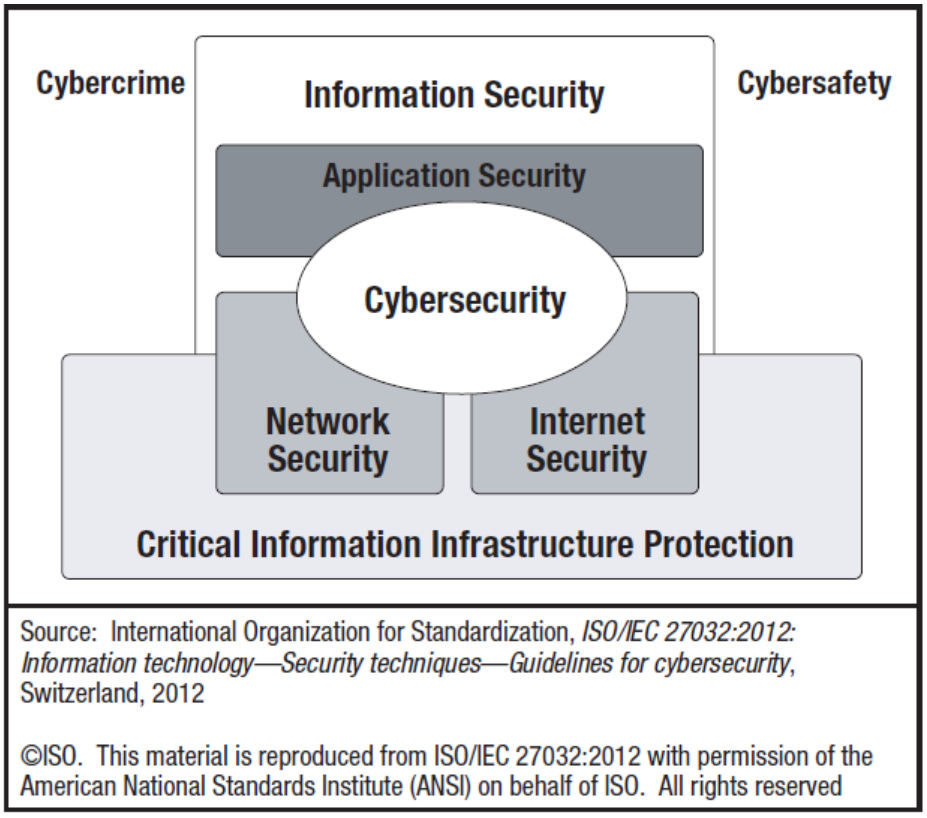
BAB 2

LANDASAN TEORI

2.1 Tinjauan Pustaka

Istilah cybersecurity dan information security/keamanan informasi sering digunakan secara bergantian, namun kenyataannya, cybersecurity merupakan bagian dari keamanan informasi. Lebih khusus lagi, cybersecurity dapat didefinisikan sebagai perlindungan aset informasi dengan mengatasi ancaman terhadap informasi yang diproses, disimpan dan diangkut oleh sistem informasi yang bekerja di internet (ISACA, 2017).

Cybersecurity mencakup semua yang melindungi perusahaan dan individu dari serangan yang disengaja, pelanggaran dan insiden serta konsekuensi. Dalam prakteknya, cybersecurity terutama menunjukkan jenis-jenis serangan, pelanggaran atau insiden yang ditargetkan, terlalu canggih dan sulit untuk mendeteksi atau mengelola cybersecurity. Bidang yang jauh lebih besar dari serangan oportunistik dan kejahatan biasanya dapat ditangani dengan menggunakan strategi dan tool sederhana namun efektif. Akibatnya, fokus cybersecurity adalah pada apa yang dikenal sebagai *Advanced Persistent Threats* (APTs). (ISACA, 2013).



Gambar 2.1. Hubungan antara cybersecurity dan domain security lainnya

Terlepas dari penggunaan umum dari istilah, cybersecurity harus diselaraskan dengan semua aspek lain dari keamanan informasi dalam perusahaan. Ini termasuk tata kelola, manajemen dan assurance. Dalam hal ini, gagasan keseluruhan keamanan adalah sistemik bukan linier, bahwasanya ide menjadi aman sebagai negara membutuhkan pemeliharaan dan perbaikan berkelanjutan untuk memenuhi kebutuhan dan persyaratan para pemangku kepentingan *(stakeholder).*

APTs termasuk serangan, pelanggaran, infiltrasi dan peristiwa keamanan lainnya yang memiliki usaha level tingkat tinggi atau sangat tinggi yang menargetkan perusahaan tertentu dan / atau individu. Beberapa APTs memiliki latar belakang profesional atau kejahatan terorganisir.

