2. LANDASAN TEORI

2.1 Konsep *Supply Chain Management* dan *Cyber Supply Chain Risk Management*

Supply Chain Management (SCM) adalah berbagai aktivitas yang mengatur dalam proses perencanaan, pengendalian, dan pelaksanaan distribusi suatu produk yang berupa proses merespons permintaan dalam jumlah besar, menyediakan sumber daya untuk permintaan ini, dan menyediakan produksi, logistik, penyimpanan, dan transportasi barang dilakukan secara efektif dengan memeriksa ulang proses yang diperlukan untuk mengoptimalkan aliran bahan mentah, informasi, dan modal (Serkan K. & Baygin, 2022, p. 78-80). Pengertian ini sejalan dengan konsep yang dikemukakan oleh Chopra & Meindl (2016) pada buku "*Supply Chain Management: Strategy, Planning, and Operation",* yang menyatakan bahwa SCM yang baik dan dapat menguntungkan perusahaan ialah SCM yang dapat mengoptimalkan waktu dalam pengiriman barang kepada pelanggan ataupun mitra dengan cepat dan tepat waktu, serta mempunyai *Internal Supply Chain Management* (ISCM)[5] yang terstruktur serta efisien dan efektif dalam SCM sehingga dapat mengatasi jika serangan *cyber* ataupun gangguan operasionalnya agar mempunyai SOP dan pedoman yang terstruktur yang lengkap dan rinci sehingga memudahkan dalam panduan ataupun tuntunan perusahaan jika terjadi adanya masalah dalam gangguan operasional.

Dalam hal mencapai proses *supply chain* yang optimal dalam operasionalnya, perusahaan mulai menggunakan suatu sistem *software* yang dapat membantu dalam meningkatkan efisiensi dan efektivitasnya. Salah satu *software* yang banyak digunakan dalam mengatur seluruh proses bisnis dalam suatu perusahaan menjadi satu kesatuan dalam pengintegrasian suatu sistem informasi perusahaan yaitu *Entreprise Resource Planning* (ERP)[6] (Heizer et al., 2019, p.618). Hal ini juga sejalan dengan pernyataan Serkan K. & Baygin (2022), mengingat bahwa era dunia bisnis sekarang yang semakin terdigitalisasi bahwa sudah menjadi suatu keharusan bagi perusahaan untuk memenuhi tuntutan menjadi perusahaan yang menerapkan sistem operasional yang lebih terdigitalisasi dan tersistematis dalam perangkat lunak sehingga dapat melakukan manajemen

[5] *Internal Supply Chain Management* (ISCM): Seluruh proses internal yang berkaitan dengan perusahaan, seperti: perencanaan kapasitas produksi dan penyimpanan internal, persiapan rencana permintaan dan pasokan,dan pemenuhan pesanan, dan sebagainya.

[6] *Entreprise Resource Planning* (ERP): Sistem perangkat lunak yang dirancang untuk mengintegrasikan dan mengelola semua aspek operasional dan fungsional dalam suatu perusahaan atau organisasi, seperti: mengintegrasikan berbagai proses bisnis manufaktur, keuangan, sumber daya manusia, distribusi, logistik, penjualan, dan layanan pelanggan ke dalam satu platform atau database tunggal.

data dalam proses SCM sehingga lebih mudah diakses untuk membantu proses bisnis agata efisien dalam operasionalnya, terlebih jika perusahaan tersebut berskala besar agar menciptakan proses SCM yang lebih efisien dengan biaya seminim mungkin namun namun menghasilkan *output* yang maksimal. Setiap kelebihan digitalisasi pastinya ada kelemahannya juga, terlebih lagi jika prose SCM berkaitan erat dengan teknologi infromasi. Kelemahannya adalah resiko serangan *cyber* dapat berupa kehilangan data ataupun disusupi oleh oknum yang tidak bertanggung jawab baik dapat berupa gangguan dari internal perusahaan maupun ancaman dari eksternal perusahaan (Ahmadi et al., 2021; Ghadge et al., 2019; Serkan K. & Baygin, 2022). Pernyataan ini didukung oleh kasus yang terjadi beberapa tahun lalu, kasus pertama ialah kasus yang terjadi di pelabuhan Belgia adanya serangan *cyber* terhadap sistem teknologi informasi beberapa perusahaan untuk menyalahgunakan distribusi kontainer yang berisi kokain oleh oknum pengedar narkoba, yang berlangsung selama dua tahun (BBC *News*, 2013). Kasus kedua ialah serangan *cyber* pada perusahaan pengiriman barang berskala internasional yang mengalami kerugian 300 juta US *Dollar* (Creazza et al., 2021; Williams, 2017).

