BAB II
LANDASAN TEORI

2.1 IT Audit

Audit adalah suatu proses sistematik yang dijalankan dengan mempertimbangkan objektivitas pihak-pihak yang berwenang dan independen dalam memperoleh dan mengevaluasi data-data yang berkaitan dengan klaim yang berkaitan dengan suatu kondisi atau peristiwa. Sasaran audit adalah untuk mengetahui dan memberikan tingkat kemiripan antara informasi yang dinilai dengan ukuran atau kriteria yang ada [8]. Audit TI adalah audit tersendiri, terpisah dari audit laporan keuangan, yang dijalankan untuk menguji *maturity* dan kesiapan organisasi dalam mengelola teknologi informasi (tata kelola TI). Tingkat kesiapan (*maturity level*) diukur dari tata kelola informasi, tingkat kepedulian seluruh pemangku kepentingan terhadap posisi saat ini dan tujuan yang diharpkan di masa depan. Oleh karena itu, perencanaan TI tidak boleh dilakukan secara sembarangan [9] Tujuan audit adalah untuk mengumpulkan informasi faktual dan bermakna berupa data hasil analisis, penilaian, dan rekomendasi auditor yang dapat digunakan oleh pihak yang diaudit atau direksi untuk berbagai tujuan, misalnya sebagai dasar pengambilan keputusan dan pengelolaan, mengendalikan, meningkatkan, atau mengubah berbagai aspek dengan tujuan memastikan kebijakan dan mencapai tujuan organisasi bersama..

2.2 Manajemen Risiko

Definisi manajemen risiko adalah suatu pengendalian risiko yang memiliki tujuan untuk meningkatkan nilai perusahaan dalam menangani masalah organisasi secara menyuluruh [10]. Manajemen risiko dapat di artikan sebagai proses identifikasi, pengukuran dan kontrol dari sebuah risiko yang menyerang aset dari sebuah perusahaan atau proyek yang dapat menimbulkan gangguan atau kerugian pada perusahaan tersebut [11]. Ancaman terhadap keamanan dapat terjadi karena alam, manusia, yang berifat kelalaian atau kesengajaan, antara lain [12] :

a) Ancaman kebakaran

Beberapa tindakan keselamatan jika terjadi bahaya kebakaran:

a. Memiliki alat pemadam kebakaran otomatis dan tabung pemadam kebakaran.
b. Memiliki pintu/tangga darurat
c. Melakukan pemeriksaan dan pengujian sistem proteksi kebakaran secara berkala untuk memastikan semuanya terpelihara dengan baik..

b) Ancaman banjir

Beberapa tindakan pengamanan jika terjadi risiko banjir :

a. Memastikan material atap, dinding, dan lantai kedap air
b. Semua material asset informasi di taruh di tempat yang tinggi
c. Perubahan tegangan sumber energi
d. Pelaksanaan pengaman untuk mengantisipasi perubahan tegangan sumber energi, misalnya : menggunakan *stabilizer* atau *power supplay* (UPS).

c) Kerusakan Strukural

Melakukan tindakan perlindungan untuk mencegah kerusakan struktur. Contohnya : Pilih lokasi perusahaan yang jarang terjadi gempa bumi, angin topan, dan banjir.

d) Penyusup Pelaksanaan pengamanan mencegah penyusup meliputi kehadiran personel keamanan dan penggunaan sistem alarm atau kamera pengintai.

e) Virus

Pelaksanaan tindakan pengamanan untuk mencegah virus adalah :

a. Tindakan preventif seperti menginstal program antivirus dan update secara berkala.
b. Detektif, misalnya memindai file sebelum digunakan.
c. Korektif, Menggunakan program antivirus pada file yang terinfeksi dan memastikan cadangan data bebas virus.

f) Hacking

Beberapa langkah keamanan telah diterapkan untuk mencegah peretasan:

a. Penggunaan *control logical* seperti pengguanaan *password* yang sulit ditebak. Personil keamanan secara teratur memantau sistem yang digunakan.

