	ST	ST	ST	R	R	T	ST	ST	ST	ST
18	Pengelolaan Risiko Bank	SR	SR	SR	SR	SR	SR	ST	R	S	ST	ST	ST	ST	ST	SR	SR	R	T	ST	ST	ST	SR	SR	SR	ST	ST	ST	ST
19	Pengelolaan Kepatuhan Bank	SR	SR	SR	SR	SR	SR	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	T	T	ST	ST	ST	SR	SR	SR	ST	ST	ST	ST
20	Layanan Pembukaan Kartu Kredit (Co-Brand)	SR	S	S	T	T	ST	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	S	S	S	ST	SR	R	R	R	S	S	S
21	Pemantauan Layanan DPK	SR	SR	SR	SR	T	T	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	T	ST	ST	ST	SR	SR	SR	R	R	S	S
22	Pemantauan layanan Kredit	SR	SR	SR	SR	SR	ST	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	T	ST	ST	ST	SR	SR	SR	SR	SR	S	S
22	Analisa Produk Bank	SR	SR	SR	SR	SR	SR	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	R	R	R	R	SR	SR	SR	SR	T	T	ST
23	Pemantauan Layanan Bisnis Kantor Cabang	SR	SR	SR	R	R	R	S	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	S	T	T	T	SR	SR	SR	SR	SR	SR	SR
24	Operasional Pelaporan	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	T	ST	ST	ST	SR	SR	SR	SR	SR	SR	SR
25	Perencanaan strategis Bank	SR	SR	SR	SR	SR	SR	ST	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	T	ST	SR	SR	SR	SR	SR	SR	SR
26	Audit	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	S	T	T	SR	SR	SR	SR	SR	SR	SR
27	Procurement	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	SR	SR	SR	SR	R	R	T
28	Layanan Promosi Bank	SR	SR	SR	SR	SR	SR	R	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	SR	R	SR	SR	SR	SR	SR	SR	R

