BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi di era revolusi industri 4.0 menghadirkan banyak dimensi kehidupan seperti dimensi engineering, science dan networking. Riset *Georgia Tech's GVU Center* menjelaskan pengguna jaringan internet melakukan pencarian search engine (mesin pencarian) sebagai alat mendapatkan informasi (Nizar, 2009) dan melakukan pencarian informasi hingga memperoleh data, *file*, jurnal, *keyword*, *website*, laporan, dll. Dengan penggunaan teknologi, masyarakat dapat memanfaatkan sistem yang terhubung digital untuk memenuhi kebutuhan di berbagai sektor yang mempengaruhi sistem informasi, komunikasi, pertumbuhan ekonomi, stabilitas nasional dan kesejahteraan industri untuk mencapai tujuan.

Menurut *World Bank*, berdasarkan ITU (*International Telecommunication Union*) porsi pengguna internet di dunia mencapai jumlah 49 persen populasi pada tahun 2017, porsi tersebut meningkat pesat dibandingkan tahun 2000 yang hanya sekitar 6,7 persen. *Internet World Stats* memperkirakan porsi pengguna internet di dunia sebesar 64,2 persen populasi pada kuartal pertama tahun 2021. Adapun jumlah pengguna internet yang diperkirakan sebanyak lebih dari 5 miliar, jumlah ini meningkat 1.300 persen dibandingkan tahun 2000. Peningkatan jumlah pengguna internet di dunia tidak terlepas dari peningkatan serangan siber.

Di Indonesia, BSSN (Badan Siber dan Sandi Negara) melaporkan bahwa pada tahun 2018, terjadi 232,4 juta serangan ini, nyaris setengahnya atau sekitar

122.43 juta merupakan serangan malware. Pada tahun 2019, jumlah serangan meningkat menjadi 290 juta, pada tahun 2020 terjadi 316 juta serangan, pada tahun 2021terjadi 266 juta serangan, dan pada tahun 2022 terjadi 370 juta serangan. Dengan ini BSSN melaporkan bahwa tidak kurang dari 311 kasus pelanggaran data terjadi di Indonesia pada tahun 2022.

Dari jumlah tersebut, 248 pemangku kepentingan terkena dampak dugaan pelanggaran data tahun lalu. Sebanyak 20 pemangku kepentingan terkena dampak dugaan pelanggaran data dari sektor teknologi, informasi dan komunikasi (TIK), diikuti oleh 15 pemangku kepentingan dari sektor pertahanan yang terkena dampak dugaan pelanggaran data. Sebanyak 11 perusahaan di industri kesehatan juga terkena dampak dugaan pelanggaran data tersebut. Sementara itu, 61 pemangku kepentingan dari sektor lain mengetahui masalah ini. Ini termasuk 50 dugaan kebocoran data dan 99 laporan proaktif pemberitahuan dark web. (Laporan DataIndonesia.id, BSSN).

Gambar 1.1. Grafik Serangan Siber di Indonesia Per-Tahun 2018-2022

Menurut ISO (Organisasi Internasional untuk Standardisasi), ISO/IEC 27032:2012 bahwa teknologi informasi - teknologi keamanan - pedoman keamanan siber. *Cybersecurity* atau keamanan dunia maya adalah upaya untuk menjaga kerahasiaan, keutuhan, dan ketersediaan informasi di dunia maya. Dunia maya adalah lingkungan kompleks yang diciptakan oleh interaksi antara manusia, perangkat lunak, dan layanan online di Internet, didukung oleh perangkat teknologi informasi dan komunikasi (TIK) dan koneksi jaringan di seluruh dunia.

Menurut Cisco, keamanan siber sekarang adalah praktik melindungi sistem, jaringan, dan perangkat lunak dari serangan digital. Keamanan dunia maya untuk memperoleh, mengubah, atau menghancurkan informasi rahasia, memeras uang dari pengguna, atau mengganggu proses bisnis operasional. Berdasarkan hasil laporan Verizon, industri keuangan menjadi industri dengan jumlah pelanggaran data terbanyak, dengan 690 insiden. Diikuti oleh sektor profesional dengan 681 kasus pelanggaran data dan sektor kesehatan dengan 571 kasus. Data Verizon berasal dari rekaman investigasi forensik pihak ketiga berbayar dan operasi intelijen menggunakan Veris Webapp. Analisis dilakukan mulai 1 November 2020 hingga 31 Oktober 2021 dengan tingkat kesalahan 1,4 persen. Berdasarkan laporan Estonia National Cyber Security Index (NCSI), Indonesia menempati peringkat ke-83 dalam indeks keamanan siber, menunjukkan bahwa ruang siber Indonesia masih belum aman.

