# BAB I

# PENDAHULUAN

## 1.1 Latar Belakang

Perkembangan Teknologi Informasi (TI) saat ini sangat pesat, dimana hampir semua sektor memanfaatkan hal ini, dan tentunya hal ini juga telah memengaruhi cara kerja berbagai industri terutama jasa keuangan, termasuk industri perbankan. Bank dapat memanfaatkan TI untuk mendukung kegiatan operasional Bank serta meningkatkan pelayanan kepada nasabah (SEOJK 29/OJK.03/2022, 2022). Dengan bantuan TI, Bank dapat memperoleh manfaat, khususnya dalam peningkatan efisiensi dan efektivitas operasional Bank, berbagai kemudahan termasuk kerja sama dengan pihak ketiga dapat dilakuan dengan mudah, sehingga penyediaan layanan kepada nasabah dapat dengan cepat dan optimal. Namun, peningkatan penggunaan TI juga dapat meningkatkan risiko operasional di sektor perbankan.

Dalam operasionalnya sendiri salah satu risiko yang dapat meningkat dengan penggunaan TI pada lingkup yang lebih besar adalah risiko yang disebabkan oleh ancaman dan kejadian insiden siber, dimana penggunaan TI saat ini sudah tumbuh besar melalui media siber khususnya untuk produk dan layanan digital bank. 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 (POJK 11/OJK.03, 2022). Bank sangat perlu menetapkan strategi dan langkah-langkah yang tepat dan berkelanjutan untuk mengatasi ancaman dan insiden siber, salah satunya adalah terkait pengelolaan Insiden siber yang melibatkan unit kerja-unit kerja Bank yang dapat mengelola insiden baik yang berdampak pada pihak eksternal maupun pihak internal sendiri.

Insiden siber pada keamanan informasi dapat merupakan kejadian tunggal atau serangkaian kejadian keamanan informasi yang tidak diduga atau tidak

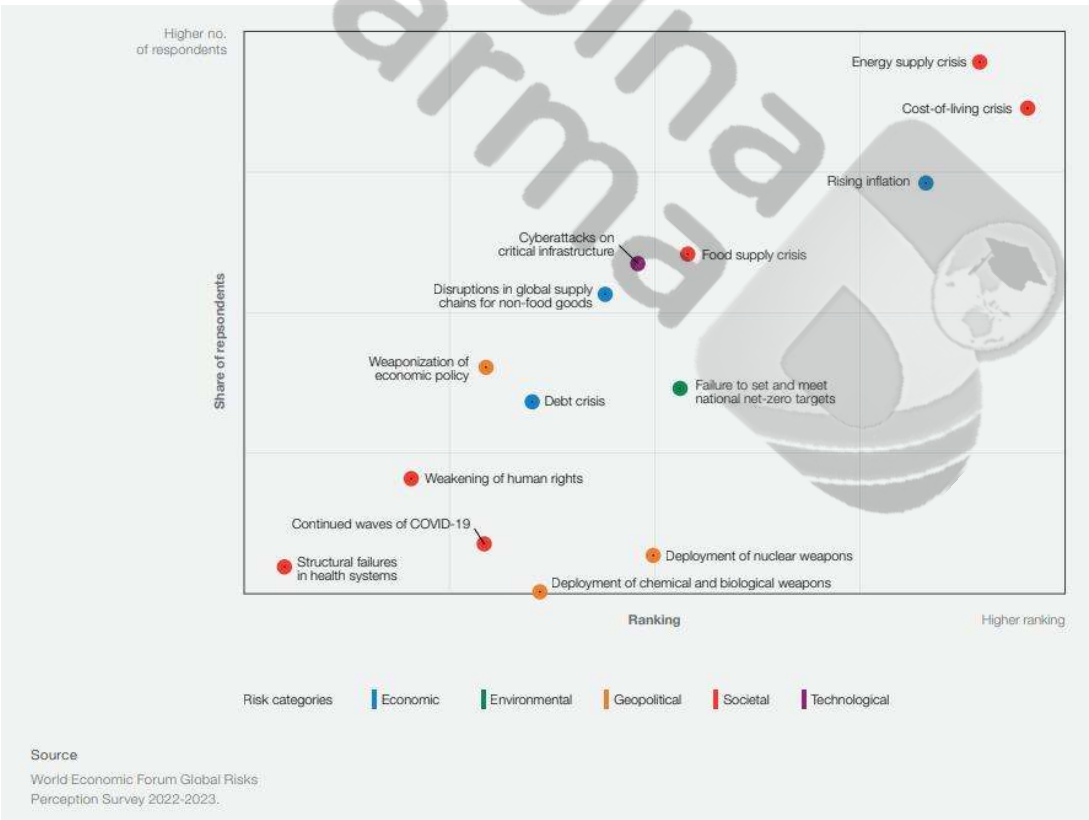
dikehendaki yang mempunyai kemungkinan besar mengganggu keberlangsungan bisnis dan mengancam keamanan informasi (ISO/IEC 27000, 2018). Insiden siber tersebut dapat dikategorikan sebagai serangan terhadap system elektronik, meliputi namun tidak terbatas pada serangan virus, malware, ransomware, DDOS, pencurian data, illegal access, modifikasi informasi, password attack maupun serangan hacking kedalam system (CSIRT Starter Kit v1.0, BSSN, 2021). Insiden siber pada Keamanan infrormasi berpotensial mengancam sistem keamanan Informasi baik yang berdampak dalam skala kecil maupun skala besar, Insiden siber berskala besar terjadi sangat serius untuk disikapi oleh Bank, karena berdampak luas kepada bisnis Bank itu sendiri. Hal tersebut harus dilakukan mengingat bisnis perbankan merupakan bisnis yang utamanya berkaitan dengan dana masyarakat sehingga memerlukan operasional yang matang dan aman (SEOJK 29/OJK.03/2022, 2022).