Permasalahan yang telah dijabarkan sebelumnya mendorong pengembangan solusi berupa *Cyber Supply Chain Risk Management* (CSCRM) yang merupakan suatu strategi manajemen perusahaan yang berfokus pada penilaian dan langkah preventif dari risiko serangan *cyber* dalam seluruh proses *supply chain*, yang mengkombinasikan proses, sumber daya manusia, dan teknologi menjadi suatu sistem terintegrasi di antara para pelaku *Supply chain* yang bersangkutan (Creazza et al., 2021). Menurut Creazza et al. (2021) yang mengutip dari Pandey et al. (2020), bahwa adanya CSCRM yang baik pada suatu perusahaan adanya kesiapsiagaan akan segala resiko serangan *cyber* agar terhindar dari segala kerugian bagi perusahaan. Penilaian konteks CSCRM dalam penelitian ini dinilai dari pengaturan *System Integration* dan *Governance* perusahaan yang menjadi objek penelitian dengan mediasi melalui CSC *Visibility* dan kontribusinya dalam mencapai CSC *Performance* yang efisien dan efektif bagi seluruh pemangku kepentingannya.

2.2 *Governance*

2.2.1 Pengertian *Governance*

Governance diartikan sebagai suatu penataan tata kelola perusahaan untuk proses pengambilan keputusan yang tepat dengan adanya penyesuaian proses, metode, kebijakan dan struktur perusahaan untuk dikoordinasikan dengan individu, proses operasional, dan teknologi dalam yang digunakan dalam perusahaan untuk mengoptimalkan proses bisnis (Ahmadi et al.,

2021). Menurut penelitian sebelumnya Gani et al. (2022), *Governance* memiliki makna yaitu struktur tata kelola yang selaras dan beriringan dengan padu antara semua anggota perusahaan yang berkaitan dengan pengambilan keputusan *supply chain management* sehingga pada saat adanya suatu kendala dalam serangan *cyber* perusahaan mempunyai SOP yang lengkap dan rinci yang menjadi panduan yang menuntun dalam intruksi kerja jika terjadi gangguan operasional terutama dalam mengatasi serangan *cyber* baik secara gangguan maupun ancaman serangan *cyber.* Menurut Maleh et al. (2021), *Governance* memiliki pengertian penataan pengelolaan aset informasi organisasi yang baik. Aset-aset ini dapat berupa data informasi yang berupa pertimbangan untuk mengelola risiko operasional bisnis, data bisnis, dan biaya dalam operasional bisnis. Berdasarkan beberapa makna yang dijabarkan dapat disimpulkan bahwa *Governance* adalah suatu pengelolaan perusahaan yang digunakan untuk mengambil keputusan dalam proses bisnis agar dapat berjalan dengan efektif dan efisien baik dalam biaya maupun waktu.

2.2.2 Faktor-Faktor Penilaian Penerapan *Governance*

Perusahaan yang menerapkan *governance* yang baik akan terlihat dari beberapa faktor-faktor penilaian. Hal tersebut diuraikan menurut Gani et al. (2022) yang mengutip dari Gani dan Fernando (2018) dalam konteks *Governance* yang baik terjadi jika adanya beberapa hal ini:

a. Proses edukasi kepada para *stakeholder* mengenai risiko keamanan *cyber.*
b. Mengembangkan pedoman dalam proses-proses *supply chain* yang dimana mitra *supply chain* yang bekerja sama dengan perusahaan terhadap keamanan *cyber* seluruh pemangku kepentingan baik internal maupun eksternal secara berkala.
c. Mengikuti pembaruan, tren, dan teknologi terkait *cyber security* serta menerapkan *patch management*[7] secara berkala pada jaringan *supply chain* dalam upaya memastikan *performance* pengoperasian sistem *supply chain* yang beroperasional secara efektif dan efisien.

Dengan demikian, adanya *Governance* yang baik dalam mengatasi masalah CSC (*Cyber Supply Chain)* pada perusahaan sangatlah penting. Hal ini disebabkan adanya pengaturan yang baik dapat menumbuhkan rasa kesadaran para anggota-anggota internal perusahaan. Dalam upaya

[7] *Patch Management:* Proses pengelolaan dan perbaikan kepada perangkat lunak, sistem operasi, atau aplikasi guna mengatasi kerentanan keamanan suatu sistem dan jaringan.

melindungi proses *supply chain* mereka, agar sampai kepada pengguna akhir tanpa ada masalah ancaman *cyber* baik dari internal maupun eksternal (Gani & Fernando, 2021).

2.2.3 Indikator *Governance*

Penelitian ini menggunakan indikator yang diambil dari penelitian Gani et al. (2022) yang memiliki lima indikator, sebagai berikut:

a. Memiliki *cross-functional teams* yang kompeten dalam bidang *cyber security* khususnya dalam serangan *cyber.*

Hal ini mengacu pada ketersediaan tim lintas-fungsi perusahaan yang berkompeten mengatasi masalah *cyber security* baik itu ancaman *cyber* dari pihak eksternal dan gangguan serangan *cyber* dari pihak internal.

b. Adanya proses komunikasi strategi *cyber security* kepada *stakeholder* secara berkala.