Sebagai tanggapan, aturan negara dan bank tidak bisa tinggal diam. Sistem keamanan digital harus diperkuat untuk mencegah kebocoran dan pembobolan data

nasabah di sektor keuangan. Atas fenomena tersebut, peneliti mengangkat tema *cybersecurity* karena banyaknya pembobolan data konsumen di era teknologi 4.0. Oleh karena itu, peneliti menulis skripsi ini dengan judul "**Analisis Implementasi *IT Governance* Menggunakan COBIT 5 Terhadap *Cybersecurity* Pada Bank XYZ (Studi Kasus)**" agar pembaca skripsi peneliti dapat digunakan sebagai referensi agar nasabah mampu menjaga kerahasiaan data dan perusahaan mampu menjaga rahasia nasabah.

Steve Albrecht dalam *Fraud Examination* (2003: 91) Prosedur (aktivitas) pengendalian baik adalah kebijakan dan praktik pengendalian fisik aset, otorisasi, pemisahan tugas, pemeriksaan independen, dan dokumentasi. Meskipun memiliki banyak keuntungan, analisis implementasi *IT Governance* terhadap cybersecurity pada bank xyz (studi kasus), memiliki pemasalahan seperti penggunaan waktu (overtime), perubahan lingkungan sistem, perubahan operasional, perubahan keamanan sistem dan perubahan manajemen yang terjadi pada saat ini. Karena itu, penelitian ini menggunakan COBIT 5 untuk mencapai hasil analisis implementasi *IT Governance* terhadap cybersecurity.

Di era Industri 4.0, teknologi informasi tidak hanya menjadi pendukung proses bisnis, tetapi menjadi elemen yang mengendalikan sebagian besar proses bisnis penting perusahaan dan memainkan peran kunci dalam pengambilan keputusan manajemen. Karena pentingnya peran teknologi informasi, pemangku kepentingan harus percaya bahwa manajemen memahami risiko dan memiliki kendali penuh atas teknologi informasi melalui *IT Governance* yang efektif.

Masalah ini telah menjadi kekuatan pendorong bagi organisasi untuk meninjau efektivitas *IT Governance*. Menurut Sambamurthy dan Zmud (1999), tata kelola TI dipahami sebagai model pemerintah/kebijakan untuk aktivitas TI (proses TI). Model ini mencakup pengembangan kebijakan dan pengelolaan infrastruktur TI, penggunaan TI yang efektif, efisien, dan aman oleh pengguna akhir, serta proses manajemen proyek TI yang efektif. Standar ISACA COBIT di AS mendefinisikan tata kelola TI sebagai "struktur hubungan dan proses untuk mengarahkan dan mengendalikan perusahaan untuk mencapai tujuan nilai bisnis sambil menyeimbangkan risiko yang terkait dengan kinerja TI dan prosesnya".

Sedangkan Oltsik (2003) mendefinisikan tata kelola TI sebagai sekumpulan kebijakan, proses/aktivitas dan prosedur yang mendukung operasi TI agar hasilnya konsisten dengan posisi strategi bisnis (strategi organisasi). Ruang lingkup tata kelola TI di perusahaan besar seringkali mencakup masalah yang berkaitan dengan manajemen perubahan, manajemen masalah, manajemen rilis, manajemen ketersediaan, dan bahkan manajemen tingkat layanan. Oltsik lebih lanjut menyatakan bahwa tata kelola TI yang baik harus berkualitas baik, proses berulang (metrik) yang terdefinisi dengan jelas dan terukur. Tata kelola TI yang dikembangkan dalam organisasi modern juga memiliki fungsi mendefinisikan (menguraikan) kebijakan TI, menetapkan proses TI yang kritis, mendokumentasikan aktivitas TI, termasuk mengembangkan perencanaan TI yang efektif berdasarkan perubahan lingkungan bisnis dan perkembangan TI..