No	Goup Proses Bisnis	Interdepedensi Unit Kerja	Maximum Toleranble Downtime (MTD)	NILAI AREA DAMPAK				Total Nilai Area Dampak	Nilai MTD	Nilai Kritikalitas	Kategori Kritikalitas
				Finansial	Operasional Bisnis	Kepatuhan	Reputasi				
1	Operasional Channel Transaksi	TSI, OPR	0 jam - 4 jam	1,100	1,000	0,933	0,933	3,967	5	85,00%	Tinggi
2	Operasional Core Proses Bank	TSI	0 jam - 4 jam	1,100	1,000	0,933	0,933	3,967	5	85,00%	
3	Operasional Core Tresuri	TSI, OPR	0 jam - 4 jam	1,100	1,000	0,933	0,933	3,967	5	85,00%	
4	Layanan Channel Service Bank	TSI, OPR, SAF	0 jam - 4 jam	1,100	1,000	0,900	0,933	3,933	5	84,29%	
5	Operasional Infrasturktur	TSI	0 jam - 4 jam	1,100	1,000	0,900	0,933	3,933	5	84,29%	
6	Operasional Support	TSI, OPR	0 jam - 4 jam	1,100	1,000	0,833	0,933	3,867	5	82,86%	
7	Layanan transaksi antar Bank Elektronik	TSI, OPR, SAF	0 jam - 4 jam	1,067	1,000	0,867	0,933	3,867	5	82,86%	
8	Operasional Payment	TSI, OPR, SAF	0 jam - 4 jam	1,067	1,000	0,867	0,933	3,867	5	82,86%	
9	Operasional Transaksi Valas	TSI, OPR	0 jam - 4 jam	1,167	0,967	0,767	0,933	3,833	5	82,14%	
10	Layanan pembukaan service Devisa	TSI, OPR	0 jam - 4 jam	1,000	1,000	0,767	0,933	3,700	5	79,29%	
11	Layanan Dukungan Bisnis Bank	TSI, OPR	0 jam - 4 jam	0,933	1,000	0,833	0,900	3,667	5	78,57%	
12	Layanan Pembukaan Deposito	TSI, OPR, Cabang	0 jam - 4 jam	1,067	0,233	0,767	0,933	3,000	5	64,29%	
13	Layanan Pembukaan Kredit	TSI, OPR, Cabang	0 jam - 4 jam	1,067	0,233	0,767	0,933	3,000	5	64,29%	
14	Layanan Pembukaan Tabungan	TSI, OPR, Cabang	0 jam - 4 jam	1,067	0,233	0,767	0,933	3,000	5	64,29%	
15	Layanan Pembayaran Elektronik Bank	TSI, OPR, SAF	0 jam - 4 jam	1,000	0,233	0,767	0,933	2,933	5	62,86%	
16	Layanan Pembelian Elektronik Bank	TSI, OPR, SAF	0 jam - 4 jam	1,000	0,233	0,767	0,933	2,933	5	62,86%	
17	Layanan Pembukaan Giro	TSI, OPR, Cabang	0 jam - 4 jam	1,000	0,233	0,767	0,933	2,933	5	62,86%	
18	Pengelolaan Risiko Bank	MER	0 jam - 4 jam	0,367	1,000	0,767	0,767	2,900	5	62,14%	
19	Pengelolaan Kepatuhan Bank	KPT	0 jam - 4 jam	0,367	0,233	0,833	0,767	2,200	5	47,14%	Sedang
20	Layanan Pembukaan Kartu Kredit (Co-Brand)	BKU, Cabang	0 jam - 4 jam	0,833	0,233	0,567	0,533	2,167	5	46,43%	
21	Pemantauan Layanan DPK	BKU, BKI, PKA	0 jam - 4 jam	0,567	0,233	0,767	0,433	2,000	5	42,86%	
22	Pemantauan layanan Kredit	BKU, BKI, PKA	0 jam - 4 jam	0,500	0,233	0,767	0,367	1,867	5	40,00%	
22	Analisa Produk Bank	PPM, KPN	0 jam - 4 jam	0,367	0,233	0,400	0,567	1,567	5	33,57%	
23	Pemantauan Layanan Bisnis Kantor Cabang	BKU, BKI, REN	0 jam - 4 jam	0,400	0,233	0,600	0,233	1,467	5	31,43%	Rendah
24	Operasional Pelaporan	PKA, SKP	0 jam - 4 jam	0,233	0,233	0,733	0,233	1,433	5	30,71%	
25	Perencanaan strategis Bank	REN	0 jam - 4 jam	0,367	0,233	0,467	0,233	1,300	5	27,86%	
26	Audit	ADT, SAF	0 jam - 4 jam	0,233	0,233	0,500	0,233	1,200	5	25,71%	
27	Procurement	UMA	0 jam - 4 jam	0,233	0,233	0,267	0,400	1,133	5	24,29%	
28	Layanan Promosi Bank	PPM, BKU,BKI	0 jam - 4 jam	0,267	0,233	0,267	0,267	1,033	5	22,14%	