g) Kegagalan jaringan, kegagalan sistem dan data

Beberapa tindakan pengamanan untuk mencegah risiko tersebut:

a. *Recovery Time Objectives* (RTO) adalah waktu yang diperlukan untuk memulihkan sistem dan data. Jika terdapat ketergantungan antar komponen layanan atau antar komponen layanan, waktu pemulihan untuk komponen yang saling bergantung dihitung secara berurutan. Jika komponen layanan tidak bergantung satu sama lain, waktu pemulihan dapat dihitung secara paralel antar komponen layanan. Maksimum RTO adalah 80% dari maksimum waktu layanan tidak befungsi yang ditoleransi atau MTDL.

b. *Recovery Point Objectives* (RPO) adalah ambang batas jumlah data yang dapat hilang sejak pencadangan terakhir. Jika pencadangan dilakukan sekali sehari pada malam hari dan kerusakan sistem/memori dapat terjadi beberapa menit sebelum operasi pencadangan dilakukan, nilai RPO adalah 24 jam. Dengan kata lain, RPO menunjukkan periode hilangnya informasi/data.

2.3 Keamanan Informasi

Keamanan informasi merupakan sebuah bentuk perlindungan informasi dan elemen pentingnya, seperti kerahasiaan, integritas, dan ketersediaan, termasuk sistem dan perangkat keras untuk menampung dan mengirimkan informasi tersebut. Tiga aspek penting keamanan informasi, yaitu [13]:

1. Kerahasiaan (*Confidentiality*) Kerahasiaan adalah elemen yang menjamin bahwa informasi hanya dapat diakses oleh pihak yang berwenang untuk mengaksesnya.
2. Integritas (*Integrity*) Integritas adalah elemen yang menjamin terjaganya kualitas, kelengkapan, dan kelengkapan data sesuai dengan keaslian data.
3. Ketersediaan (*Availability*) Kerahasiaan adalah elemen yang menjamin bahwa pihak-pihak yang mempunyai akses terhadap informasi dapat mengaksesnya dalam format yang mereka perlukan tanpa campur tangan atau hambatan.

Masing-masing hal di atas berperan terhadap program keamanan informasi secara menyeluruh. Keamanan informasi adalah perlindungan informasi, meliputi perangkat dan sistem yang dipakai untuk menyimpan dan mengirimkan informasi tersebut. Melindungi informasi dari berbagai ancaman dapat menjamin kelangsungan bisnis, mengurangi kerugian akibat ancaman, dan meningkatkan investasi dan peluang bisnis.

2.4 *Cybersecurity* NIST *Framework*

NIST (*National Institute of Standard and Technology*) merupakan panduan standar dari Pemerintah Federal US dalam melakukan penilaian Manajemen Risiko untuk Sistem Teknologi Informasi. Metodologi ini dirancang untuk menilai perhitungan kualitatif yang didasarkan pada analisa keamanan yang sesuai publik inginkan, sehingga secara teknis pada bagian sistem ini petugas teknis benar-benar mengidentifikasi, mengevaluasi dan mengelola risiko pada sistem TI. Proses ini meliputi segala sesuatu dari ancaman-sumber identifikasi untuk evaluasi berkelanjutan dan penilaian, yang sangat komprehensif. *Framework* ini dapat menjadi acuan untuk meningkatkan keamanan *cybersecurity* yang menyediakan panduan implementasi melalui proses tujuh langkah.

- *Step 1: Prioritize and Scope*
- *Step 2: Orient*

- *Step 3: Create a Current Profile*
- *Step 4: Conduct a Risk Assessment*
- *Step 5: Create a Target Profile*
- *Step 6: Determine, Analyze, and Prioritize Gaps*
- *Step 7: Implement Action Plan*

Pada NIST terdapat 5 *Compenen* utama sebagai berikut ini (nistgov):

- *Fungction*

  Mengatur kegiatan keamanan *cyber* dasar pada level tertingginya. FungSI-fungsi ini yaitu *Identify, Protect, Detect, Respond, Recover*. Juga membantu organisasi menyatakan manajemen risiko keamanan *cyber*nya dengan mengatur informasi, sehingga memungkinkan keputusan manajemen risiko, mengatasi ancaman, dan meningkat dengan belajar dari kegiatan sebelumnya. Fungsi ini juga selaras dengan metodologi yang ada untuk manajemen insiden dan membantu menunjukkan dampak investasi pada keamanan *cyber*. Misalnya, investasi d alam perencanaan dan pelaksanaan mendukung tindakan respons dan pemulihan secara tepat waktu, yang mengakibatkan berkurangnya dampak pada pemberian layanan.
- *Category*

  Adalah subdivisi dari suatu *fungction* dalam kelompok hasil keamanan *cyber* yang terikat erat dengan kebutuhan terprogram dan kegiatan tertentu.
- *Subcategory*

  Selanjutnya membagi kategori menjadi hasil teknis dan/atau manajemen kegiatan spesifik. sub kategori memberikan serangkaian hasil yang, meskipun tidak menyeluruh,

membantu mendukung pencapaian hasil pada masing-masing kategori.

