BAB I

PENDAHULUAN

I.1. Latar Belakang

Sebagai instansi keuangan, bank berperan penting dalam pembangunan ekonomi Indonesia. Suatu lembaga yang dikenal dengan nama bank memiliki kegiatan usaha berupa menghimpun dana dari masyarakat serta menyalurkan dananya kembali kepada masyarakat (Munawir & Maskupah, 2021).

Perkembangan teknologi yang semakin maju memungkinkan masyarakat untuk menggunakan perangkat *digital* seperti telepon genggam dan komputer untuk memenuhi kebutuhan sehari-hari. Hal ini memungkinkan industri perbankan untuk mengembangkan produk serta layanan terkait dengan teknologi. Dengan berkembangnya *digital banking*, layanan perbankan menjadi lebih mudah karena dapat diakses secara *online* tanpa harus mengunjungi ke cabang bank terdekat. Jumlah pertumbuhan nasabah diharapkan semakin meningkat akibat adanya layanan *digital banking* (Silvia, 2022).

Menurut Sulisrudatin (2018) kejahatan perbankan berkaitan dengan kemajuan ilmu pengetahuan dan teknologi. Jenis kejahatan ini termasuk dalam kategori kejahatan yang dilakukan oleh individu atau golongan orang yang memiliki pengetahuan serta keterampilan khusus, tidak semua orang dapat melakukannya. Seiring dengan kemajuan dan perkembangan peradaban manusia, berbagai bentuk dan pola kejahatan bermunculan. Setelah komputer menjadi populer di berbagai belahan dunia, masyarakat mulai khawatir dan terganggu dengan dampak negatifnya, termasuk kejahatan yang dilakukan melalui komputer. Menurut Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber disebutkan bahwa *cyber* (siber) adalah tempat di mana komunitas saling terhubung satu sama lain melalui jaringan (seperti internet) untuk melaksanakan aktivitas sehari-hari.

Menurut Karyono (2013, hlm.4) *fraud* adalah pelanggaran yang melibatkan tindakan yang berdampak terhadap hukum dan bertujuan untuk mencapai suatu tujuan tertentu, misalnya penipuan atau menyampaikan informasi yang menyesatkan yang diberikan kepada pihak lain, baik oleh individu yang berada di

dalam maupun di luar organisasi. Berdasarkan pengertian yang telah disebutkan, maka *cyber fraud* merupakan kejahatan yang dilakukan melalui jaringan internet dengan maksud menipu korban disertai dengan kerugian materiel maupun imateriel dengan tujuan untuk memperoleh keuntungan bagi pelakunya.

Tabel 1 Perkembangan Kasus *Cyber Fraud* pada Sektor Perbankan di Indonesia Tahun 2018-2022

Tahun	Total Kasus	Kerugian
2018	247.218	3,2 triliun
2019	269.324	3,5 triliun
2020	294.281	4,2 triliun
2021	323.972	6,9 triliun
2022	272.962	3,8 triliun

Sumber : Badan Siber dan Sandi Negara (BSSN)

Badan Siber dan Sandi Negara (BSSN) mencatat kasus *cyber fraud* di sektor perbankan mengalami kenaikan selama 3 tahun terhitung mulai dari tahun 2019-2021. Total kasus *cyber fraud* pada tahun 2019 sejumlah 269.324 kasus dengan total kerugian sebesar 3,5 triliun. Kemudian pada tahun 2020 kembali meningkat sebesar 294.281 kasus dengan total kerugian sebesar 4,2 triliun. Selanjutnya pada tahun 2021 semakin meningkat sebesar 323.972 dengan total kerugian sebesar 6,9 triliun. Kemudian pada tahun 2022 turun sebesar 272.962 dengan total kerugian sebesar 3,8 triliun.

Menurut PT Bank Central Asia (www.bca.co.id) per Juli 2022, fenomena yang melanda PT Bank Central Asia saat ini adalah kian maraknya modus *cyber fraud* yang terjadi belakangan ini. Kejadian ini tentu saja sangat merugikan nasabah yang terkena kasus penipuan serta pihak bank yang bersangkutan akan dipandang buruk oleh masyarakat. Seperti insiden yang terjadi belakangan ini yaitu adanya modus kejahatan berupa oknum yang mengaku sebagai kurir suatu jasa ekspedisi yang mengirimkan foto paket kepada target korbannya dan ternyata isi dari *file* tersebut berupa situs yang bertujuan untuk mencuri data diri dari korban. Hal tersebut memungkinkan data pribadi korban dapat terserap oleh pelaku, sehingga pelaku dapat melakukan kejahatannya.

Menurut PT Bank Central Asia (www.bca.co.id) per Juli 2022, terdapat beberapa modus kejahatan perbankan yang sering terjadi. Di antaranya yaitu *Phishing* dan *Social Engineering*. *Phishing* adalah metode yang digunakan penipu

untuk mencuri informasi pribadi korban melalui situs web palsu. *Social Engineering* adalah tindak kejahatan yang dilakukan untuk memanipulasi korban agar memberikan data pribadi, mengakses suatu sistem, atau melakukan tindakan sesuai arahan penipu. Teknik penipuan ini menggunakan strategi psikologis seperti persuasi, intimidasi, atau pengaruh psikologis lainnya.