7. Hasil Penyusunan Tim TTIS/CSIRT

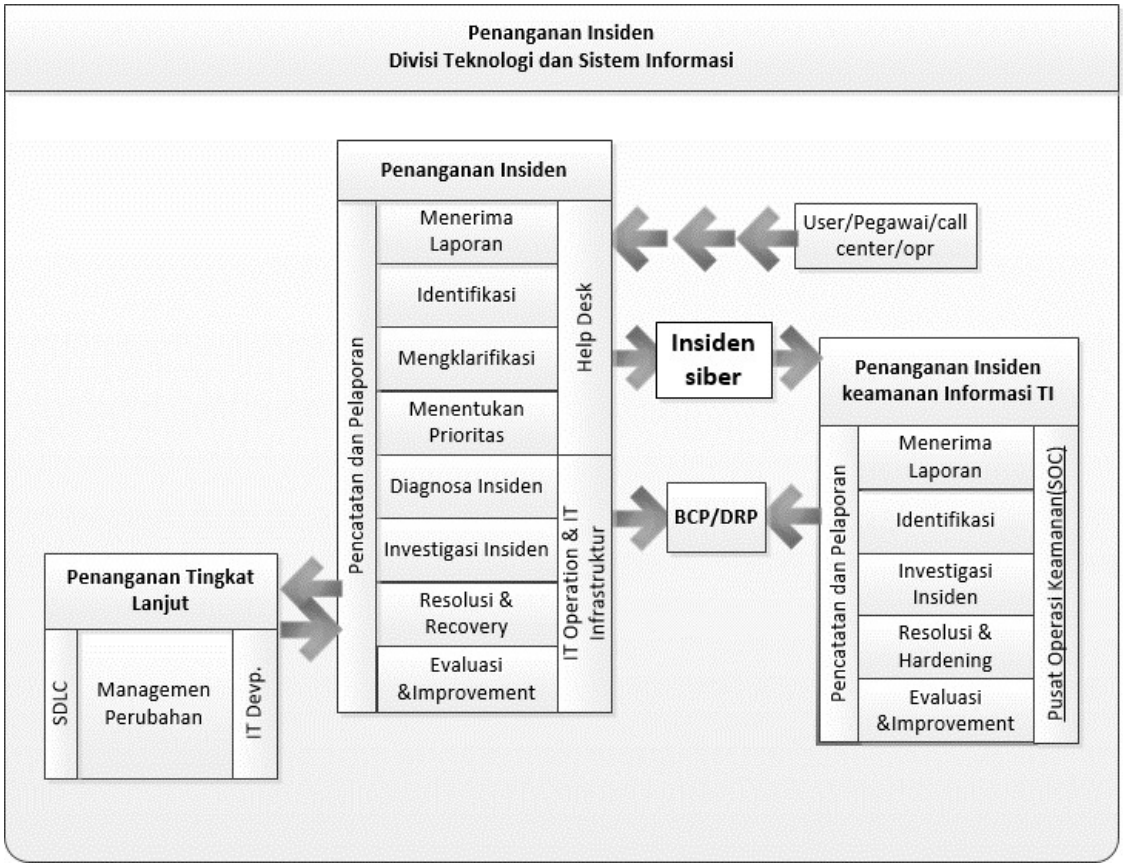
Dilakukan penyusunan Tim TTIS/CSIRT dengan mengacu pada referansi ISO 27035-2:2021 (ISO/IEC 27035-2, 2023) dan unit kerja hasil interdepedensi dari BIA untuk tingkat kritikalitas "Tinggi", sebagai berikut:



Gambar 1. Struktur Tim TTIS/CSIRT

8. Hasil Penyusunan Alur Kerja Tim (Alur Kerja Eksisting)

Berikut merupakan alur kerja penanganan insiden keamanan informasi yang dikelolah oleh Divisi Teknologi Informasi:



Gambar 2. Alur kerja eksisting pengelolaan Insiden

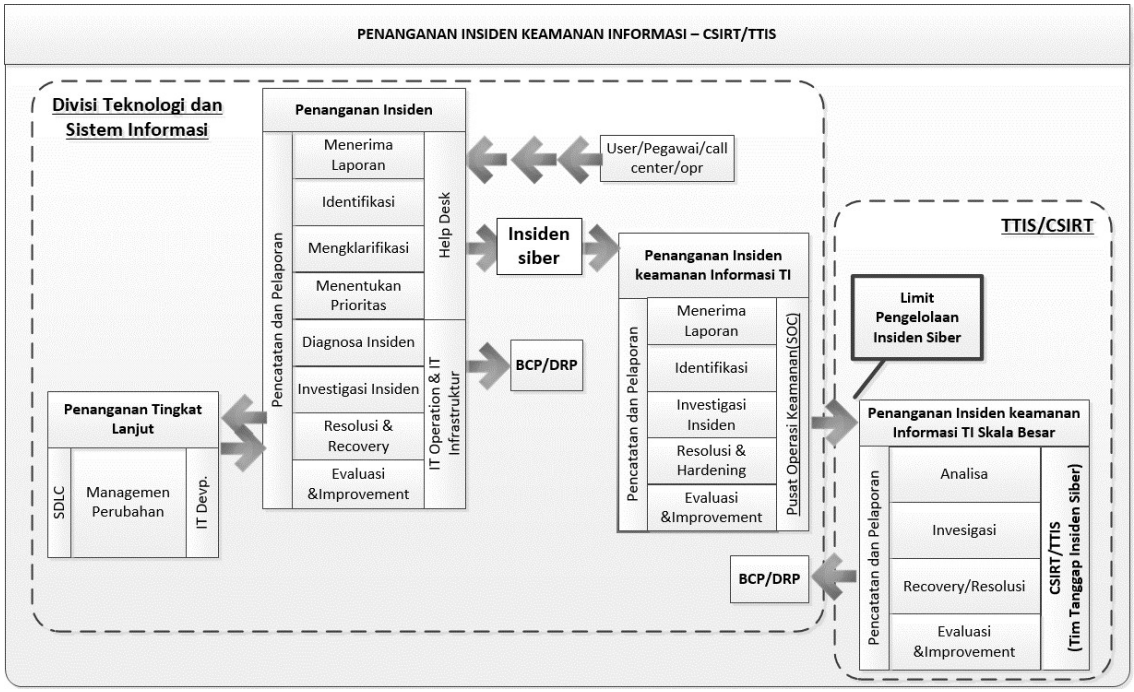
Dari alur tersebut peneliti menganalisa sebagai berikut:

1) Pada alur tersebut terlihat semua pengelolaan insiden keamanan dikelola untuk semua tahapan oleh Divisi Teknologi dan Sistem Informasi baik sekala besar atau bukan.
2) Tidak adanya fungsi yang menghandle isu publik, pengembangan resource pegawai, Analisa risiko, hingga kebutuhan proses hukum dan kedisiplinan khususnya terkait insiden skala besar.

Dari kondisi tersebut tentunya perlu dilakukan pengembangan guna pengelolaan insiden skala besar yang efektif dan efisien.

