

# PANDUAN RESILIENSI DIGITAL (*DIGITAL RESILIENCE*)

DEPARTEMEN PENGATURAN DAN PENGEMBANGAN PERBANKAN  
OTORITAS JASA KEUANGAN





Halaman ini sengaja dikosongkan

# PANDUAN RESILIENSI DIGITAL *(DIGITAL RESILIENCE)*

DEPARTEMEN PENGATURAN DAN  
PENGEMBANGAN PERBANKAN  
OTORITAS JASA KEUANGAN



# DAFTAR ISI

SAMBUTAN KEPALA EKSEKUTIF PENGAWAS PERBANKAN	X
LATAR BELAKANG	2
Ketergantungan terhadap Teknologi	4
VUCA & the Unknown Risk	5
Interkoneksi Ekosistem Digital	6
Transformasi dan Dinamika Bisnis Keuangan Digital	7
Tantangan yang Akan Datang	13
RESILIENSI DIGITAL	18
Definisi	20
Digital Resilience vs Cyber Security	21
Aspek Resiliensi Digital	21
Kebijakan dan Regulasi terkait Resiliensi	22
KERANGKA RESILIENSI DIGITAL	24
Resiliensi Terhadap Dinamika Bisnis	27
Adopsi Teknologi ( <i>Technology Adoption</i> )	27
Faktor Pertimbangan dalam Adopsi Teknologi	28
Kerangka Adopsi Teknologi ( <i>Technology Adoption Framework</i> )	31
Sumber Daya Manusia dan Organisasi di Era Digital ( <i>People &amp; Organization</i> )	41
Kepemimpinan Digital ( <i>Digital Leadership</i> )	42
Budaya Digital ( <i>Digital Culture</i> )	43
Talenta Digital ( <i>Digital Talent</i> )	44
Desain Organisasi ( <i>Organizational Design</i> )	45
Pengembangan Produk yang Berorientasi Konsumen ( <i>Customer-centric Product Development</i> )	48
Keterikatan Konsumen ( <i>Customer Engagement</i> )	49
Pengalaman Konsumen ( <i>Customer Experience</i> )	49



Pemahaman terkait Konsumen <i>(Customer Insight)</i>	50	Respon atas Insiden <i>(Incident Response)</i>	86
Kepercayaan dan Persepsi Konsumen <i>(Customer Trust and Perception)</i>	50	Manajemen Krisis <i>(Crisis Management)</i>	86
Resiliensi Bank terhadap gangguan atau Disrupsi dalam Lanskap Digital	53	Pemulihan Bencana <i>(Disaster Recovery)</i>	87
Antisipasi <i>(Anticipate)</i>	53	Manajemen Komunikasi Insiden <i>(Incident Communication Management)</i>	87
Tata Kelola Kelangsungan Bisnis <i>(Business Continuity Management Governance)</i>	53	Berkelanjutan <i>(Sustain)</i>	91
Analisis Dampak Bisnis <i>(Business Impact Analysis)</i>	57	Root-Cause Analysis (RCA) atas Insiden	92
Penilaian Risiko <i>(Risk Assessment)</i>	65	A Crisis After-action Review	93
Strategi Ketahanan <i>(Resilience Strategy)</i>	66	Pelatihan dan Peningkatan Kesadaran <i>(Training and Awareness)</i>	93
Rencana Kelangsungan Bisnis <i>(Business Continuity Plan)</i>	70	Pengembangan <i>(Continuous Improvement)</i>	94
Pengujian Ketahanan <i>(Resilience Assessment)</i>	79	Resiliensi Nasabah di Era Digital	99
Bertahan dan Pulih <i>(Withstand and Recover)</i>	84	Manajemen Insiden bagi Konsumen <i>(Customer Incident Management)</i>	99
Penilaian Pelanggaran Keamanan <i>(Compromise Assessment)</i>	85	Pemulihan Insiden bagi Konsumen <i>(Customer Incident Recovery)</i>	100
		Layanan Pasca- Insiden bagi Konsumen <i>(Customer Post-Recovery Services)</i>	101

# DAFTAR SINGKATAN

5G	<i>Fifth Generation</i>	POJK	Peraturan Otoritas Jasa Keuangan
AI	<i>Artificial Intelligence</i>	RBS	Royal Bank of Scotland
APK	<i>Android Package Kit</i>	RCA	<i>Root-Cause-Analysis</i>
ATM	Anjungan Tunai Mandiri	RPO	<i>Recovery Point Objective</i>
BCM	<i>Business Continuity Management</i>	RTO	<i>Recovery Time Objective</i>
BCP	<i>Business Continuity Plan</i>	SDM	Sumber Daya Manusia
BIA	<i>Business Impact Analysis</i>	SEOJK	Surat Edaran Otoritas Jasa Keuangan
DC	<i>Domain Controller</i>	SLA	<i>Service Level Agreement</i>
DDoS	<i>Distributed Denial of Service</i>	SRTO	<i>Service Recovery Time Objective</i>
EU	<i>European Union</i>	TI	Teknologi Informasi
FAQ	<i>Frequently Ask Question</i>	UI/UX	<i>User Interface/User Experience</i>
LJK	Lembaga Jasa Keuangan	UK	United Kingdom
MTD	<i>Maximum Tolerable Downtime</i>	UU	Undang-Undang
MVP	<i>Minimum Viable Product</i>	VPN	<i>Virtual Private Network</i>
OJK	Otoritas Jasa Keuangan	VUCA	<i>Volatility Uncertainty Complexity Ambiguity</i>
OS	<i>Operating System</i>	WEF	World Economic Forum
OTP	<i>One-Time-Password</i>		
PIN	<i>Personal Identification Number</i>		
POC	<i>Proof-of-Concept</i>		

## DAFTAR ISTILAH

<i>Cloud Computing</i>	Layanan bisnis yang menyediakan akses jaringan ke sumber daya komputer ( <i>server, database storage, aplikasi, services</i> ) yang dapat dikonfigurasi dan digunakan sesuai permintaan, disediakan secara cepat dengan interaksi yang minimal.
CIA Triad	Rancangan model yang digunakan untuk menjadi panduan atau membantu seseorang baik secara individu maupun organisasi tertentu dalam membentuk atau membuat sebuah aplikasi, sistem, prosedur, atau kebijakan yang berhubungan dengan keamanan informasi.
<i>Blockchain</i>	Teknologi yang digunakan sebagai sistem penyimpanan data digital yang terhubung melalui kriptografi.
<i>Artificial Intelligence</i>	Analisis dan teknik berbasis logika untuk menginterpretasikan peristiwa, mendukung dan mengotomatisasi proses pengambilan keputusan dan aksi.
<i>Big Data Analytics</i>	Teknik analisis lanjutan ( <i>advanced</i> ) untuk mengolah set data berjumlah besar dan beranekaragam, dari data yang terstruktur, semi-terstruktur, dan tidak terstruktur, yang diperoleh dari berbagai sumber dan ukuran (terabytes to zettabytes).
<i>Emerging Technology</i>	Pengembangan, kombinasi, atau integrasi dari beberapa teknologi yang sudah ada sebelumnya.
<i>Fintech</i>	Inovasi teknologi jasa keuangan yang menghasilkan model bisnis, aplikasi, proses, dan/atau produk baru.
<i>Machine Learning</i>	Bentuk dari <i>artificial intelligence</i> yang memungkinkan suatu sistem untuk belajar dari data ketimbang dari proses pemrograman yang eksplisit.
<i>Biometrics</i>	Studi dan penerapan metode ilmiah dan/atau teknologi yang dirancang untuk mengukur, menganalisis, dan/atau mencatat karakteristik fisiologis atau perilaku unik manusia.
<i>Internet of Things</i>	Digitalisasi atas dunia/aplikasi fisik.
<i>Augmented Reality</i>	Teknologi yang menggabungkan benda maya dua dimensi dan ataupun tiga dimensi ke dalam sebuah lingkungan nyata lalu memproyeksikan benda-benda maya tersebut secara realitas dalam waktu nyata

<i>Social Engineering</i>	Teknik manipulasi yang memanfaatkan kesalahan manusia untuk mendapatkan akses pada informasi pribadi atau data-data berharga.
<i>Cyber Fraud</i>	Kejahatan yang dilakukan dalam sistem berbasis komputer maupun jaringan internet yang bertujuan untuk memanipulasi informasi keuangan guna mengeruk keuntungan sebesar-besarnya.
<i>Cyber Crime</i>	Kejahatan di dunia maya yang memanfaatkan teknologi komputer dan jaringan internet untuk mencuri data pribadi seseorang demi kepentingan pribadi
<i>Use Case</i>	Sebuah teknik pemodelan yang digunakan untuk menjelaskan apa yang harus dilakukan sebuah sistem baru
<i>Proof-of-Concept</i>	Pendekatan yang digunakan untuk memvalidasi konsep atau ide dari segi fungsional, penerapan, teknis atau metode sebuah perangkat lunak sebelum masuk tahap pengembangan.
<i>Minimum Viable Product</i>	Istilah yang digunakan untuk menyebut sebuah produk teknologi yang masih sangat mendasar, hanya dibekali fitur-fitur dasar namun unik dan mampu menarik perhatian <i>user</i> atau pengguna
<i>Business Intelligence</i>	Proses bisnis yang dapat memanfaatkan teknologi tertentu agar dapat menganalisa data dan menyajikan data tersebut sebagai bentuk informasi yang mudah dipahami untuk keperluan bisnis
<i>Malware</i>	Program yang dirancang dengan tujuan untuk merusak dengan menyusup ke sistem komputer
<i>data corruption</i>	Data mengalami kerusakan sehingga tidak dapat digunakan, tidak dapat dibaca atau dengan cara lain tidak dapat diakses oleh pengguna atau aplikasi
<i>Reverse Social Engineering</i>	Teknik serangan kepada personal melalui kontak/pendekatan secara langsung dengan target untuk mendapatkan informasi/data sensitif milik target melalui manipulasi psikologis
<i>Ransomware</i>	Jenis <i>malicious software</i> tertentu yang menuntut tebusan finansial dari seorang korban dengan melakukan penahanan pada asset atau data yang bersifat pribadi.
<i>PowerShell</i>	Jenis <i>command line interface</i> yang mendukung teknik pemrograman berorientasi objek pada Windows
<i>Service Recovery Time Objective (SRTO) / Recovery Time Objective (RTO)</i>	Mengacu pada target durasi untuk memulihkan fungsi dan layanan bisnis kritikal masing-masing.

## DAFTAR GAMBAR

Gambar 1	Klasifikasi Jenis Risiko	5
Gambar 2	Evolusi Industri Perbankan	8
Gambar 3	Transformasi Layanan Perbankan	9
Gambar 4	Sepuluh Risiko Global Terbesar dalam 2 hingga 10 tahun ke depan	13
Gambar 5	Kemungkinan dan Dampak Risiko Geopolitik Teratas 2023	14
Gambar 6	Tren Peristiwa Serangan Siber di Indonesia	14
Gambar 7	<i>National Risk Perception, by Region: Cybercrime and Cyber Insecurity</i>	15
Gambar 8	Aspek Digital Resilience	22
Gambar 9	Kebijakan dan Regulasi terkait Resiliensi	23
Gambar 10	Faktor Pertimbangan dalam Adopsi Teknologi	28
Gambar 11	Tahapan dalam Adopsi Teknologi	31
Gambar 12	Kapasitas Digital	42
Gambar 13	Kapasitas Kepemimpinan	43
Gambar 14	Talenta Digital	45
Gambar 15	Desain Organisasi yang Mendukung Transformasi Digital	45
Gambar 16	<i>Customer-centric Orientation Services</i>	49
Gambar 17	Komponen dalam BCM	53
Gambar 18	Objektif Pemulihan sesuai dengan Alur Peristiwa	64
Gambar 19	Langkah-Langkah dalam rangka Bertahan dan Pulih dari Insiden	88
Gambar 20	Diagram Stakeholder Risk vs Visibility Matrix	89
Gambar 21	Alur Penyiapan Komunikasi Ketika Terjadi Gangguan	91
Gambar 22	Langkah-Langkah dalam rangka Ketahanan Berkelanjutan	95
Gambar 23	Aktivitas dalam Mendukung Resiliensi	97

## DAFTAR TABEL

Tabel 1	Aspek Utama Budaya Digital	44
Tabel 2	Contoh Layanan Bisnis Kritis di Sektor Jasa Keuangan	58

## DAFTAR GRAFIK

Grafik 1	Nilai Transaksi Melalui <i>Electronic Channel Bank</i>	10
Grafik 2	Volume Transaksi Melalui <i>Electronic Channel Bank</i>	10
Grafik 3	Nilai Transaksi Belanja Uang Elektronik	10
Grafik 4	Volume Transaksi Belanja Uang Elektronik	10

# SAMBUTAN KEPALA EKSEKUTIF PENGAWAS PERBANKAN



**Dian Ediana Rae**

Kepala Eksekutif Pengawas Perbankan –  
Anggota Dewan Komisioner OJK

*Assalamu'alaikum Wr. Wb., Salam Sejahtera bagi kita semua, Om Swastyastu, Namo Buddhaya, Salam Kebajikan.*

Puji dan syukur kami panjatkan ke hadirat Tuhan Yang Maha Esa, karena berkat limpahan rahmat dan karunia-Nya, Panduan Resiliensi Digital Perbankan ini telah selesai kami susun dan dapat kami sajikan kepada para pemangku kepentingan sebagai panduan.

Perkembangan teknologi informasi yang pesat telah mengubah lanskap perbankan nasional ke arah model bisnis digital. Hal ini menuntut Bank untuk melakukan akselerasi transformasi digital dalam rangka memenuhi ekspektasi nasabah dan berkompetisi dengan pelaku sektor jasa keuangan lain. Model bisnis Bank yang semakin terdigitalisasi juga didukung oleh potensi ekonomi digital Indonesia yang semakin meningkat, sehingga di masa depan, produk dan keuangan berbasis digital diprediksi akan menjadi salah satu kebutuhan utama bagi masyarakat dalam mendukung aktivitas ekonomi sehari-hari.

Digitalisasi memberikan manfaat untuk meningkatkan efisiensi di berbagai aspek. Namun demikian, digitalisasi turut menghadirkan sejumlah tantangan dan risiko bagi perbankan yang perlu diantisipasi dan dimitigasi. Disamping itu, transformasi digital yang saat ini sedang dilakukan oleh industri perbankan nasional akan meningkatkan kompleksitas penggunaan dan ketergantungan (*interdependency*) terhadap teknologi informasi (TI) dalam operasional bisnis perbankan.

Digitalisasi turut mendorong adanya kolaborasi yang menyebabkan Bank semakin terkoneksi dengan pihak ketiga, sehingga ekosistem bisnis semakin besar dan kompleks. Tanpa adanya sistem perbankan yang resilien, maka satu serangan siber pada titik-titik koneksi dan interaksi tersebut akan menghasilkan efek yang signifikan bagi kelangsungan operasional dan usaha Bank. Dengan demikian, Bank perlu meningkatkan resiliensi digital (*digital resilience*).

Kerangka resiliensi digital yang terstruktur menjadi strategi penting dalam membentengi diri dari berbagai risiko digital yang muncul. Konteks resiliensi digital tidak hanya sebatas ketahanan terkait infrastruktur digital dan implementasi teknologi dari Bank. Hal ini berkaitan juga dengan proses mitigasi, kebijakan terkait digital, serta aspek yang paling utama dan justru kritikal adalah aspek *people* yaitu sumber daya manusia (SDM) dan konsumen, mengingat aspek *people* berpeluang menjadi celah dalam pengamanan dan ketahanan siber.

Pentingnya aspek non teknis seperti SDM dan kepemimpinan tercermin dalam kemampuan Bank dalam menghadapi bisnis di era digital yang bergerak cepat, dinamis, dan mengikuti tren masa kini sehingga membutuhkan kematangan strategi untuk dapat bertahan dan berkompetisi di sektor jasa keuangan yang semakin kompetitif.

Dalam rangka mengawal Bank untuk mempersiapkan resiliensi digital, OJK telah menyusun kerangka kerja Panduan Resiliensi Digital (*Digital Resilience Framework*). Secara umum kerangka resiliensi digital meliputi ketahanan terhadap dinamika bisnis dan ketahanan terhadap disruptif/gangguan.

Resiliensi terhadap dinamika bisnis tercermin dalam dimensi *digital competitiveness* yang meliputi pengembangan produk yang berorientasi konsumen, adopsi teknologi, serta transformasi desain organisasi, kepemimpinan digital, budaya digital, dan talenta digital.

Resiliensi Bank terhadap gangguan/disrupsi dalam lanskap digital tercermin dalam kerangka manajemen kelangsungan bisnis yang terdiri atas 3 (tiga) tahapan utama, meliputi tahap Antisipasi (*Anticipate*) melalui penerapan *Business Continuity Management* (BCM), tahap Bertahan dan Pulih (*Withstand and Recover*)

berupa aktivasi rencana kelangsungan bisnis yang telah disusun, dan tahap Berkelanjutan (*Sustain*) berupa evaluasi dan pengembangan atas pemahaman dan kesiapan Bank terhadap gangguan/disrupsi ke depannya.

Sebagai bagian dari perlindungan konsumen di era digital, kerangka resiliensi digital turut mencakup aspek pelindungan konsumen yang meliputi Manajemen Insiden bagi Konsumen (*Customer Incident Management*), Pemulihan Insiden bagi Konsumen (*Customer Incident Recovery*), dan Layanan Pasca-Insiden bagi Konsumen (*Customer Post-Recovery Services*)

Panduan Resiliensi Digital disusun untuk melengkapi rangkaian kebijakan akselerasi transformasi digital perbankan yang telah dituangkan oleh OJK antara lain Cetak Biru Transformasi Digital Perbankan, POJK No.11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum, SEOJK No.29/SEOJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum, dan SEOJK No.24/SEOJK.03/2023 tentang Penilaian Tingkat Maturitas Digital Bank Umum.

Akhir kata, saya menyampaikan apresiasi yang sebesar-besarnya kepada seluruh pihak yang telah terlibat dalam memberikan masukan, komentar, serta saran-saran yang sangat berharga dalam penyusunan Panduan Resiliensi Digital Perbankan. Semoga Tuhan Yang Maha Kuasa senantiasa melapangkan dan memudahkan jalan setiap ikhtiar baik yang kita lakukan, khususnya keinginan untuk mewujudkan industri perbankan nasional yang resilien, adaptif, berdaya saing, dan kontributif.

*Wassalamu'alaikum Wr. Wb., Om Shanti Shanti Shanti Om, Namo Buddhaya,  
Salam Kebajikan*

Dian Ediana Rae

Kepala Eksekutif Pengawas Perbankan –  
Anggota Dewan Komisioner OJK



Halaman ini sengaja dikosongkan



# LATAR BELAKANG





# 1

## Ketergantungan terhadap Teknologi

Perkembangan teknologi informasi yang pesat telah mengubah lanskap perbankan nasional ke arah model bisnis digital. Perubahan signifikan ini semakin dipercepat dengan adanya pandemi Covid-19 yang menuntut Bank melakukan akselerasi transformasi digital untuk dapat memenuhi ekspektasi nasabah dan berkompetisi dengan pelaku sektor jasa keuangan lain dalam memberikan produk dan layanan keuangan yang inovatif dan sesuai dengan tren terkini. Model bisnis Bank yang semakin terdigitalisasi juga didukung oleh potensi ekonomi digital Indonesia yang semakin meningkat sehingga di masa depan produk dan keuangan berbasis digital diprediksi akan menjadi salah satu kebutuhan utama bagi masyarakat dalam mendukung aktivitas ekonomi sehari-hari. Berdasarkan laporan dari *We Are Social* tahun 2023, jumlah pengguna internet di Indonesia mencapai 212,9 juta orang atau sekitar 77% dari total populasi Indonesia. Penggunaan media sosial menjadi tren bagi masyarakat Indonesia, hal ini tercermin dari jumlah pengguna media sosial yang mencapai 167 juta orang atau setara dengan 60,4% dari total populasi per Januari 2023. Peluang digitalisasi di sektor keuangan semakin besar ke depan, dengan total penggunaan internet untuk mengakses aplikasi (*mobile apps*) terkait dengan jasa keuangan seperti bank, investasi, dan asuransi mencapai 29,1%. Dalam beberapa tahun ke depan, tingkat ketergantungan masyarakat terhadap teknologi berpotensi akan meningkat. Berdasarkan riset IDC, pada tahun 2025 diprediksi terdapat lebih dari 41 Miliar perangkat di dunia yang terkoneksi *Internet of Things* (IoT), sementara menurut Huawei, populasi dunia yang tercover jaringan 5G akan mencapai 58% di tahun yang sama.