Hal ini mengacu adanya penyampaian rencana keamanan *cyber* secara rutin kepada para *stakeholder.*

c. Memiliki *compliance*[8] pada prosedur regulasi yang berlaku dari pemerintah ataupun industri tertentu

Hal ini mengacu bahwa perusahaan taat dalam mengikuti pedoman *cyber security* sesuai yang ditentukan oleh pemerintah dan industri (seperti: sertifikasi IS0 27001, atapun sertifikasi lainnya).

d. Adanya verifikasi mitra *supply chain* perusahaan yang sesuai dengan SOP.

Hal ini mengacu penveritifikasian bahwa mitra *supply chain* yang bekerja sama dengan perusahaan telah mengikuti pedoman sesuai yang ditentukan oleh pemerintah dan industri.

e. Selalu beradaptasi terhadap perubahan bisnis terkini.

Hal ini mengacu pada penyesuaian pengoperasian struktur yang memudahkan dalam pedoman menjadi SOP secara lengkap agar memudahkan jika terjadi pada serangan *cyber* dalm sistem *cyber supply chain* untuk beradaptasi dengan perubahan bisnis terkini.

[8] *Compliance*: Kepatuhan perusahaan akan regulasi dan kebijakan yang telah ditetapkan oleh pemerintah atau industri tertentu.

2.3 *System Integration*

2.3.1 Pengertian *System Integration*

System Integration memiliki pengertian suatu penggabungan sistem yang secara sistematis untuk memastikan kelancaran perusahaan dalam perancangan solusi yang lebih efisien untuk menghilangkan inefisiensi akibat fragmentasi yang berhubungan dengan logistik dan komunikasi informasi (Tan et al., 2022). Konsep sistematis yang dimaksud dalam literatur yang dikemukakan oleh Tan et al. (2022), ialah cara proses sistematis dari adanya penggunaan software *Entreprise Resource Planning* (ERP), data dari sistem ERP akan diekspor dan dimuat ke *Google Big Query* menggunakan alat ekspor data yang sesuai. Berdasarkan platform *Google Cloud Big Query*, proses ini melibatkan pemetaan struktur data ERP ke dalam format yang dapat diterima oleh *Big Query*. Setelah data terunggah, analisis dan pertanyaan penelitian akan diterapkan menggunakan kueri SQL[9] *(Structured Query Language)* dengan penggabungan penggunaan *Big Query*, memanfaatkan kecepatan dan skala komputasi yang besar dari *platform* ini, yang berguna dalam manajemen data sehingga dapat diolah agar operasionalnya menjadi efektif dan mudah terakses dalam ERP yang mencakup mencakup langkah-langkah penting seperti pemahaman visualisasi data melalui sistem.

Menurut salah satu ulasan literatur yang diteliti oleh Tiwari (2020), *System Integration* didefinisikan sistem perusahaan yang melancarkan hubungan antar mitra *supply chain* ataupun proses intra-organisasi yang dengan tujuan mencapai proses aliran dalam bentuk fisikal, informasi, dan finansial dengan efisiensi yang optimal untuk penciptaan keunggulan kompetitif perusahaan dalam persaingan bisnis. Menurut Cheng et al. (2022), *System Integration* memiliki makna yaitu suatu sistem yang efisien dalam mengelola proses internal dan eksternal perusahaan agar efisien menciptakan *value* bagi pelanggan dengan biaya yang rendah. Menurut Tiwari (2020), *System Integration* bermakna sebagai suatu sistem yang baik antar lintas fungsional dari proses-proses operasional dan aktivitas-aktivitas *supply chain* yang melibatkan *supplier* dan konsumen yang memiliki transparansi dalam proses logistiknya sehingga jelas dimana lokasi barang yang dikirim. Berdasarkan beberapa pengertian di atas, dapat disimpulkan bahwa semakin terintegratif suatu perusahaan maka perusahaan tersebut akan bekerja sama baik secara internal maupun eksternal untuk mencapai tujuan efisiensi dalam penciptaan nilai lebih dan efektif dalam kegiatan operasionalnya dalam waktu dan biaya. Perusahaan yang

[9]SQL *(Structured Query Language)*: Bahasa pemrograman yang digunakan untuk mengakses, mengelola, dan mengambil data dari basis data relasional yang berperan penting dalam penggunaan ERP dan pengelolaan basis data karena memungkinkan pengguna untuk melakukan berbagai tugas, seperti mengambil data yang spesifik.

memiliki *System Integration* baik, akan berdampak saat adanya proses pengambilan keputusan yang tepat. Jika hal ini diolah dan berhubungan antara sistem satu dengan lainnya yang dapat menciptakan *Cyber Supply Chain Visibility* agar beroperasi secara *real-time* dapat menghasilkan peningkatan *performance* perusahaan yang menjadi efisien dalam waktu dan sumber dayanya baik dalam biaya maupun sumber daya manusianya dengan memudahkan pengidentifikasian serangan *cyber* yang bisa terjadi kapan saja (Gani et al., 2022).