Sebagai lawan bentuk yang lebih rendah dari serangan, eksekusi APT biasanya menyiratkan upaya yang signifikan dalam hal waktu dan investasi. Tergantung pada target dan daya tarik, APTs mungkin melibatkan solusi custom-made yang hanya digunakan sekali. Berbeda dengan vektor serangan yang lebih luas dan tersedia untuk umum dan tools, APTs jauh lebih diprediksi, sulit untuk mengenali dan sering sulit untuk melacak kembali ke asal-usul nya.

2.2 Landasan Teori

2.2.1 *Malware dan Ransomware*

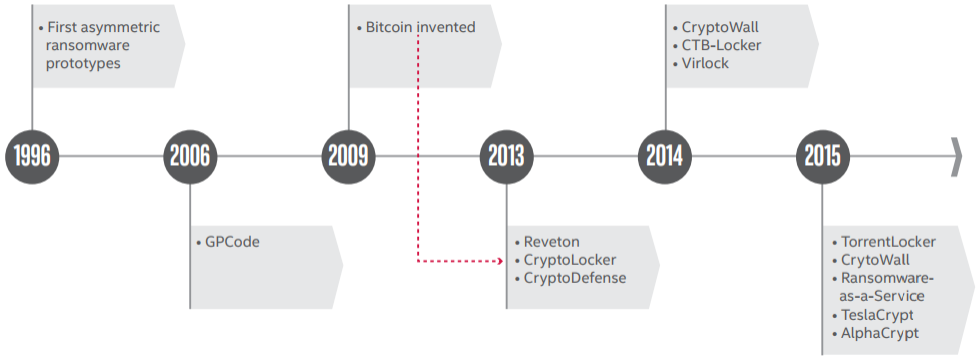
Malware atau disebut juga dengan *malicious code* merupakan perangkat lunak yang dirancang untuk mendapatkan akses ke sistem komputer yang ditargetkan, mencuri informasi atau mengganggu operasi komputer. Ada beberapa jenis malware, yang paling penting adalah virus komputer, *worm* dan *trojan horse*, yang dibedakan dengan cara operasi atau penyebarannya.

Sebagai contoh, worm yang dikenal dengan Stuxnet menyoroti potensi *malware* untuk mengganggu sistem SCADA dan Programmable Language Control (PLC), biasanya digunakan untuk mengotomatisasi proses mekanis di lingkungan pabrik atau pembangkit listrik. Ditemukan pada tahun 2010, Stuxnet digunakan untuk mengkompromi sistem dan perangkat lunak nuklir Iran.

Ransomware sudah ada sejak lama. Prototipe pertama ransomware asimetris dikembangkan pada pertengahan tahun 1990-an. Gagasan

menggunakan *public key cryptography* untuk serangan komputer diperkenalkan pada tahun 1996 oleh Adam L. Young dan Moti Yung di Prosiding Simposium IEEE tahun 1996 tentang Keamanan dan Privasi.

Apa arti "asimetris" dan mengapa hal itu penting? Karakteristik yang menentukan dari publickey kriptografi adalah penggunaan kunci enkripsi oleh satu pihak untuk melakukan enkripsi atau dekripsi dan penggunaan kunci lain dalam operasi pendamping. Dalam algoritma kunci simetris, ada satu kunci yang digunakan dan dibagi antara receiver dan pengirim, sehingga kunci yang digunakan oleh receiver dan pengirimnya "simetris" karena sama saja. Penggunaan beberapa tombol pada publickey asimetris kriptografi memungkinkan ransomware untuk mengenkripsi item pada sistem dengan kunci publik sementara tidak pernah membuka kunci pribadi, sehingga merahasiakannya. Untuk ransomware, ini penting untuk "mangling" dta file tanpa mengekspos sesuatu yang bisa digunakan seseorang untuk mengetahui bagaimana cara meng-undo enkripsi.