Tren digitalisasi yang relatif cepat menyebabkan kegiatan ekonomi dan keuangan masyarakat seakan tidak mengenal batas ruang dan waktu. Transaksi ekonomi dan keuangan dapat dilakukan dimana saja, kapan saja, dan darimana saja. Hal ini menyebabkan bank dituntut untuk melakukan perubahan agar dapat memenuhi kebutuhan dalam kegiatan ekonomi dan keuangan masyarakat yang timbul akibat transformasi digital, dan lebih lanjut agar dapat terus bertahan di pasar yang terus bergerak secara dinamis. Tren digitalisasi di masyarakat



mendorong transformasi digital pada perbankan sehingga meningkatkan implementasi teknologi pada operasional bank secara menyeluruh, termasuk penggunaan pihak penyedia jasa teknologi informasi atau pihak ketiga. Hal ini tentunya akan meningkatkan kompleksitas penggunaan dan ketergantungan (*interdependency*) perbankan terhadap teknologi informasi (TI) dalam operasional bisnis perbankan. Dengan demikian, jika terjadi kegagalan sistem teknologi informasi dapat mengakibatkan ketidakmampuan bank untuk beroperasi dan pulih secara cepat sehingga menimbulkan gangguan operasional yang dapat mempengaruhi kegiatan ekonomi nasabah secara signifikan, serta meningkatkan risiko reputasi yang dapat mengancam bisnis Bank.

## 2 VUCA & the Unknown Risk

Perbankan sebagai penyedia layanan keuangan perlu menyikapi perkembangan ekonomi dan keuangan digital, berikut dengan perubahan perilaku masyarakat ke arah layanan digital, sebagai suatu peluang sekaligus tantangan. Perubahan ekosistem sektor keuangan yang didorong oleh arus digitalisasi dapat menimbulkan disrupti yang memicu *Volatility* (Volatilitas), *Uncertainty* (Ketidakpastian), *Complexity* (Kompleksitas), dan *Ambiguity* (Ambiguitas), atau dikenal sebagai VUCA di industri perbankan akan terus meningkat. Selain VUCA, arus digitalisasi yang masif juga menimbulkan potensi peningkatan berbagai macam risiko yang tidak dapat diprediksi atau yang lebih dikenal dengan *unknown-unknown risk*.

Gambar 1 Klasifikasi Jenis Risiko

		Empirical Knowledge	
		Data	No Data
Measurement Model	Known-known	Unknown-known	
	<p><i>Things we are aware of and understand</i></p> <p>Contoh: risiko kecelakaan kerja yang terjadi di lokasi konstruksi sehingga tindakan pencegahan dapat dilakukan atau klaim tagihan asuransi kendaraan</p>	<p><i>Things we understand but are not aware of</i></p> <p>Contoh: bias yang terjadi dari suatu penelitian/percobaan</p>	
No Model	Known-unknown	Unknown-unknown	
	<p><i>Things we are aware of but don't understand</i></p> <p>Contoh: virus yang berevolusi menjadi bentuk baru dan tidak terduga -&gt; WHO mengusulkan agar para ilmuwan dan praktisi kesehatan masyarakat bersiap untuk menghadapi "known unknown pathogen" yang disebut Disease-X (Nuki &amp; Shaikh, 2018)</p>	<p><i>Things we are neither aware of nor understand</i></p> <p>Contoh: kejadian "Black Swan", bencana alam yang belum pernah terjadi sebelumnya, wabah penyakit, instabilitas politik, pandemi global, dan serangan alien.</p>	

Sumber : Casti (2011); Daase and Kessler (2007) dalam Pererra dan Higgins (2017), dimodifikasi

*Unknown-unknown risk* didefinisikan sebagai suatu ketidakpastian yang terjadi akibat dari suatu kejadian atau faktor yang tidak teridentifikasi dan tidak dapat diprediksi. Risiko ini mencakup semua risiko yang tidak dapat diidentifikasi sebelumnya mengingat tidak ada probabilitas yang dapat ditentukan terhadap keterjadian peristiwa tersebut. Salah satu contoh *unknown-unknown risk* adalah pandemi Covid-19 yang terjadi secara mendadak dan membawa perubahan pada pola kehidupan masyarakat, seperti aktivitas yang sebelumnya dilakukan secara langsung (tatap muka) kemudian berubah menjadi tidak langsung (daring, melalui aplikasi digital, dll). Ketidakpastian yang terjadi saat ini dan di masa mendatang menuntut Bank untuk dapat secara efektif merespon perubahan secara cepat dan tepat. Bank perlu secara aktif melakukan penilaian yang akurat atas berbagai potensi risiko berikut dampaknya terhadap fungsi bisnis Bank, serta menyiapkan pertahanan yang memadai dalam hal terjadi kejadian yang tidak dapat diprediksi, sehingga bisnis Bank dapat terus bertahan (resilien) dan berkembang di masa depan. Resiliensi memungkinkan Bank untuk dapat merespon dan menghadapi era VUCA, serta memastikan Bank mampu bertahan dalam menghadapi risiko tidak terduga (*the unknown risk*) dengan tepat saat muncul.

## 3 Interkoneksi Ekosistem Digital

Meningkatnya digitalisasi layanan keuangan yang dikombinasikan dengan kehadiran aset dan data bernilai tinggi membuat sistem keuangan rentan terhadap insiden siber. Interkoneksi yang tinggi antar lembaga keuangan, pasar keuangan berikut infrastrukturnya, khususnya dalam hal ketergantungan antar-sistem TI mereka, merupakan sebuah 'celah' karena insiden siber yang terlokalisasi dapat dengan cepat menyebar dan memengaruhi keseluruhan sistem dan jaringan. Seperti, dalam hal pembayaran dan infrastruktur keuangan termasuk perbankan ritel *online* yang telah menjadi digital. Ketergantungan pada infrastruktur (sistem) TI dan sarana komunikasi elektronik inilah yang akan memperparah dampak apabila insiden siber terjadi. Selain itu, adopsi teknologi baru seperti *cloud computing*, menciptakan ketergantungan baru terhadap entitas luar (*third-parties*) yang operasionalnya dapat berada di luar batasan dan cakupan sistem keuangan yang telah diatur, sehingga akan melahirkan risiko-risiko baru.

Salah satu contoh komponen yang rentan adalah data. Dalam mengelola data yang dimiliki, sistem keuangan membutuhkan infrastruktur (sistem) TI yang kuat. Sistem TI, dengan karakteristik komponennya yang saling terkoneksi dan saling bergantung, berperan penting dalam berjalannya fungsi utama sistem keuangan. Data yang dikelola wajib dilindungi dengan memperhatikan aspek

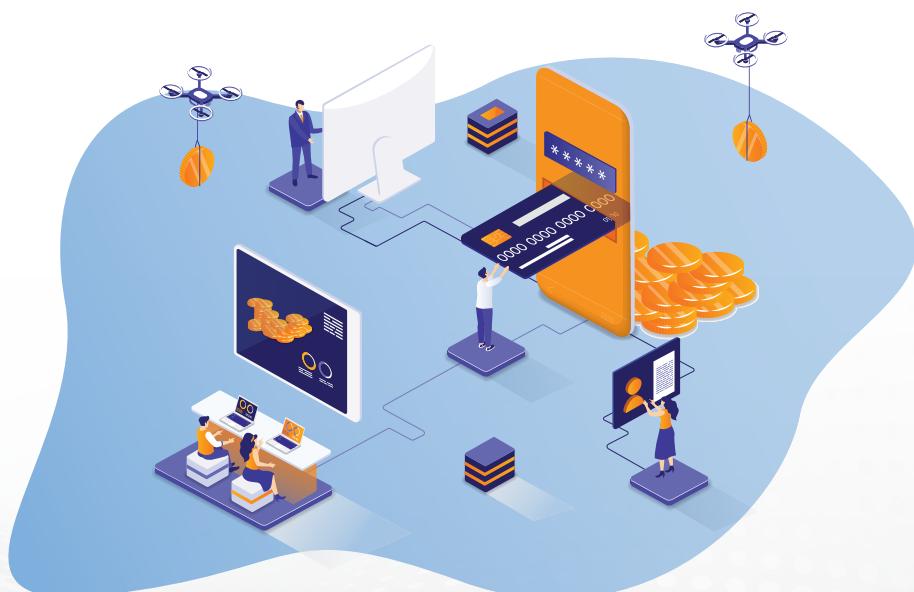
*confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan) atau dikenal sebagai "CIA Triad", yang merupakan 3 (tiga) sifat penting dari data yang diproses oleh sistem (*European Systemic Risk Board*, 2020).

Meskipun demikian, tidak dapat dipungkiri bahwa kombinasi teknologi dan komponen lain dalam satu ekosistem digital (*interconnectedness*) dapat melipatgandakan potensi dan daya saing Bank. Lebih lanjut, interkoneksi dalam ekosistem keuangan bukan merupakan sesuatu yang harus dihindari, melainkan dihadapi dan diimbangi dengan strategi ketahanan yang memadai.

## 4

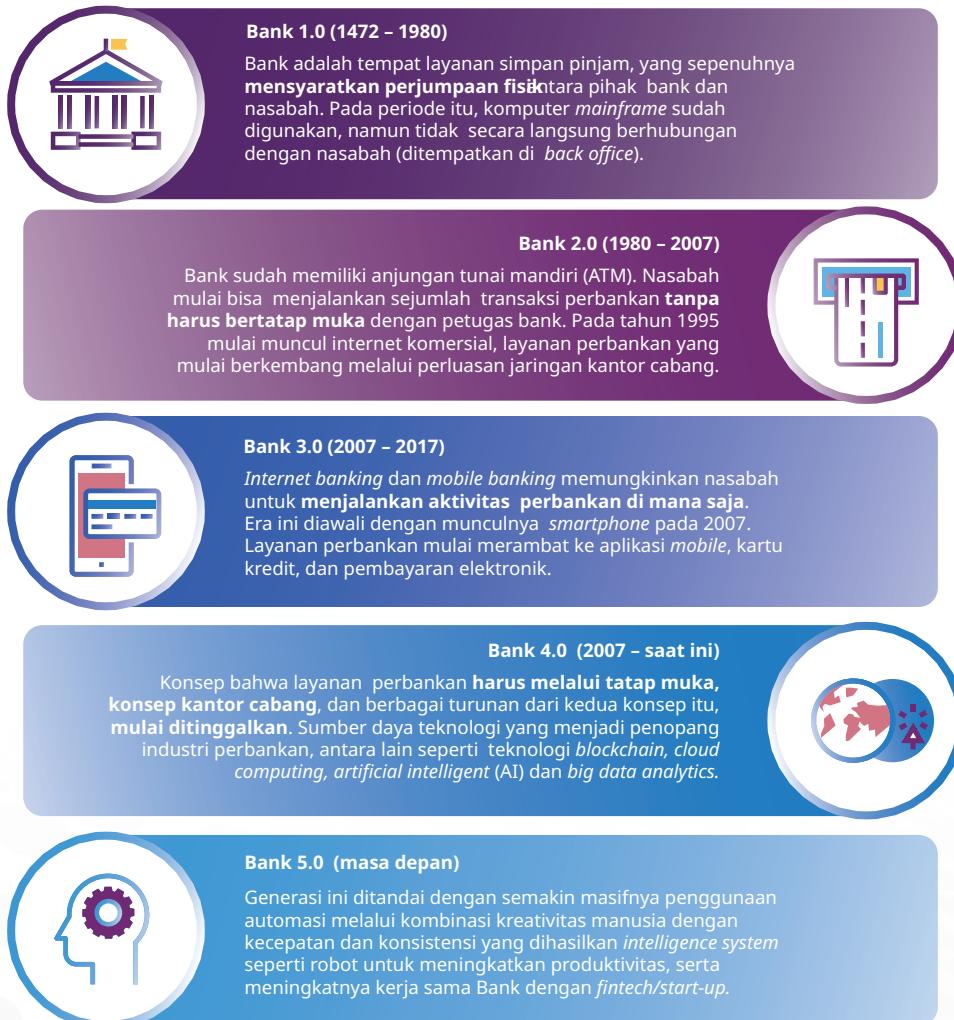
## Transformasi dan Dinamika Bisnis Keuangan Digital

Industri Perbankan telah melalui 5 (lima) fase perkembangan sampai saat ini. Diawali dengan fase Bank 1.0, bank dengan bentuk paling konvensional yang berfungsi sebagai tempat layanan simpan pinjam dengan sepenuhnya mensyaratkan perjumpaan fisik antara pihak bank dan nasabah. Selanjutnya, fase Bank 2.0 dimana bank pada umumnya telah memiliki mesin anjungan tunai mandiri (ATM), serta nasabah mulai dapat melakukan beberapa aktivitas transaksi perbankan tanpa harus bertatap muka dengan petugas bank (*self-service banking*). Fase Bank 3.0 dimulai di tahun 2007 s.d. 2017, ditandai dengan kehadiran *internet banking* dan *mobile banking* yang memungkinkan nasabah untuk menjalankan aktivitas perbankan dari manapun. Memasuki fase Bank 4.0, dimana konsep layanan perbankan 'tatap muka', konsep kantor cabang, dan berbagai turunannya mulai ditinggalkan.



Industri bank pada fase ini identik dengan penggunaan teknologi seperti *blockchain*, *artificial intelligent (AI)*, serta *big data analytics* sebagai sumber daya penopang. Pasca Pandemi yang dikenal dengan era *New Normal*, perbankan mulai memasuki era baru yang dinamakan Bank 5.0. Nicoletti dalam buku nya Bank 5.0 memaparkan bahwa Generasi Bank 5.0 ditandai dengan semakin masifnya penggunaan automasi melalui kombinasi antara kreativitas manusia dengan kecepatan, produktivitas, dan konsistensi yang dihasilkan *intelligence system* seperti robot untuk meningkatkan produktivitas, serta meningkatnya aliansi/kemitraan Bank dengan pelaku ekosistem digital lain seperti *fintech/start-up*. Hal ini menunjukkan bahwa adopsi *emerging technology* akan menjadi suatu kebutuhan sehingga Bank dapat meningkatkan penetrasi pasar dan meningkatkan daya saing.

Gambar 2 Evolusi Industri Perbankan



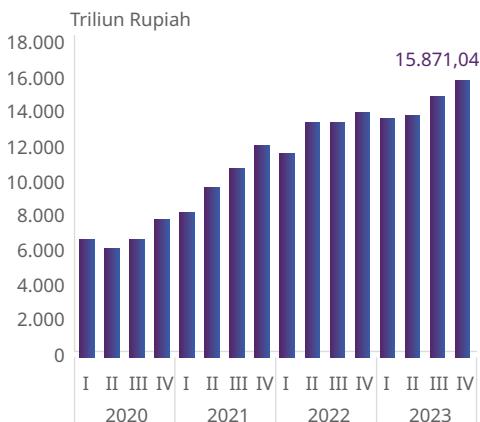
Produk dan layanan perbankan yang masyarakat rasakan saat ini merupakan hasil dari evolusi yang terjadi di industri perbankan. Di masa lampau, perbankan identik dengan layanan tatap muka di kantor cabang. Seiring dengan perkembangan zaman dan teknologi yang meningkatkan kebutuhan nasabah, layanan perbankan terus berevolusi dan berinovasi mulai dari instrumen keuangan berupa cek, *bank notes*, kartu debit/kredit, kemudian penggunaan teknologi melalui penyediaan mesin Anjungan Tunai Mandiri (ATM), *online banking*, *mobile banking*, *digital wallet*, maupun *social media banking* untuk meningkatkan *engagement* dengan nasabah terutama yang termasuk dalam generasi milenial, hingga akhirnya sampai pada revolusi teknologi yang lebih masif untuk menciptakan layanan perbankan yang berorientasi pada kebutuhan dan ekspektasi nasabah dengan penggunaan *emerging technology* seperti *Biometrics*, *Cloud Computing*, *Artificial Intelligence*, *Machine Learning*, *Internet of Things*, dan *Augmented Reality*. Di masa depan, peluang berkembangnya jenis layanan perbankan yang baru cukup besar, mengingat tuntutan kepada perbankan untuk lebih berorientasi dan menyesuaikan produk dan layanannya dengan kebutuhan nasabah (layanan perbankan berorientasi nasabah yang dapat dipersonalisasi), dengan memanfaatkan *emerging technology*.

**Gambar 3** Transformasi Layanan Perbankan



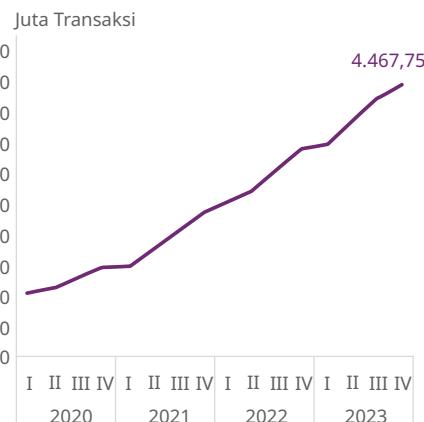
Secara statistik, tren transaksi digital di masyarakat mengalami peningkatan dari tahun ke tahun. Transaksi digital perbankan, yaitu transaksi yang dilakukan melalui *electronic channel* seperti *internet banking*, *mobile/SMS banking* dan *phone banking*, terus menunjukkan pertumbuhan yang positif. Pada Triwulan IV 2023, nilai transaksi digital perbankan mencapai Rp 15.871,04 triliun, dengan volume transaksi mencapai 4.467,75 juta transaksi. Sejalan dengan hal tersebut, transaksi belanja uang elektronik juga mencatatkan pertumbuhan yang positif. Pada Triwulan IV 2023, nilai transaksi belanja uang elektronik mencapai Rp126,35 triliun, dengan volume transaksi mencapai 2.134,21 juta transaksi.

**Grafik 1** Nilai Transaksi Melalui *Electronic Channel Bank*



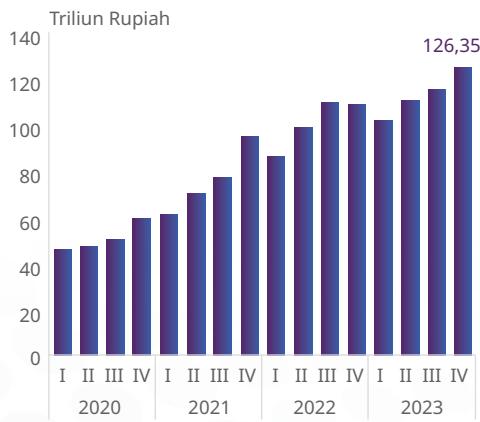
Sumber : Bank Indonesia (2024)

**Grafik 2** Volume Transaksi Melalui *Electronic Channel Bank*



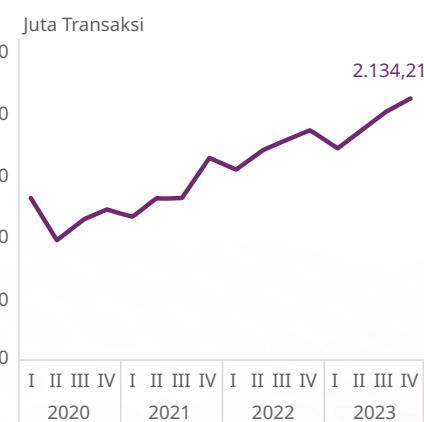
Sumber : Bank Indonesia (2024)

**Grafik 3** Nilai Transaksi Belanja Uang Elektronik



Sumber : Bank Indonesia (2024)

**Grafik 4** Volume Transaksi Belanja Uang Elektronik

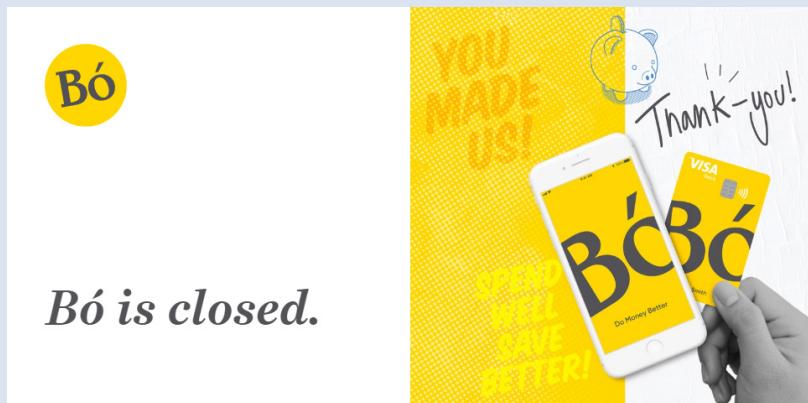


Sumber : Bank Indonesia (2024)

Pesatnya pertumbuhan digitalisasi di Indonesia mendorong bank-bank untuk melakukan transformasi pada model bisnisnya menjadi model bisnis Bank Digital. Beberapa bank melakukan akuisisi bank-bank dengan skala lebih kecil untuk dilakukan transformasi menjadi Bank dengan model bisnis *fully digital* dan melakukan kemitraan dengan berbagai industri seperti telekomunikasi dan *e-commerce* yang dapat mendukung ekosistem layanan keuangan digital perbankan. Model bisnis digital merupakan model bisnis yang sangat dinamis dengan persaingan yang tinggi sehingga Bank dengan model bisnis ini perlu memiliki resiliensi dari sisi operasional Bank dan keandalan teknologi informasi untuk menopang layanan bisnis digital yang membutuhkan kecepatan, ketepatan, dan fleksibilitas yang tinggi. Namun demikian, ketahanan operasional saja tidak akan cukup bagi bank untuk bertahan dan berkembang dalam beberapa dekade mendatang. Inovasi teknologi dalam beberapa waktu ke depan diprediksi akan semakin masif. Perubahan ini akan mengubah ekspektasi nasabah dalam menikmati produk dan layanan keuangan. Di samping itu, Bank juga akan menghadapi pesaing baru seperti perusahaan-perusahaan *financial technology* yang menawarkan berbagai inovasi produk dengan dukungan teknologi canggih.