- Referensi Informatif

  Pada komponen ini memberikan informasi dan refrensi untuk perusahan. Hal ini bertujuan untuk membantu perusahaan dalam melalukan pecegahan dan peningkatan sistem dan tekonlogi informasi berdasarkan sumber yang valid seperti *Top 20 Critical Security Controls* (CCS CSC) dan Cobit.

Berdasarkan fungsi dari *framework* NIST terdapat 5 fungsi utama sebagai berikut ini [14]:

Gambar 2. 1 Framework NIST Cybersecurity

- *Identify* - Fungsi dari *Identify* adalah untuk membantu mengidentifikasi seluruh aset IT yang terdapat pada organisasi tersebut supaya lebih mudah untuk melakukan *cybersecurity management.*
- *Protect* - Fungsi dari *protect* yaitu untuk melakukan proteksi terhadap aset IT yang terdapat pada organisasi sehingga dapat meminimalisir potensi *cyber attacks*.

- *Detect* - Pada tahap ini, organisasi melakukan pemantauan terhadap aktivitas yang terjadi pada infrastruktur IT agar dapat mengetahui lebih cepat jika terjadi aktivitas yang tidak normal pada infrastruktur IT.
- *Respond* - Fungsi dari *respond* yaitu ketika terjadi kerusakan pada aset TI, organisasi harus melakukan tindakan yang tepat untuk meminimalisir kerusakan tersebut.
- *Recovery* - Pada tahap *recovery,* organisasi melakukan pemulihan terhadap kerusakan aset IT akibat *cyber attacks* agar dapat beroperasi seperti semula.

2.5 *WatchTowr*

WatchTowr merupakan sebuah alat yang digunakan untuk memahami postur keamanan *cyber* sebuah perusahaan dari sudut pandang musuh agar perusahaan dapat mendeteksi dan memitigasi potensi ancaman secara langsung [15]. *WatchTowr* melakukan integrase, mengenali, memvisualisasikan, dan bertindak pada setiap ancaman dan risiko yang masuk atau menyerang. Mengautentikasi data streaming dan mencatat transaksi streaming sekaligus meningkatkan keamanan dengan mencegah akses tingkat rendah ke API gRPC. Mesin Adversary Sight *WatchTowr* memberikan pandangan penyerang terhadap permukaan serangan eksternal Anda, menggunakan teknik pengintaian di dunia nyata. Platform SaaS yang tidak dikenal, penyedia infrastruktur, lingkungan cloud, anak perusahaan, dan TI bayangan adalah sasaran empuk bagi penyerang.

2.6 Penelitian Terdahulu

Terdapat penelitian terdahulu yang digunakan sebagai sumber referensi untuk mendukung pengerjaan penelitian ini. Berikut ini adalah penelitian terdahulu yang digunakan antara lain:

Table 2. 1 Tabel penelitian terdahulu

No	Peneliti	Tahun	Nama Jurnal	Metode	Hasil Penelitian
1	Tony Tan, Benfano Soewito	May 2022	Manajemen Risiko Serangan *Cyber* Menggunakan *Framework Nist Cybersecurity* Di Universitas ZXC	Dalam penelitian ini, mereka mengkaji keamanan *cyber* di ZXC University menggunakan kerangka keamanan *cyber* NIST. Pengumpulan data dilakukan melalui wawancara, dokumen tasi kejadian, dan observasi. Evaluasi 39 sistem layanan web dan situs web. Penulis juga menggunakan alat Nessus untuk mengevaluasi tingkat cacat dan ancaman	Dengan menggunakan Kerangka Keamanan *Cyber* NIST, Universitas ZXC didukung untuk menilai keamanan *cyber* saat ini. *Framework* ini juga sangat cocok digunakan karena dapat beradaptasi dengan perubahan dan perkembangan teknologi di masa depan. Tidak hanya bagi ZXC University, rekomendasi penggunaan NIST *Cybersecurity Framework* juga