Dengan ini penerapan *IT Governance* menjadi faktor penting untuk dapat

memastikan keamanan siber. Kerangka kerja untuk membantu pengelolaan *IT Governance* Bank XYZ adalah menggunakan metode COBIT 5 (*Control Objectives for Information and Related Technology* 5) kerangka kerja untuk mengelola dan monitoring penggunaan teknologi informasi di perusahaan Bank XYZ termasuk dalam aspek keamanan dan perlindungan data pribadi nasabah. Bank XYZ merupakan bank terbesar di Indonesia yang memiliki tanggung jawab menjaga keamanan siber.

Berdasarkan pemaparan di atas selain dengan bagusnya *IT Governance* sebaiknya kita perlu mengingat terhadap kasus terdahulu sebagai evaluasi bahwa *IT Governance* masih perlu untuk ditingkatkan, dengan mempertimbangkan insiden-insiden yang terjadi selama *IT Governance* beroperasi di perusahaan perbankan indonesia, seperti kasus yang terjadi di BNI diaman pada bulan Maret – Juli 2022. Dengan adanya Modus Pelaku Penggandaan Data Mobile Banking 150 Nasabah Bank BUMN, dimana terjadinya pembobolan data rekening nasabah yang dilakukan oleh dua pelaku dengan menduplikasi rekening nasabah, dimana data nasabah yang terdiri dari *username, password* dan *Personal Identification Number* (PIN) digandakan menggunakan aplikasi khusus. Total kerugian akibat pembobolan data nasabah mencapai lebih dari Rp 800 juta, dan pada tanggal 17 Juli 2023, BNI telah melaporkan dugaan tindak pidana kejahatan informasi dan transaksi elektronik ke Polda Metro Jaya terkait modus penipuan yang mengatasnamakan BNI dengan berkedok kenaikan biaya transfer antar bank. Informasi palsu tersebut disebar melalui aplikasi pesan elektronik, email, dan media sosial.

Dari penjelasan tersebut “Analisis Implementasi *IT Governance* Menggunakan COBIT 5 terhadap Cybersecurity Pada Bank XYZ (Studi Kasus)” bertujuan untuk menganalisis implementasi *IT Governance* terhadap cybersecurity pada bank xyz menggunakan software COBIT 5 dan disusun dengan memperhatikan permasalahan digital yang begitu krusial pada saat ini. Oleh karena itu, penelitian ini fokus pada proses analisis implementasi *IT Governance* menggunakan COBIT 5 *cybersecurity* pada Bank XYZ. Diharapkan hasil dari penelitian ini dapat memberikan informasi berguna bagi Bank XYZ dan institusi keuangan lain dalam mengelola *cybersecurity* agar lebih efektif.

1.2 Identifikasi Masalah

Adapun pada penjelasan latar belakang diatas dapat diketahui bahwa di era digital saat ini, analisis implementasi *IT Governance* terhadap cybersecurity pada bank xyz (studi kasus) menjadi hal penting. Oleh karena itu, identifikasi masalah pada penelitian ini diantarannya :

1. Peran COBIT 5 dalam analisis implementasi *IT Governance* terhadap keamanan siber pada Bank XYZ .
2. Peran Capability level dari *IT Governance* dan *Good Corporate Goverrnance* pada Bank XYZ menggunakan COBIT 5.
3. Kematangan Capability level terhadap penggunaan framework COBIT 5 sebagai referensi audit TI dan penilaian *IT Governance* terhadap keamanan siber pada Bank XYZ dengan proses pengonsepan dan pengelolaan (APO), akuisisi dan penerapan (BAI), penguraian dan dukungan (DSS), dan pemeriksaan (MEA).

Dengan mengidentifikasi masalah-masalah tersebut, penelitian ini dapat memberikan wawasan yang berharga dalam meningkatkan implementasi *IT Governance*, mengatasi tantangan keamanan siber, memastikan kepatuhan terhadap standar industri, melindungi data pribadi nasabah, dan mengambil pembelajaran dari kasus-kasus terkenal untuk mendorong perbaikan dalam lingkungan perbankan Bank XYZ.