2.3.2 Indikator *System Integration*

Penelitian ini menggunakan indikator yang diambil dari penelitian Gani et al. (2022) yang memiliki lima indikator, sebagai berikut:

a. Memiliki sistem keamanan yang terintegrasi dengan pemasok utama.

   Hal ini mengacu pada perencanaan *cyber security* yang selalu terintegrasi penggabungan sistem antara perusahaan dengan para *supplier* utama agar saling terhubung dan memudahkan dalam berbagi data visual rantai pasokan secara efisien dan efektif.

b. Memiliki sistem keamanan yang terintegrasi dengan pihak eksternal atau regulator.

   Hal ini mengacu pada rencana *cyber security* antara perusahaan dengan pihak eksternal yang berperan sebagai regulator, seperti: badan atau lembaga yang bertanggung jawab dalam mengatur ataupun mengawasi suatu kegiatan industri.

c. Memiliki kesepakatan kebijakan mengenai resiko *cyber supply chain* antar pemasok dan perusahaan.

   Hal ini mengacu pada adanya kesepakatan mengenai kebijakan-kebijakan akan penerapan dalam mengatasi risiko *cyber supply chain* yang disepakati oleh perusahaan dan pemasok.

d. Pembaruan rutin *Cyber Supply Chain Risk Management* oleh pemasok.

   Hal ini mengacu pada pembaruan status atau *update* secara berkala mengenai *Cyber Supply Chain Risk Management* (CSCRM) akan potensi serangan *cyber* terbaru dalam menghadapi tantangan atau hambatan lingkungan bisnis yang selalu berubah.

e. Memiliki sistem informasi *real-time* untuk tindakan antisipatif dalam mencegah ataupun saat penanggulangan insiden serangan *cyber* terhadap mitra pemasok.

   Hal ini mengacu pada perusahaan memiliki sistem informasi perusahaan *real-time* yang siap dan cepat tanggap dalam mengidentifikasi dalam menghadapi insiden

serangan *cyber* baik dalam langkah pencegahan ataupun penanggulangan serangan *cyber* terhadap mitra *supply chain.*

2.4 *Cyber Supply Chain* (CSC) *Visibility*

2.4.1 Pengertian CSC *Visibility*

Cyber Supply Chain (CSC) *Visibility* memiliki pengertian yaitu keterbukaan proses bisnis suatu perusahaan dalam melihat data visual terhadap informasi permintaan dan pasokan secara *real-time* dan akurat yang berguna bagi operasional perusahaan (Kalaiarasan et al., 2022). Menurut Baah et al. (2021), *CSC Visibility* bermakna keterbukaan dalam informasi yang dianggap akurat, terpercaya, tepat waktu, berguna dalam kegiatan *supply chain* ataupun kegiatan operasional perusahaan. Selain ini, *CSC Visibility* berpengertian sebagai keterbukaan dalam pengaksesan untuk melihat suatu elemen informasi yang relevan pada tingkat yang dipilih oleh para *stakeholder supply chain* (Somapa et al., 2018).

Dengan penguraian beberapa pengertian CSC *Visibility*, dapat disimpulkan bahwa CSC *Visibility* adalah kemampuan melihat data informasi perusahaan yang akurat secara *real-time* untuk membantu para *stakeholder* dalam proses bisnis. Oleh sebab itu, CSC *Visibility* yang baik dapat membuat perusahaan menjadi fleksibilitas dalam pengelolaan *supply chain,* sebab dengan keterbukaan dalam penglihatan data visual informasi yang mudah oleh para pelaku *supply chain* yang dapat meningkatkan efektivitas dalam operasional yang dimana memiliki peran penting dalam peningkatan *Cyber Supply Chain* (CSC) *Performance* (Kalaiarasan et al., 2022). Pernyataan ini juga didukung oleh penelitian sebelumnya oleh Somapa et al. (2018), bahwa perusahaan yang memiliki CSC *Visibility* yang baik adalah perusahaan yang memiliki penangkapan informasi yang terperinci mengenai arus pengiriman dan status stok di beberapa lokasi serta peringatan mengenai peristiwa penting selama perjalanan logistik yang dimana hal ini termasuk perencanaan produksi dan pengiriman di pabrik, hingga penyimpanan dan pergerakan oleh perusahaan ekspedisi, inspeksi dan izin oleh otoritas bea cukai, hingga transportasi darat ke tujuan akhir sampai ditangan konsumen. Dalam penelitian sebelumnya, juga ditemukan konsep bahwa dengan adanya sistem integrasi perusahaan yang efektif serta kemampuan visibilitas dalam *supply chain* yang baik akan menghasilkan peningkatan *Cyber Supply Chain* (CSC) *Performance* (Gani et al., 2022).