Bank Sumsel Babel saat ini telah melakukan banyak inovasi pengembangan layanan/produk TI berbasis digital platform, dimana hal ini merupakan bentuk dari adaptasi kebutuhan bisnis Bank pada era global saat ini, banyak akses ke rana siber yang digunakan dalam operasional layanan Bank, termasuk aplikasi yang dibangun untuk memenuhi kebutuhan bisnis dalam menciptakan kemudahan transaksi layanan bagi nasabah. Namun tentunya Bank Sumsel Babel harus menjaga keamanan dari serangan siber terhadap layanan ini. Saat ini semua alokasi aset terkait layanan Bank ditempatkan di area Datacenter dengan filter akses keamanan diterapkan baik secara logik maupun fisik dan menggunakan jaringan yang tersegmentasi melalui perangkat keamanan yang terus diperbarui, Semua aset dipantau secara berkala 7x24 Jam untuk memastikan operasional perangkat dan perlindungan keamanan berjalan dengan seharusnya.

Divisi Teknologi dan Sistem Informasi Bank Sumsel Babel merupakan divisi yang bertanggung jawab dalam mengelola semua aset teknologi khususnya yang berbasis TI dalam menunjang produk dan layanan digital Bank. Tata Kelola TI pun telah dibangun diantarannya dengan menyiapkan standard, prosedur dan kebijakan di masing-masing pengelolaan TI hingga pengguna TI yang sesuaikan berdasarkan Peraturan Regulasi Bank dalam hal ini OJK dan Bank Indonesia, selain itu fungsi-fungsi pengelolaan TI ini sendiri juga dituangkan dalam bentuk

sub unit kerja dalam struktur organisasi Divisi Teknologi dan Sistem Informasi, Selanjutnya khusus fungsi Operasional Keamanan Informasi, Bank Sumsel Babel telah menyiapkan unit kerja khusus pada Divisi Teknologi dan Sisem Informasi ini yang bertanggung jawab pada operasional keamanan teknologi Informasi Bank, termasuk didalamnya terkait penanggulanangan Insiden Keamanan Informasi termasuk area siber, unit kerja ini dibangun untuk dapat semaksimal mungkin menanggulangi adanya Insiden siber pada keamanan informasi yang mengarah ke semua aset teknologi Bank.

Insiden Siber ini sendiri saat ini sudah menjadi ancaman dunia dengan dampak risiko tinggi, bahkan dalam Global Risk Report 2023, "Cyber-attack" termasuk dalam 5 risiko tertinggi untuk potensi dampak kerugian terbesar dunia (Global Risks Report 2023, 2023).