Transformasi digital yang dilakukan oleh perbankan perlu dilakukan secara menyeluruh dengan strategi yang matang. Kedepan, tuntutan nasabah akan kenyamanan mengharuskan bank untuk memiliki model layanan teknologi tercanggih secara global. Mengadopsi teknologi canggih untuk meningkatkan proses internal saja tidaklah cukup, Bank perlu melakukan inovasi yang berorientasi nasabah dalam rangka memenuhi kebutuhan nasabah yang semakin familiar dengan teknologi canggih di tengah lingkungan bisnis yang semakin kompetitif. Apabila transformasi digital yang dilakukan tidak direncanakan dan dieksekusi dengan matang, Bank akan menghadapi risiko kehilangan pelanggan dengan cepat dan pada akhirnya Bank tidak mampu bersaing dengan kompetitor lainnya. Hal ini dapat dilihat dari kasus Bó Bank, salah satu bank digital di UK yang tutup hanya setelah beroperasi selama 6 (enam) bulan dari rilisnya yakni pada tahun 2019.





Sumber : <https://wearebo.co.uk/>

Kegagalan Bó Bank ini dipengaruhi oleh beberapa faktor dan kesalahan dalam strategi bisnisnya, seperti :

- Tidak memiliki *unique selling point* dan keunggulan kompetitif, produk dan layanan yang ditawarkan oleh Bó sama dengan produk yang telah dijalankan oleh digital bank lainnya, seperti Monzo dan Starling sejak 4 (empat) s.d. 5 (lima) tahun silam.
- *Customer engagement* yang rendah, selama 6 (enam) bulan beroperasi Bó hanya berhasil menarik 11.000 pelanggan yang bisa jadi disebabkan oleh diferensiasi produk yang ditawarkan minim.
- Aplikasi Bó memiliki banyak kelemahan sehingga 3 (tiga) bulan pertama pasca peluncuran hanya digunakan untuk memperbaiki *bugs* saja dalam aplikasi Bank. Kekurangan ini juga ditunjukkan dengan *rating* aplikasi Bó hanya sebesar 3,2 dari 5, jauh di bawah induknya the Royal Bank of Scotland (RBS) (4,7 dari 5).
- Sumber daya manusia yang digunakan dalam pengembangan Bó sebagai digital bank hanya bergantung pada 1 (satu) orang, sehingga Bank ini mengalami kejatuhan ketika CEO Mark Baille mundur akibat konflik internal dengan RBS. Diketahui bahwa Baille merupakan sosok yang memiliki kapasitas *digital leader* yang mumpuni, dan merupakan pihak dibalik berdirinya Bó Bank sendiri.

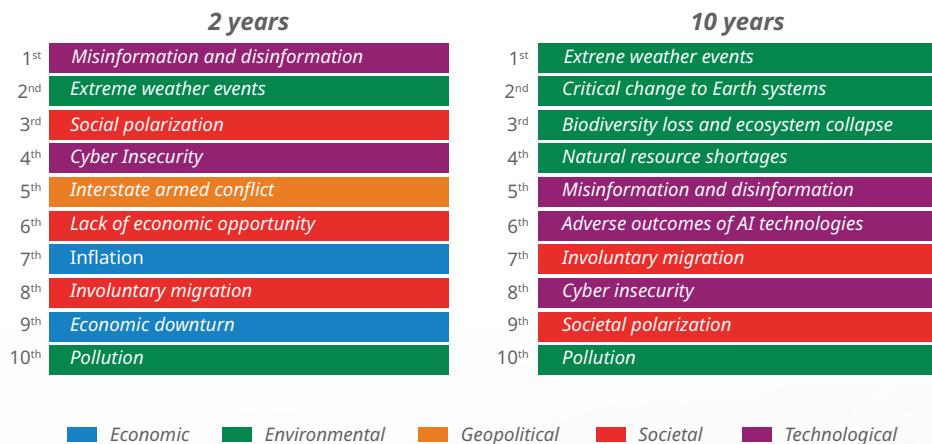
# 5

## Tantangan yang Akan Datang

Transformasi digital mengakselerasi ketergantungan digital pada aktivitas ekonomi dan sosial yang kritis, dan akan terus berjalan demikian ke depan. Pada saat yang bersamaan, ancaman keamanan digital juga semakin meningkat baik dalam hal jumlah maupun jenis dan ‘kecanggihan’ jenis serangannya. Seiring dengan transformasi digital yang harus dilakukan oleh perbankan, terdapat pula risiko dan tantangan yang mengikuti, mulai dari risiko kebocoran data, risiko strategis (dhi. investasi teknologi), kecukupan SDM, risiko operasional dan *emerging risks*, rendahnya literasi keuangan dan digital, infrastruktur, hingga risiko inheren dalam hal penerapan IT, yaitu serangan siber.

Menurut *World Economic Forum* (WEF) Global Risk Report 2024, kerentanan siber diproyeksikan akan menjadi salah satu risiko global tertinggi dalam periode 2 (dua) dan 10 (sepuluh) tahun yang akan datang. Lebih lanjut, serangan siber termasuk sebagai 3 (tiga) perhatian utama dalam era digital saat ini, baik dalam sektor pemerintah maupun privat. Kerentanan siber muncul akibat integrasi yang cepat dari teknologi maju (*advanced technologies*) di negara-negara maju dan para pelaku kejahatan siber pun akan terus menyesuaikan dan mengembangkan modus, pola, dan jenis serangan mereka sesuai dengan model bisnis yang ditargetkan.

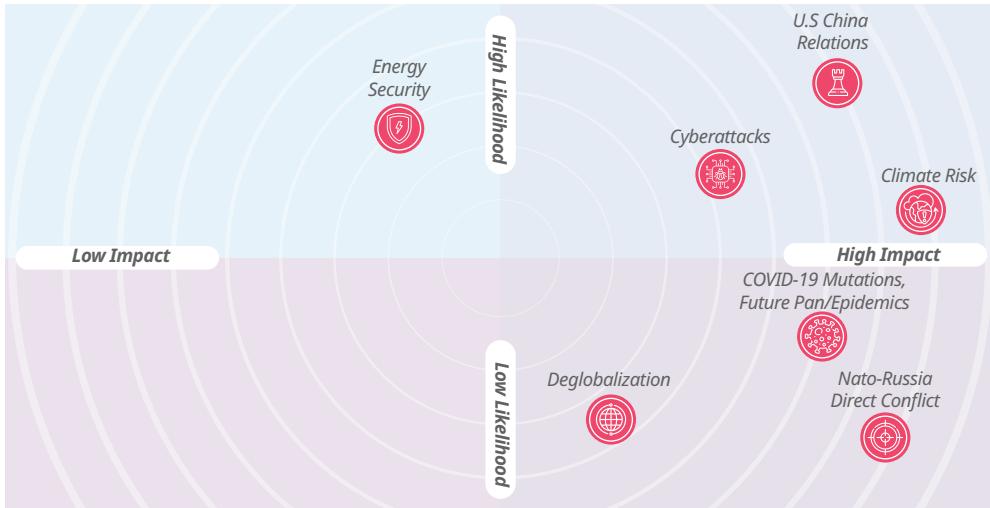
Gambar 4 Sepuluh Risiko Global Terbesar dalam 2 hingga 10 tahun ke depan



Sumber : WEF (2024)

Hal yang sama juga disampaikan oleh S&P Global (2023), yang menguraikan bahwa serangan siber merupakan urutan ke-2 (dua) sebagai risiko geopolitik dengan tingkat kemungkinan terjadi (*likelihood*) paling tinggi serta memiliki dampak yang paling signifikan secara keseluruhan, mengingat frekuensi kejadian yang kian meningkat, semakin besar, rumit, dan tanpa henti, serta merupakan ancaman bagi organisasi tertentu maupun keamanan nasional.

Gambar 5 Kemungkinan dan Dampak Risiko Geopolitik Teratas 2023



Sumber : S&P Global (2023)

Pada tahun 2022 lalu, Indonesia menempati posisi 3 (tiga) besar dunia terkait akun pembobol data terbanyak mencapai 13,2 juta pengguna internet dengan tren anomali trafik/serangan siber yang cenderung mengalami peningkatan pada rentang tahun 2019 sampai 2020, serta meningkat hingga lebih dari 3 kali lipat di tahun 2021. Meskipun tahun berikutnya menunjukkan tren anomali trafik yang relatif menurun, namun potensi ancaman siber tetap ada serta semakin *advanced* dan bervariasi.

Gambar 6 Tren Peristiwa Serangan Siber di Indonesia

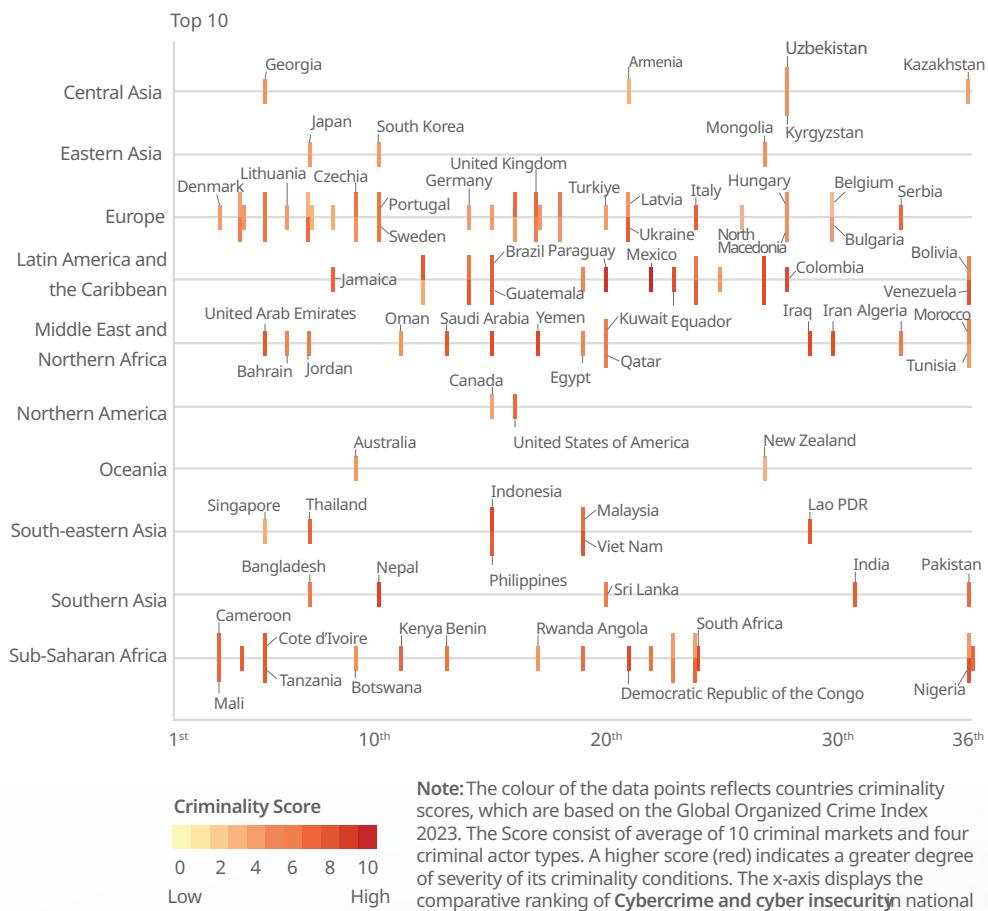


Sumber: Lanskap Keamanan Siber Indonesia & Laporan Bulanan Monitoring Keamanan Siber BSSN, diolah.

Lebih lanjut, di tahun yang sama sektor keuangan menempati peringkat kedua sebagai sasaran utama serangan siber, setelah pada tahun 2020 menduduki posisi pertama. Meskipun menduduki peringkat kedua, secara umum gangguan dan kerugian akibat serangan siber di sektor keuangan masih menduduki peringkat teratas posisi tertinggi.

Adapun *World Economic Forum (WEF) Executive Opinion Survey 2023*, menunjukkan bahwa Indonesia berada dalam daftar 15 negara teratas yang terancam risiko kejahatan siber dan kerentanan siber dengan tingkat kriminalitas berada di skor 7 (tujuh) yaitu kategori *Moderate to High*.

**Gambar 7** National Risk Perception, by Region: Cybercrime and Cyber Insecurity



Sumber : WEF (2024)

Meskipun demikian, perlu dipahami bahwa resiliensi digital sebuah bank tidak hanya membutuhkan peran bank sebagai penyelenggara layanan, namun juga peran nasabah selaku pengguna layanan. Dari sisi konsumen, peningkatan penipuan siber (*cyber fraud*) seperti kasus pembobolan rekening nasabah yang dilakukan melalui rekayasa sosial (*social engineering*) juga kian meningkat. Pembobolan rekening dilakukan dengan modus yang sangat beragam dan terkesan ‘nyata’, antara lain berkedok sebagai undangan pernikahan palsu berbentuk file APK, pemasangan iklan palsu di media sosial, *link* modus perubahan tarif, hingga file foto berbentuk APK fiktif, serta masih banyak lagi modus lainnya yang juga terus berkembang.

Hal-hal tersebut menunjukkan bahwa peristiwa dimaksud disebabkan oleh masih kurang dalamnya pemahaman dan kesadaran konsumen terhadap potensi dan risiko baru yang kini hadir seiring dengan perkembangan digital saat ini. *National Literacy Index* posisi tahun 2022 berada di angka 49,68%, dengan Indeks Literasi Digital berada di kategori Sedang dengan nilai 3,54 dari skala 1 – 5. Melihat hal tersebut, dapat diketahui bahwa terdapat *gap* yang cukup besar antara indeks literasi keuangan dan indeks inklusi keuangan Indonesia yang berada di persentase 85,10% posisi tahun 2022. Terdapat beberapa tantangan yang dihadapi dalam peningkatan literasi keuangan masyarakat Indonesia, beberapa di antaranya ialah sebagai berikut:

- a. Terdapat 21 (dua puluh satu) provinsi dengan indeks literasi yang di bawah indeks literasi Nasional;
- b. Infrastruktur (akses internet yang belum merata di seluruh daerah di Indonesia);
- c. Kondisi geografis Indonesia yang berbentuk kepulauan;
- d. *Gap* dalam hal tingkat Pendidikan dan perekonomian masing-masing wilayah di Indonesia; serta
- e. *Gap* indeks literasi keuangan di wilayah pedesaan dan perkotaan.



Selain itu, aspek literasi digital masyarakat juga memiliki andil yang cukup besar dalam fenomena ini. Diketahui bahwa Literasi Digital Indonesia pada tahun ini mengalami peningkatan sebesar 0,5 poin dari tahun 2021. Terdapat 3 (tiga) pilar yang mengalami peningkatan, antara lain Pilar 1 - *Digital Skill* (0,08 poin), Pilar 2 - *Digital Ethics* (0,15 poin), dan Pilar 3 - *Digital Safety* (0,02 poin) dengan Pilar 4 - *Digital Culture* mengalami penurunan sebesar 0,06 poin.

Perlu disadari bahwa literasi keuangan digital sangat diperlukan agar konsumen dapat menggunakan produk dan layanan keuangan digital dengan aman dan dapat menghasilkan keputusan keuangan yang berkualitas baik berupa pengetahuan, keterampilan, keyakinan, maupun kompetensi. Literasi Keuangan Digital penting mengingat kedepannya digitalisasi akan semakin berkembang dan terus terjadi, khususnya pada sektor keuangan, dan faktor keamanan merupakan isu penting dalam melakukan transaksi keuangan digital dimaksud. Selain itu, dengan dimilikinya literasi keuangan digital yang memadai, akan memudahkan seseorang dalam mengakses produk dan layanan jasa keuangan serta akan berdampak pada efisiensi dan efektivitas transaksi keuangan seseorang karena menjadi lebih mudah dan praktis.



# RESILIENSI DIGITAL





# 1 Definisi

*Resilience* atau ketahanan dapat didefinisikan sebagai suatu proses untuk memanfaatkan sumber daya yang dimiliki guna mempertahankan kontinuitas bisnis, dimana penerapan konsep ini ialah dalam hal teknologi dan internet pada era digital saat ini. Lebih lanjut, Deloitte (2023) menjelaskan bahwa Resiliensi Digital adalah elemen kunci dari kemampuan organisasi untuk bersiap terhadap gangguan dan beradaptasi terhadap perubahan, yang berfokus untuk mengatasi kejadian atau insiden siber.

Selain itu, *Digital Europe* (2023) melihat *digital resilience* sebagai sebuah kemampuan dalam menggunakan teknologi digital untuk mencegah dan menghadapi krisis seperti pandemi, bencana alam, serangan siber, dengan tetap dapat mempertahankan aset keuangan dan keamanan yang dimiliki. Sementara *European Union* (EU) melalui peraturannya Regulation 6 2022/2554, memberikan konteks lebih khusus kepada aspek operasionalnya, bahwa digital operational resilience didefinisikan sebagai kemampuan suatu entitas keuangan untuk membangun, menjamin, dan meninjau integritas dan keandalan operasionalnya termasuk apabila terjadi disrupsi.

Lebih lanjut, *European Committee of the Regions* (2023) mendefinisikan *digital resilience* bagi otoritas setempat dan kawasan (*local and regional authorities*) sebagai kemampuan untuk *resist*, *absorb*, dan *recover* dari gangguan yang disebabkan oleh ancaman digital eksternal atau bencana alam melalui penegakan peraturan terkait keamanan dan ketahanan siber, ketersediaan sumber daya kritis yang mumpuni, serta penggunaan keterampilan digital dan keamanan siber yang sesuai.



## 2

## Digital Resilience vs Cyber Security

Dalam konteks digitalisasi, ketahanan dan keamanan siber (*cyber security*) merupakan hal yang umum dipahami oleh pelaku bisnis. Namun demikian resiliensi digital (*digital resilience*) memiliki lingkup yang lebih luas dari keamanan siber karena terkait dengan kemampuan suatu organisasi/bisnis untuk dapat bertahan dan tumbuh di tengah lingkungan yang berubah secara dinamis dan bergantung pada teknologi (CSO Online, 2018).

Ketahanan dan keamanan siber berfokus pada kemampuan organisasi untuk bertahan dan pulih dari serangan siber, mencakup kemampuan organisasi untuk mengidentifikasi, melindungi, mendeteksi, menanggapi, dan memulihkan diri dari serangan yang terjadi pada infrastruktur TI yang dimiliki. Sementara itu, resiliensi digital berfokus pada kemampuan organisasi secara keseluruhan untuk beradaptasi terhadap lingkungan digital (*digital environment*) dengan cepat, termasuk keamanan siber, pergeseran ekspektasi konsumen, perubahan regulasi, kemajuan teknologi, termasuk memiliki fleksibilitas dan *agility* untuk merespon perubahan dan menemukan peluang baru untuk dapat mempertahankan bisnis.

## 3

## Aspek Resiliensi Digital

Secara umum, aspek dari resiliensi digital terbagi dalam 2 (dua) kategori, yaitu resiliensi terhadap dinamika bisnis dan resiliensi terhadap disrupsi atau gangguan.

Resiliensi terhadap dinamika bisnis merupakan kemampuan bank untuk bertahan dalam dinamika bisnis era digital sehingga bisnis bank dapat tetap relevan di pasar. Beberapa aspek yang masuk dalam kategori ini yaitu, kecepatan dalam mengadopsi teknologi terkini (*Technology Adoption*), kemampuan organisasi bank untuk beradaptasi dan bertransformasi sesuai dengan kondisi terkini (*Organizational Change*), dan pengembangan keunggulan kompetitif yang mampu meningkatkan daya saing bank terhadap kompetitor di bisnis serupa (*Business Competitiveness*).

Sementara itu, resiliensi terhadap disrupsi atau gangguan adalah kemampuan bank untuk bertahan dari faktor eksternal maupun internal yang menyebabkan gangguan pada operasional bank, seperti serangan siber. Beberapa aspek yang masuk dalam kategori ini yaitu, manajemen risiko, ketahanan operasional, dan manajemen kontinuitas bisnis (*Business Continuity Management*).