Gambar 2.2. Perkembangan ransomware

2.2.2 *Advanced Persistent Threats (APT)*

Advanced Persistent Threats (APT) adalah fenomena yang relatif baru bagi banyak organisasi. Motif di balik mereka tidak sepenuhnya baru, tetapi tingkat perencanaan dan sumber daya yang digunakan dan teknik yang digunakan dalam serangan yang belum pernah terjadi sebelumnya. Ancaman ini menuntut tingkat kewaspadaan dan satu set penanggulangan yang di atas dan di luar yang rutin digunakan untuk melawan ancaman keamanan sehari-hari dari hacker komputer, virus atau spammer.

Praktik-praktik ini tidak asing bagi profesional keamanan, tetapi tingkat pengalaman, keterampilan dan teknologi yang dibutuhkan untuk melawan serangan APT umumnya melebihi yang ditemukan dalam kebanyakan perusahaan publik dan swasta. Penelitian ini bertujuan untuk membantu menjembatani kesenjangan ini dengan menyoroti langkah-langkah tambahan atau ditingkatkan bahwa setiap organisasi perlu untuk mencegah, mendeteksi dan menanggapi serangan APT profesional. (*ISACA, 2016)*

Gambar 2.3. Cara kerja Advanced Persistent Threats

APTs menggunakan beberapa fase untuk masuk ke jaringan, menghindari deteksi, dan mengumpulkan informasi berharga dalam jangka panjang. Rincian infografis, fase serangan, metode, dan motivasi yang membedakan APT dari serangan yang ditargetkan lainnya. (https://www.symantec.com/theme.jsp?themeid=apt-infographic-1).

2.2.3 Mengatasi Kerentanan *Cybersecurity*

Penyerang hanya perlu menemukan satu kelemahan untuk masuk ke sistem perusahaan dan menyebarkan jangkauan mereka. Pembela perlu merencanakan untuk pelanggaran tak terelakkan dan memiliki rencana di tempat. Jika perusahaan kehabisan pilihan untuk menangani serangan *cyber*, mereka selesai. Perusahaan perlu memastikan bahwa mereka mengelola *cybersecurity* saat mereka pergi. Keamanan profesional akan harus membuat investasi yang benar dalam infrastruktur keamanan berdasarkan rencana

cybersecurity suara yang memanfaatkan standar industri dan melampaui standar keamanan tradisional untuk memastikan langkah-langkah pencegahan yang kuat, deteksi lebih cepat, respon dan pemulihan (harus pelanggaran terjadi).

Untuk saat ini, para pengambil keputusan dalam sektor pemerintah dan swasta perlu mengerahkan lebih banyak upaya untuk itu, menciptakan cara-cara baru dan kreatif untuk melindungi infrastruktur TI, mengadopsi praktik keamanan terbaik, dan mendidik pengguna akhir dengan kebijakan keamanan yang ditetapkan secara resmi untuk meminimalkan kebocoran data (Mosca, 2015).

2.2.4 *Cybersecurity Capability Maturity Model for Information Technology Services*

Ancaman *cyber* adalah salah satu jenis risiko operasional yang paling serius dan menantang yang dihadapi organisasi modern. Keamanan nasional dan ekonomi Amerika Serikat bergantung pada fungsi yang dapat diandalkan dari layanan teknologi informasi (TI) yang melayani infrastruktur penting Bangsa dalam menghadapi ancaman tersebut. Di luar infrastruktur penting, vitalitas ekonomi Bangsa tergantung pada operasi berkelanjutan layanan TI perusahaan dari semua jenis organisasi. Pendahuluan ini menjelaskan Model Kematangan Kemampuan Cyber untuk Layanan Teknologi Informasi (C2M2 untuk Layanan TI), yang membantu organisasi penyedia layanan TI dari semua sektor, jenis, dan ukuran mengevaluasi dan membuat perbaikan untuk program keamanan *cyber* mereka. (Curtis, Mehravari, Stevens, 2015)

2.2.5 *Cyber security risk assessment methods on SCADA*

Seni didalam penilaian risiko keamanan *cybe*r sistem *Supervisory Control and Data Acquisition* (SCADA). Dipiilih secara rinci dua puluh empat metode penilaian risiko yang dikembangkan untuk atau diterapkan dalam konteks sistem SCADA. Digambarkan esensi dari metode dan kemudian menganalisanya dalam hal tujuan, domain aplikasi, tahapan manajemen risiko ditangani, konsep manajemen risiko utama yang dicakup, dampak pengukuran, sumber data probabilistik, evaluasi dan dukungan alat. Berdasarkan analisis, Disarankan skema intuitif untuk pengkategorian metode penilaian risiko keamanan *cyber* untuk sistem SCADA. Diuraikan lima tantangan penelitian yang dihadapi domain dan menunjukkan pendekatan yang mungkin diambil. (Cherdantseva, Burnap, Blyth, Eden, Jones, Soulsby, Stoddart , 2015).

