BAB 3

METODOLOGI

3.1 Latar Belakang Perusahaan

PT. ABC merupakan sebuah Bank swasta yang menawarkan produk dan jasa inovatif serta komprehensif terutama disisi delivery channel-nya termasuk Internet Banking dan Mobile Banking. PT. ABC memiliki aspirasi untuk menjadi penyedia jasa keuangan terkemuka di Indonesia, dengan fokus di segmen Konsumer dan Komersial.

PT. ABC melayani sekitar 2 juta nasabah di 60 kota di Indonesia serta memiliki 329 cabang (16 Cabang Syariah & 313 Cabang Konvensional), 940 ATM dengan akses di lebih dari 69.000 ATM (VisaPlus, Visa Electron, MasterCard, Alto, ATM Bersama dan ATM Prima) dan jutaan ATM di seluruh dunia yang terhubung dengan jaringan Visa, Mastercard, Cirrus.

Untuk memberikan layanan yang optimal kepada nasabah, PT. ABC telah menyediakan beberapa layanan transaksi online melalui media electronic banking, yaitu:

- Internet Banking

  Internet Banking merupakan channel layanan transaksi perbankan melalui media internet dengan berbagai fitur, seperti:

  – Informasi saldo

  – Informasi 90 hari Transaksi terakhir

- Tagihan kartu kredit
- Tagihan ponsel
- Harga Pulsa
- PLN
- Mata uang asing dll
- Transfer antar rekening
- Transfer ke e-wallet / esaving
- Transfer ke bank lain anggota jaringan ALTO, ATM Bersama dan Prima via Online
- Transfer ke bank lain anggota jaringan ALTO, ATM Bersama dan Prima via LLG & RTGS
- Isi ulang pulsa ponsel
- Isi Ulang Internet
- Layanan Umum PLN, Telkom, Telkom Speedy, Palyja dll

- Mobile Banking

  Mobile Banking merupakan channel layanan transaksi perbankan melalui media smartphone dimana nasabah diharuskan untuk melakukan installasi aplikasi mobile banking pada smartphone nasabah.

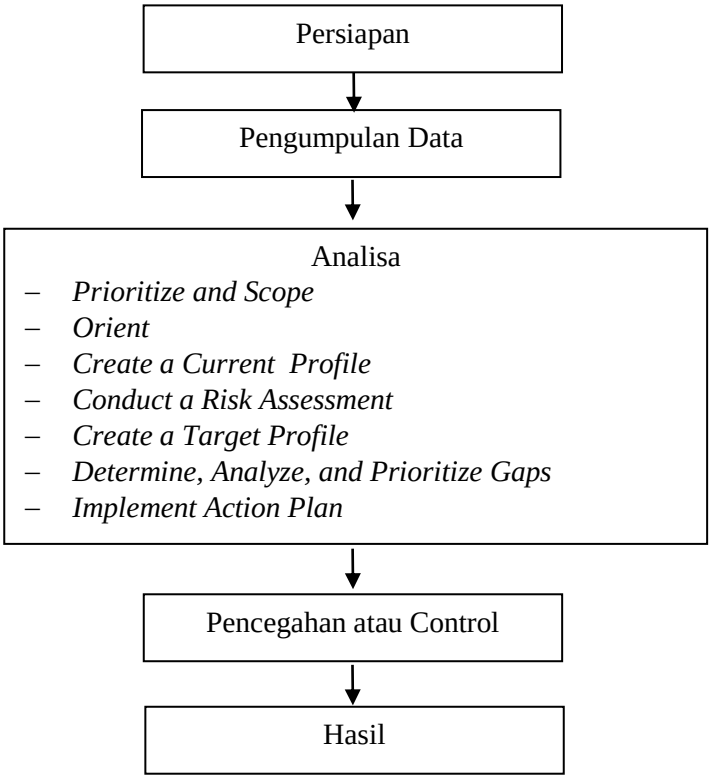
  Beberapa fitur yang disediakan diantaranya:

  - Informasi saldo
  - Informasi 4 transaksi terakhir
  - Tagihan kartu kredit
  - Tagihan ponsel
  - Harga pulsa isi ulang