Gambar 8 Aspek Digital Resilience



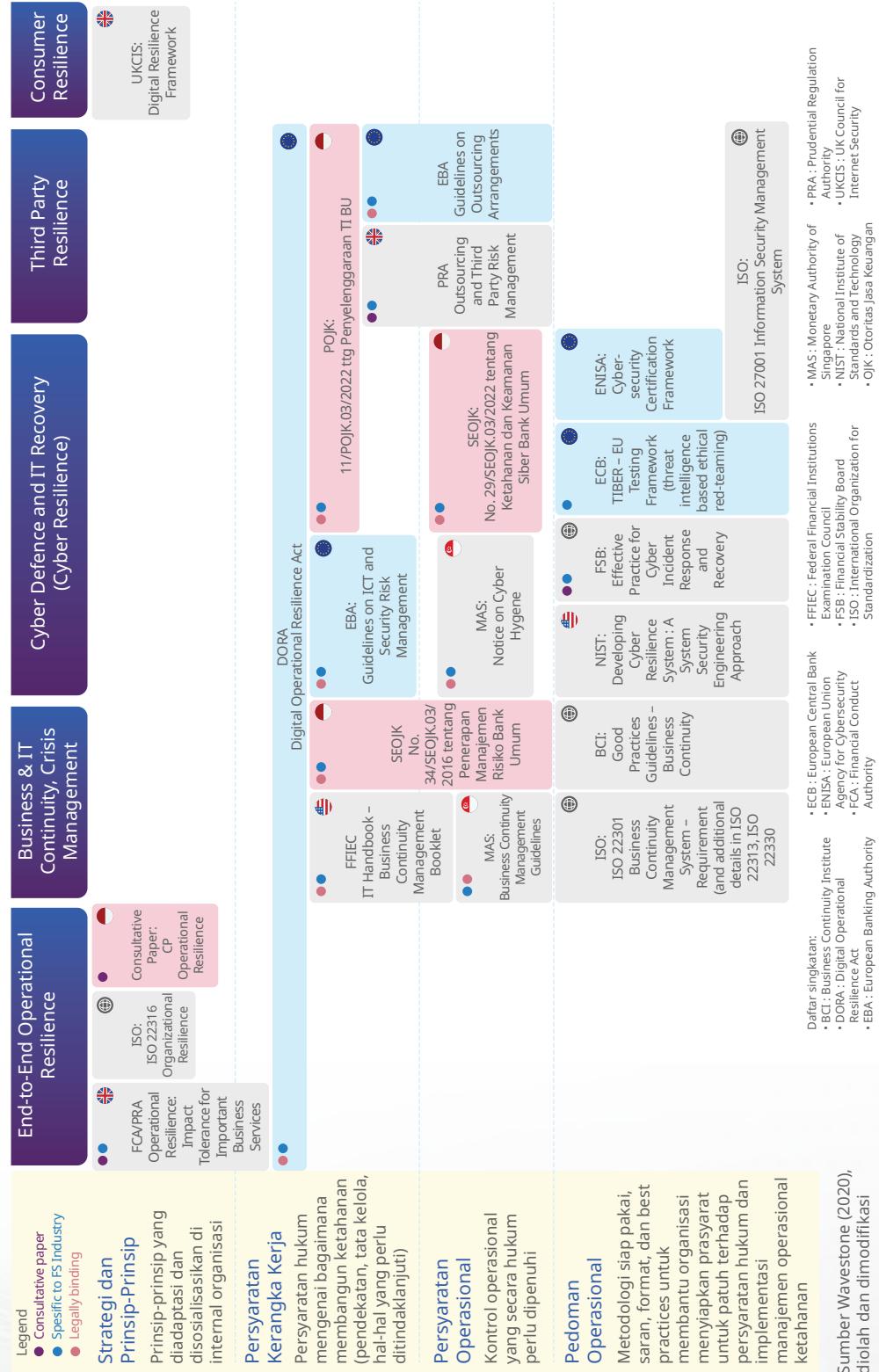
Sumber : Garside, D (2018)

## 4 Kebijakan dan Regulasi terkait Resiliensi

Kebijakan dan regulasi terkait resiliensi dapat terbagi menjadi beberapa topik, antara lain *end-to-end operational resilience*, *business & IT continuity* dan *crisis management*, *cyber defence and IT recovery*, *third party resilience*, dan *consumer resilience*. Selanjutnya, berdasarkan sifatnya, kebijakan dan regulasi dimaksud juga terbagi menjadi 4 (empat), yaitu:

- a. Strategi dan Prinsip, yaitu prinsip yang diadaptasi dan disosialisasikan di internal organisasi.
- b. Persyaratan Kerangka Kerja, yaitu persyaratan hukum mengenai cara untuk membangun resiliensi (pendekatan yang digunakan, tata kelola, serta hal yang perlu ditindaklanjuti).
- c. Persyaratan Operasional, yaitu kontrol operasional yang secara hukum perlu dipenuhi.
- d. Pedoman Operasional, metodologi siap pakai, saran, format, dan *best practices* untuk membantu organisasi menyiapkan prasyarat untuk patuh terhadap persyaratan hukum dan implementasi manajemen operasional ketahanan.

**Gambar 9** Kebijakan dan Regulasi terkait Resiliensi



# KERANGKA RESILIENSI DIGITAL



Dalam rangka menerapkan resiliensi digital, Bank dapat mengacu pada Kerangka Resiliensi Digital (*Digital Resilience Framework*). Kerangka tersebut terdiri atas 3 (tiga) aspek utama, yaitu resiliensi terhadap dinamika bisnis, resiliensi bank terhadap gangguan atau disrupti, dan resiliensi nasabah di era digital.



- Resiliensi bank dari dinamika bisnis era digital sehingga bank tetap relevan di market
- Menjaga *Digital Competitiveness* melalui:
  1. *Technology Adoption*,
  2. *People & Organization*, dan
  3. *Customer-centric Product Development*

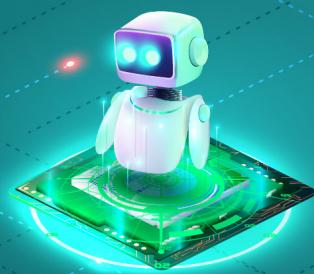
- Resiliensi bank dari disrupti atau gangguan terhadap bank, contoh: serangan siber.
- Hal ini terbagi menjadi 3 kapabilitas, yaitu *Anticipate*, *Withstand & Recover*, dan *Sustain*

- Upaya bank dalam menjaga resiliensi nasabah dari disrupti atau gangguan terhadap produk bank, contoh: *phising*, *scam*.
- Terdiri atas 3 proses, yaitu:
  - a. *Customer Incident Management*,
  - b. *Customer Incident Recovery*, dan
  - c. *Customer Post-Recovery Services*



01

## RESILIENSI TERHADAP DINAMIKA BISNIS



*Technology Adoption*



*People & Organization*



*Customer-centric  
Product Development*

# 1

## Resiliensi Terhadap Dinamika Bisnis (*Digital Competitiveness*)

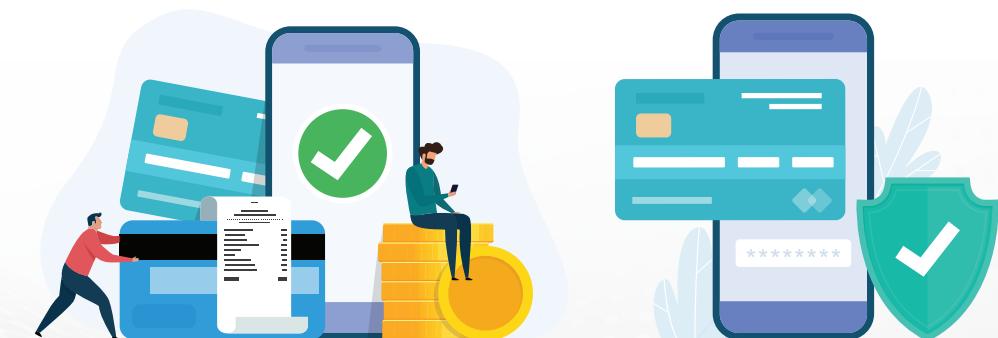
Resiliensi terhadap dinamika bisnis merupakan kemampuan bank untuk bertahan dalam dinamika bisnis era digital sehingga bisnis bank tetap relevan di pasar. Hal tersebut dapat dicapai dengan menjaga daya saing digital (*digital competitiveness*) bank yang meliputi 3 (tiga) hal, yaitu adopsi teknologi, sumber daya manusia dan organisasi di era digital, dan pengembangan produk yang berorientasi konsumen.

### A. Adopsi Teknologi (*Technology Adoption*)

Teknologi merupakan *enabler* yang krusial dalam mendukung transformasi digital bank. Dalam konteks resiliensi digital, pilihan teknologi bank merupakan faktor yang mempengaruhi daya saing bisnis bank karena akan menentukan produk dan layanan apa yang dapat diberikan oleh bank, serta ekosistem yang dapat dimasuki oleh bank.

Untuk mempertahankan daya saing di era digitalisasi bank didorong untuk terus melakukan inovasi atas produk dan layanan baik secara mandiri ataupun melalui kolaborasi dengan pihak lain. Teknologi yang dimiliki oleh bank dapat menjadi penguat atau malah menjadi penghambat dalam proses kolaborasi. Oleh karena itu, adopsi teknologi baru harus dilakukan secara terukur, sehingga manfaat yang diperoleh setara dengan biaya yang dikeluarkan oleh Bank.

Sejalan dengan hal tersebut, diperlukan langkah sistematis dalam mengadopsi teknologi baru bagi suatu bank sehingga proses adopsi teknologi dapat berjalan lancar dengan mempertimbangkan potensi risiko yang terkait.



**1. Faktor Pertimbangan dalam Adopsi Teknologi**

Dalam adopsi teknologi, terdapat beberapa faktor yang perlu menjadi pertimbangan. Secara umum, faktor dimaksud dapat dibagi menjadi 4 (empat) klaster yaitu: pembiayaan dan sumber daya pendukung, keahlian dan pengetahuan, budaya organisasi, dan regulasi.

**Gambar 10** Faktor Pertimbangan dalam Adopsi Teknologi



Sumber : Digital Government Authority of Saudi Arabia (2023)

**1.1. Klaster Pembiayaan dan Sumber Daya Pendukung**

Klaster ini menekankan pada kebutuhan untuk mempertimbangkan dan memastikan ketersediaan dukungan fungsional dan teknis terhadap kesuksesan dan efektivitas dari suatu teknologi. Klaster ini berfokus pada faktor yang dapat berpotensi menghambat kelayakan penerapan teknologi yang diinginkan dari sisi teknis dan fungsional.

Beberapa faktor dalam klaster ini meliputi:

- Alokasi investasi, biaya operasional, dan anggaran;
- Ketersediaan infrastruktur teknologi yang diperlukan;
- Ketersediaan *framework* dan *tools* untuk memaksimalkan efektivitas penggunaan teknologi; dan
- Ketersediaan metode pengukuran untuk melakukan *cost & benefit analysis*.

**1.2. Klaster Keahlian dan Pengetahuan**

Adopsi teknologi, khususnya *emerging technology* seperti *artificial intelligence*, *blockchain*, dsb., agar dapat dilakukan secara efektif memerlukan keahlian dan pengetahuan yang memadai untuk memitigasi kemungkinan dan dampak dari potensi penyalahgunaan, risiko, dan konsekuensi yang tidak diharapkan. Faktor pada klaster ini pada dasarnya memastikan pemanfaatan yang tepat dari teknologi sehingga bank dapat memanfaatkan kemampuan dan memaksimalkan potensi dari teknologi tersebut.

Beberapa faktor dalam klaster ini meliputi:

- a. Keterampilan yang diperlukan untuk memastikan kesuksesan adopsi teknologi.
- b. Pemahaman (*familiarity*) dan kompetensi atas teknologi yang diadopsi untuk memastikan pengoperasian dan penanganan yang efektif.
- c. Ketersediaan program peningkatan *awareness* dan pelatihan kepada pegawai untuk memastikan pegawai memahami tren pasar dan perkembangan teknologi.

**1.3. Klaster Budaya Organisasi**

Budaya organisasi tercermin pada nilai, norma, dan perilaku pegawai. Budaya untuk terus berinovasi merupakan salah satu pilar yang mendukung kesuksesan proses adopsi teknologi karena hal tersebut membantu pegawai dalam upaya adopsi teknologi dan meningkatkan kemampuan organisasi dalam berinovasi.



Beberapa faktor dalam klaster ini meliputi:

- a. Karakter pegawai yang mampu bersikap dan berpendapat terhadap adopsi teknologi;
- b. Penerapan proses dan alur kerja digital untuk menumbuhkan pola pikir *agile* yang meningkatkan efisiensi;
- c. Kesediaan pegawai untuk menginvestasikan waktu dan upaya untuk menerima perubahan dan memanfaatkan teknologi baru yang memerlukan serangkaian praktik baru; dan
- d. Kesesuaian budaya dari teknologi untuk memastikan bahwa teknologi tersebut selaras dengan norma dan praktik yang dianut.

#### **1.4. Klaster Regulasi**

Penggunaan teknologi tidak terlepas dari ketentuan peraturan perundang-undangan yang melingkupinya. Dengan demikian, penggunaan teknologi juga memiliki risiko hukum bagi bank. Hal ini perlu menjadi perhatian Bank sebelum bank memutuskan untuk menggunakan teknologi tertentu. Beberapa faktor dalam klaster ini meliputi:

- a. Kesesuaian dengan ketentuan peraturan perundang-undangan yang terkait, baik di tingkat nasional maupun internasional.
- b. Tata kelola dan kepemilikan (*ownership*) dari teknologi, mengingat dampaknya secara langsung terhadap kemampuan bank untuk mengelola risiko dan memperoleh manfaat dari penggunaan teknologi.
- c. Tantangan keamanan data pribadi yang mungkin muncul dari pemanfaatan teknologi.



## 2. Kerangka Adopsi Teknologi (*Technology Adoption Framework*)

Dengan mempertimbangkan faktor-faktor yang mempengaruhi penggunaan teknologi, proses adopsi teknologi perlu mengikuti pendekatan sistematis untuk mendukung kelancaran adopsi teknologi dengan tetap memperhatikan potensi risiko yang terkait. Oleh karena itu, diperlukan suatu kerangka yang dapat menjadi acuan bagi Bank dalam mengadopsi suatu teknologi, khususnya *emerging technology* yang belum secara umum diimplementasikan di sektor perbankan.

Kerangka adopsi teknologi terdiri atas 5 (lima) tahapan, yaitu penelitian, penilaian, analisis, pembuktian, dan implementasi & perluasan.

**Gambar 11** Tahapan dalam Adopsi Teknologi



Sumber: Digital Government Authority of Saudi Arabia (2023)

## 2.1. Tahap Penelitian



Adopsi teknologi diawali dengan penyusunan rumusan masalah yang menjadi landasan utama penggunaan suatu teknologi. Ketika rumusan masalah telah disusun, proses yang perlu dilakukan adalah melakukan kajian terkait solusi atau produk yang diperlukan dan bagaimana bank dapat mengintegrasikannya dengan proses dan alur kerja yang telah ada. Pada tahap ini, penting bagi bank untuk memahami budaya organisasi dan mempertimbangkan berbagai upaya yang sesuai untuk mencegah kegagalan adopsi teknologi. Dengan demikian, penelitian bank diharapkan lebih mengutamakan pada cara agar suatu teknologi dapat memberikan solusi atas permasalahan serta spesifikasi dan karakteristik yang harus dimiliki oleh suatu teknologi agar dapat memberikan nilai tambah, dibandingkan memfokuskan penelitian hanya pada teknologi itu sendiri.

Hal-hal yang dilakukan:

- a. Meninjau penggunaan teknologi tertentu melalui studi kasus yang relevan.
- b. Melakukan studi literatur terkait teknologi tertentu.
- c. Mengkaji tren penggunaan teknologi tertentu (*market research*) untuk dapat mengukur kesuksesan dan kesesuaian dari teknologi tersebut.

Tahapan penelitian ini akan membantu bank dalam menyusun daftar pilihan teknologi yang dapat dipertimbangkan lebih lanjut sesuai rumusan masalah yang telah ditetapkan di awal.



## 2.2. Tahap Penilaian



Pada tahap ini, bank melakukan validasi terhadap teknologi yang telah diidentifikasi pada tahap penelitian untuk memastikan kesesuaianya dengan rumusan masalah dan batasan yang teridentifikasi, serta mengidentifikasi faktor eksternal yang berpengaruh terhadap penerapan teknologi dimaksud. Selain itu, bank juga perlu melakukan evaluasi terhadap fungsi yang bertanggung jawab atas inovasi pada bank untuk memastikan fungsi tersebut memiliki kompetensi yang sesuai untuk mencapai tujuan bisnis, memantau pasar dan tren teknologi, serta mengelola proyek yang terkait dengan adopsi teknologi.

Hal yang dilakukan:

- a. Memastikan kesesuaian teknologi dengan rumusan masalah yang ditetapkan.
- b. Mengidentifikasi batasan yang dimiliki oleh bank, seperti kesiapan organisasi dan ketersediaan perangkat atau infrastruktur pendukung.
- c. Mengidentifikasi ketentuan peraturan perundang-undangan yang relevan dengan implementasi teknologi tersebut.
- d. Mempertimbangkan dampak terhadap penerimaan pengguna (termasuk nasabah) atas penerapan teknologi dimaksud.
- e. Melibatkan pihak terkait yang secara proaktif terlibat dalam proses perencanaan dan pengambilan keputusan terkait dengan adopsi teknologi.



Setelah tahapan penilaian ini dilaksanakan, bank akan memiliki:

- a. Pemahaman yang komprehensif atas kesesuaian teknologi termasuk persepsi pengguna terhadap penerapan teknologi dimaksud.
- b. Tanggapan dan masukan yang dapat menjadi komponen utama dalam pengembangan berkelanjutan.
- c. Pandangan menyeluruh terhadap kinerja teknologi dengan mempertimbangkan metrik dan indikator yang telah diidentifikasi, sekaligus memastikan ketersediaan data yang dibutuhkan untuk tahapan berikutnya.

### **2.3. Tahap Analisis**



Pada tahap ini, bank melakukan analisis terhadap faktor-faktor yang terkait dengan penerapan teknologi, antara lain kelayakan teknis dan finansial, serta kepatuhan terhadap ketentuan peraturan perundang-undangan yang berlaku. Tujuan utama dari tahap ini adalah untuk memberikan justifikasi yang memadai dalam mengadopsi suatu teknologi serta memitigasi kemungkinan dan dampak dari risiko yang belum terukur.

Hal yang dilakukan:

Mengevaluasi kesesuaian dari pilihan teknologi terhadap persyaratan dan kriteria yang ditentukan sebelumnya. Beberapa faktor yang perlu dipertimbangkan adalah sebagai berikut:

- a. Persyaratan Fungsional, yang meliputi:
  1. Analisis terhadap persyaratan utama atas *use case* tertentu dan indikator terukur yang menentukan kesuksesan *use case* tersebut.
  2. Validasi pemenuhan persyaratan oleh pilihan teknologi, hasilnya dapat berupa "memenuhi", "memenuhi secara terbatas", dan "tidak memenuhi".
  3. Analisis kesesuaian dan penyelarasan pilihan teknologi dengan arsitektur teknologi bank saat ini maupun rencana ke depan.

- b. Persyaratan Non-fungsional, yang meliputi hal seperti keamanan, keandalan, performa, pemeliharaan, skalabilitas, dan kemudahan penggunaan. Faktor tersebut merupakan hal yang penting untuk dipertimbangkan karena berpengaruh terhadap proses adopsi dan efektivitas teknologi. Persyaratan ini bukan bagian dari kapabilitas utama, namun sangat dibutuhkan dalam implementasi teknologi.

Setelah tahapan analisis ini dilaksanakan, bank akan memiliki:

- a. Pilihan teknologi yang akan dilakukan pengujian lebih lanjut; dan
- b. Dokumentasi dari seluruh faktor yang telah dianalisis yang menjadi dasar bagi bank dalam menentukan pilihan teknologi sesuai dengan kebutuhan dan cara untuk mengintegrasikannya dengan tepat.



## 2.4. Tahap Pembuktian



Pada tahap ini, bank melakukan serangkaian pengujian terhadap teknologi yang sudah dipilih. Tahap ini terbagi menjadi 2 (dua) langkah utama, yaitu *proof-of-concept* (POC) dan *prototype*. POC menguji kelayakan teknis dari suatu ide/konsep dengan memanfaatkan model sederhana yang dapat berfungsi pada skala kecil. Sementara itu, *prototype* menguji kemudahan penggunaan, tampilan dan nuansa (*feel*) dari produk/solusi yang dikembangkan dengan tujuan untuk memvalidasi desain *user interface* dan *user experience* (UI/UX) serta alur pengguna (*user flow*).

Hal yang dilakukan pada tahap POC:

- a. Pendefinisian konsep, yang terdiri atas:
  1. Menentukan pihak yang akan dibutuhkan dalam pengujian (a.l. tim atau fungsi terkait) sesuai dengan *use case* yang dipilih.
  2. Menentukan tujuan, input, capaian, lingkup, dan kriteria kesuksesan.
  3. Menyusun alokasi sumber daya dan jadwal pelaksanaan POC.
- b. Formulasi hipotesis, yang terdiri atas:
  1. Mengidentifikasi fungsionalitas minimal yang sangat dibutuhkan dalam lingkup POC.
  2. Melibatkan pihak terkait untuk menganalisis ide atau konsep awal dan memprioritaskan fungsionalitas.





c. Pengujian hipotesis, yang terdiri atas:

1. Menguji solusi terhadap *use case* dan melakukan riset, termasuk diskusi dengan ahli jika diperlukan, untuk menetapkan kelayakan solusi tersebut.
2. Meninjau dan memvalidasi hasil pengujian dengan pihak terkait.
3. Membandingkan hasil pengujian terhadap kriteria kesuksesan untuk menyusun ringkasan temuan dan pelajaran terpetik (*lesson learned*).

Hal yang dilakukan pada tahap *prototype*:

a. Pengembangan *prototype* awal, yang terdiri atas:

1. Menyusun gambaran awal atas produk/solusi yang akan dikembangkan.
2. Mengonfigurasi dan menguji infrastruktur yang dibutuhkan dan menguji untuk replikasi solusi dalam lingkungan operasi terbatas (*closed operational environment*) jika diperlukan.

b. Evaluasi POC, yang terdiri atas:

1. Mempresentasikan model awal dari produk atau solusi yang dapat berfungsi kepada pihak terkait yang penting.
2. Mengumpulkan masukan dan tanggapan dari pengguna dan menggunakan untuk pengembangan selanjutnya.