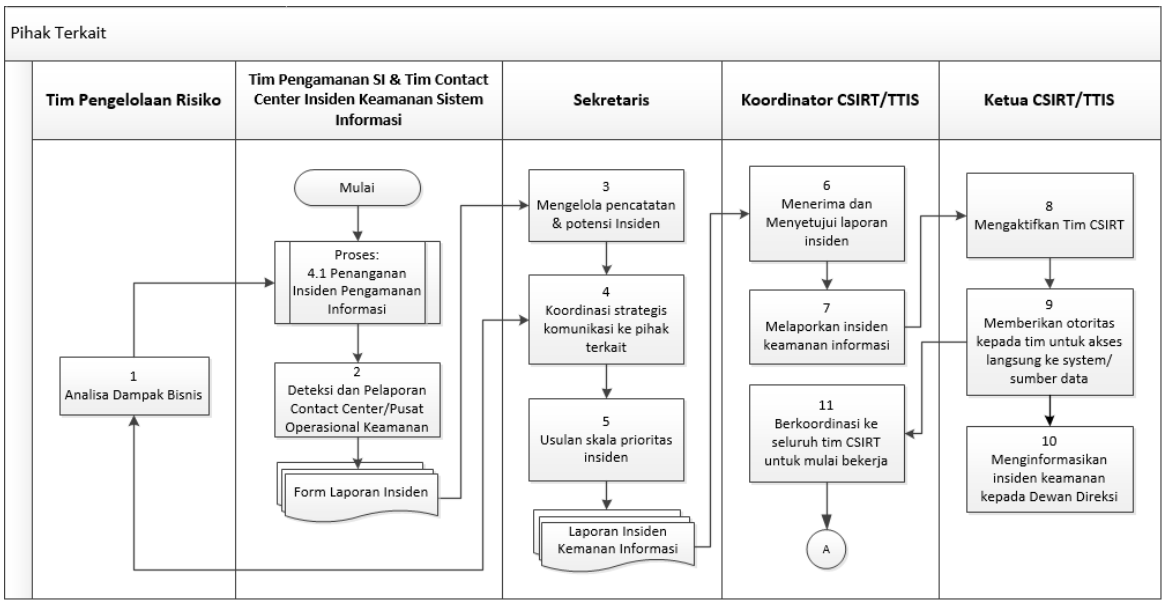
9. Hasil Pengembangan Alur Kerja Tim

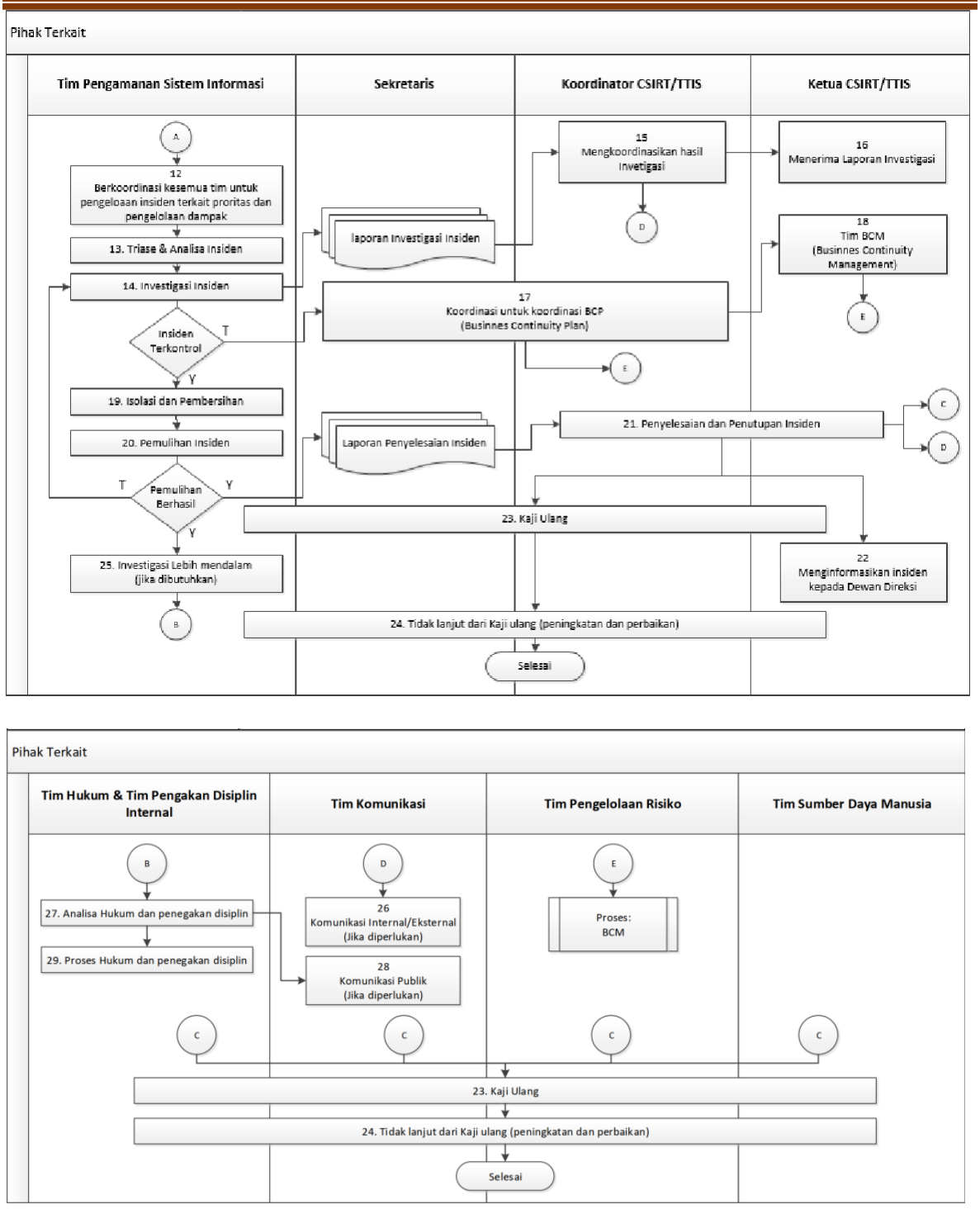
Pengembangan yang dilakukan peneliti menjadi:



Gambar 3. Alur kerja pengembangan pengelolaan Insiden

Detil alur kerja tim TTIS/CSIRT Alur tersebut disusun dengan mengacu pada proses pengelolaan insiden ISO 27035-1:2023 (ISO/IEC 27035-1, 2023), dimana insiden tetap dikelola oleh Divisi Teknologi dan Sistem Infomasi namun jika dampak sudah mencapai Limit Pengelolaan Insiden siber (masuk dalam kategori skala besar), maka akan diambi alih Tim TTIS/CSIRT, dengan alur detilnya sebagai berikut:





Gambar 4. Detil Alur kerja pengembangan pengelolaan Insiden besar

10. Hasil Analisa Untuk Lingkup Kerja Tim TTIS/CSIRT

Trigger Pengelolaan Insiden Keamanan Informasi/Siber dampak berskala besar

Dari hasil observasi dan wawancara disusun parameter limit dampak sebagai trigger Tim TTIS/CSIRT ini mulai bekerja mengambil alih pengeloaan insiden dari Divisi Teknologi Informasi sebagai mana pada alur.

Tabel 8. Parameter Limit Dampak

Kategori	Parameter Dampak Insiden Siber	Limit Dampak	
		Parameter	Satuan
Finansial	Kerugian Finansial Operasional	> 450.000,-	Rupiah
Non Finansial	Berhentinya Operasional Bank	>2	Jam
	Reputasi Buruk di Media	>1	Berita
	Keluhan Nasabah	>23	Keluhan
	Surat Teguran Regulator	≥1	Teguran

1) Parameter Limit Dampak Insiden Siber diambil mengacu pada Tipe Area Dampak yang menjadi parameter penyusunan BIA.
2) Parameter kerugian finansial operasional dan keluhan nasabah diambil dari data historikal bank akibat insiden siber selama 5 tahun kebelakang.
3) Parameter selain poin 2 diambil dari data trend insiden keamanan informasi khususnya insiden keamanan informasi yang pernah dipublikasi oleh media publik 3 tahun ke belakang.
4) Paramater ini disusun dan mendapatkan pengesahan dari manajemen.

11. Lingkup Pengelolaan Insiden Keamanan Tim TTIS/CSIRT pada Proses Bisnis Bank

Untuk penentuan lingkup kerja area layanan yang dikelola oleh Tim TTIS/CSIRT adalah pengelolaan insiden keamanan pada proses bisnis dengan tingkat kritikalitas “Tinggi” yang diidentifikasi dari hasil analisis BIA saat terjadi insiden skala besar. Triger pengelolaannya sendiri berdasarkan parameter limit dampak yang telah ditentukan. Hal ini dimaksudkan agar Tim TTIS/CSIRT bekerja secara efektif, mengingat sumber daya yang digunakan melibatkan banyak unit kerja.

