1 PENDAHULUAN

Bagian pendahuluan akan menjelaskan terkait dengan latar belakang, perumusan masalah, tujuan, hipotesis, rencana kegiatan dan jadwal kegiatan berdasarkan penelitian tugas akhir yang dilakukan.

1.1 Latar Belakang

Tuntutan arus globalisasi, perubahan regulasi, dan tingkat persaingan yang kian ketat telah memaksa institusi perbankan tak terkecuali Bank Syariah mau tidak mau untuk berkembang mengikuti perkembangan teknologi Informasi. Beberapa produk teknologi dari dunia perbankan antara lain ATM (*Automated Teller Machine), Transfer Network*, dan *Electronic Funds Transfer* [1]. Implementasi kemajuan Teknologi Informasi selain membawa kemudahan juga membawa risiko tersendiri karena setiap organisasi atau Instansi yang memiliki hak akses akan data-data dan informasi sensitive pasti akan memiliki risiko keamanan. Terlebih jika data dan informasi yang dimiliki memiliki nilai ekonomi [2].

Bank Syariah, selaku bank terbesar di Indonesia tentunya melayani jutaan pelanggan setiap harinya. Mereka mengatur kegiatan ekonomi dengan menyimpan dan menjaga aset berharga serta keuangan para pelanggannya. Pada pelaksanaannya proses bisnis dapat dilakukan secara konvensional ataupun melalui aplikasi mobile. Dalam aplikasi ini beragam proses bisnis dapat dilakukan mulai dari transfer uang, membayar tagihan dan lainnya. Kompleksitas proses bisnis ini menyebabkan adanya kerentanan dan ancaman pada aset Bank Syariah.

Melihat kondisi seperti ini, Bank Syariah tentu dinilai sebagai entitas yang rentan terhadap risiko dan salah satu sasaran dari tindak kejahatan Siber (*Cybercrime).* Departemen CISO menjadi departemen yang bertugas untuk mencegah dan meminimalisir ancaman *Cyber* pada Bank Syariah, oleh karena itu departemen CISO memiliki nilai strategis yang tinggi dan perlu proteksi dari ancaman juga. Data yang dipublikasikan oleh FBI (*Federal Bureau of Investigation)* atau biro investigasi Amerika Serikat menyatakan terdapat kerugian yang signifikan akibat dari aktivitas *Cybercrime,* Hal tersebut dimuat dalam Internet Crime Report 2020 [3]. Meninjau fakta fakta yang telah didapat dari hasil penelitian sebelumnya tentu implementasi dari standar Manajemen Keamanan Informasi mutlak dibutuhkan dalam industri Perbankan. Standar tersebut

dibahas dalam ISO 27001:2013. Salah satu hal penting dalam standar ISO 27001:2013 ialah perlu dilakukannya pengelolaan risiko.

Sebagai salah satu upaya untuk mengelola risiko yang mungkin dapat timbul sehingga mendisrupsi proses bisnis pada Bank Syariah, perlu dilakukan kegiatan penilaian (*assessment)* risiko terhadap sistem yang ada. Beberapa aktivitas dalam penilaian nanti adalah identifikasi risiko, penilaian risiko itu sendiri dan mitigasi risiko. Serta Standar yang akan digunakan adalah ISO/IEC 27005:2018 yang mana adalah *framework* atau standar dalam melakukan proses Manajemen Risiko (di dalamnya termasuk proses *Risk Assessment)*. Dibanding dengan standar atau framework yang lain seperti NIST SP 800-30 dan Octave Allegro, ISO/IEC 27005 memiliki dokumentasi kontrol yang dibahas pada dokumen ISO 27002 [4]. Serta mengingat bahwa Bank Syariah sudah menggunakan standar ISO 27001 tentu masuk akan jika lebih baik menggunakan standar yang sama dan saling berkoresponden.

Penilaian risiko akan mengacu kepada metode FMEA *(Failures Modes and Effect Analysis)* yang merupakan metode penilaian risiko yang awalnya dikembangkan oleh militer Amerika Serikat dan sudah digunakan oleh banyak industri diantaranya industri *microchip,* dan Aeronautika [5]. Penelitian ini menggunakan metode FMEA untuk keperluan penilaian risiko karena FMEA akan menilai suatu risiko berdasarkan tiga kategori yang salah satunya adalah deteksi. Nilai Deteksi sangat berkorelasi dengan ancaman siber yang mana diperlukan kemampuan deteksi yang baik untuk menentukann ada tidaknya suatu ancaman di departemen CISO.

Dari hasil penilaian risiko tersebut diharapkan akan memberikan gambaran mengenai risiko yang ada pada aset-aset di Bank Syariah. Serta juga memberikan gambaran mengenai kesiapan aset menghadapi risiko. Pada akhirnya dapat menghasilkan rancangan mitigasi, rekomendasi perbaikan untuk penguatan keamanan pada Bank Syariah Departemen CISO *(Chief of Information Security Officer)*.

1.2 Perumusan Masalah

Berdasarkan pemaparan latar belakang penelitian ini, ada beberapa rumusan masalah yang dapat difokuskan menjadi beberapa hal untuk dibahas pada penelitian kali ini. Permasalahan yang ada meliputi :

1. Bagaimana penilaian risiko yang terjadi pada Bank Syariah dengan menggunakan standar ISO/IEC 27005:2018?
2 Bagaimana mitigasi risiko yang tepat untuk risiko tertentu pada Bank Syariah?

1.3 Batasan Masalah

Berikut adalah beberapa dari batasan masalah yang telah ditetapkan dan menjadi perhatian pada pelaksanaan penelitian ini :

1. Studi Kasus pada penelitian ini ialah Bank Syariah, secara khusus di departemen CISO *(Chief of Information Security Officer)*
2. Standar atau *Framework* yang akan diterapkan dalam penelitian ini adalah ISO/IEC 27005:2018 dan ISO/IEC 27001:2013
3. Penelitian akan menganalisis risiko berdasarkan aset-aset keamanan dan informasi yang ada pada Bank Syariah di Departemen CISO *(Chief of Information Security Officer)*.
4. Metode penilaian risiko yang digunakan adalah FMEA

1.4 Tujuan

Berdasarkan dengan apa yang teelah dirumuskan dalam rumusan masalah pada penelitian ini, dapat dideduksi bahwa tujuan dari dilakukannya penelitian ini adalah :

1. Melakukan proses penilaian risiko *(Risk Assessment)* terhadap risiko-risiko yang mungkin terjadi pada Departemen CISO *(Chief of Information Security Officer)* menggunakan standar ISO/IEC 27005:2018
2. Menyusun tindakan mitigasi yang tepat pada Departemen CISO *(Chief of Information Security Officer)* di Bank Syariah