- c. Perbaikan dan penyempurnaan POC, yang terdiri atas:
  1. Meninjau masukan dan tanggapan dengan mempertimbangkan kembali faktor yang berpengaruh seperti waktu dan anggaran serta kelayakan teknis dalam implementasi sesungguhnya.
  2. Menyempurnakan dan mengkinikan *prototype* hingga ekspektasi pengguna atau nasabah terpenuhi.

Setelah tahapan pembuktian ini dilaksanakan, bank akan memiliki:

- a. Informasi terkait *timeline* dan sumber daya yang diperlukan untuk pengembangan produk atau solusi dengan teknologi yang dipilih.
- b. Dokumen kebutuhan bisnis (*business requirement*).
- c. Bukti kelayakan konsep dan penerapan dalam model bisnis.
- d. Alur pengguna dalam menggunakan produk atau solusi (*user journey*).
- e. Model awal dari produk atau solusi yang dapat berfungsi.
- f. Hasil evaluasi POC.

## 2.5. **Tahap Implementasi dan Perluasan**



Tahap implementasi dan perluasan adalah tahapan terakhir yang dilakukan dalam proses adopsi teknologi. Pada tahap ini, bank mengembangkan *minimum viable product* (MVP) berdasarkan hasil POC dan *prototype*. MVP adalah sebuah versi dari produk baru yang hanya dibekali dengan fitur yang sangat terbatas namun cukup dan mampu untuk memenuhi kebutuhan utama dari pengguna/konsumen awal



sehingga terbuka untuk memperoleh masukan (*feedback*) yang bermanfaat bagi pengembangan selanjutnya dengan fitur yang lebih banyak. Dengan fitur yang terbatas dan menitikberatkan pada kebutuhan utama, pengembangan MVP memerlukan waktu dan upaya yang lebih sedikit dibandingkan pengembangan produk dengan fitur lengkap. Dengan demikian, MVP berguna untuk menguji coba produk atau solusi dan memperoleh informasi terkait kesesuaianya terhadap kebutuhan pengguna/konsumen.

Selanjutnya, setelah produk atau solusi yang memanfaatkan suatu teknologi telah diimplementasikan, bank juga perlu mempertimbangkan cara untuk meluncurkan dan memperluas penggunaannya. Bank perlu untuk mencari peluang di masa depan melalui upaya inovasi yang didorong oleh perkembangan teknologi.

Hal yang dilakukan:

- a. Penyeleksian *use case* atau POC, yang terdiri atas:
  1. Menentukan POC yang akan dipertimbangkan dalam pengembangan MVP.
  2. Menilai kembali model bisnis dan kelayakan dengan mempertimbangkan faktor seperti anggaran dan sumber daya, kepentingan strategis, dan capaian jangka pendek (*quick wins*) untuk memastikan kemampuan bank dalam mengembangkan MVP tersebut.
- b. Identifikasi *use case* dan kebutuhan penggunaan pihak ketiga, yang terdiri atas:
  1. Mengidentifikasi fungsionalitas minimal yang sangat dibutuhkan dalam lingkup POC.





2. Mendefinisikan hasil yang diharapkan dan parameter kesuksesan.
  3. Apabila menggunakan pihak ketiga, bank menyusun kriteria persyaratan pihak ketiga untuk mengidentifikasi pihak ketiga atau mitra yang tepat.
- c. Pengembangan atau kustomisasi MVP, yang terdiri atas:
1. Mengalokasikan sumber daya yang tepat untuk tujuan pengembangan atau identifikasi mitra yang sesuai.
  2. Apabila menggunakan pihak ketiga, bank menyampaikan persyaratan dan ekspektasi bank kepada pihak ketiga untuk membantu pihak ketiga menyusun penawaran. Selanjutnya, bank meninjau penawaran pihak ketiga dan memberikan keputusan.
- d. Peluncuran dan pengujian, yang terdiri atas:
1. Mengonfigurasi dan menguji infrastruktur yang dibutuhkan, serta menguji untuk replikasi solusi dalam lingkungan operasi secara terbatas (*limited operational environment*). Pada tahap ini, bank mengumpulkan data pendukung dalam menentukan kesuksesan MVP maupun aspek teknis lainnya.
  2. Apabila menggunakan pihak ketiga, bank mengundang pihak ketiga untuk meluncurkan dan mendemonstrasikan solusi dari pihak ketiga dalam lingkungan operasi yang relevan.

- e. Iterasi dan pengembangan, yang terdiri atas:
  - 1. Mempresentasikan model awal dari pengembangan produk atau solusi yang dapat berfungsi kepada pihak terkait yang penting.
  - 2. Mengumpulkan masukan dan tanggapan dari pengguna dan menggunakan untuk pengembangan selanjutnya.

Setelah tahapan ini dilaksanakan, bank akan memiliki:

- a. Pilihan mitra utama yang dapat membantu dalam pembangunan, persiapan dan konfigurasi, dan peluncuran solusi teknologi.
- b. Kemampuan untuk mengimplementasikan teknologi yang dipilih dan perluasannya ke depan untuk mengantisipasi peluang di masa depan.
- c. Hasil identifikasi area untuk pengembangan kemitraan dan dukungan dalam komersialisasi produk atau layanan yang menggunakan teknologi tertentu.

**B.  
Sumber Daya  
Manusia dan  
Organisasi  
di Era Digital  
(*People &  
Organization*)**

Sumber daya manusia merupakan penggerak utama bisnis bank. Dalam konteks resiliensi digital, diperlukan sumber daya manusia dan struktur organisasi yang mampu beradaptasi dengan perkembangan teknologi dan bisnis yang dinamis. Dengan dukungan sumber daya manusia dan struktur organisasi yang memadai, bank dapat bertahan dalam persaingan bisnis era digital melalui inovasi dan implementasi teknologi.

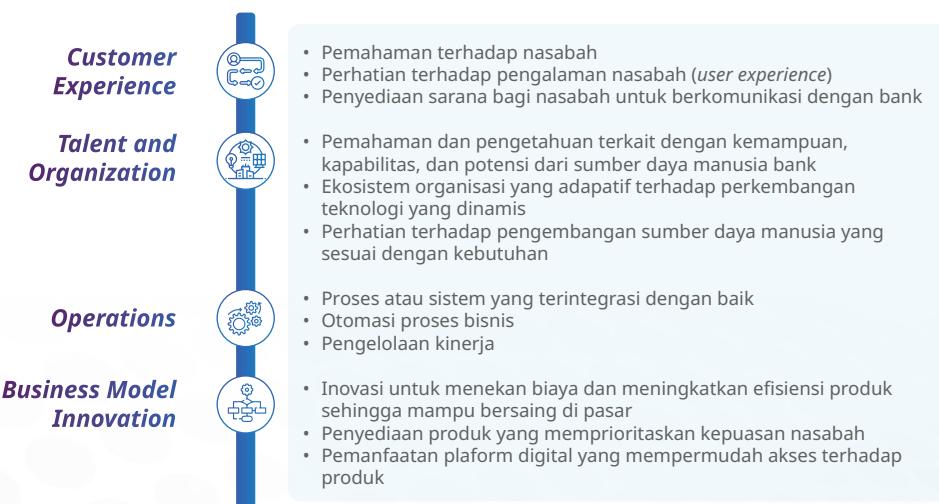


Terdapat beberapa faktor yang mendukung sumber daya manusia dan organisasi di era digital **yaitu kepemimpinan digital, budaya digital, talenta digital, serta desain organisasi**. Keempat faktor tersebut juga telah dicantumkan dalam Cetak Biru Transformasi Digital Perbankan OJK secara umum, sehingga dapat menjadi salah satu acuan dalam pengembangan organisasi dan sumber daya manusia pada bank.

**1. Kepemimpinan Digital (Digital Leadership)** Kepemimpinan digital (*digital leadership*) adalah kepemimpinan strategis yang dapat memanfaatkan aset digital perusahaan untuk mencapai tujuan organisasi. Menurut riset Capgemini (2018), *digital leadership* merupakan kombinasi dari pengembangan **kapasitas digital (digital capabilities)** dan **kapasitas kepemimpinan (leadership capabilities)**.

**1.1. Kapasitas Digital (Digital Capabilities)** Kapasitas digital meliputi kemampuan dalam penggunaan teknologi untuk mengubah proses bisnis Bank. Terdapat 4 (empat) aspek utama terkait dengan hal ini, yaitu interaksi Bank dengan konsumen (*customer experience*), pengembangan talenta dan organisasi (*talent and organization*), operasionalisasi proses internal (*operations*), serta perumusan model bisnis (*business model innovation*).

Gambar 12 | Kapasitas Digital



Sumber: Capgemini (2018)

## 1.2. Kapasitas Kepemimpinan (Leadership Capabilities)

Kapasitas kepemimpinan meliputi kemampuan untuk mengerakkan dan memimpin transformasi digital dalam hal teknologi dan bisnis, visi dan tujuan, pemberdayaan tenaga kerja, tata kelola, serta budaya dan keterlibatan.

Gambar 13 | Kapasitas Kepemimpinan



Sumber: Capgemini (2018)

## 2. Budaya Digital (Digital Culture)

Budaya digital cukup penting dalam upaya perwujudan resiliensi digital, yakni berperan sebagai fondasi yang kuat dalam mengubah pola pikir dan pemahaman pengurus Bank agar dapat berorientasi pada visi digital guna mendukung transformasi digital perusahaan. Hal ini diperlukan agar bank tetap kompetitif dan relevan di pasar. Secara singkat, *digital culture* sangat terkait dengan fleksibilitas bank dan sumber daya manusia bank yang siap dan mampu merespon tantangan baru agar tetap dapat bersaing dan tidak tertinggal.

World Economic Forum (2021) membagi budaya digital ke dalam 4(empat) aspek utama, yaitu kolaboratif, *data-driven*, *customer-centric*, dan inovatif, yang masing-masing disertai rincian nilai dan pola pikir yang dapat menjadi pedoman bagi perusahaan dalam mengidentifikasi hal-hal apa saja yang *in-line* dan dapat mempercepat penerapan budaya digital dalam *workforce* perusahaan, yaitu:

Tabel 1 Aspek Utama Budaya Digital

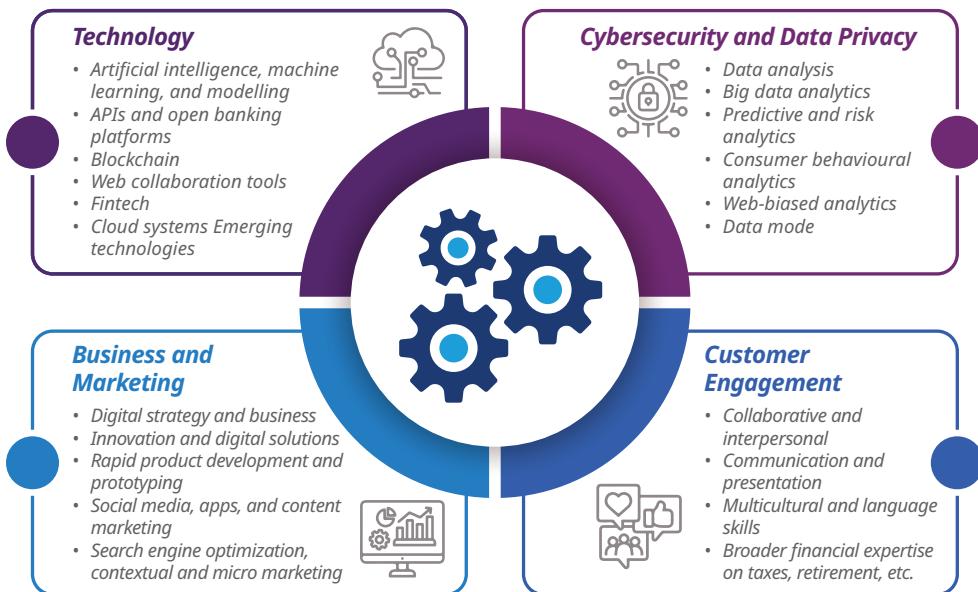
No.	Aspek	Values	Mindsets	Behaviours & Org. practices
1.	<b>Collaborative</b>	<ul style="list-style-type: none"> <li>• Trust</li> <li>• Curiosity</li> <li>• Inclusion</li> <li>• Speed</li> </ul> 	<ul style="list-style-type: none"> <li>• Pemahaman bahwa pekerjaan akan menjadi lebih cepat terselesaikan apabila melibatkan orang lain.</li> <li>• Mengakui bahwa dengan melibatkan orang lain, akan memberikan perspektif baru yang berarti.</li> <li>• Akan ada manfaat yang lebih besar jika semua pihak saling berkolaborasi.</li> </ul>	<ul style="list-style-type: none"> <li>• Kolaborasi antar bagian sering dilakukan.</li> <li>• Ketua tim dievaluasi berdasarkan <i>feedback</i> dari anggota tim mereka</li> </ul>
2.	<b>Data-driven</b>	<ul style="list-style-type: none"> <li>• Accuracy</li> <li>• Efficiency</li> </ul> 	<ul style="list-style-type: none"> <li>• Teknologi dan data adalah <i>key enablers</i>.</li> <li>• Demokratisasi data dapat mengoptimalkan <i>value</i>.</li> </ul>	<ul style="list-style-type: none"> <li>• Panduan dan strategi penyusunan <i>key performance indicators</i> (KPIs) yang bersifat kuantitatif dan relevan</li> <li>• Struktur tata kelola memastikan penggunaan data yang inklusif, berkelanjutan, dan aman.</li> </ul>
3.	<b>Customer-centric</b>	<ul style="list-style-type: none"> <li>• Curiosity</li> <li>• Trust</li> </ul> 	<ul style="list-style-type: none"> <li>• Karakter yang selalu aktif dan inisiatif dalam mendengarkan aspirasi <i>customer</i>.</li> <li>• Penyampaian produk/jasa sebagai interaksi yang berkelanjutan.</li> </ul>	<ul style="list-style-type: none"> <li>• Interaksi dengan <i>customer</i> secara berkala dalam rangka memahami kebutuhan <i>customer</i>.</li> <li>• Membina hubungan dengan <i>customer</i> melalui personalisasi dan kontak yang sering.</li> </ul>
4.	<b>Innovative</b>	<ul style="list-style-type: none"> <li>• Flexibility, freedom</li> <li>• Risk Aware</li> <li>• Transparency, trust</li> <li>• Cross-company/industry collaboration</li> <li>• Learning, development</li> </ul> 	<ul style="list-style-type: none"> <li>• Menerima kegagalan sebagai bagian dari pembelajaran.</li> <li>• Saran akan dipertimbangkan dan disertakan.</li> </ul>	<ul style="list-style-type: none"> <li>• <i>Product development</i> secara berkelanjutan.</li> </ul>

Sumber: World Economic Forum (2021), diolah

### 3. Talenta Digital (*Digital Talent*)

Pengembangan talenta berorientasi pada pengembangan *hard digital skills* (seperti *data analytics*) dan *soft digital skills* (seperti *digital-first mindset*). Dalam melakukan pengembangan talenta digital, Bank perlu mengidentifikasi jenis keahlian (*skill set*) yang dibutuhkan bagi perusahaan yang akan bertransformasi ke arah digital. Adapun *skill set* yang relevan bagi bank dapat dikategorikan menjadi 4 (empat) area, yaitu teknologi, keamanan siber dan pelindungan data pribadi, bisnis dan pemasaran, dan keterlibatan konsumen (*customer engagement*).

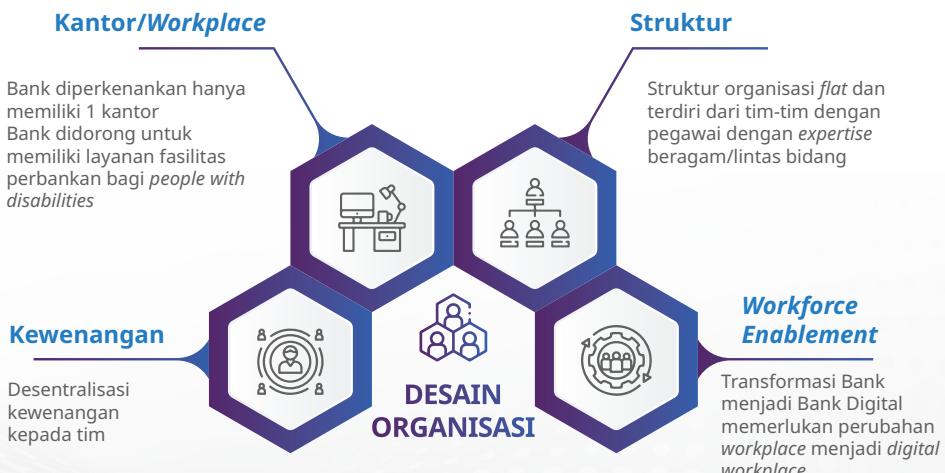
Gambar 14 | Talenta Digital



Sumber : Roubini ThoughtLab (2017) dan Brett King (2019), dimodifikasi kembali dalam Cetak Biru Transformasi Digital Perbankan

4. **Desain Organisasi (Organizational Design)** Desain organisasi yang sesuai dengan upaya digitalisasi bank dapat dilihat dari beberapa aspek yaitu struktur organisasi, kewenangan, dan pemberdayaan tenaga kerja (workforce enablement).

Gambar 15 | Desain Organisasi yang Mendukung Transformasi Digital



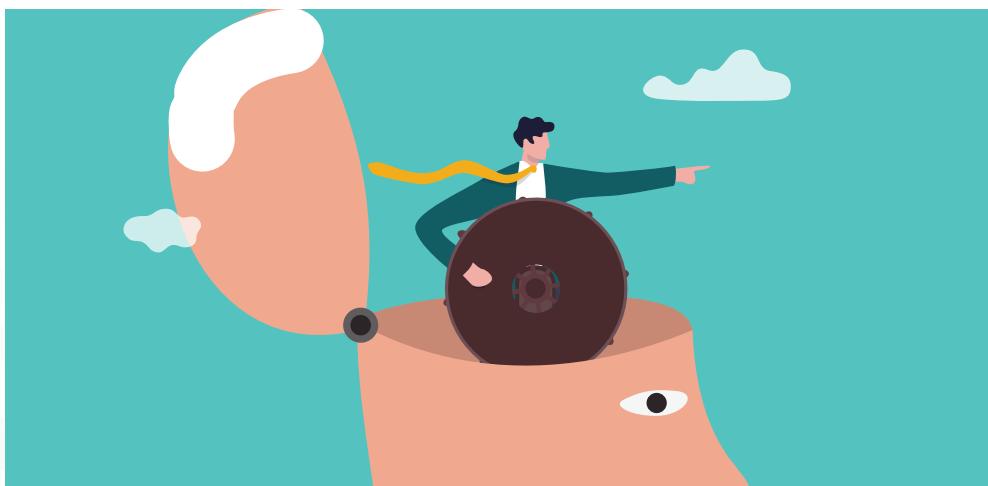
Sumber : Martech (2021) dan Russel Reynold (2017), diolah kembali dalam Cetak Biru Transformasi Digital Perbankan

**4.1. Struktur Organisasi** Diperlukan struktur organisasi yang mendukung kolaborasi dan memungkinkan adanya interaksi yang lebih luas antar unit kerja melalui pemanfaatan teknologi terdistribusi seperti *blockchain* atau teknologi berbasis IP. Hal ini diharapkan dapat menghindari timbulnya unit kerja yang bersifat *silo*.

Karakteristik dari struktur organisasi yang mendukung transformasi digital, antara lain:

- a. Struktur organisasi minim terhadap *organizational layers* (proses birokrasi).
- b. Memiliki pekerjaan yang bersifat *user-centric, iterative, dan collaborative*.
- c. Tugas pokok dan fungsi jabatan berfokus pada tujuan dan peran.
- d. Memiliki fokus terhadap profesi digital.

**4.2. Kewenangan** Diperlukan adanya desentralisasi kewenangan sehingga memungkinkan proses pengambilan keputusan yang efisien. Kewenangan dapat didistribusikan hingga pada level unit kerja atau tim sehingga pengambilan keputusan semakin dekat dengan konsumen. Bank perlu memberdayakan setiap unit kerja dengan *self-service analytics* dalam membuat keputusan yang lebih baik dan cepat, sesuai dengan wawasan dan kebutuhan masing-masing unit kerja. Bank juga dapat memanfaatkan penggunaan **teknologi melalui model *Business Intelligence* yang berbasis *data analytics*** untuk mendapatkan informasi yang relevan sehingga proses pengambilan keputusan dapat dilakukan dengan segera.





#### **4.3. Pemberdayaan Tenaga Kerja**

Diperlukan dukungan yang memadai bagi tenaga kerja agar upaya digitalisasi bank dapat dilaksanakan dengan baik. Hal tersebut dilakukan dengan menciptakan lingkungan kerja yang mendukung digitalisasi atau yang disebut sebagai *digital workplace*.