2.4.2 Indikator CSC *Visibility*

Penelitian ini menggunakan indikator yang diambil dari penelitian Gani et al. (2022) yang memiliki empat indikator, sebagai berikut:

a. Memiliki kemampuan dalam mengindetifikasi akan kerentanan atau resiko serangan *cyber* dari mitra *supply chain*.

   Perusahaan yang memiliki kemampuan dalam mengidentifikasi kerentanan ataupun resiko serangan *cyber* yang berasal dari mitra *supply chain* yang bekerja sama dengan perusahaan.

b. Memiliki kemampuan dalam mengenal serangan *cyber* yang berpotensi sebagai salah satu langkah preventif dalam mengatasi serangan *cyber.*

   Perusahaan memiliki kemampuan dalam mengenal kemungkinan ancaman *cyber* yang berpotensi menjadi serangan *cyber* sebagai langkah pencegahan agar mencegah kerugian yang mungkin dialami perusahan jika terjadi serangan *cyber.*

c. Memiliki respon yang cepat tanggap dalam proses penanggulangan serangan *cyber* saat diretas oleh oknum-oknum yang tidak bertanggung jawab.

   Perusahaan memiliki respon yang cepat tanggap dalam mengatasi serangan *cyber* saat sistem perusahaan disusupi oleh oknum-oknum yang tidak bertanggung jawab, sehingga dapat meminimalisir kerugian yang dialami perusahan khususnya dalam memastikan keamanan informasi perusahaan tetap terjaga secara optimal.

d. Adanya pemeriksaan vital secara berkala untuk memastikan sistem *cyber supply chain* tetap aman dari serangan cyber.

   Perusahaan melakukan pemeriksaan vital secara berkala untuk memastikan komponen-komponen sistem *cyber supply chain* berjalan dengan benar dan tetap aman dari serangan *cyber,* sehingga dapat memastikan operasional *supply chain* dapat berjalan secara optimal dan tidak terhambat karena adanya serangan *cyber.*

2.5 *Cyber Supply Chain* (CSC) *Performance*

2.5.1 Pengertian *Cyber Supply Chain* (CSC) *Performance*

Cyber Supply Chain (CSC) *Performance* memiliki pengertian status *ouput* performa perusahaaan dalam penggunaan teknologi yang dapat meningkatkan efisiensi dan efektivitas seluruh rantai dalam mengelola *supply chain* (P. N., 2021)*. Cyber Supply Chain* (CSC) *Performance* menurut Gawankar et al. (2019), CSC *Performance* adalah sebuah status atau nilai keluaran dari cara kerja sistem informasi perusahaan dengan melakukan evaluasi melalui efisiensi strategi

perusahaan, taktik perusahaan yang lebih baik, dan keputusan operasional yang efektif. Bukan hanya pengukuran efisiensi dan efektivitas melainkan juga adanya penggabungan sumber daya manusia, proses, dan teknologi untuk mengelola risiko *cyber* dengan efektif dan membantu perusahaan mencapai *supply chain* yang lebih kuat dan tahan akan serangan *cyber.* Oleh sebab itu, menurut P. N. (2021) yang mengutip dari Beamon (1999) terdapat tiga hal yang menandakan bahwa *performance* perusahaan berjalan dengan baik yaitu fleksibilitas pengelolaan *supply chain*, pengukuran sumber daya yang berasal dari *supplier*, dan ketangkasan dalam daya tanggap *supply chain* sebagai *output.* Bedasarkan beberapa pernyataan sebelumnya, dapat disimpulkan bahwa CSC *Performance* adalah nilai dari status atau kondisi perusahaan dengan pemanfaatan sistem informasi dan teknologi dalam peningkatannya dalam efisiensi dan efektivitas kegiatan operasional perusahaan. Dalam penelitian sebelumnya CSC *Performance* juga memiliki beberapa pengukuran yaitu fleksibilitas dalam *supply chain*, pengukuran *performance* sumber daya *supplier*, dan daya tanggap *supply chain* akan *output.* Oleh karena itu, terbagilah menjadi dua sektor dalam penilaian variabel ini yaitu melalui pihak internal dan pihak eksternal (Gani et al., 2022).