Metodologi dalam menguraikan enam langkah yang harus dilakukan untuk melakukan penilaian risiko keamanan *cyber* selama sistem dan desain komponen, dan tahap pasokan peralatan:

- identifikasi sistem dan pemodelan keamanan *cyber*
- analisis aset dan dampak,
- analisis ancaman,
- analisis kerentanan,
- desain kontrol keamanan, dan
- tes penetrasi.

Mempertimbangkan jumlah serangan, perlu diingat bahwa hanya sejumlah kecil insiden keamanan yang dilaporkan. Potensi kerugian dari

serangan *cyber* bisa sangat parah sehingga risiko, yang dihitung sebagai produk dari kerugian dari serangan dan kemungkinan serangan, diperkirakan cukup besar bahkan dengan kemungkinan terjadinya serangan yang sangat rendah.

Panggilan risiko besar untuk investasi keamanan yang proporsional. Metode penilaian risiko keamanan cyber untuk sistem SCADA dapat ditingkatkan dalam hal

(1) mengatasi tahap pembentukan konteks dari proses manajemen risiko,

(2) mengatasi serangan atau kegagalan orientasi,

(3) akuntansi untuk faktor manusia,

(4) menangkap dan formalisasi pendapat ahli,

(5) peningkatan keandalan data probabilistik;

(6) evaluasi dan validasi,

(7) dukungan tool.

2.2.6 *Military-Based Cyber Risk Assessment Framework*

Teknologi Informasi (TI) Manajemen Risiko dirancang untuk mengkonfirmasi kecukupan keamanan informasi. Ada banyak standar manajemen risiko atau penilaian, misal IS0 27005: 2011 dan NIST SP 800-30rev1, yang terutama dirancang untuk organisasi umum seperti pemerintah atau bisnis. Pengkajian risiko cyber yang difokuskan pada strategi militer jarang dipelajari. Oleh karena itu, makalah ini menyajikan kerangka konseptual penilaian risiko cyber inovatif bernama "Penilaian Risiko Maya (CRA)" yang diperpanjang dari pekerjaan sebelumnya dengan Evaluasi Risiko Militer (MRE). CRA yang diusulkan ini adalah pengumpulan dan

integrasi data kuantitatif dan kualitatif. Alat *Vulnerability Detection* (VD) dalam *Network Risk Evaluation* (studi sebelumnya) digunakan untuk pengumpulan data kuantitatif dan kelompok fokus dalam MRE (metode yang diusulkan) digunakan untuk mengumpulkan data kualitatif, yang meningkatkan standar penilaian risiko umum untuk mencapai tujuan penelitian. Kompleksitas domain dunia maya dengan perspektif militer secara serius direnungkan ke dalam penilaian risiko dunia maya untuk keamanan cyber nasional. Hasil dari kerangka yang diusulkan memungkinkan kemungkinan evaluasi risiko cyber ke dalam skor untuk perencanaan keamanan cyber nasional. (Hemanidhi, Chimmanee, 2017)

Keamanan TI sangat signifikan saat ini. Informasi adalah salah satu properti paling berharga yang perlu dikelola dengan aman dan efektif. Banyak keamanan informasi dan standar manajemen risiko yang ditawarkan untuk menyediakan prosedur untuk keamanan sistem informasi organisasi. Penilaian risiko memainkan peran penting sebagai proses inti dalam manajemen risiko. Namun, serunya operasi maya yang berbahaya terus berkembang. *Cyberspace* diakui sebagai medan perang militer baru pada tahun 2014. *Cyberwar t*elah menjadi ancaman baru yang berpengaruh terhadap keamanan nasional. Sayangnya, keamanan TI saat ini dan standar manajemen risiko yang diinginkan untuk perspektif umum, khususnya untuk kelangsungan bisnis, daripada keamanan nasional. Tidak hanya standar manajemen risiko IT yang spesifik, tetapi juga metodologi penilaian risiko TI, secara langsung dicakup untuk operasi militer. Oleh karena itu, makalah ini mengusulkan ide inovatif dari penilaian risiko cyber untuk meningkatkan