No	Peneliti	Tahun	Nama Jurnal	Metode	Hasil Penelitian
					dapat diterapkan di tempat lain, termasuk universitas.
2	Victor Ilyas Sugara, Hadi Syahrial, Muhammad Syafrullah	Januari 2019	Sistem Pemeriksa Keamanan Informasi Menggunakan *National Institute Of Standards And Technology (NIST) Cybersecurity Framework*	Metode yang digunakan sebagai *best practice* adalah *National Institute of Standards and Technology* (NIST) *Cybersecurity Framework*.	Hasil pengujian Identifikasi 16,67%, Proteksi 32,86%, Deteksi 25%, Respon 23,33%, dan Pemulihan 58,33%. Namun secara keseluruhan skor NIST Security *Framework* yang diperoleh hanya sebesar 27,55%. Hal ini membuktikan kemampuan keamanan informasi PT NPI masih sangat lemah. Memang banyak fungsi NIST *Cybersecurity Framework* yang belum sepenuhnya diterapkan sehingga menimbulkan 3kerentanan keaman

No	Peneliti	Tahun	Nama Jurnal	Metode	Hasil Penelitian
					an informasi di PT N4PI.
3	Suhardjono, Arman Syah Putra, Nurul Aisyah,V.H. Valentino	2020	*Analysis Of Nist Methods On Facebook Messenger For Forensic Evidence*	NIST, dengan metode ini dapat diuraikan satu persatu tahapan yang akan dilakukan. Selain itu digunakan juga metode *Literature review* untuk melakukan analisis terhadap *Facebook Messenger* yang akan digunakan sebagai tempat uji dalam penelitian ini sehingga dapat dibuktikan adanya bukti forensik	Pe5nelitian ini menghasilkan bukti ber6upa gambar, konten obrolan, dan suara. Membuktikan bahwa menggunakan metode NIST, dapat ditemukannya bukti forensik terhadap *Facebook Messenger* sehingga dapat digunakan sebagai bukti di kemudian hari.
4	Lawrence A. Gordon, Martin P. Loeb, Lei Zhou	2020	*Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model*	*Model GL, Cybersecurity risk managemen*	Analisis menunjukkan bahwa Model GL memberikan pendekatan logis untuk digunakan ketika mempertimbangkan aspek biaya-manfaat dari investasi keamanan *cyber* selama proses

No	Peneliti	Tahun	Nama Jurnal	Metode	Hasil Penelitian
					organisasi dalam memilih tingkat Tingkat Implementasi NIST yang paling sesuai.
5	Najat Tissir, Said El Kafhali , Noureddine Aboutabit	2020	*Cybersecurity Management In Cloud Computing: Semantic Literature Review And Conceptual Framework Proposal*	Metode penulisan artikel ilmiah ini adalah dengan metode kualitatif dan kajian pustaka (*Library Research*). Mengkaji teori dan hubungan kebutu han manajemen keamanan *cyber* di *Cloud Computing*	Memberikan panduan kepada organisasi tentang cara menetapkan pendekatan yang tepat terhadap manajemen risiko keamanan *cyber* di *Cloud Computing* atau untuk melengkapi proses yang sudah mereka miliki
6	Pandey, S., Singh, R.K., Gunase karan, A. and Kaush ik, A	2020	*Cyber Security Risks In Globalized Supply Chains: Conceptual Fram ework*	Makalah ini mencoba mengidentifikasi risiko keamanan *cyber* di *supply chain global*. Mereka selanjutnya mencoba mengkategorikan risiko keamanan *cyber* ini dari sudut pandang strategis	Makalah ini memperkenalkan fenomena baru dalam bidang manajemen yang mempunyai potensi untuk menyelidiki bidang-bidang penelitian baru di masa depan. Berdasarkan kategorisasi tersebut,