2.5.2 Indikator *Cyber Supply Chain* (CSC) *Performance*

Penelitian ini menggunakan delapan indikator yang diambil dari penelitian Gani et al. (2022) yang memiliki delapan indikator, sebagai berikut:

a. Adanya kebijakan dan prosedur keamanan sesuai SOP antar perusahaan dan mitra supply chain untuk memastikan aliran data sistem yang aman.

   Hal ini mengacu pada perusahaan dan mitra *supply chain* memiliki kebijakan dan prosedur yang terdokumentasi dengan baik untuk memastikan aliran data informasi terproses dengan aman serta terlindung dari berbagai serangan *cyber* dan sesuai dengan standar keamanan yang ditetapkan oleh regulator.

b. Perusahaan dan mitra *supply chain* memiliki transparansi akan informasi yang berpotensi merugikan kedua pihak dalam jika terjadi serangan cyber.

   Hal ini mengacu pada perusahaan dan mitra *supply chain* yang bekerja sama dengan perusahaan saling memberi informasi tentang kejadian jika adanya serangan cyber yang mungkin dapat berdampak negatif bagi kedua pihak.

c. Perusahaan menerapkan pengaturan akses data visual yang tepat.

   Hal ini mengacu pada perusahaan telah memiliki penerapan pengaturan akses data visual yang tepat dalam hal proses pengolahan perusahaan dari serangan *cyber* yang

bisa terjadi untuk langkah preventifnya ataupun penanggulangannya agar mengurangi kerugian yang terjadi bagi perusahaan secara finansial maupun non-finansial.

d. Memiliki kontrol aset fisik yang tepat sebagai tindakan preventif kejahatan *cyber.*

   Hal ini mengacu pada perusahaan memiliki pengontrolan aset fisiknya yang dapat berupa fasilitas fisik, penyimpanan pusat data, serta infrastruktur fisik lainnya dari akses pihak yang tidak berwenang ataupun para oknum hacker sebagai langkah preventif dalam mengatasi kejahatan *cyber.*

e. Memiliki penerapan budaya keamanan informasi yang baik oleh para sumber daya manusianya.

   Hal ini mengacu pada perusahaan memiliki dan menjaga budaya keamanan informasi yang baik yang ditingkat melalui sumber daya manusianya dapat berupa, seperti: meningkatkan keyakinan dan kesadaran akan pentingnya keamanan informasi, serta memotivasi para karyawan untuk terus aktif dalam meningkatkan kemampuan IT dengan mengikuti program pelatihan.

f. Penerapan prosedur keamanan sistem informasi secara konsisten.

   Hal ini mengacu pada penerapan prosedur keamanan sistem infromasi perusahaan secara konsisten yang merupakan salah satu aspek penting dalam memastikan keamanan aliran data informasi perusahaan. Adanya prosedur dapat memastikan tingkat kepatuhan perusahaan akan regulasi yang ada, pengaturan akan keterbukaan akses visual data informasi perusahan yang tepat, pembaruan perangkat lunak, serta tindakan yang berfungsi untuk mengurangi resiko akan potensi ataupun penanggulangan serangan *cyber.*

2.6 Hubungan Antar Konsep dan Hipotesis Penelitian

2.6.1 Hubungan *Governance* terhadap CSC *Visibility*

Berdasarkan Gani et al. (2022) yang mengutip dari Hong et al. (2018), menjelaskan bahwa dengan adanya CSC *Visibility* dalam jaringan *supply chain* sangat berperan penting dalam penyelesaian masalah *supply chain* secara global yang sangat dinamis dan cepat berubah. Penelitian juga mengekemukakan, bahwa perusahaan harus menerapkan praktik yang meningkatkan visibilitas dalam sistem *cyber supply chain* melalui tata kelola dari kolaborasi dari sistem integrasi dan informasi agar mencapai *performance* yang efisien dan efektif (Dubey et al.,2017). Dalam penelitiannya sebelumnya, juga berpendapat bahwa *governance* perusahaan

meningkatkan *performance*nya karena mendukung tindakan yang terbaik bagi kepentingan seluruh pemegang saham (Wijethilake & Lama, 2018). Dengan demikian, *Governance* diduga berpengaruh terhadap CSC *Visibility.*

H_1: *Governance* berpengaruh terhadap CSC *Visibility.*

2.6.2 Hubungan *System Integration* terhadap CSC *Visibility*

Menurut penelitian yang oleh Kalaiarasan et al. (2022), dengan sistem integrasi yang terproses dan memiliki melihat data visual terhadap informasi permintaan dan pasokan secara *real-time* memfasilitasi pengambilan keputusan yang efektif. Berdasarkan Baah et al. (2021), dengan perusahaan melakukan kolaborasi dengan mitra *supply chain*nya akan informasi data yang diolah pada waktu yang tepat sehingga menciptakan efisiensi yang optimal untuk penciptaan keunggulan kompetitif perusahaan dalam persaingan bisnis. Beberapa temuan ini juga sejalan dengan temuan Gani et al. (2022) yang mengutip dari Tan et al. (2022), yaitu semakin terintegrasi suatu sistem perusahaan maka pengambilan keputusan akan menjadi lebih baik dalam lingkungan bisnis yang saling terhubung dan mudah dalam melihat data visual informasi secara real-time yang akan berdampak pada *performance* perusahaan. Dengan demikian, *System Integration* diduga berpengaruh terhadap CSC *Visibility.*