**Gambar 1.1 Laporan Risk Global 2023**

Divisi Teknologi dan Sistem Informasi tentunya dituntut untuk dapat memastikan keamanan pada semua aset, dan memastikan pemulihan secepat mungkin jika terjadi gangguan disemua aset tersebut baik berdampak besar maupun kecil. Namun

jika belajar pada kejadian serangan siber yang diberitakan di media massa dengan dampak yang besar, baik terhadap reputasi perusahaan maupun kerugian finansial perusahaan akibat kegagalan operasional, tentunya saat penanganan insiden siber semacam ini tidak hanya bergantung pada unit kerja yang membidangi Teknologi Informasi saja, banyak unit lain yang harus terlibat khususnya untuk penanganan dampak non teknis seperti Informasi ke publik, pelaporan ke pihak berwajib, koordinasi mitra bisnis dan lainnya yang tidak mungkin di kerjakan oleh unit yang membidangi Teknologi Informasi saja, mengingat unit kerja Teknologi Informasi ini tentunya hanya akan fokus kepada pemulihan layanan secara teknis TI saja, sehingga dibutuhkan kolaborasi lintas unit kerja yang memang berkopetensi dalam mengelola dampak non teknis dari insiden keamanan ini, agar pemulihan dapat berlangsung dengan efektif dan efisien, hal ini merupakan tujuan utama dalam setiap pemulihan.

Berdasarkan uraian di atas, tentunya perlu dibangun Tim yang nantinya diharapkan beroperasi secara efektif dan efisien sesuai dengan kompetensi masing-masing unit kerja yang dimiliki, Tim ini dikenal dengan TTIS (Tim Tanggap Insiden Siber) atau secara umum dikenal dengan CSIRT (Computer Security Incident Response Team), secara spesifik tidak ada panduan khusus untuk perbankan mengenai penyusunan Tim ini. CSIRT dibentuk berdasarkan Tujuan dan latar belakang masing-masing organisasi sehingga CSIRT akan memiliki model/struktur yang berbeda-beda, hal ini juga akan menyebabkan operasional setiap tim CSIRT dapat berbeda-beda.(CSIRT Starter Kit v1.0, BSSN, 2021)

Tujuan dari penelitian ini secara besaran adalah untuk mengembangkan pengelolaan insiden keamanan yang ada di Bank Sumsel Babel khusus untuk insiden dengan skala besar, melalui pembentukan TTIS yang melibatkan kolaborasi dari banyak unit kerja terkait di Bank Sumsel Babel, beserta alur kerja dan batasan lingkup kerjanya, Juga termasuk penetuan parameter limit dampak yang menjadi triger untuk pengaktifan tim ini. Batasan-batasan ini sendiri harus melihat sejauh mana tingkat kritikalitas proses bisnis terhadap produk dan layanan Bank melalui analisis BIA (Business Impact Analysis), sehingga tidak semua area saat terjadi gangguan keamanan harus dikelolah oleh tim, karena jika tingkat kritikalitasnya tidak tinggi, maka cukup oleh Divisi Teknologi dan Informasi saja.

## 1.2 Identifikasi Masalah

Berdasarkan latar belakang penelitian, dapat diidentifikasi masalah sebagai berikut:

1. Belum adanya tim yang secara spesifik menangani insiden siber khusus skala besar, dalam hal ini terkait fungsi kerja yang tidak hanya melakukan pemulihan insiden secara teknis saja, melainkan juga secara berkolaboratif dari sisi non teknis, mengingat reputasi bank dipertaruhkan saat pemulihan berlangsung.
2. Untuk pengelolaan insiden skala besar belum spesifik diatur mengenai koordinasi lintas Divisi, sehingga perlu adanya alur kerja yang spesifik dalam melibatkan lintas Divisi khususnya untuk tim tanggap insiden siber.
3. Lingkup kerja Divisi TI dalam mengelola insiden siber saat ini belum memiliki batasan kerja yang spesifik, sehingga dikhawatirkan menjadi tidak effektif khususnya untuk pengelolaan insiden skala besar, sehingga perlu disusun parameter yang nantinya akan menjadi acuan Tim TTIS/CSIRT ini mulai aktif.
4. Selain Limit dampak, aset Bank juga harus ditentukan mana yang menjadi lingkup kerja Tim, hal ini dilakukan agar unit kerja dan Tim dapat melaksanakan masing-masing tugasnya secara efektif.

## 1.3 Batasan Masalah

Batasan masalah dalam penelitian ini dimaksudkan agar penelitian lebih terarah dan tidak keluar dari permasalahan yang ditentukan, batasan berupa penyusunan tim dan alur kerja beserta pembatasan lingkup area kerja Tim TTIS/CSIRT berdasarkan tingkat kritikalitas produk/layanan Bank yang diperoleh dari hasil analisis BIA. Adapun objek penelitiannya adalah unit kerja terkait TI, Hubungan publik dan unit kerja terkait Operasional layanan Bank

## 1.4 Rumusan Permasalahan

Dari latar belakang diatas, maka dirumuskan permasalahan dalam penelitian sebagai berikut :

1. Faktor-faktor yang apa saja yang dibutuhkan dalam menyusun Tim TTIS/CSIRT yang efektif dan efisien berdasarkan kondisi yang dimiliki bank?