- Tagihan Telkom
- Tagihan PLN
- Tagihan lainnya
- Forex
- Isi Ulang Pulsa Ponsel SimPATI, Kartu As, XL Prabayar, Mentari, StarOne, IM3, IM2, Fren, Esia, Flexy, Smart, Hepi, 3 dan Axis
- Isi Ulang Internet
- Transfer antar rekening
- Transfer ke Bank lain via Online, LLG & RTGS
- Mobile Cash (Reservasi , Pembatalan)
- Change Primary Account (untuk mengganti account aktif yang digunakan bertransaksi)
- Lock (untuk mengamankan agar layanan ini tidak dapat diakses untuk sementara
- Unlock (untuk dapat menggunakan layanan kembali)
- Tagihan Kartu kredit
- Tagihan Handphone
- Tagihan Telkom
- Layanan Umum PLN, Paljaya, PAM Bintaro dll

3.2 Kerangka Pikir

Secara ringkas gambaran kerangka pemikiran dari implementasi NIST Cybersecurity Framework ini dapat dilihat pada gambar berikut.



Gambar 3.1. Kerangka pikir penelitian

3.3 Langkah-langkah Penelitian

Pada penelitian ini, Penulis melakukan studi kasus untuk menganalisis keamanan cyber di PT. ABC. Secara garis besar, langkah penelitian yang dilakukan dibagi menjadi 5 langkah, yaitu persiapan, pengumpulan data, analisa, pencegahan atau control, dan hasil.

a. Langkah Persiapan

– Melakukan proses identifikasi terhadap permasalahan yang ada

  Pada langkah ini akan dipelajari latar belakang perusahaan, budaya, dan organisasinya. Demikian juga dengan latar belakang metodologi penelitian. Kemudian dipelajari bagaimana perusahaan melakukan pengelolaan terhadap aset informasi perusahaan terutama pengelolaan iternet banking dan mobile banking.

– Mengumpulkan study literatur

Melakukan pencarian landasan teori dan referensi yang dibutuhkan untuk membantu menyelesaikan masalah, baik melalui buku, jurnal.

b. Langkah pengumpulan data

Pengumpulan data dapat dilakukan dengan beberapa cara, yaitu:

– Observasi

Dilakukan observasi langsung ke lapangan untuk mendapatkan data

– Interview/wawancara

Interview/wawancara dilakukan dengan user untuk mendapatkan informasi. Instrumen untuk wawancara menggunakan alat ukur yang di generate dari NIST Cybersecurity Framework (Lampiran 1).

Untuk langkah interview ini secara detail dapat dilihat pada tabel berikut.

Tabel 3.1. Interview dengan User

No	PIC untuk diinterview	Data/Informasi yang diharapkan	Tujuan Interview
1.	*Chief Information Security Officer (CISO)*	- Struktur Organisasi IT - List IT Asset (hardware dan software) - Policy dan Procedure terkait Information Security dan Risk - List security incident - List vendor	- Memahami prioritas investasi di IT, terutama Information Security - Identifikasi ancaman, vulnerability dari IT Asset - Menentukan profil risiko tiap asset - Mendapatkan informasi key control
2.	*Head IT Infrastructure*	- Policy dan Procedure terkait IT Infrastructure - List project dan	Identifikasi infrastruktur IT yang kritikal

		inisiatif terkait infrastruktur	
3.	*Head IT Application*	- Policy dan Procedure terkait IT Application - List Semua Aplikasi - List project dan inisiatif terkait aplikasi	Identifikasi aplikasi yang kritikal

Informasi yang di dapat pada tabel di atas diperlukan untuk melakukan risk assessment sehingga diperoleh informasi ancaman dan vulnerability terhadap masing-masing aset serta likelihood dan impact dari cybersecurity event. Hal ini merupakan langkah awal dalam menetukan cybersecurity framework.

Untuk mendapatkan target profile, yaitu requirement terhadap pihak external seperti customer, rekan bisnis, vendor dll. Dari hasil target profile ini bisa dibuat prioritasisasi action plan, gap, langkah-langkah untuk mengurangi gap, cost benefit analysis, resource apa saja yang dibutuhkan untuk meminimalisir gap dll. Untuk lebih jelas dapat dilihat pada bagian analisis.

– Review dokumen

Dilakukan proses review terhadap dokumen yang diperoleh dari PT. ABC. Data yang diharapkan diperoleh dari PT. ABC diantaranya melalui:

✓ Unit kerja di PT. ABC

✓ Website perusahaan

- ✓ Media informasi perusahaan
- ✓ Regulator
- ✓ Lembaga lain
- ✓ Karya ilmiah yang sudah di publish

c. Langkah Analisa

Tujuh (7) langkah berikut menunjukan bagaimana suatu perusahaan menggunakan framework untuk membuat program cybersecurity atau meningkatkan program yang sudah ada.