keamanan cyber nasional dengan spesifik niat untuk menyengaja perang cyber yang dapat mempengaruhi operasi militer. Aktivitas di domain logis ini dapat mengirim dampak signifikan ke domain fisik yang sebenarnya. Spektrum ancaman juga telah berkembang dari konsep dasar ke operasi yang paling rumit. Evaluasi risiko jaringan dari standar utama tidak sesuai dengan risiko cyber dalam istilah militer, karenanya, beberapa standar manajemen risiko dikembangkan untuk kebutuhan organisasi nirlaba tetapi mereka belum mempertimbangkan lingkungan cyberwar.

2.2.7 *Case Study in Cybersecurity Regulation*

Amerika Serikat dan Kanada saling bergantung sepanjang sejumlah dimensi, seperti saling ketergantungan mereka pada infrastruktur kritis bersama. Akibatnya, upaya pengaturan yang bertujuan untuk mengamankan infrastruktur penting di satu negara berdampak yang lain, termasuk dalam konteks *cybersecurity*. Artikel ini mengeksplorasi satu inovasi tersebut dalam bentuk NIST *Framework*. Ini meninjau evolusi *Framework* NIST, membandingkan dan mengkontraskannya dengan upaya Kanada yang sedang berlangsung untuk mengamankan infrastruktur penting yang rentan terhadap ancaman *cyber*. Tujuannya adalah untuk menemukan tren tata kelola Amerika Utara yang dapat berdampak pada perdebatan yang lebih luas tentang peran yang tepat dari sektor publik dan swasta dalam meningkatkan *cybersecurity*. (Shackelford, Bohm, 2016)

2.2.8 *Cyber Security Governance And Management*

Peristiwa keamanan cyber dalam infrastruktur penting telah membangkitkan minat dan kekhawatiran utilitas energi, pemerintah, badan

pengatur, dan konsumen serta lembaga akademis dan penelitian. Jika di satu sisi itu menonjol kerentanan dunia maya, yang menambah risiko serangan di lingkungan organisasi, di sisi lain, penelitian yang mengarah ke alternatif untuk tata kelola dan manajemen struktur kritis ini masih terlalu baru jadi. Penelitian ini bertujuan untuk membangun model teoritis-empiris dari tata kelola dan manajemen keamanan cyber dan mengujinya bersama dengan para ahli akademis dan profesional dari sektor energi.

Dengan menggunakan metode Delphi dan teknik statistik untuk validasi, instrumen asesmen dikembangkan berdasarkan pada kedua konstruk: tata kelola dan manajemen; dan sembilan dimensi dengan variabel masing-masing yang memungkinkan untuk analisis situasi utilitas energi Brasil mengenai perlindungan cyberspaces mereka. Kontribusi artikel mencapai dua front: yang konseptual dan empiris karena memperluas dan mensistematisasi pengetahuan tentang aspek tata kelola dan manajemen ruang maya; dan yang metodologis karena mengusulkan mengukur dimensi-dimensi tersebut dalam utilitas energi.(Pardini, Heinisch, Parreiras, 2017).

2.2.9 *An Integrated Cyber Security Risk Management*

Cyber Physical System (CPS) adalah kombinasi komponen sistem fisik dengan kemampuan maya yang memiliki interkoneksi yang sangat ketat. CPS adalah teknologi yang banyak digunakan di banyak aplikasi, termasuk sistem tenaga listrik, komunikasi, dan transportasi, dan perawatan kesehatan sistem. Ini adalah infrastruktur nasional yang sangat penting. Serangan *cybersecurity* adalah salah satu ancaman utama bagi CPS karena banyak alasan, termasuk kompleksitas dan interdependensi di

antara berbagai sistem komponen, integrasi komunikasi, komputasi, dan teknologi kontrol. Keamanan serangan cyber dapat menyebabkan berbagai risiko yang mempengaruhi kontinuitas bisnis infrastruktur kritis, termasuk degradasi produksi dan kinerja, tidak tersedianya layanan penting, dan pelanggaran peraturan itu.