KESIMPULAN DAN REKOMENDASI

Hasil BIA memberikan gambaran yang jelas mengenai tingkat kritikalitas proses bisnis yang dimiliki Bank. Penentuan tingkat kritikalitas sangat membantu dalam penyusunan tim TTIS/CSIRT yang efektif dan efisien dalam upaya penangan insiden keamanan informasi skala besar. Khususnya terkait dengan unit kerja mana yang memiliki interdepedensi dari bisnis proses dengan tingkat kritikal tinggi untuk dilibatkan dalam tim dan prioritas proses bisnis apa saja harus segera dipulihkan saat terjadi insiden. Selain itu dalam pelaksanaannya dapat juga secara jelas disusun mengenai kapan tim ini mulai akan bekerja dan alur kerjanya beserta proses bisnis apa saja yang menjadi lingkup area layanannya berdasarkan hasil analisis BIA.

Untuk peningkatan kualitas kerja Tim tentu perlu dilakukan pengujian berkala untuk melihat keefektifan dan efisiensi TTIS/CSIRT ini. Disarankan untuk dapat berkoordinasi dengan TTIS/CSIRT Nasional untuk berkolaborasi menjadi bagian dari TTIS/CSIRT sektor keuangan. Hal ini dapat memperkuat ketahanan siber bank. Selain itu juga untuk memastikan apakah tim masih relevan dengan kondisi berjalan. Terkait dengan hasil analisis BIA dapat juga digunakan tidak hanya untuk pembentukan tim TTIS/CSIRT saja namun dapat juga menunjang kegiatan lainnya, diantaranya dalam mengambil keputusan investasi, treatmen mitigasi risiko, termasuk proritas pengembangan atau evaluasi dari produk dan layanan yang ada.

REFERENSI

Andress, J. (2014). The Basics of Information Security: Understanding the fundamentals of infosec in Theory and Practice. Sygress.

Bellini, Y., & Sutabri, T. (2023). Sistem pakar mendeteksi tindak pidana cybercrime untuk penanganan komputer forensik menggunakan backward chaining. Jurnal Digital Teknologi Informasi.

CSIRT Starter Kit v1.0, BSSN. (2021). CSIRT Starter Kit v1.0. Jakarta: BSSN.

ISO 22317. (2021). ISO/TS 22317 Guidelines fir business impact analysis. Switzerland: ISO.

ISO/IEC 27000. (2018). ISO/IEC 27000 Information Security Management Systems-Overview and vocabulary. Switzerland: ISO.

ISO/IEC 27001. (2022). ISO/IEC 27001 Information Secuirty Management System-Requirement. Switzerland: ISO.

ISO/IEC 27035-1. (2023). ISO/IEC 27035-1 Principles and process. Switzerland : ISO Copyright .

ISO/IEC 27035-2. (2023). ISO/IEC 27035-2 Guidlines to plan and prepare for insiden response. Switzerland: ISO.

Matondang, N. I. (2018). Analisis Manajemen Risiko Keamanan Data Sistem Informasi (Studi Kasus: RSUD XYZ). RESTI (Rekayasa Sistem Dan Teknologi Informasi) 2(1):282–87. doi:10.29207/resti.v2i1.96.

Napitupulu, D., & Sutabri, T. (2019). Sistem Informasi Bisnis. Andi Offset.

POJK 11/OJK.03. (2022). Peraturan OJK No.11/POJK.03/2022 tentang Penyelengaraan Teknologi Informasi Bank Umum. Jakarta: Otoritas Jasa Keuangan.

POJK 21/OJK.03. (2017). Pertauran OJK No.21/POJK.03/2017 tentang Manajemen Risiko Teknologi bagi Bank Umum. Jakarta: Otoritas Jasa Keuangan.

Raharja. (2022, Januari 5). Teknik Pengumpulan Data Pada Tesis. Retrieved from Raharja.Ac.Id: https://raharja.ac.id/2019/12/27/teknik-pegumpulan-data-pada-tesis

SEOJK 29/OJK.03/2022. (2022). SEOJK 29/OJK.03/2022 Tentang Ketahanan dan Keamanan Siber bagi Bank Umum. Jakarta: Otoritas Jasa Keuangan.

Tiatama, A. (2016). Manajemen Keamanan Informasi Menggunakan Information Technology Infrastructure Library (ITIL) V3. Pada D ~ Net Surabaya.