1. Langkah 1: *Prioritize and Scope*

   Perusahaan mengidentifikasi tujuan bisnis dan prioritas perusahaan pada tingkat tinggi (hight level). Dengan informasi ini, organisasi membuat keputusan-keputusan strategis mengenai implementasi cybersecurity dan menentukan ruang lingkup sistem dan aset yang mendukung lini bisnis atau proses yang dipilih.

   Tujuan dari langkah ini adalah untuk mengidentifikasi fungsi-fungsi bisnis yang ada di perusahaan serta sistem yang mendukung lini bisnis. Fungsi-fungsi bisnis ini kemudian diurutkan berdasarkan prioritas. Beberapa hal yang harus dilakukan adalah:

   a. Mengidentifikasi fungsi bisnis yang ada di perusahaan.

      Contohnya:

No	Contoh Fungsi bisnis
1	Teknologi Informasi
2	Syariah
3	Treasury
4	Msmal Medium Enterprise (SME)

b. Membuat tabel fungsi bisnis berikut sistem yang digunakan pada fungsi bisnis tersebut.

Contohnya sebagai berikut:

No	Contoh Fungsi bisnis	Sistem
1	Teknologi Informasi	JHA, SAP
2	Syariah	SAP, T24
3	Treasury	JHA, Bloomberg
4	Msmal Medium Enterprise (SME)	JHA, ILoan

2. Langkah 2 : *Orient*

Setelah lingkup program cybersecurity telah ditentukan untuk lini bisnis atau proses, organisasi mengidentifikasi sistem terkait dan aset, persyaratan peraturan, dan pendekatan risiko secara keseluruhan. Organisasi kemudian mengidentifikasi ancaman, kerentanan (vulnerability), dan sistem terkait dengan aset. Output dari aktifitas ini adalah list aplikasi berdasarkan prioritas. Dalam menentukan prioritas suatu aplikasi maka dapat digunakan beberapa cara dan kriteria.

Contoh:

Aplikasi	Impact (H, M, L)	Likelihood (1-5)	Risiko	Risk Rating (H, M, L)	Priority Rating Aplikasi (H, M, L)

Dalam menilai prioritas suatu apliaksi, dapat dilakukan dengan:

- Menentukan seberapa besar impact aplikasi terhadap perusahaan.
- Seberapa sering aplikasi digunakan atau seberapa banyak user pengguna aplikasi tersebut. Misal 1=sangat jarang, 2=jarang, 3=cukup, 4=sering, 5=sangat sering.
- Risiko apa saja yang ada pada apliaksi tersebut.
- Seberapa besar risikonya, apakah High (H), Medium (M), atau Low (L).

Tabel diatas beserta cara menentukan prioritas aplikasi hanyalah contoh saja. Pada akhirnya setiap perusahaan tentu memiliki cara dan kriteria sendiri dalam menentukan prioritas aplikasi.

Berdasarkan fungsi bisnis yang sudah dipilih, perusahaan juga dapat mengidentifikasi ruang lingkup :

- Aset (seperti: orang, informasi, teknologi, fasilitas dll)
- Regulatory dan referensi informasi (cybersecurity standard, tool dll)

3. Langkah 3:*Create a Current Profile*

Dalam langkah ini dibuat suatu Current Profile yang menunjukkan Category dan Subcategory yang ada pada Framework Core yang saat ini sedang dicapai. Pada masing-masing subcategory dilakukan penilaian apakah penerapan pengamanan cybersecurity sudah tercapai sesuai dengan yang diinginkan perisahaan.

Untuk menilai tingkat pencapaiannya dapat digunakan skala pada tabel berikut.

Tabel 3.2. Tabel skala tingkat pencapaian.

Inisial	Deskripsi	Pencapaian
N	*Not achieved*	- Belum tercapai dan/atau - 0 – 15%
P	*Partially achieved*	- Sudah dilakukan, namun ada beberapa area yang bisa di tingkatkan, dan/atau - >15 – 50%
L	*Largelly achieved*	- Sudah lengkap dilakukan, namun masih ada area yang bisa ditingkatkan, dan/atau - >50 – 85%
F	*Fully achieved*	- Sudah lengkap dilakukan, dan/atau - >85 – 100%

Sumber: ISO 15504-2:2003, Section 5.7.2, on pages 10-11, with the permission of ANSI on behalf of ISO. © ISO 2014 - All rights reserved

Contohnya dapat dilihat untuk function Identify berikut:

Function	***Category***	***Subcategory***	***Current Profile***
IDENTIFY (ID)	***Asset Management (ID.AM):*** *The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.*	***ID.AM-1****: Physical devices and systems within the organization are inventoried*	F
		ID.AM-2: *Software platforms and applications within the organization are inventoried*	F
		ID.AM-3: *Organizational communication and data flows are mapped*	L
		ID.AM-4: *External information systems are catalogued*	P
		ID.AM-5: *Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value*	L
		ID.AM-6: *Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established*	L

4. Langkah 4: *Conduct a Risk Assessment*

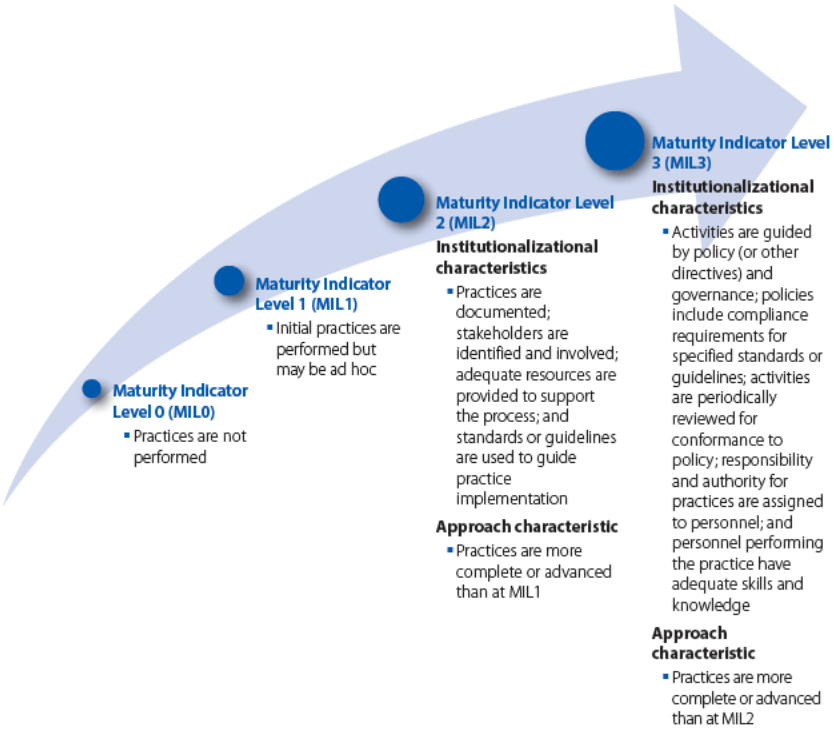
Risk assessment dilakukan untuk mengidentifikasi security dari fungsi bisnis. Hal ini dapat dilakukan dengan menentukan tier masing-masing fungsi bisnis dengan menggunakan framework

implementation tiers dan Cyber Security Maturity Model untuk menentukan cybersecurity maturity level di dalam 10 security domain.

Dalam maturity model ini digunakan 4 Maturity Indicator Level (MIL) seperti pada tabel berikut.

Tabel 3.3. Tabel maturity indicator level.

Level	**Karakteristik**
MIL0	Belum dilakukan
MIL1	Tahap awal sudah dilakukan tapi ad hoc
MIL2	Karakteristik Institusionalisasi: - Prakteknya telah didokumentasikan - Stakeholder telah diidentifikasi dan terlibat - Sumberdayanya cukup - Standar atau guideline telah digunakan dalam implementasi Karakterikstik Pendekatan: - Prakteknya telah lengkap atau lebih baik dari MIL1
MIL3	Karakteristik Institusionalisasi: - Aktifitasnya telah mengacu kepada policy terkait dan governance - Policynya termasuk compliance requirement untuk standar atau guideline tertentu - Aktifitas secara periodik direview untuk memastikan telah sesuai policy - Tanggungjawab dan otoritas untuk praktek telah ditunjuk pada personel tertentu - Personel yang melakukan praktek memiliki skil dan pengetahuan yang cukup. Karakterikstik Pendekatan: - Praktek lebih lengkap atau lebih baik dari MIL2



Tabel 3.4. Tabel Framework Implementation Tier

Framework Implementation Tier	***Tier Category***	***Characteristics***
Tier 1 : Partial	*Risk Management Process*	*Organizational cybersecurity risk management practices are not formalized, and risk is managed in an ad hoc and sometimes reactive manner.*
		Prioritization of cybersecurity activities may not be directly informed by organizational risk objectives, the threat environment, or business/mission requirements
	Integrated Risk Management Program	*There is limited awareness of cybersecurity risk at the organizational level and an organization-wide approach to managing cybersecurity risk has not been established.*
		The organization implements cybersecurity risk management on an irregular, case-by-case basis due to varied experience or information gained from outside sources.