Mengelola risiko cybersecurity sangat penting untuk melindungi CPS. Namun, manajemen risiko menantang karena sifat kompleks dan berkembang dari sistem CPS dan tren serangan terbaru. Makalah ini menyajikan kerangka kerja manajemen risiko *cybersecurity* yang terintegrasi untuk menilai dan mengelola risiko secara proaktif. Pekerjaan kami mengikuti manajemen risiko yang ada berlatih dan standar dan mempertimbangkan risiko dari model stakeholder, cyber, dan sistem fisik komponen bersama dengan dependensi mereka. Pendekatan ini memungkinkan identifikasi aset CPS yang kritis dan menilai dampak dari kerentanan yang mempengaruhi aset. Ini juga menyajikan serangan cybersecurity skenario yang menggabungkan efek Cascading dari ancaman dan kerentanan terhadap aset. Serangan itu model membantu menentukan tingkat risiko yang tepat dan proses mitigasi yang sesuai. Kami menyajikan sistem jaringan listrik untuk menggambarkan penerapan pekerjaan kami. Hasilnya menunjukkan itu risiko dalam CPS dari infrastruktur penting sangat tergantung pada skenario serangan cyber-fisik dan konteks organisasi. Risiko yang terlibat dalam konteks yang dipelajari adalah dari teknis dan aspek nonteknis dari CPS. (Kure, Islam, Razzaque, 2018)

Inisiasi manajemen risiko ditentukan oleh lingkup manajemen risiko, jadwal, sumber daya yang tersedia, strategi pemantauan risiko, dan perlakuan risiko, berdasarkan tujuan organisasi infrastruktur yang kritis. Ini termasuk tiga langkah yang diberikan di bawah ini.

- Langkah 1: Identifikasi sistem dan komponen dan praktik manajemen risiko yang ada
- Langkah 2: Tentukan tujuan dan indikator kinerja utama (KPI)
- Langkah 3: Tingkat penerimaan risiko

2.2.10 *Framework Cybersecurity*

Framework cybersecurity yang digunakan pada thesis ini adalah NIST Cybersecurity Framework. 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

Kebutuhan stakeholder di cybersecurity mungkin cukup beragam pada kebanyakan perusahaan. Sementara manajemen harus menerapkan dan menegakkan kasus bisnis, rekan individu mungkin memiliki kebutuhan sehari-hari perlindungan dan bimbingan hands-on. Demikian pula, mitra

bisnis eksternal dan pelanggan memiliki satu set harapan dan kebutuhan yang mencakup kepercayaan organisasi, keandalan dan *track record* yang bersih dalam hal serangan dan pelanggaran.

Secara umum, perusahaan harus mengidentifikasi stakeholder utama baik internal dan eksternal sebagai bagian dari perencanaan bisnis, dan lebih khusus sebagai bagian dari tata kelola keamanan informasi. Untuk tujuan cybersecurity, para pemangku kepentingan akan jarang berubah, tapi kebutuhan spesifik mereka dan harapan mungkin agak berbeda dari yang diidentifikasi untuk keamanan informasi secara umum. (ISACA, 2013).

Tabel 2.1. Langkah Implementasi Cybersecurity pada Framework NIST

Step	***CSF Implementation Steps***
1	*Prioritize and Scope—Directs implementers to identify business/mission objectives and high-level organizational priorities. This mission understanding is critical to ensure that resulting risk decisions are prioritized and aligned with stakeholder goals, ensuring effective risk management and optimizing investment.*
2	*Orient—The organization identifies an overall risk approach, considering enterprise people, processes and technology along with external drivers such as regulatory requirements. It identifies threats to, and vulnerabilities of, those assets.*
3	*Create a Current Profile—Through use of a Profile template (example provided later in this publication) the organization determines the current state of Category and Subcategory outcomes from the Framework Core (analogous to COBIT 5 governance and management enablers) and how each is currently being achieved.*
4	*Conduct a Risk Assessment—The organization, guided by its risk management process, analyzes the operational environment to discern the likelihood of a cybersecurity event and the impact that the event could have. Incorporate emerging risk, threat, and vulnerability data to facilitate a robust understanding of the likelihood and impact of cybersecurity events.*
5	*Create a Target Profile—The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes. The organizations may develop additional Categories and Subcategories to account for unique organizational risk. It may also consider influences and requirements of external stakeholders such as sector entities, customers and*