No	Peneliti	Tahun	Nama Jurnal	Metode	Hasil Penelitian
					makalah ini memberikan wawasan tentang bagaimana risiko keamanan *cyber* berdampak pada kelangsungan operasi *supply chain.*
7	Mohamed JumahALDhanhani, Jessnor Elmy Mat Jizat	2021	*Review of Cyber Security on Oil and Gas Industry in United Arab Emirates: Analysis on the Effectiveness of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework*	Metodologi penelitian yang digunakan dalam penelitian ini didasarkan pada tinjauan sistematis literatur terkini mengenai keamanan *cyber* dan kerangka kerjanya	Pendekatan yang efektif untuk memerangi kejahatan *cyber*, mengingat fleksibilitasnya yang mendorong perbaikan berkelanjutan. Secara khusus, struktur kerangka ini dapat membantu pemangku kepentingan untuk mengidentifikasi potensi ancaman dan selanjutnya menerapkan langkah-langkah untuk menjaga keamanan sistem informasi

No	Peneliti	Tahun	Nama Jurnal	Metode	Hasil Penelitian
8	Kamalanathan Kandasamy, Sethuraman Srinivas, Krishnashree Achuthan & Venkat P. Rangan	2022	*Iot Cyber Risk: A Holistic Analysis Of Cyber Risk Assessment Frameworks, Risk Vectors, And Risk Ranking Process*	Metode pemeringkatan risiko unik untuk menentukan peringkat dan mengukur risiko IoT diperkenalkan dalam penelitian ini. Metode pemeringkatan ini mengawali pendekatan penilaian risiko secara eksklusif untuk sistem IoT dengan mengkuantifikasi vektor risiko IoT, sehingga menghasilkan strategi dan teknik mitigasi risiko yang efektif	Pengenalan model komputasi risiko IoT baru, yang menghitung dampak risiko dan kemungkinan risiko, yang menghasilkan risiko.
9	Aileen Angelin, Ahmad Faza	2023	Evaluasi Tata Kelola Teknologi Informasi Menggunakan *Framework* Cobit 2019 Pada PT XYZ	*Framework* COBIT 2019 pada focus area keamanan dan pendekatan kualitatif dengan melakukan pengumpulan data melalui proses wawancara dan studi literatur	Rekomendasi yang diberikan berfokus pada pengelolaan pencatatan risiko yang berhubungan dengan keamanan proses bisnis dan sumber daya TI, memastikan semua karyawan memahami

No	Peneliti	Tahun	Nama Jurnal	Metode	Hasil Penelitian
					peran dan tanggung jawabnya dalam mengelola keamanan informasi, dan pembuatan laporan mengenai pemantauan permintaan layanan dan penyelesaian insiden.
10	Gavrilla Claudia	2023	Evaluasi dan Rekomendasi Sistem Manajemen Keamanan Informasi pada PT XYZ Berdasarkan Standar ISO 27001:2013 Menggunakan Indeks KAMI	*PDCA (Plan-Do-Check-Act menggunakan indeks KAMI dan ISO 27001)*	Diketahui bahwa PUSDATIN berhenti pada level 1+ diarea warna kuning dan dinyatakn "perlu perbaikan", oleh karena itu dibuatkan rekomendasi yang di hasilkan dari temuan indeks KAMI dan dibandingkan dengan *control* ISO 27001

Berdasarkan pada penelitian terdahulu, seperti yang telah dicantumkan pada tabel 2.1, ada beberapa jurnal yang memiliki persamaan dan juga perbedaan. Untuk persamaan antara penelitian saat ini dan dahulu yaitu melakukan penelitian mengenai system keamanan informasi seperti jurnal 1,2,3, dan 10, selain itu adapun juga persamaan penelitian terdahulu dengan penelitian yang sekarang ialah memakai framework NIST Cybersecurity untuk

melakukan peningkatan keamanan siber yang sama seperti jurnal 1 hingga 8. Sedangkan perbedaan penelitian terdahulu dan penelitian yang dilakukan saat ini adalah, ruang lingkup penelitian yang berbeda serta *framework* yang digunakan beberapa penelitan berbeda seperti jurnal 9 & 10 dan penelitian ini menggunakan *tools* vulnerability scanning yaitu WatchTowr sebagai alat untuk mengidentifikasi kerentanan pada setiap sistem operasi web dan situs web sehingga setiap sistem operasi web dan situs web dapat meningkatkan keamanannya. Bukan hanya meningkatkan keamanan siber tetapi penelitian saat ini juga akan dilakukan penentuan prioritas pada penanganan setiap serangan yang masuk.