H_2: *System Integration* berpengaruh terhadap CSC *Visibility.*

2.6.3 Hubungan CSC *Visibility* terhadap CSC *Performance*

Dalam penelitian sebelumnya, dengan adanya transparansi komunikasi yang mudah bagi para pelaku *supply chain* yang dapat meningkatkan efisiensi dan efektivitas dalam operasional yang dimana memiliki peran penting dalam peningkatan sistem *cyber supply chain performance* (Kalaiarasan et al., 2022). Menurut asumsi Gani et al. (2022) CSC *Visibility* sangat penting dalam peningkatan CSC, sebab dari proses ini diperoleh melalui berbagi informasi dan konektivitas memungkinkan peningkatan ketahanan dan ketahanan *supply chain*. Dengan demikian, hal ini akan berdampak secara langsung maupun tidak langsung terhadap CSC *Performance.* Hal ini sejalan dengan penelitian Colicchia et al. (2018), yang mengutip dari dua literatur yaitu Han dan Shin (2016) serta Tukamuhabwa et al. (2017), menyatakan bahwa dengan kemampuan visibilitas perusahaan yang baik dapat berdampak kepada *performance* perusahaan khususnya dalam mengatasi resiko *cyber* yang dapat berasal dari internal maupun eksternal. Dengan demikian, CSC *Visibility* diduga berpengaruh terhadap CSC *Performance.*

H_3: CSC *Visibility* berpengaruh terhadap CSC *Performance.*

2.6.4 Hubungan *Governance* terhadap CSC *Performance*

Dalam penelitian Maleh et al. (2021) yang mengutip dari Lunardi et al. (2014), terdapat pernyataan bahwa dengan adanya *Governance* yang baik dapat meningkatkan *Performance.* Hal ini dikarenakan adanya *Governance* yang meningkat akan menimbulkan *Performance* yang lebih baik baik dalam bidang *supply chain* ataupun finansial. Sedangkan dalam penelitian Gani et al. (2022) dinyatakan bahwa *Governance* yang baik dapat meningkatkan CSC *Performance*, sebab menjadi salah satu faktor pendukung pengambilan suatu keputusan tindakan yang terbaik bagi kepentingan semua pihak pemegang saham. Dengan demikian, *Governance* berpengaruh terhadap CSC *Performance.*

H_4: *Governance* berpengaruh terhadap CSC *Performance.*

2.6.5 Hubungan *System Integration* terhadap CSC *Performance*

Berdasarkan penelitian yang sebelumnya yang dikemukakan oleh Gani et al. (2022), dengan adanya *System Integration* yang baik akan menghasilkan pengambilan keputusan yang baik dalam operasional secara umum ataupun proses *supply chain* perusahaan yang akan berpengaruh secara signfikan terhadap CSC *Performance*. Hal ini diperkuat dengan penelitian Tan et al. (2022), yang berpendapat bahwa *System Integration* yang baik adalah sebuah sistem yang terkoneksi yang membuat pengambilan keputusan dapat berjalan secara efektif sehingga semakin baik dan terintegrasi maka CSC *Performance* akan semakin meningkat juga. Dengan demikian, bahwa *System Integration* diduga berpengaruh terhadap CSC *Performance.*

H_5: *System Integration* berpengaruh terhadap CSC *Performance.*

2.6.6 Hubungan *Governance* terhadap CSC *Performance* melalui CSC *Visibility*

Pengaturan *Governance* yang baik pada *Supply chain* akan membuat adanya peningkatan efisiensi dari operasional bisnis yang kemudian akan berdampak positif pada CSC *Performance*. Pernyataan ini diperkuat dengan penelitian sebelumnya oleh Gani et al. (2022), pentingnya *Governance* dalam hubungan CSC *Performance* dan CSC *Visibility* yang menjadi landasan dalam praktik *Cyber Supply Chain Risk Management* (CSCRM) dalam upaya pencegahan dan meminimalisir dampak maupun langkah preventifnya serangan *cyber* dalam seluruh proses *supply chain* (Creazza et al., 2021). Dengan demikian, *Governance* diduga berpengaruh terhadap *CSC Performance* melalui *CSC Visibility*

H_6: *Governance* berpengaruh terhadap *CSC Performance* melalui *CSC Visibility.*