Kondisi Risiko Operasional yang timbul akibat *cyber fraud* dapat berdampak pada kerahasiaan, ketersediaan, dan integritas informasi serta sistem teknologi. Kejadian *cyber fraud* memiliki potensi untuk menyebabkan kerugian serius bagi bank dan nasabahnya. Apabila dilihat secara lebih luas, *cyber fraud* juga memiliki potensi untuk menyebabkan ketidakstabilan dalam sistem keuangan. (Khotimah, 2022).

Kondisi Risiko Reputasi yang timbul akibat *cyber fraud* dapat terjadi akibat dampak dari pemberitaan media atau tersebarnya berita negatif terhadap bank yang dapat merusak citra dan reputasi bank di mata masyarakat. (Fatoni & Halim, 2016).

Kondisi Risiko Strategis akibat *cyber fraud* dapat terjadi karena adanya ketidakcocokan antara teknologi informasi yang digunakan oleh suatu bank dengan tujuan strategis serta rencana strategis yang telah ditentukan dalam rangka memperoleh suatu tujuan. Faktor penyebabnya adalah pelaksanaan teknologi informasi yang kurang berkualitas dan sumber daya yang digunakan tidak memadai. Sumber daya ini termasuk saluran komunikasi, sistem operasi, jaringan pengiriman, serta kapasitas dan kemampuan manajemen teknologi informasi. (Fatoni & Halim, 2016).

Cyber fraud merupakan ancaman serius bagi bisnis perbankan karena berpotensi menyebabkan risiko baik bagi bank itu sendiri maupun nasabahnya, baik secara fisik maupun psikologis. Untuk mengurangi risiko tersebut, bank perlu melatih dan mendidik karyawan mereka tentang ancaman keamanan yang ada serta bagaimana mengenali dan mengantisipasi serangan *cyber fraud*. Untuk mencegah dampak *cyber fraud* pada sektor perbankan, diperlukan tindakan antisipatif seperti mencegah kebocoran kata sandi, memastikan keamanan akses informasi, melakukan verifikasi kontak, mengikuti prosedur yang ditetapkan, melaporkan tindakan mencurigakan, memberikan pelatihan berkelanjutan, dan memberikan edukasi kepada nasabah. (Junaedi, 2017).

Dengan adanya kemunculan berbagai risiko dalam suatu perusahaan, diperlukan adanya pengelolaan dan pengendalian risiko supaya perusahaan mampu menjaga dan meningkatkan bisnisnya terutama di tengah persaingan yang sangat ketat seperti saat ini. Bentuk strategi untuk mengendalikan dan mengurangi dampak dari risiko yaitu melalui penerapan praktik manajemen risiko (Fitriani, 2013). Metode yang dilakukan dalam praktik manajemen risiko di perusahaan yaitu dengan melakukan pengukuran menggunakan *Enterprise Risk Management* (Haryani, 2019).

Menurut Darmawi (2014, hlm.5) *Enterprise Risk Management* adalah variabel sebagai alat ukur perusahaan dalam melaksanakan suatu kebijakan agar mampu mengelola risiko yang bertujuan untuk memberikan kepercayaan yang memadai mengenai pencapaian dari tujuan perusahaan. Indikator yang diukur dalam variabel ini yaitu Identifikasi Risiko, Penilaian Risiko, Matriks Risiko, Respons Risiko, dan Pengendalian Risiko.

Mengenai latar belakang serta fenomena berdasarkan uraian di atas, penulis tertarik untuk menyusun Tugas Akhir dengan judul **"Analisis Risiko Bank Terhadap Tindakan *Cyber Fraud* Pada PT Bank Central Asia".**

I.2 Tujuan Penulisan Tugas Akhir

Berdasarkan atas pembahasan dari permasalahan di atas, maka tujuan penulisan Tugas Akhir ini yaitu untuk memahami penerapan *Enterprise Risk Management* sebagai pengukuran risiko untuk mengetahui kondisi Risiko Operasional, Risiko Reputasi, dan Risiko Strategis akibat *cyber fraud* yang mengatasnamakan PT Bank Central Asia yang terdiri dari :

1. Identifikasi Risiko
2. Penilaian Risiko
3. Matriks Risiko
4. Respons Risiko
5. Pengendalian Risiko

I.3 Manfaat Tugas Akhir

Berikut adalah manfaat yang dapat diperoleh dari penulisan Tugas Akhir ini yaitu :

1. Aspek Teoritis

   Diharapkan dapat menambah pengetahuan serta wawasan mengenai risiko perbankan terhadap tindakan *cyber fraud* pada PT Bank Central Asia.

2. Aspek Praktis

   a. Bagi Perbankan

      Dapat digunakan sebagai referensi bagi Perbankan mengenai risiko bank yang timbul terhadap tindakan *cyber fraud*.

   b. Bagi Masyarakat

      Dapat berguna bagi masyarakat sebagai pengetahuan untuk menambah