		The organization may not have processes that enable cybersecurity information to be shared within the organization.
	External Participation	*An organization may not have the processes in place to participate in coordination or collaboration with other entities*
Tier 2: Risk Informed	*Risk Management Process*	*Risk management practices are approved by management but may not be established as organizational-wide policy.*
		Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
	Integrated Risk Management Program	*There is an awareness of cybersecurity risk at the organizational level but an organization-wide approach to managing cybersecurity risk has not been established.*
		Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties.
		Cybersecurity information is shared within the organization on an informal basis.
	External Participation	*The organization knows its role in the larger ecosystem, but has not formalized its capabilities to interact and share information externally*
Tier 3: Repeatable	*Risk Management Process*	*The organization's risk management practices are formally approved and expressed as policy.*
		Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape.
	Integrated Risk Management	*There is an organization-wide approach to manage cybersecurity risk.*

	Program	*Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed.*
		Consistent methods are in place to respond effectively to changes in risk. Personnel possess the knowledge and skills to perform their appointed roles and responsibilities.
	External Participation	*The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.*
Tier 4: Adaptive	*Risk Management Process*	*The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities.*
		Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner
	Integrated Risk Management Program	*There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events.*
		Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
	External Participation	*The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a*

		cybersecurity event occurs

5. Langkah 5: *Create a Target Profile*

Target Profile berfokus pada penilaian categories dan subcategories yang menggambarkan hasil yang diinginkan oleh perusahaan. Perusahaan juga dapat mengembangkan categories dan subcategories tambahan sendiri untuk memperhitungkan risiko perusahaan. Perusahaan juga dapat mempertimbangkan pengaruh dan persyaratan pemangku kepentingan eksternal seperti entitas sektor, pelanggan, dan mitra bisnis saat membuat Target Profile.

Tabel 3.5. Target Profile Framework Cybersecurity

Function	Category	Subcategory	Current Profile	Target Profile
IDENTIFY (ID)	***Asset Management (ID.AM):*** *The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.*	***ID.AM-1****: Physical devices and systems within the organization are inventoried*	F	F
		ID.AM-2: *Software platforms and applications within the organization are inventoried*	F	F
		ID.AM-3: *Organizational communication and data flows are mapped*	L	F
		ID.AM-4: *External information systems are catalogued*	P	L
		ID.AM-5: *Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value*	L	F
		ID.AM-6: *Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established*	L	F

6. Langkah 6: *Determine, Analyze, and Prioritize Gaps*

   Bandingkan current profile dan target profile untuk menentukan gap. Kemudian buat action plan untuk mengatasi gap tersebut. Action plan disesuaikan dengan misi perusahaan, cost/benefit analysis, dan pemahaman risiko untuk mencapai hasil dalam target profile. Kemudian tentukan sumber daya untuk mencapai target profile tersebut.

7. Langkah 7: *Implement Action Plan*.

   Perusahaan menentukan tindakan terkait gap yang diidentifikasi. Kemudian memonitor praktek cybersecurity dibandingkan dengan Target Profile. Lebih lanjut, framework mengidentifikasi contoh referensi terkait categories dan subcategories. Namun demikian perusahaan harus menentukan standar yang mana, guideline, dan praktek yang mana yang sesuai dengan perusahaan.

d. Langkah Pencegahan dan Control

   Dilakukan evaluasi terhadap keamanan cyber dan langkah-langkah untuk melakukan pencegahan atau control terhadap vulnerability yang ditemukan.

e. Langkah final/hasil

   - Dokumentasi hasil analisa.
   - Dokumen hasil identifikasi modus serangan.
   - Dokumen hasil identifikasi aset.

3.4 Metode Pengumpulan Data

Pengumpulan data dapat dilakukan dengan beberapa cara, yaitu:

- Observasi

  Dilakukan observasi langsung ke lapangan untuk mendapatkan data

- Interview/wawancara

  Interview/wawancara dilakukan dengan user untuk mendapatkan informasi

- Review dokumen

  Dilakukan proses review terhadap dokumen yang diperoleh dari PT. ABC

  Data yang diharapkan diperoleh dari PT. ABC diantaranya melalui:

  - ✓ Dari website perusahaan
  - ✓ Media informasi perusahaan
  - ✓ Regulator
  - ✓ Lembaga lain
  - ✓ Karya ilmiah yang sudah di publish