2.6.7 Hubungan *System Integration* terhadap *CSC Performance* melalui *CSC Visibility*

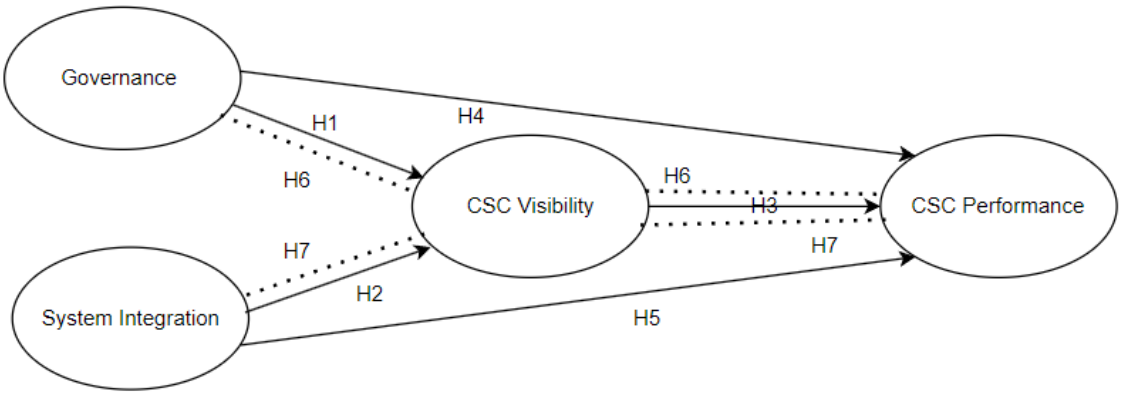
Perusahaan memiliki CSC *Performance* yang lebih baik saat adanya peningkatan dari *System Integration* dengan mediasi CSC *Visibility.* Hal ini didukung dari pernyataan dari penelitian sebelumnya, bahwa kemampuan untuk berbagi informasi secara *real-time* dengan mitra *supply chain* sangat penting untuk memperoleh informasi mengenai risiko atau kerentanan apapun yang dapat menyebabkan gangguan pada rantai pasokan akan berdampak pada CSC *Performance* suatu perusahaan (Gani et al., 2022). Dengan demikian, adanya peningkatkan *System Integration* pada *supply chain* yang secara sistematis dengan adanya pengguanaan software buatan lainnya sehingga memudahkan dalam dalam manajemen data dalam sistem *Big Query* dapat meningkatkan CSC *Performance* namun perlu ada pembagian informasi secara *real-time* dan akurat yang berguna bagi operasional perusahaan (Cheng et al., 2022). Sedangkan, menurut Kalaiarasan et al. (2022), pengelolaan *supply chain* yang terintegrasi dengan baik serta kemudahan dalam melihat data visual informasi dengan mudah oleh para pelaku *supply chain* yang dapat meningkatkan efektivitas dalam operasional yang dimana memiliki peran penting dalam peningkatan kinerja supply chain yang tersistem. Dengan demikian, *System Integration* diduga berpengaruh terhadap CSC *Performance* melalui CSC *Visibility.*

H_7: *System Integration* berpengaruh terhadap *CSC Performance* melalui *CSC Visibility*.

2.7 Kerangka Penelitian

Gambar 2.1

Kerangka Penelitian



Sumber : Gani, A. B. D., Fernando, Y., Lan, S., Lim, M. K., & Tseng, M.-L. (2022). Interplay between cyber supply chain risk management practices and cyber security performance. *Industrial Management & Data*

Systems, *123*(3). https://doi.org/10.1108/imds-05-2022-0313

Menurut kerangka penelitian ini, dapat disimpulkan dengan adanya analisis hubungan langsung antara *Governance* dan *System Integration* dalam suatu perusahaan terhadap *Cyber Supply Chain Performance* dengan *Cyber Supply Chain* (CSC) *Visibility* sebagai variabel *intervening*. Pada penelitian ini akan menganalisis pengaruh CSC *Visibility* sebagai mediasi antara adanya *Governance* dan *System Integration* perusahaan yang baik akan berpengaruh pada CSC *Performance* di perusahaan-perusahaan yang menerapkan kegiatan *supply chain.* Penelitian ini juga akan menguji antara hubungan langsung *Governance* dan *System Integration* tanpa adanya mediasi dari CSC *Visibility* pada perusahaan manufaktur yang menerapkan proses *supply chain* di Indonesia. Selain hubungan langsung yang diteliti semua variabel di atas juga akan diteliti satu sama lain juga dalam hubungan tidak langsungnya yang menganalisis antara hubungan langsung *Governance* dan *System Integration* dengan adanya mediasi dari CSC *Visibility* dan dampaknya terhadap CSC *Performance* pada perusahaan manufaktur yang menerapkan proses *supply chain* di Indonesia.