Berdasarkan laporan Deloitte (2021), *digital workplace* terdiri dari 4 (empat) aspek utama, yaitu:

a. Kolaborasi, Komunikasi, dan Koneksi

Pada dasarnya *digital workplace* meliputi kemampuan pegawai dalam melakukan tugasnya dengan berkolaborasi, berkomunikasi, dan berhubungan dengan pegawai lainnya. Tujuannya adalah untuk memperkuat hubungan bisnis yang produktif baik di dalam maupun di luar kelompok/unit kerja dan memungkinkan adanya pertukaran informasi antar unit kerja dalam organisasi.

b. Teknologi

Teknologi berperan dalam mewujudkan *digital workplace*. Setiap organisasi memiliki kriteria *digital workplace* yang bervariasi sesuai kategori industri dan lingkungan bisnis, dengan demikian teknologi yang dibutuhkan untuk mendukung *digital workplace* perlu disesuaikan dengan kebutuhan dan strategi organisasi.

c. Kontrol

Efektivitas penggunaan teknologi pada *digital workplace* perlu didukung oleh pengendalian yang tepat, meliputi struktur tata kelola, proses manajemen, dan kepatuhan. Alur informasi hendaknya tetap memenuhi kebijakan organisasi dan regulasi industri.

d. *Business Drivers*

Untuk memperoleh manfaat yang diharapkan, *digital workplace* perlu disesuaikan dengan arah dan strategi dari organisasi.

Lebih lanjut, berdasarkan laporan Capgemini (2018), kriteria *digital workplace* yang efektif sebagai berikut:

- a. mempertimbangkan semua teknologi yang digunakan karyawan untuk menyelesaikan pekerjaan mulai dari aplikasi keuangan, SDM, dan bisnis inti organisasi hingga *email enterprise, social media tools, and virtual meeting tools*;
- b. menyediakan *platform* komunikasi terpadu untuk membuat karyawan terhubung sepanjang waktu dan menyediakan akses ke alat dan informasi perusahaan melalui perangkat seluler mereka kapan saja, di mana saja; dan
- c. memungkinkan adanya tenaga kerja digital berupa tim robot perangkat lunak yang dapat bekerja bersama karyawan untuk menyelesaikan tugas dan proses yang berulang.

**C.  
Pengembangan  
Produk yang  
Berorientasi  
Konsumen  
(Customer-  
centric Product  
Development)**

Untuk dapat memastikan bahwa produk bank tetap kompetitif serta relevan di pasar, bank perlu memberikan produk dan layanan yang sesuai dengan kebutuhan konsumen atau mencapai *customer centric orientation services*. Hal tersebut dilakukan dengan memperhatikan 4(empat) hal yaitu *customer engagement, customer experience, customer insight* dan *customer trust and perception*. Keempat hal tersebut juga telah dicantumkan dalam Cetak Biru Transformasi Digital Perbankan OJK secara umum, sehingga dapat menjadi salah satu acuan dalam pengembangan produk pada bank, khususnya yang terkait dengan digitalisasi.



Gambar 16 Customer-centric Orientation Services



Sumber: Otoritas Jasa Keuangan (2021)

- 1. Keterikatan Konsumen (Customer Engagement)** Keterikatan konsumen (*customer engagement*) merujuk kepada keterikatan atau ketergantungan konsumen terhadap layanan digital dari bank. Hal itu dapat terjadi melalui suatu interaksi, reaksi, efek, atau pengalaman yang dirasakan konsumen secara keseluruhan terhadap produk atau layanan jasa yang mereka pilih.



Hal tersebut dapat dicapai melalui:

- Evaluasi keberhasilan produk dan layanan Bank serta pengukuran keterikatan nasabah dalam rangka melakukan perbaikan produk ke depan.
- Penerapan strategi untuk mempertahankan konsumen agar tidak beralih ke layanan dan produk bank pesaing, seperti menawarkan produk dalam suatu ekosistem keuangan digital atau menawarkan produk yang bersifat personal menyesuaikan kebutuhan individu atau segmen tertentu sehingga mampu meningkatkan loyalitas nasabah.

- 2. Pengalaman Konsumen (Customer Experience)**



Pengalaman Konsumen (*customer experience*) mengukur seberapa jauh tingkat kepuasan konsumen akan layanan perbankan yang ditawarkan oleh Bank. Jika konsumen sudah mendapatkan pengalaman yang puas, tentunya akan membangun rasa loyalitasnya terhadap produk dari perbankan tersebut.

Dalam meningkatkan pengalaman konsumen bank melakukan:

- Evaluasi produk dan layanan berdasarkan pengalaman nasabah.

- b. Analisis pengalaman nasabah dalam menggunakan produk dan/atau layanan digital yang diberikan oleh Bank, antara lain respon atas desain produk, jenis produk, dan kecepatan akses aplikasi bank.
- c. Perbaikan dan pengkinian atas produk dan layanan digital.

### **3. Pemahaman terkait Konsumen (Customer Insight)**



*Customer insight* merujuk pada bagaimana Bank mampu memahami tentang perilaku, preferensi, dan kebutuhan konsumen dengan memanfaatkan data konsumen. Bank dapat berkomunikasi dengan setiap konsumen dengan cara yang sangat personal dan secara konsisten memberi konsumen nilai tambah yang mengarah pada loyalitas yang kuat dan hubungan jangka panjang.

Dalam meningkatkan pemahaman terkait konsumen, Bank melakukan:

- a. Pemanfaatan data dan informasi nasabah dalam rangka pengembangan produk dan layanan, antara lain demografi, perilaku, preferensi dan kebutuhan nasabah.
- b. Kolaborasi dengan nasabah dalam menciptakan produk Bank dengan melibatkan baik ide ataupun peran serta nasabah dalam proses pengembangan produk dan layanan Bank.

### **4. Kepercayaan dan Persepsi Konsumen (Customer Trust and Perception)**

Kepercayaan dan persepsi konsumen sangat berpengaruh terhadap kesuksesan produk dan layanan bank. Hal tersebut dibangun dengan memberikan rasa aman bagi konsumen dalam menggunakan produk bank. Di samping itu, keandalan produk bank juga berpengaruh terhadap persepsi konsumen terhadap bank. Kepercayaan dan persepsi yang positif atas suatu produk akan turut meningkatkan loyalitas konsumen terhadap bank.



Dalam menjaga kepercayaan dan persepsi konsumen, Bank melakukan:

- a. Penguatan sistem keamanan pada bank dan peningkatan keandalan produk bank.
- b. Evaluasi produk dan layanan berdasarkan persepsi dan tingkat kepercayaan nasabah, antara lain diukur melalui kualitas produk, layanan, biaya, dan reputasi aplikasi bank.
- c. Penyediaan saluran umpan balik (*feedback*) untuk mendapatkan masukan dari nasabah.



Halaman ini sengaja dikosongkan



02

## RESILIENSI BANK TERHADAP GANGGUAN ATAU DISRUPSI DALAM LANSKAP DIGITAL



*Anticipate*



*Withstand & Recover*



*Sustain*

## Resiliensi Bank terhadap Gangguan atau Disrupsi dalam Lanskap Digital

### A. Antisipasi (*Anticipate*)

Tahap *Anticipate* adalah proses di mana organisasi mempersiapkan diri untuk menghadapi kemungkinan gangguan atau ancaman dalam lingkungan digital. Dalam tahapan ini Bank melakukan antisipasi terhadap gangguan atau disrupsi melalui penerapan kerangka *Business Continuity Management* (BCM). BCM merupakan serangkaian praktik yang mencakup penerapan kebijakan, standar, proses, dan langkah-langkah untuk mempertahankan fungsi Bank selama gangguan operasional.

BCM yang disusun oleh Bank terdiri dari beberapa komponen yang meliputi Tata Kelola Kelangsungan Bisnis, Analisis Dampak Bisnis (*Business Impact Analysis*), Penilaian Risiko (*Risk Assessment*), Strategi Ketahanan dan Rencana Kelangsungan Bisnis (*Resilience Strategy*), dan Pengujian Ketahanan (*Exercise and Test*).

Gambar 17 Komponen dalam BCM



Sumber: FFIEC (2019), diolah



- Tata Kelola Kelangsungan Bisnis (Business Continuity Management Governance)**

Tata Kelola BCM mencakup:

- Keselarasan antara BCM dan *risk appetite* Bank.
- Identifikasi tingkat kelangsungan (*continuity level*) yang diperlukan dan konsisten dengan kritikalitas operasi bisnis. Semakin kritis suatu fungsi, maka semakin tinggi tingkat kelangsungan yang diperlukan.



- c. Penyusunan kebijakan dan rencana kelangsungan bisnis (*Business Continuity Plan*).
- d. Alokasi sumber daya dalam implementasi BCM.
- e. Alokasi manajemen Bank yang kompeten dalam implementasi BCM.
- f. Pemantauan atas penerapan BCM.

Untuk memastikan bahwa tata kelola atas implementasi BCM berjalan dengan memadai, diperlukan peran penting Dewan Komisaris dan Direksi. Adapun Dewan Komisaris dan Direksi dalam menjalankan tugas pokok dan fungsinya memiliki tanggung jawab sebagai berikut:

- a. Dewan Komisaris dan Direksi memastikan kelangsungan bisnis Bank. Gangguan yang berkepanjangan dapat secara signifikan mempengaruhi reputasi, keamanan dan kesehatan keuangan, atau dalam beberapa kasus, dapat berdampak pada fungsi ekosistem keuangan.
- b. Dewan Komisaris dan Direksi wajib memberikan arahan strategis untuk mewujudkan tata kelola BCM yang memadai. Hal ini untuk memastikan bahwa Bank mampu secara efektif merespon dan pulih dari gangguan operasional yang signifikan yang terjadi.
- c. Dewan Komisaris dan Direksi perlu memastikan terwujudnya budaya organisasi dengan aspek kesiapan kelangsungan bisnis telah tertanam dalam manajemen risiko harian Bank, serta terintegrasi dalam kerangka kerja manajemen risiko operasional agar identifikasi dan pengelolaan risiko yang efektif di seluruh fungsi Bank dapat dilakukan.

Direksi bertanggung jawab untuk memastikan bahwa:

- a. kerangka kerja BCM yang efektif dan komprehensif diterapkan dan dipertahankan sebagai upaya dalam mengelola potensi gangguan operasional, dan untuk dapat memenuhi kebutuhan dan kewajiban bisnisnya;
- b. implementasi BCM telah berjalan dan Bank memiliki sumber daya yang cukup untuk mengawasi penerapan kerangka kerja BCM secara *organisation-wide* agar kesiapan kelangsungan bisnis (*business continuity preparedness*) yang diinginkan dapat tercapai;
- c. manajemen bank, selaku yang bertanggung jawab dalam menjalankan kerangka BCM, memiliki kewenangan, kompetensi, dan sumber daya yang memadai, serta terdapat mekanisme pelaporan yang sistematis kepada Direksi;
- d. efektivitas kerangka BCM yang diterapkan ditinjau dan dievaluasi secara berkala terhadap adanya kejadian eksternal, perubahan profil risiko, prioritas bisnis, proses, atau sistem, serta produk dan/atau layanan baru; dan
- e. telah dilaksanakan audit independen untuk menilai efektivitas dari mekanisme pengendalian, manajemen risiko, dan tata kelola dari kesiapan kelangsungan bisnis yang dimiliki oleh Bank.

Direksi bersama Manajemen Bank memiliki tanggung jawab untuk:

- a. mendefinisikan peran, tanggung jawab, dan tujuan dari penerapan BCM untuk mendukung proses bisnis dan resiliensi Bank;
- b. menyusun dan menerapkan kebijakan, standar, dan prosedur yang memadai serta *prudent* untuk mengelola gangguan operasional;



- c. mengalokasikan personel/sumber daya manusia yang memiliki kapasitas memadai dan memastikan bahwa personel tersebut memahami tugas dan tanggung jawabnya dalam implementasi BCM, serta memastikan kecukupan sumber daya keuangan;
- d. memastikan bahwa layanan dan fungsi bisnis utama Bank telah teridentifikasi, serta *Service Recovery Time Objective* (SRTO) dan *Recovery Time Objective* (RTO) untuk masing-masing layanan dan fungsi utama telah ditentukan dengan mempertimbangkan kebutuhan dan kritikalitas fungsinya dalam proses bisnis Bank;
- e. menetapkan target terukur sebagai bagian dari penilaian kinerja atas implementasi BCM, seperti level kesiapan (*level of preparedness*) dan target resiliensi (*resilience target*);
- f. merancang dan mengimplementasikan strategi simulasi/pengujian (*testing*) yang komprehensif atas kelangsungan bisnis dan konsisten dengan strategi BCM.
- g. memastikan rencana kelangsungan bisnis diuji secara berkala untuk mengetahui tingkat efektivitasnya terhadap skenario gangguan operasional yang parah namun masuk akal (*severe but plausible*) dan memverifikasi bahwa layanan dan fungsi bisnis utama Bank dapat pulih dalam jangka waktu SRTO dan RTO sesuai yang telah ditetapkan.
- h. memastikan kelemahan (*gap*) yang melebihi *risk appetite* Bank dan teridentifikasi dalam simulasi, pengujian, dan audit dapat diperbaiki/diselesaikan dengan segera.



- i. melakukan pertemuan secara berkala dengan komite/unit yang menangani kelangsungan bisnis (*business continuity*) untuk mendiskusikan perubahan kebijakan, simulasi, pengujian, dan rencana pelatihan; dan
  - j. menilai dan mengkinikan strategi dan rencana kelangsungan bisnis yang mencerminkan kondisi bisnis terkini.
- 2. Analisis Dampak Bisnis (Business Impact Analysis)**



Bank perlu melakukan *Business Impact Analysis* (BIA) untuk mengidentifikasi semua fungsi bisnis dan prioritisasi fungsi bisnis sesuai dengan tingkat kritikalitas. BIA bertujuan untuk menganalisis keterkaitan dalam proses bisnis dan sistem Bank, serta menilai bagaimana dampaknya terhadap proses bisnis jika terjadi disrupsi/gangguan pada suatu fungsi/sistem. Melalui BIA, Bank dapat mengidentifikasi tingkat ketergantungan pada operasional bisnis yang kritikal, unit kerja/departemen, pegawai, jasa, dan fungsi yang memiliki eksposur tinggi terhadap gangguan/disrupsi. Selanjutnya, Bank melakukan identifikasi sumber daya utama yang dibutuhkan oleh fungsi kritikal tersebut dan menentukan aspek mana saja yang perlu diproteksi lebih lanjut, termasuk menentukan biaya finansial dan sumber daya lainnya yang diperlukan untuk memulihkan fungsi kritikal tersebut jika mengalami gangguan.

Dalam melakukan analisis BIA, Bank melakukan **3 (tiga) tahapan** yaitu **Identifikasi atas Fungsi Bisnis Utama, Pemetaan dan Analisis Ketergantungan, serta Analisis Dampak Disrupsi dan Penentuan Objektif Pemulihan**.



**2.1. Identifikasi atas Fungsi Bisnis Utama (*Identification of Critical Business Functions*)**

Fungsi bisnis mendasari penyediaan layanan bisnis kepada nasabah. Ketika suatu fungsi bisnis terganggu, semua layanan bisnis yang bergantung pada fungsi tersebut dapat terganggu, sehingga berpotensi meningkatkan dampak operasional atau bisnis terhadap Bank. Selain itu, terdapat kemungkinan adanya beberapa fungsi bisnis yang tidak berkontribusi langsung terhadap layanan bisnis utama Bank, namun disruptif pada fungsi tersebut dapat berdampak pada keamanan dan kesehatan Bank. Dalam hal terjadi gangguan, pemulihan seluruh layanan dan fungsi bisnis tidak dapat dilakukan secara serempak dan sedini mungkin karena keterbatasan waktu dan sumber daya. Oleh karena itu, Bank perlu menentukan prioritas pemulihan layanan dan fungsi bisnis berdasarkan tingkat kritisnya, serta menentukan strategi pemulihan dan alokasi sumber daya yang tepat. Untuk menentukan prioritas pemulihan layanan, Bank perlu melakukan identifikasi layanan bisnis yang kritis. Penentuan tingkat kritis atas layanan/fungsi bisnis bergantung pada beberapa variabel antara lain ukuran, kompleksitas bisnis, dan segmen nasabah dari masing-masing Bank sehingga definisi layanan kritis antar satu Bank dengan Bank lainnya mungkin berbeda.

**Dalam melakukan identifikasi fungsi bisnis kritis, Bank mengidentifikasi dan memetakan ketergantungan dari awal hingga akhir (*end-to-end dependencies*) yang meliputi orang, proses, teknologi, dan sumber daya lainnya (termasuk yang melibatkan pihak ketiga) yang mendukung setiap layanan bisnis penting. Selanjutnya, Bank dapat menentukan mana di antara beberapa layanan bisnis mereka yang termasuk layanan bisnis kritis.**

**Tabel 2** Contoh Layanan Bisnis Kritis di Sektor Jasa Keuangan

Lembaga Jasa Keuangan	Contoh Layanan Bisnis Utama
Bank	<i>Cash Transactions</i> <i>Lending</i> <i>Deposit-taking</i> <i>Treasury</i> <i>Private banking and wealth management</i> <i>Investment banking or corporate finance</i> <i>Trade services</i>
Asuransi	<i>Claims servicing (including surrender)</i> <i>Policy renewal and servicing</i> <i>Policy inception</i>

Infrastruktur Pasar Keuangan	<i>Derivatives trading, clearing, settlement and reporting</i> <i>Securities trading, clearing, settlement and depository</i> <i>Administering of benchmarks</i> <i>Payment clearing and settlement</i>
Broking and Custody	<i>Trading, clearing, settlement and custody</i>
Manajemen Aset	<i>Portfolio management and trading</i> <i>Trade settlement and operations</i> <i>Trustee services (termasuk fund admin and valuation)</i> <i>Processing of subscriptions and redemptions in fund units (transfer-agency)</i>
Payment Services	<i>Cross-border and domestic funds transfer</i> <i>Credit/debit card payments</i> <i>E-wallet payments/prepaid card payments</i>

Sumber : Bank of England (2022)

## **2.2. Pemetaan dan Analisis Ketergantungan (Dependency Mapping and Analysis)**

Sektor perbankan memiliki interkoneksi yang tinggi terhadap teknologi informasi dan penyedia jasa TI (pihak ketiga). Sebagai langkah awal untuk memitigasi risiko yang timbul dari ketergantungan terhadap TI, Bank melakukan identifikasi dan pemetaan ketergantungan dari awal hingga akhir sebagaimana dalam sub-bab 2.1 di atas.

Adapun analisis dan pemetaan ketergantungan dimaksud bertujuan untuk mengidentifikasi ketergantungan (*dependency*) antar fungsi/layanan bisnis Bank sehingga selaras dengan objektif resiliensi dan prioritas pemulihan. Dalam melakukan analisis dan pemetaan, Bank melakukan identifikasi titik-titik yang berpotensi terpapar eksposur/gangguan misalnya jalur telekomunikasi, koneksi jaringan antar cabang, ketergantungan pada satu sumber listrik, lokasi pusat data yang berdekatan secara geografis, termasuk keterbatasan sumber daya manusia yang kompeten.

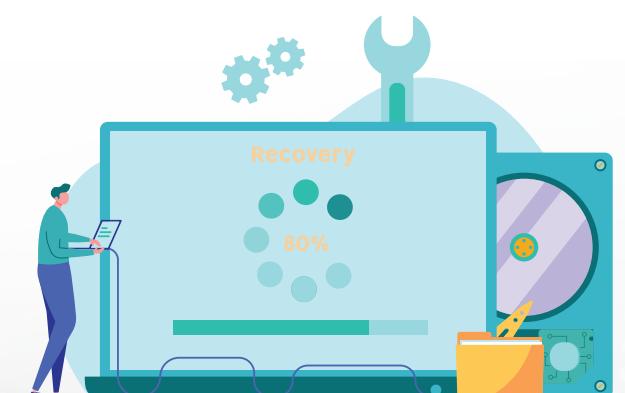
Beberapa aspek pemetaan yang perlu dilakukan oleh Bank meliputi:

- 1. Pemetaan atas Sumber Daya Manusia.** Bank perlu memahami kebutuhan SDM dan melakukan alokasi SDM yang bertanggungjawab atas proses, teknologi dan implementasi serta pemantauan untuk masing-masing fungsi/layanan bisnis, termasuk penentuan individu yang bertanggungjawab untuk kapabilitas tertentu dan berapa jumlah personel yang dibutuhkan sesuai dengan tingkat kritikalitas dari fungsi/layanan bisnis.
- 2. Pemetaan atas Teknologi.** Bank melakukan pemetaan sistem dan arsitektur yang mendasari untuk mendukung penyediaan layanan TI.
- 3. Pemetaan atas Proses Bisnis.** Bank melakukan pemetaan terhadap kumpulan aktivitas terstruktur yang dirancang untuk menghasilkan keluaran/*output* tertentu.
- 4. Pemetaan atas Data dan Informasi.** Pemetaan terhadap data dan Informasi yang dibutuhkan oleh Bank untuk melaksanakan jasanya yang mendukung keberlangsungan Layanan Bisnis Kritis, seperti klasifikasi, pemetaan, dan penandaan data.
- 5. Pemetaan atas Penggunaan Penyedia Jasa/Pihak Ketiga.** Penggunaan pihak ketiga dalam penyediaan fungsi/layanan bisnis kritis berpotensi meningkatkan risiko operasional Bank jika terjadi gangguan atau kegagalan pada sistem pihak ketiga. Sebagai langkah mitigasi risiko, Bank perlu melakukan pemetaan ketergantungan sumber daya (*resource dependency*) dan identifikasi potensi-potensi gangguan terhadap fungsi/layanan bisnis yang menggunakan jasa pihak ketiga,



khususnya untuk fungsi/layanan bisnis yang kritikal. Selanjutnya, Bank perlu menerapkan langkah-langkah dalam rangka memastikan bahwa Pihak Penyedia Jasa/ Pihak Ketiga memenuhi *Service Recovery Time Objective* (SRTO) atas fungsi/layanan bisnis kritikal, antara lain:

- a. menetapkan dan meninjau *operational level* atau *service level agreement* (SLA) secara berkala atas fungsi/layanan yang menggunakan pihak ketiga. SLA tersebut perlu mencakup penentuan target pemulihan (*recovery expectations*) yang spesifik dan terukur, serta sejalan dengan strategi BCM Bank.
- b. melakukan reviu atas rencana kelangsungan bisnis/ *Business Continuity Plan* (BCP) milik pihak ketiga untuk memastikan bahwa BCP dimaksud telah memenuhi standar dan sejalan dengan rencana kelangsungan bisnis Bank, serta melakukan pengujian atas BCP pihak ketiga secara berkala.
- c. melakukan koordinasi dengan pihak ketiga untuk menjaga ketersediaan sumber daya yang kompeten untuk menjadi penanggung jawab pada fungsi/layanan yang menggunakan pihak ketiga, misalnya meminta kepada pihak ketiga untuk menyediakan tenaga kerja khusus (*dedicated manpower*).
- d. melakukan audit terhadap prosedur, kinerja, dan sistem yang disediakan oleh pihak ketiga. Audit dapat dilakukan oleh pihak eksternal yang independen. Bank perlu meninjau dan memastikan bahwa ruang lingkup audit yang akan dilakukan oleh pihak eksternal sudah memadai dan telah mencakup



semua aspek yang ingin dinilai oleh Bank sehingga dapat meningkatkan kredibilitas atas layanan yang disediakan oleh pihak ketiga.