1.3 Pembatasan Masalah

Batasan masalah dalam penelitian ini adalah berfokus pada perbankan dan *IT Governance* menggunakan COBIT 5 terhadap cybersecurity dalam kasus bank, dimana ruang lingkup wilayah dalam penelitian ini adalah Bank Negara Indonesia (Bank BNI) di wilayah Jakarta Selatan tepatnya di Kantor Pusat Memara BNI Pejompongan, tidak dengan bank lainnya atau bank sejenis BNI di wilayah lainnya.

1.4 Rumusan Masalah

Selain memiliki identifikasi dan pembatasan masalah, pada penelitian ini, peneliti akan membahas beberapa rumusan masalah. Berdasarkan latar belakang yang dijelaskan, penelitian berfokus pada analisis implementasi *IT Governance* menggunakan kerangka kerja COBIT 5 terhadap cybersecurity pada Bank XYZ. Rumusan masalah penelitian ini adalah :

1. Bagaimana menerapkan framework COBIT 5 pada Bank XYZ untuk meningkatkan keamanan siber ?
2. Bagaimana tingkat maturity yang ada di Bank XYZ ketika diukur dengan COBIT 5 ?
3. Bagaimana Solusi dan analisis GAP COBIT 5 untuk Penanganan

serangan siber yang dialami pada Bank XYZ ?

1.5 Tujuan Penelitian

Tujuan dari penelitian ini dalam menganalisis implementasi *IT Governance* terhadap cybersecurity pada Bank XYZ menggunakan kerangka kerja COBIT 5, adalah:

1. Analisis penerapan framework COBIT 5 untuk meningkatkan keamanan siber.
2. Untuk mengukur tingkat maturity yang ada di Bank XYZ dengan COBIT 5.
3. Untuk menganalisis solusi dan GAP COBIT 5 untuk Penanganan serangan siber yang dialami pada Bank XYZ.

1.6 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan hasil pengujian literatur serta saran manajerial insight yang dapat menjadi pertimbangan bagi para manajemen yang meneliti hal serupa di masa mendatang. Adapun manfaat penelitian ini yaitu:

1. Menjadi saran Bank XYZ bagaimana meningkatkan keamanan siber dari serangan siber yang membahayakan.
2. Bagi industri perbankan, penelitian ini memberi gambaran implementasi *IT Governance* dalam menjaga keamanan siber untuk meningkatkan sistem keamanan siber perbankan secara umum.
3. Bagi peneliti selanjutnya, penelitian menjadi referensi peneliti selanjutnya yang ingin melakukan penelitian implementasi *IT Governance* terhadap *cybersecurity* industri perbankan, serta sebagai acuan dalam menggunakan

metode penelitian COBIT 5.

4. Bagi masyarakat, penelitian ini memberikan pemahaman yang lebih baik mengenai pentingnya implementasi *IT Governance* terhadap *cybersecurity* industri perbankan, serta sebagai acuan dalam menggunakan metode penelitian COBIT 5.

1.7 Sistematika Penulisan

Sistematika penulisan untuk mempermudah pembaca memahami maksud dan tujuan penelitian, adapun sistematika penulisan penelitian ini yaitu :

BAB I PENDAHULUAN

Bab ini menjelaskan pendahuluan pada penelitian ini yang berisikan latar belakang masalah, identifikasi masalah, pembatasan masalah, perumusan masalah, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini menjelaskan pembahasan tinjauan pustaka dengan menguraikan teori serta pengertian yang akan digunakan pada penelitian ini. Bab ini juga akan membahas kerangka pemikiran serta hipotesis penelitian.

BAB III METODE PENELITIAN

Pada bab ini akan berisikan objek penelitian, populasi dan sampel , jenis dan sumber data yang digunakan, metode pengumpulan data, serta metode analisis data yang digunakan dalam melakukan analisis masalah pada penelitian.

BAB IV ANALISIS DAN PEMBAHASAN MASALAH

Pada bab ini akan membahas pengujian hipotesis penelitian serta penyajian hasil dari pengujian hipotesis tersebut. Selain itu bab ini juga akan membahas hasil

pengujian dengan teori terkait.

BAB V KESIMPULAN DAN SARAN

Pada bab ini akan berisikan kesimpulan dari hasil pengujian yang dilakukan pada Bab IV, keterbatasan masalah penelitian, serta saran penelitian selanjutnya.