	business partners when creating a Target Profile.
6	*Determine, Analyze, and Prioritize Gaps—The organization compares Current and Target Profiles to determine gaps. It creates a prioritized action plan to address those gaps, drawing on mission drivers, cost/benefit analysis, and risk understanding to achieve the target outcomes. The organization determines the resources necessary to address the gaps.*
7	*Implement Action Plan—The organization determines which actions to take in regard to the gaps, if any, identified in the previous step. It then monitors its current cybersecurity practices against the Target Profile. For further guidance, the CSF identifies example Informative References regarding the Categories and Subcategories, but organizations should determine which standards, guidelines and practices, including those that are sector-specific, work best for their needs.* *An organization may repeat the steps as needed to continuously assess and improve its cybersecurity. For instance, organizations may find that more frequent repetition of the Orient step improves the quality of risk assessments. Furthermore, organizations may monitor progress through iterative updates to the current profile, subsequently comparing the Current Profile to the Target Profile. Organizations may utilize this process to align their cybersecurity program with their desired Implementation Tier.*

Dalam thesis ini penulis memilih untuk menggunakan NIST. Hal ini disebabkan karena:

1. NIST akan membantu dalam memahami risiko cybersecurity dari perusahaan. Hal ini karena salah satu fungsi dari Framework NIST adalah Identify. Menurut NIST dengan Identify akan membantu perusahaan untuk mengelola risiko *cybersecurity* terhadap sistem, aset, dan data.
2. NIST Framework sepenuhnya gratis untuk digunakan.
3. Bahasa yang digunakan di dalam NIST Framework mudah dimengerti semua kalangan, baik IT maupun manajemen.
4. National Institute of Standards and Technology (NIST) merupakan sebuah badan non-regulator dari bagian Administrasi Teknologi dari

Departemen Perdagangan Amerika Serikat. Misi dari badan ini adalah untuk membuat dan mendorong pengukuran, standar, dan teknologi untuk meningkatkan produktivitas, mendukung perdagangan, dan memperbaiki kualitas hidup semua orang.

Dalam NIST, terdapat 3 *framework,* yaitu:

1. *Framework Core*

   Framework Core menyediakan serangkaian aktifitas untuk mencapai hasil tertentu dari cybersecurity, serta beberapa referensi yang dijadikan acuan dalam mencapai hasil tersebut. Framework Core bukanlah daftar tindakan yang harus dilakukan, namun menunjukkan hasil cybersecurity yang utama yang diidentifikasi oleh perusahaan dalam mengelola risiko cybersecurity. Framework Core terdiri dari 4 elemen, yaitu: *Function, Categories, Subcategories dan Informative Reference.*

   – *Functions* mengatur beberapa aktifitas cybersecurity yang dasar pada tingkat tertinggi. Functions ini terdiri dari Identify, Protect, Detect, Respond, dan Recover.
   – *Categories* merupakan subdivisi dari suatu Function kedalam kelompok hasil cybersecurity yang terkait dengan kebutuhan program kegiatan tertentu. Contoh dari Categories diantaranya *Asset Management, Access Control, Detection Process* dll.
   – *Subcategories* membagi Categories kedalam hasil yang lebih spesifik dari aktifitas teknikal dan/atau aktifitas manajemen.

– *Informative References* merupakan bagian dari standar, pedoman, dan praktek umum diseputar sektor infrastruktur yang kritikal yang menunjukkan metode yang digunakan dalam mancapai hasil untuk setiap subcategory.

Lebih jelas dapat dilihat pada tabel dibawah ini.

Tabel 2.2. Function, Categories, Subcategories dan Informative Reference pada Framework NIST.

Functions	Categories	Subcategories	Informative References
Identify			
Protect			
Detect			
Respond			
Recover			

2. Framework Implementation Tiers

Framework Implementation Tier menunjukkan keadaan bagaimana suatu perusahaan melihat risiko cybersecurity dan proses-proses apa saja yang dilakukan untuk mengelola risiko tersebut. Tier menunjukkan tingkat ketelitian dan kecanggihan dalam pengelolaan risiko cybersecurity. Tier terdiri dari 4 tingkatan, yaitu: Tier 1 : Partial, Tier 2 : Risk Informed, Tier 3 : Repeatable, Tier 4 : Adaptive. NIST menyarankan agar perusahaan dapat mencapai Tier 3 atau Tier 4.