- e. melakukan pengujian dan simulasi bersama dengan pihak ketiga.
6. **Pemetaan atas Potensi Risiko Konsentrasi.** Sentralisasi sumber daya manusia, teknologi, atau sumber daya lain di fungsi/layanan bisnis tertentu dapat meningkatkan efisiensi bank. Namun demikian, hal tersebut juga dapat menimbulkan risiko konsentrasi. Bank perlu menerapkan mitigasi yang memadai dan responsif mengingat SDM dan teknologi merupakan aspek yang tidak dapat disubstitusi dengan cepat. Bank dapat mengadopsi beberapa pendekatan sebagai berikut untuk memitigasi risiko konsentrasi dan mengurangi dampak apabila terjadi gangguan:
  - a. Melakukan pemisahan antara *primary* dan *secondary sites* dari layanan dan fungsi bisnis kritikal, atau infrastruktur (seperti pusat data) ke masing-masing area yang berbeda, untuk memitigasi *wide-area disruption*;
  - b. Memisahkan fungsi bisnis kritikal ke dalam area yang berbeda untuk memitigasi risiko kehilangan fungsi bisnis kritikal sekaligus, dalam hal terjadi *wide-area disruptions*;
  - c. Menggerakkan *critical personnel* pada seluruh area, atau membentuk tim cadangan guna menghilangkan ketergantungan pada SDM tertentu;
  - d. Mengidentifikasi *skill* atau peran kritikal, dan mengembangkan *cross-training program* untuk membangun kecakapan bagi para pihak utama yang terlibat dalam peran ini;





Selain langkah-langkah di atas, **Bank perlu menyusun rencana dan prosedur dalam mengantisipasi setiap gangguan, kegagalan, atau pembatalan perjanjian dengan pihak ketiga yang tidak terduga**, yang bertujuan untuk meminimalisir dampaknya terhadap kelangsungan layanan bisnis kritikal Bank. Salah satu contohnya dengan membangun kemampuan internal (*in-house capability*) jika pihak ketiga/ pihak penyedia jasa utama tidak dapat memberikan dukungan segera ketika terjadi gangguan/disrupsi. Disamping itu, Bank perlu menyiapkan mitigasi untuk gangguan/disrupsi pada utilitas dasar seperti jaringan telekomunikasi dan suplai kelistrikan.

### 2.3. Analisis Dampak Disrupsi dan Penentuan Objektif Pemulihan

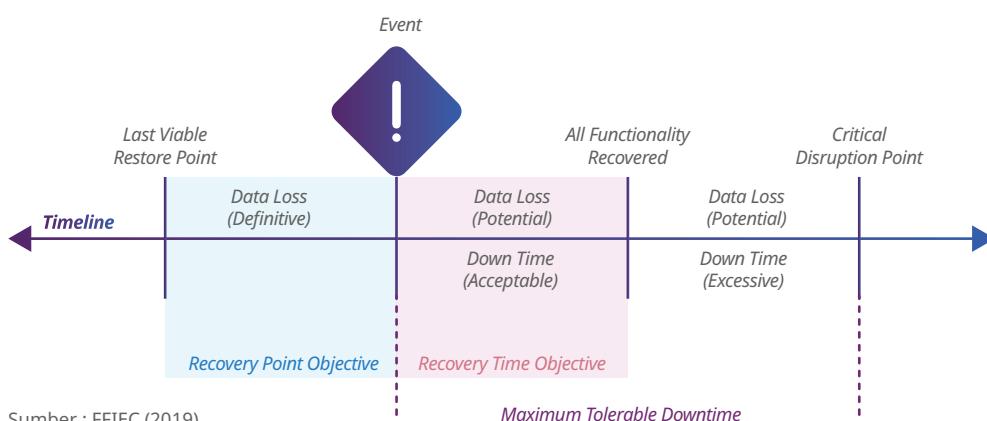
Bank perlu menetapkan toleransi dampak sebagai batas maksimum tingkat gangguan yang dapat ditoleransi terhadap layanan bisnis kritikal. Indikator yang umum digunakan sebagai berikut:

- a. ***Recovery Point Objective (RPO)*** adalah titik waktu sebelum gangguan, dimana data dapat dipulihkan (diberikan salinan cadangan data terbaru) setelah pemadaman.
- b. ***Recovery Time Objective (RTO) dan Service Recovery Time Objective (SRTO)*** adalah target waktu untuk mengembalikan fungsi bisnis tertentu dari kondisi mengalami gangguan hingga kembali pada kondisi semula sebelum terjadinya gangguan.

- c. **Maximum Tolerable Downtime (MTD)** adalah jumlah total waktu yang dapat diterima atau ditoleransi ketika terjadi gangguan proses bisnis, dengan mempertimbangkan dampak yang ditimbulkan.

Penetapan kriteria yang jelas terkait dengan toleransi dampak dapat membantu Bank ketika melakukan aktivasi rencana kelangsungan bisnis/BCP pada saat layanan bisnis kritikal mengalami gangguan. Hal ini dapat membantu Bank melakukan aktivasi BCP dengan tepat waktu dan tegas sebelum dampak yang ditimbulkan semakin besar.

**Gambar 18** Objektif Pemulihan sesuai dengan Alur Peristiwa



Sumber : FFIEC (2019)

Sebagai contoh, jika Bank yang menyediakan layanan kustodian mengidentifikasi penyimpanan sekuritas untuk pelanggan sebagai layanan bisnis yang kritikal, maka Bank perlu menentukan toleransi dampak ketika layanan tersebut mengalami gangguan dan mengidentifikasi potensi dampak yang ditimbulkan. Misalnya, setelah enam jam gangguan, hal ini berdampak pada kemampuan pelanggan untuk menyelesaikan transaksi sehingga menimbulkan risiko kerugian konsumen dan setelah delapan jam gangguan, hal ini menimbulkan risiko reputasi yang mengancam keamanan dan kesehatan dari Bank. Dengan demikian, Bank perlu mengidentifikasi kerentanan dalam sistem pengamanannya dan meningkatkan investasi untuk memperkuat ketahanan sistem agar tetap berada dalam toleransi dampak yang lebih pendek untuk meminimalisir risiko.

### 3. Penilaian Risiko (Risk Assessment)



Selain melakukan pemetaan atas fungsi/layanan kritikal, Bank perlu melakukan identifikasi dan penilaian risiko serta pengukuran frekuensi (*likelihood*) dan dampak (*impact*) terhadap:

- a. aset/sumber daya internal dan eksternal;
- b. berbagai potensi bahaya antara lain bencana alam, perubahan teknologi, dan perbuatan manusia (*human-caused*). Masing-masing potensi bahaya dikategorikan berdasarkan sumbernya apakah berasal dari internal atau eksternal, bersifat sistemik/non-sistemik, serta dengan atau tanpa peringatan;
- c. potensi risiko terkait wilayah geografis;
- d. risiko geopolitik;
- e. risiko keamanan siber; dan
- f. pengendalian yang ada (*existing control*).

Selanjutnya, Bank perlu melakukan antara lain:

- a. mengevaluasi probabilitas dan dampak atas kejadian yang mengganggu (*disruptive event*), misalnya kejadian dengan probabilitas tinggi dan dampak ringan (*high probability/low impact*), seperti gangguan listrik singkat atau kejadian dengan probabilitas rendah dan dampak serius (*low probability/high impact*), seperti pandemi. Adapun jenis risiko yang paling sulit diantisipasi adalah risiko dengan dampak yang berat namun kemungkinan terjadi yang rendah; dan
- b. mengukur dampak dan mendefinisikan kriteria kerugian sebagai kategori kuantitatif (contoh: keuangan) atau kualitatif (contoh: dampak terhadap *customer*, dampak terhadap reputasi).



**4.  
Strategi  
Ketahanan  
(*Resilience  
Strategy*)**



Resiliensi atau Ketahanan adalah kemampuan untuk bersiap dan beradaptasi terhadap perubahan kondisi serta bertahan dan pulih dengan cepat dari gangguan. Ketahanan mencakup kemampuan untuk bertahan dan pulih dari serangan yang disengaja, kecelakaan, atau ancaman maupun insiden yang terjadi secara alami. Meningkatkan ketahanan berarti melakukan langkah-langkah proaktif untuk memitigasi risiko atas peristiwa/gangguan yang terjadi dalam operasional Bank keseluruhan.

Strategi ketahanan, termasuk menjaga standar keamanan, harus diterapkan pada seluruh bisnis, termasuk terhadap aktivitas yang dialihdayakan kepada pihak ketiga. Bank perlu melakukan evaluasi ketersediaan sumber daya (seperti SDM, keuangan, teknologi, infrastruktur) yang memadai untuk meningkatkan ketahanan Bank terhadap segala bentuk disruptif di era digital. Dalam mengembangkan strategi resiliensi digital untuk mendukung kelangsungan bisnis, Bank perlu mempertimbangkan hasil evaluasi dan pembelajaran dari peristiwa-peristiwa sebelumnya.

Strategi ketahanan yang dikembangkan oleh Bank mencakup:

**a. Ketahanan Infrastruktur Fisik (*Physical Resilience*)**

Ketahanan infrastruktur fisik meliputi arsitektur teknologi informasi, infrastruktur, fasilitas, dan jaringan telekomunikasi. Untuk menghindari potensi kegagalan setelah adanya gangguan, Bank perlu melakukan diversifikasi jalur telekomunikasi, membangun koneksi/jaringan yang aman antara cabang dan pusat data, menyiapkan *backup system*, menyediakan alternatif sumber listrik/energi, dan membangun/menempatkan pusat data dan infrastuktur vital yang tersebar secara geografis, tidak terkonsentrasi pada



daerah tertentu, dan berlokasi di daerah dengan potensi bencana alam yang rendah.

**b. Ketahanan Siber (*Cyber Resilience*)**

Ketahanan siber meliputi ketahanan siber sebagaimana yang telah diatur dalam Surat Edaran OJK (SEOJK) No. 29/POJK.03/2022 tentang Ketahanan dan Keamanan Siber bagi Bank Umum, mencakup proses identifikasi aset, ancaman, dan kerentanan; pelindungan aset; deteksi insiden siber; serta penanggulangan dan pemulihian insiden siber.

**c. Ketahanan dan Replikasi Data (*Data Backup and Replication*)**

Pencadangan dan replikasi data merupakan aspek penting untuk memulihkan fungsi bisnis kritikal jika terjadi gangguan. Dokumen cadangan dibuat secara elektronik, dicadangkan di media yang dapat dipindahkan, disimpan sementara di *server* jaringan, atau dicadangkan pada komputasi awan (*cloud*). Cadangan data harus mudah diakses dan sesuai dengan kebijakan keamanan informasi Bank.

Strategi pencadangan dan pemulihan data disesuaikan dengan perkembangan teknologi dan derajat ancaman/gangguan. Sebagai contoh, untuk sistem *real-time* atau sistem bervolume tinggi diperlukan metode duplikasi dan pencadangan data tingkat lanjut. Disamping pencadangan data, pencadangan perangkat lunak (*software backup*) yang memadai merupakan aspek yang perlu diperhatikan. Kegagalan dalam pencadangan konfigurasi perangkat lunak dapat berdampak pada pemulihan sistem yang lebih lambat. Pencadangan perangkat lunak meliputi





sistem operasi (*operating systems*), aplikasi (*applications*), program utilitas (*utility programs*), basis data (*databases*), dan perangkat lunak penting lainnya sebagaimana yang teridentifikasi pada tahapan BIA.

Dalam menetapkan prosedur pemulihan jaringan dan sistem yang bersifat *critical*, Bank perlu mempertimbangkan beberapa aspek antara lain, bentuk cadangan (fisik atau virtual), tingkat cadangan (penuh, inkremental, atau diferensial), pembaruan dan frekuensi siklus retensi, tinjauan kompatibilitas perangkat lunak dan perangkat keras, kontrol transmisi data, serta pemeliharaan penyimpanan data.

Replikasi data yang disebut juga sebagai sinkronisasi atau pencerminan data (*mirroring*), bertujuan untuk mempertahankan kumpulan data yang identik di lokasi terpisah. Bank perlu mempertimbangkan kontrol integritas selama replikasi data sehingga perubahan data dalam lingkungan produksi, pengembangan, dan penjaminan mutu diterapkan di seluruh jaringan.

Bank perlu menentukan periode penyimpanan yang tepat untuk setiap iterasi pencadangan data. Bank juga perlu mewaspada replikasi *malware* dan *data corruption* ketika melakukan replikasi data. Risiko ini semakin besar dengan penggunaan sistem replikasi data yang hampir *real-time*, karena *malware* dapat direplikasi tanpa terdeteksi.

**d. Ketahanan Tenaga Kerja (*Workforce Resilience*)**

Tenaga kerja atau sumber daya manusia memegang peranan penting dalam menjaga resiliensi digital Bank. Ketahanan Bank bergantung pada ketersediaan personel untuk menjaga proses bisnis yang penting. Ketika terjadi gangguan/disrupsi Bank perlu memperhatikan ketersediaan SDM yang dapat mengatasi gangguan tersebut dan menyiapkan rencana alternatif ketika SDM dimaksud tidak tersedia (berhalangan hadir, *resign*, mutasi, sakit, dan lain-lain). Bank perlu mengembangkan strategi penempatan pegawai (*staffing*) secara akurat yang memiliki kemampuan yang dibutuhkan dalam mengelola dan mengoperasikan fungsi/layanan bisnis yang bersifat *critical* untuk mempertahankan kelangsungan bisnis.

**e. Ketahanan terkait Penyedia Jasa Pihak Ketiga (*Third-Party Service Providers*)**

Dalam hal Bank menggunakan penyedia jasa pihak ketiga, khususnya dalam operasional sistem TI, Bank perlu menilai potensi kerentanan penyedia jasa pihak ketiga terhadap berbagai skenario kejadian dan memverifikasi kemampuan ketahanan pihak ketiga tersebut. Rencana ketahanan Bank perlu dikoordinasikan dengan penyedia jasa pihak ketiga agar sejalan dengan rencana kelangsungan bisnis dari pihak ketiga. Disamping itu, Bank perlu menetapkan ekspektasi yang jelas dan SLA atas layanan yang disediakan pihak ketiga.



**5. Rencana Kelangsungan Bisnis (Business Continuity Plan)**



Rencana kelangsungan bisnis (*Business Continuity Plan/BCP*) mendokumentasikan serangkaian praktik dan prosedur untuk melanjutkan operasional bisnis selama terjadi gangguan. BCP berfokus pada fungsi bisnis yang bersifat *critical* dan bervariasi sesuai dengan ukuran dan kompleksitas Bank. BCP perlu disusun secara komprehensif meliputi aspek antara lain:

- a. pembagian peran, tanggung jawab, dan identifikasi keahlian yang dibutuhkan, baik personel Bank maupun pihak ketiga;
- b. alternatif dan solusi untuk berbagai jenis disruptif/gangguan, termasuk insiden dan serangan siber;
- c. ambang batas eskalasi masalah (*escalation threshold*);
- d. langkah-langkah untuk memproteksi personel dan nasabah, serta langkah untuk meminimalisir dampak yang ditimbulkan dari gangguan;
- e. prioritisasi dan prosedur untuk memulihkan fungsi, layanan, dan proses; dan
- f. proteksi atas informasi penting (*critical information*).

Secara rinci, BCP perlu mencakup beberapa komponen sebagai berikut:

**1. Manajemen Peristiwa (Event Management)**

BCP mendefinisikan berbagai situasi sebagai peristiwa, gangguan, atau pemicu. Peristiwa adalah kejadian atau perubahan keadaan yang dapat mempengaruhi operasional bisnis. Suatu peristiwa dapat bersifat fisik, virtual, atau kombinasi keduanya. Gangguan adalah peristiwa yang diantisipasi atau tidak direncanakan yang menyebabkan operasional bisnis menurun atau gagal untuk jangka waktu yang tidak dapat diterima



(misalnya, pemadaman listrik kecil atau diperpanjang, jaringan yang tidak tersedia diperpanjang, atau kerusakan atau kehancuran peralatan atau fasilitas). Pemicu adalah peristiwa yang mendorong respons manajemen.

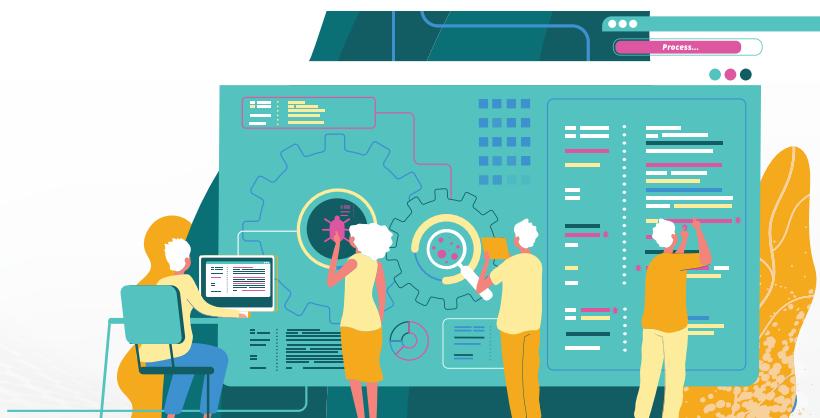
BCP perlu mencakup prosedur pengelolaan kejadian yang merinci jenis kejadian yang dapat diperkirakan secara wajar dan memberikan ambang batas dan tanggapan. Prosedur harus menjelaskan bagaimana melaporkan suatu peristiwa kepada manajemen dan situasi yang memerlukan pemberitahuan kepada pihak yang menangani peristiwa tersebut.

Manajemen perlu mempertimbangkan untuk membentuk tim yang bertugas menangani peristiwa/kejadian/disrupsi. Tim bertanggung jawab untuk mengelola peristiwa/kejadian/disrupsi dan berkomunikasi dengan pemangku kepentingan, pemantauan peristiwa/kejadian/disrupsi merupakan tanggung jawab seluruh entitas (misalnya Direksi, Manajemen, dan personel lainnya).

## 2. Kelangsungan dan Pemulihan (*Continuity and Recovery*)

BCP memuat mekanisme untuk mendukung kelangsungan bisnis dan pemulihan sistem antara lain:

- a. Mengatasi permintaan layanan dari nasabah selama *downtime* / gangguan.
- b. Melacak transaksi harian.
- c. Rekonsiliasi akun buku besar.
- d. Mendokumentasikan tugas-tugas operasional.
- e. Meposting entri setelah pemulihan sistem.





- f. Menyimpan catatan cadangan untuk memberikan informasi akun nasabah (misalnya, nomor akun, nama nasabah, alamat, status rekening, dan saldo rekening).
- g. Mendokumentasikan langkah-langkah untuk pemulihan dan memulai ulang / *reset* perangkat keras dan perangkat lunak sistem.
- h. Langkah-langkah manual untuk fungsi kritis, seperti operasional *back-office*, operasional terkait pemrosesan pinjaman/kredit, dan layanan nasabah (*customer support*).
- i. Metode verifikasi identitas alternatif.
- j. Prosedur menangani identifikasi penipuan dan pelaporan aktivitas mencurigakan.

Rencana dan prosedur kelangsungan bisnis perlu disusun secara jelas, ringkas, sistematis, dan mudah diterapkan dalam keadaan darurat.

### **3. Fasilitas dan Infrastruktur**

BCP harus mengidentifikasi alternatif untuk operasional utama (*core operation*), fasilitas, sistem infrastruktur, mitra bisnis yang saling bergantung/terkait, dan personel kunci (*key personnel*). Fasilitas dan infrastruktur cadangan mencerminkan fungsionalitas operasional utama.