2. Bagaimana mengidentifikasi tingkat kritikalitas proses bisnis Bank dalam upaya proritas perlindungan terhadap adanya insiden siber bersekala besar yang nantinya akan menjadi lingkup kerja dari tim TTIS/CSIRT.
3. Bagaimana menyusun alur kerja Tim TTIS/CSIRT yang effektif dan effisien berdasarkan kondisi yang dimiliki Bank?

## 1.5 Tujuan Penelitian

Tujuan penelitan perancangan Tim TTIS/CSRT: studi kualitatif berdasarkan Business Impact Analysis di Bank Sumsel Babel, meliputi :

1. Menganalisa faktor-faktor yang dibutuhkan dalam menyusun Tim TTIS/CSIRT yang efektif dan efisien dengan mengacu pada analisis BIA.
2. Menidentifikasi tingkat kritikalitas proses bisnis Bank dalam upaya proritas perlindungan terhadap adanya insiden siber bersekala besar, untuk nantinya akan menjadi lingkup kerja Tim Tanggap Insiden Siber.
3. Mangalisa alur kerja yang dibutuhkan Tim TTIS/CSIRT yang efektif dan efisien berdasarkan hasil identifikasi tingkat kritikalitas dan kondisi Bank.

Selanjutnya dari tujuan penelitian tersebut menghasilkan Dokumen berupa hasil analisis BIA, struktur Tim TTIS/CSIRT yang mengkolaborasikan banyak Divisi beserta prosedur alur kerjanya, Kebijakan terkait lingkup kerja bagi tim TTIS/CSIRT yang mengacu pada hasil identifikasi kritikalitas proses bisnis, dan parameter limit yang menjadi acuan kapan Tim TTIS/CSIRT ini mulai bekerja.

## 1.6 Manfaat Penelitian

Adapun manfaat dari penelitian ini yang penulis gunakan dalam melakukan penelitian ini adalah :

1. Mempersiapkan tim yang secara spesifik akan mengelola insiden siber skala besar.
2. Mempersiapkan alur kerja Tim saat terjadi insiden keamanan siber skala besar sehingga pengelolaan insiden akan lebih efektif dan efesien, yang nantinya merupakan pengembangan dari alur kerja dari unit kerja yang ada.
3. Dapat mengetahui tingkat kritikalitas produk/layanan Bank, sehingga dalam pengelolaannya dapat lebih diproritaskan.

4. Efektitas dalam kegiatan tim dapat memperpendek waktu pemulihan saat terjadi insiden siber, dan dapat mengantisipasi kerugian lebih besar sebagai dampak dari insiden siber yang terjadi baik teknis maupun non teknis seperti pemberitaan negatif maupun terkait hukum, karena tim akan berkolaporasi secara bersama-sama mengelola insiden siber tersebut sesuai dengan alur kerja masing-masing.

## 1.7 Susunan Dan Struktur Penelitian

Susunan dan struktur tesis ini maksudnya agar dapat memberikan garis besarnya secara jelas sehingga terlihat hubungan antara bab yang satu dengan bab yang lainnya. Susunan dan struktur tesis dijabarkan di bawah ini sebagai berikut :

**BAB I PENDAHULUAN**

Pada bab ini membahas tentang latar belakang, identifikasi masalah, batasan masalah, rumusan masalah, tujuan dan manfaat penelitian, serta susunan dan struktur tesis.

**BAB II TINJAUAN PUSTAKA**

Pada bab ini membahas tentang tinjauan umum, kajian pustaka, penelitian terdahulu dan kerangka konseptual penelitian yang akan dilakukan.

**BAB III METODOLOGI PENELITIAN**

Pada bab ini pembahasannya yang terdiri dari desain dan jadwal penelitian dan metode penelitian yang digunakan serta metode pengumpulan data.

**BAB IV HASIL DAN PEMBAHASAN**

Pada bab ini menguraikan tentang hasil penelitian secara menyeluruh.

**BAB V PENUTUP**

Pada bab ini adalah bagian akhir dari penelitian. Menguraikan rangkuman dari hasil penelitian dalam bentuk kesimpulan dan saran untuk mengembangkan penelitian berikutnya.