Tabel 2.3. Tabel tier dari cybersecurity maturity.

Tier	Nama	Deskripsi
Tier 1	*Partial*	Risk Managementnya ad hoc, dengan awareness risiko yang terbatas, dan tidak ada kolaborasi dengan pihak lain
Tier 2	*Risk Informed*	Proses risk management dan programnya sudah ada, tapi tidak terintegrasi secara enterprise-wide (seluruh pihak di perusahaan). Kolaborasi dipahami tapi tidak secara formal.
Tier 3	*Repeatable*	Kebijakan mengenai proses menegement risiko serta programnya sudah ada secara enterprose-wide, dengan kolaborasi dengan pihak luar.
Tier 4	*Adaptive*	Proses Risk Managemnet dan programnya berdasarkan lesson learned dan telah melekat dala budaya perusahaan, dengan kolaborasi yang proaktif.

3. Framework Profile

Framework Profile (disingkat dengan "Profile") merupakan penyelarasan antara Functions, Categories, dan Subcategories dengan kebutuhan bisnis, toleransi risiko, dan sumber daya perusahaan. Sebuah Profile memungkinkan perusahaan untuk menetapkan suatu roadmap untuk mengurangi risiko cybersecurity yang selaras dengan tujuan perusahaan, memperhitungkan persyaratan hukum / peraturan dan best practice, dan mencerminkan prioritas dari manajemen risiko. Mengingat kompleksitas dari perusahaan, perusahaan mungkin memilih untuk memiliki beberapa profile, selaras dengan komponen tertentu dan kebutuhan masing-masing.

Framework Profile dapat digunakan untuk menggambarkan keadaan terkini atau tahapan target yang diinginkan dari aktifitas cybersecurity tertentu. Profil terkini menunjukkan keluaran cybersecurity terkini sedang

dicapai. Target Profil menunjukkan keluaran yang dibutuhkan untuk mencapai tujuan manajemen risiko cybersecurity yang diinginkan. Profil mendukung kebutuhan bisnis / misi dan bantuan dalam komunikasi risiko dalam dan antar organisasi. Dokumen Kerangka ini tidak menyarankan template profil, sehingga memungkinkan untuk fleksibilitas dalam implementasi.

Perbandingan Profil (misalnya, Profil saat ini dan Profil Target) dapat mengungkapkan kesenjangan yang harus ditangani untuk memenuhi tujuan manajemen risiko cybersecurity. Rencana aksi untuk mengatasi kesenjangan ini dapat berkontribusi pada roadmap yang dijelaskan di atas. Prioritas mitigasi kesenjangan didorong oleh kebutuhan bisnis organisasi dan proses manajemen risiko. Pendekatan berbasis risiko ini memungkinkan organisasi untuk mengukur estimasi sumber daya (misalnya, staf, pendanaan) untuk mencapai tujuan cybersecurity secara hemat biaya, dan berprioritas.

Selain 3 framework NIST tersebut, terdapat satu framework yang dapat digunakan untuk menghitung kapabilitas suatu fungsi dasar, yaitu Cybersecurity Capability Maturity Model (C2M2). C2M2 merupakan framework yang dapat digunakan untuk mengukur kapabilitas atau kemampuan dari suatu perusahaan atau suatu fungsi dasar. Sebagai suatu maturity model, C2M2 menyediakan sekumpulan karakteristik yang merepresentasikan kapabilitas dan progresi di dalam area cybersecurity yang berbeda. Karakteristik ini berasal dari best practice, standar dan guideline. (Muneer, 2014)

Cyber Security Maturity Model digunakan untuk menentukan cybersecurity maturity level di dalam 10 security domain sbb:

- *Risk Management*
- *Asset Identification, Change, and Configuration Management*
- *Identify and Access Management*
- *Threat and Vulnerability Management*
- *Situation Awareness*
- *Information Sharing and Communications*
- *Event and Incident Response, Continuity of Operations, and Service Restoration*
- *Supply Chain Management*
- *Workforce Management*
- *Cybersecurity Program Management*