Saat memilih fasilitas dan infrastruktur cadangan, bank harus merencanakan skalabilitas karena suatu peristiwa/kejadian/disrupsi dapat berlangsung dalam jangka waktu yang lama. Bank perlu memverifikasi bahwa alternatif pemulihan dapat mengakomodasi layanan dan kemampuan pemrosesan yang memengaruhi operasional penting.

Sebagai contoh, Bank merencanakan alternatif untuk pemulihan pusat data. Beberapa alternatif yang dapat dipertimbangkan antara lain:

- a. *Cold site*: Fasilitas cadangan yang memiliki komponen listrik dan fisik yang diperlukan dari fasilitas komputer, namun tidak memiliki peralatan komputer pada tempatnya. Fasilitas tersebut siap menerima peralatan komputer ketika personel berpindah dari lokasi komputasi utama ke fasilitas cadangan. Kekurangan dari alternatif ini adalah memerlukan waktu yang lama untuk memasang dan mengaktifkan infrastruktur sementara pengujian komprehensif tidak dapat dilakukan sampai infrastruktur dibangun.
- b. *Warm site*: Fasilitas cadangan yang telah dilengkapi dengan sistem informasi dan peralatan telekomunikasi untuk mendukung operasional relokasi apabila terjadi gangguan. Namun, perangkat keras yang disediakan belum diinstalasi dengan perangkat lunak khusus yang biasa digunakan dalam kegiatan bisnis untuk melanjutkan operasional sehingga memerlukan intervensi manual untuk *reboot* sistem agar dapat melanjutkan operasional bisnis yang *critical*.
- c. *Hot site*: Fasilitas cadangan yang membutuhkan pembiayaan yang paling besar namun mempunyai nilai efisiensi dan efektivitas yang tinggi. *Hot site* dibuat persis dengan lingkungan kerja sebenarnya. Dengan perangkat keras dan perangkat lunak yang biasa digunakan serta data-data yang sudah terintegrasi. Sehingga ketika bencana terjadi, hanya tempat bekerjanya saja yang dipindah, tetapi lingkungannya sama dan sudah siap digunakan.



- d. *Mirrored data recovery sites*: Dua atau lebih situs aktif terpisah yang saling mendukung satu sama lain dan masing-masing situs secara independen mendukung fungsi bisnis penting. Seperti *Hot site*, situs ini berisi semua peralatan dan kemampuan koneksi namun terdapat salinan data yang duplikat.
- e. *Mobile site*: fasilitas cadangan ini memiliki struktur portabel yang dilengkapi dengan peralatan komputasi yang tersedia untuk pelanggan atau personel. Aktivasi situs seluler sepenuhnya bergantung pada seberapa cepat situs tersebut dapat dikirimkan dan cadangan dipulihkan.
- f. *Colocation facility*: fasilitas cadangan yang menyediakan ruang, listrik, infrastruktur, pengendalian lingkungan, dan kemampuan telekomunikasi untuk beberapa penyewa yang tidak terkait. Jika Bank bergantung pada *colocation facility* untuk menyalurkan sumber daya, terdapat risiko bahwa kapasitas penyedia *colocation facility* mungkin tidak dapat mendukung operasi Bank selama peristiwa gangguan berskala regional atau besar.
- g. *Reciprocal agreement*: Perjanjian yang memungkinkan dua entitas untuk saling mendukung. Meskipun perjanjian ini mungkin hemat biaya, perjanjian ini hanya dapat dilaksanakan jika terdapat kelebihan kapasitas yang memadai pada *reciprocal financial institution* dan keduanya beroperasi pada versi dan konfigurasi perangkat lunak inti yang sama. Pertimbangan harus diberikan pada keamanan dan privasi, karena informasi sensitif pelanggan dapat diungkapkan kepada staf di *reciprocal financial institution*. Meskipun pengaturan ini mungkin dapat diterima sebagai solusi jangka pendek, perlu diperhatikan bahwa solusi ini mungkin tidak dapat diandalkan sebagai solusi pemulihan jangka panjang.



- h. *Disaster recovery as a service (DRaaS)*: Solusi komputasi awan untuk mereplikasi dan *hosting* infrastruktur, aplikasi, dan data yang menyediakan layanan *failover* dan pemulihan.

Contoh lainnya adalah relokasi cabang. Kejadian yang merugikan dapat menyebabkan bank untuk sementara waktu membatasi atau menghentikan operasi cabang atau untuk sementara mengalihkan operasi cabang ke lokasi alternatif. Komponen BCP dapat mencakup menetapkan lokasi fisik tempat pegawai dan nasabah mengakses untuk menjalankan bisnis.

#### 4. Sistem Pembayaran

BCP perlu mencakup pengaturan alternatif jika sistem pembayaran gagal (misalnya mesin anjungan tunai mandiri (ATM), transfer dana, perbankan elektronik). Solusi alternatif dapat mencakup prosedur manual untuk menelepon atau mengirim faks otomatis ke lembaga keuangan koresponden. Selain itu, sistem berbasis web atau perangkat lunak pihak ketiga dapat digunakan untuk melakukan transaksi. Bank perlu memelihara dokumentasi untuk posting entri yang tepat waktu ketika sistem dipulihkan. BCP juga harus mengatasi permintaan uang tunai yang meningkat dan memindahkan dana melalui sistem elektronik, termasuk internet dan *mobile banking*.

#### 5. Likuiditas

BCP merinci proses untuk mengatasi potensi kebutuhan likuiditas selama kejadian / disruptif. Pengaturan untuk membantu memenuhi kebutuhan likuiditas dapat meliputi:

- a. Akses pinjaman darurat.
- b. Alternatif pengiriman tunai.



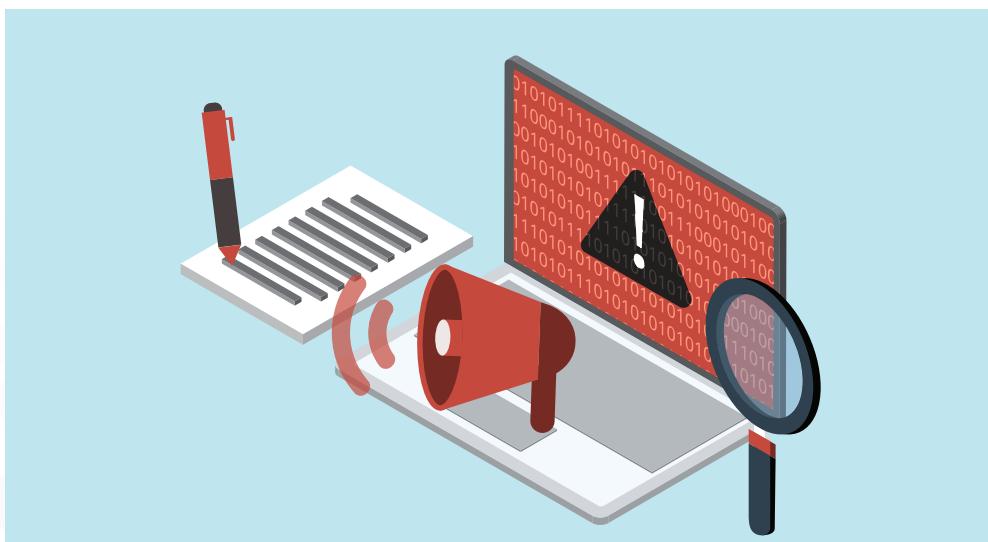
- c. Prosedur untuk mengamankan, menyerahkan, dan mendistribusikan uang tunai.

## 6. Rencana Tanggap Insiden (*Incident Response Plan*)

BCP perlu mencakup rencana tanggap insiden. Rencana tanggap insiden meliputi aspek stabilisasi insiden serta komunikasi dengan pemangku kepentingan (misalnya personel yang terkena dampak, penyedia layanan pihak ketiga, pelanggan, regulator, dan penegak hukum). Tim tanggap insiden harus mengoordinasikan komunikasi dengan pemangku kepentingan.

Bank menyelaraskan prosedur respons insiden dengan proses terkait lainnya (misalnya, keamanan siber, operasi jaringan, dan keamanan fisik), layanan *outsourcing* (misalnya, kewajiban bagi penyedia jasa pihak ketiga untuk menyiapkan rencana tanggap insiden). Bank dapat menunjuk juru bicara untuk berkomunikasi dengan media berita.

Bank harus mempertimbangkan berbagai skenario tanggapan yang direncanakan sebelumnya yang disetujui oleh Dewan Komisaris dan Direksi. Komunikasi dengan media berita dan media sosial penting untuk menyebarkan informasi yang akurat. Pemantauan media sosial selama disruptif membantu manajemen Bank untuk mengklarifikasi informasi simpang siur dan secara proaktif menanggapi masalah dan kekhawatiran dari pemangku kepentingan.





## 7. Rencana Pemulihan Bencana (*Disaster Recovery Plan*)

Bank melakukan identifikasi proses dan aktivitas bisnis utama yang harus dipelihara saat sistem dan aplikasi TI tidak tersedia dan memprioritaskan urutan pemulihan sistem ini, yang harus tercermin dalam BIA. Bank perlu mengembangkan strategi terkoordinasi untuk pemulihan pusat data, jaringan, *server*, penyimpanan, pemantauan layanan, dukungan pengguna, dan perangkat lunak terkait.

Rencana pemulihan harus mengatasi berbagai kejadian buruk (misalnya, bencana alam, kegagalan infrastruktur, kegagalan teknologi, ketidaktersediaan staf, atau serangan dunia maya). Pemulihan bencana harus membahas pedoman untuk mengembalikan operasi ke keadaan normal dengan gangguan minimum.

Rencana pemulihan bencana juga harus mengatasi hal-hal berikut:

- a. Kontrol dan protokol keamanan, termasuk fisik dan logis, untuk implementasi dan pengoperasian sistem pemulihan.
- b. Prosedur untuk memulihkan aktivitas yang tertunda atau transaksi yang hilang.
- c. Instruksi untuk mengakses repositori informasi penting dan sumber daya lainnya saat fasilitas utama tidak tersedia.

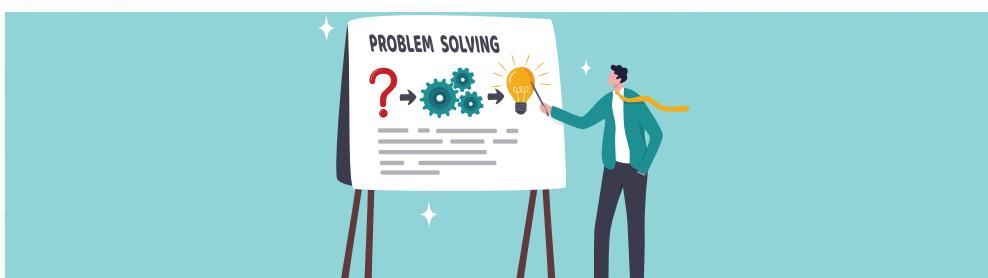
Saat mengembangkan rencana pemulihan bencana, Bank harus berhati-hati saat mengidentifikasi sistem kritis dan non-kritis. Sebagai contoh, *phone banking*, *internet banking*, atau ATM mungkin tidak tampak penting ketika sistem beroperasi secara normal; namun, sistem ini memainkan peran penting dalam memberikan layanan

kepada nasabah selama terjadi gangguan. Demikian pula, sistem email mungkin tidak tampak kritis tetapi mungkin merupakan sistem utama yang tersedia untuk komunikasi selama kejadian buruk.

## 8. Rencana Manajemen Krisis (*Crisis Management Plan*)

Bank menyiapkan dan menyusun rencana manajemen krisis. Rencana manajemen krisis meliputi:

- a. struktur manajemen krisis, dengan peran, tanggung jawab, alur pelaporan, dan rantai komando yang telah terbagi dengan jelas (termasuk menunjuk pengganti untuk perwakilan utama);
- b. seperangkat mekanisme (pemicu dan kriteria) yang telah ditentukan sebelumnya untuk mengaktifkan mekanisme/struktur manajemen krisis secara tepat waktu;
- c. rencana dan prosedur sebagai panduan bagi Bank dalam melaksanakan tindakan dan/atau keputusan selama krisis berlangsung;
- d. alat dan proses untuk memfasilitasi pemutakhiran dan asesmen situasi terkini dengan tepat waktu untuk mendukung *decision-making* selama krisis berlangsung;
- e. daftar seluruh *stakeholders* internal dan eksternal yang akan diinformasikan apabila gangguan layanan bisnis kritikal sedang terjadi, berikut dengan rencana dan persyaratan koordinasi;
- f. saluran komunikasi (*mainstream* dan media sosial) agar komunikasi yang efektif dapat dilakukan dengan para *stakeholders*, termasuk saluran alternatif dalam hal saluran komunikasi utama sedang tidak tersedia.





## 6. Pengujian Ketahanan (*Resilience Assessment*)

Pelatihan atau *exercise* adalah aktivitas yang melibatkan SDM dan proses yang dirancang untuk memvalidasi satu atau lebih aspek BCP atau prosedur terkait, yang dapat mencakup simulasi berbasis skenario dari elemen BCP. Misalnya, *exercise* dapat mencakup melakukan tugas dalam lingkungan yang disimulasikan atau berbasis diskusi (seperti *tabletop*).



Pengujian atau *test* adalah jenis *exercise* yang dimaksudkan untuk memverifikasi kualitas, kinerja, atau keandalan ketahanan sistem dalam lingkungan operasional. Pengujian mungkin berfokus pada opsi pencadangan dan pemulihan sistem. Tingkat pengujian dapat bervariasi, mulai dari komponen sistem individual hingga pengujian komprehensif semua komponen sistem yang mendukung operasi bisnis.

Aspek yang perlu diperhatikan dalam melakukan *exercise and test* meliputi:

1. ***Exercise & Test Program***, yang mencakup:
  - a. Kebijakan dan strategi *exercise and test*.
  - b. Pembagian tugas dan tanggung jawab program.
  - c. Kecukupan personel untuk melaksanakan *exercise or test*; mengawasi dan mendokumentasi hasil.
  - d. Tindakan untuk melindungi data seperti melakukan backup sebelum melakukan *exercise and test*.
  - e. Perbandingan hasil terhadap BCP untuk mengidentifikasi kesenjangan antara *excercise* atau *test* atau proses pengujian dan panduan pemulihan.
  - f. Tinjauan independen atas BCP dan *exercise and test program* (internal dan eksternal).

**2. *Exercise and Test Objectives*, yang mencakup:**

- a. Membangun keyakinan bahwa ketahanan dan strategi pemulihan memenuhi persyaratan bisnis.
- b. Menunjukkan bahwa layanan penting dapat dipulihkan sesuai target pemulihan yang ditetapkan (RTO, RPO, SLA dan MTD).
- c. Layanan kritis dapat dipulihkan jika terjadi insiden di lokasi pemulihan.
- d. Membiasakan staf dengan proses pemulihan.
- e. Verifikasi bahwa personel cukup terlatih dan memiliki pengetahuan tentang rencana dan prosedur pemulihan.
- f. Memastikan bahwa rencana latihan dan pengujian tetap kompatibel dengan BCP dan infrastruktur.
- g. Mengidentifikasi kesenjangan dan kekurangan.

**3. *Exercise and Test Scenarios***

Bank mengembangkan skenario *excercise and test* yang realistik berdasarkan risiko, melakukan simulasi gangguan dalam fungsi bisnis sehingga Bank dapat menentukan langkah yang harus dilakukan untuk mengatasi masalah, mempertahankan layanan bisnis, dan memenuhi ekspektasi nasabah.

Bank perlu mengidentifikasi dan mendokumentasikan asumsi yang digunakan dalam mengembangkan setiap skenario. Skenario mencakup ancaman yang dapat memengaruhi penyedia layanan pihak ketiga dan lainnya, seperti mitra bisnis yang signifikan. *Exercise and test* juga perlu mencakup simulasi atas protokol komunikasi dengan pemangku kepentingan yang berlaku.

Bank perlu mempertimbangkan semua risiko yang dapat diperkirakan secara wajar yang dapat timbul dari koneksi antara sistem/fungsi bisnis dalam Bank,





sistem Bank dengan penyedia jasa pihak ketiga, kolaborasi dengan pihak lainnya seperti mitra bisnis, maupun dengan pihak-pihak yang melakukan transaksi bisnis yang signifikan dengan Bank. Alternatif skenario dapat meliputi:

- a. serangan serentak yang mempengaruhi Bank dan penyedia jasa pihak ketiga;
- b. peristiwa terkait dunia maya (misalnya, serangan *malware* terisolasi, serangan DDoS, *data corruption*, atau penghentian pusat data);
- c. penggunaan *mirrored sites* untuk mengetahui efektivitas situs alternatif dalam mendukung kebutuhan nasabah, volume pekerjaan, dan proses bisnis ketika terjadi gangguan pada sistem utama; dan
- d. memproses pekerjaan sehari penuh dengan volume maksimum.

Bank perlu mengembangkan naskah *exercise and test* untuk memandu peserta dan memenuhi tujuan. Setiap naskah harus mendokumentasikan prosedur yang dapat meliputi aplikasi, proses bisnis, sistem, atau fasilitas yang ditinjau. Naskah dimaksud berisi langkah-langkah sistematis secara berurutan untuk dilakukan oleh karyawan atau pihak eksternal, prosedur untuk memandu proses kerja manual, jadwal rinci untuk penyelesaian, dan metode untuk mencatat hasil *exercise and test*.

**4. *Third-Party Service Provider Testing*,** yang mencakup:

- a. Identifikasi peran dan tanggung jawab utama.
- b. Fekuensi minimum, ruang lingkup, dan persyaratan pelaporan.
- c. Dokumentasi yang konsisten di seluruh proses bisnis.

- d. Proses untuk memperbaiki kekurangan yang teridentifikasi selama *exercise and test*.
- e. Pengujian komunikasi dan konektivitas antara Bank dan pihak ketiga penyedia jasa.

*Third-party service provider testing* dilakukan berdasarkan tingkat kritikalitas penyedia jasa dan fungsi bisnis. Bank berpartisipasi dalam pengujian penyedia jasa pihak ketiga sebagaimana yang tercantum dalam kontrak dan harus mendapatkan jaminan bahwa penyedia layanan pihak ketiga dapat diandalkan dan memiliki infrastruktur dan personel yang memadai untuk memulihkan layanan penting yang konsisten dengan persyaratan bisnis dan kontrak.

Bank perlu secara aktif berpartisipasi dalam program pengujian penyedia layanan pihak ketiga dan memverifikasi bahwa strategi pengujian mencakup kemungkinan peristiwa gangguan yang signifikan. Bank perlu memastikan bahwa penyedia jasa pihak ketiga transparan mengenai parameter dan hasil pengujian dari layanan yang diberikan. Bank menerima hasil pengujian dan laporan, rencana tindakan remediasi dan laporan status setelah penyelesaiannya, dan analisis atau pemodelan terkait.

Dalam hal terdapat masalah yang teridentifikasi dari hasil pengujian, Bank perlu memastikan bahwa penyedia jasa pihak ketiga dapat menyelesaikan masalah tersebut secara tepat waktu, sesuai dengan tingkat keparahan masalah tersebut. Setiap hasil pengujian yang berpotensi mempengaruhi operasional Bank perlu disampaikan kepada Direksi.





**5. *Post-Exercise and Post-Test Actions*, yang mencakup:**

- a. Rencana multi-tahun untuk melaksanakan latihan dan pengujian secara mendalam dan luas untuk mengidentifikasi kesenjangan dalam program dengan menggunakan metodologi dan skenario yang berbeda dari waktu ke waktu.
- b. Target pemulihan infrastruktur, kapasitas, dan integritas data.
- c. Asumsi, metodologi yang digunakan.
- d. *Lesson-learned* dari kejadian/disrupsi fungsi bisnis yang kritis.

Bank harus mendokumentasikan masalah yang teridentifikasi selama *exercise and test* dan membuat rencana aksi yang dilengkapi dengan tanggal target untuk menyelesaikan masalah. Hasil latihan dan tes perlu dianalisis dan dibandingkan dengan tujuan dan kriteria keberhasilan dalam rencana *exercise and test*, dan dilaporkan ke tingkat manajemen yang tepat. Untuk hal yang tidak dapat diperbaiki, Bank perlu mendokumentasikan keputusan untuk menerima risiko yang teridentifikasi selama *exercise and test*.

Bank perlu menguji tindakan korektif yang diterapkan sebagai akibat dari tujuan pemulihan yang gagal atau untuk mengatasi masalah utama yang dihadapi. Bank dapat memilih untuk menguji ulang selama atau sebelum *exercise and test* terjadwal berikutnya tergantung pada tingkat keparahan masalah. Bank perlu memperbarui BCP berdasarkan hasil pengujian dan menyesuaikan proses BCM.

Proses *exercise and test* dapat mencakup dokumentasi sebagai berikut:

- a. Tanggal dan lokasi.
- b. Ringkasan eksekutif yang berisi perbandingan antara tujuan dan hasil.
- c. Penyimpangan signifikan dari rencana, termasuk apakah partisipasi yang diinginkan tercapai.
- d. Masalah diidentifikasi dan pelajaran yang dipetik (*lesson learned*).
- e. Penugasan tanggung jawab untuk menyelesaikan masalah yang diidentifikasi dengan tepat waktu.

Bank perlu melakukan analisis berkala untuk menentukan apakah isu yang timbul berasal dari sumber yang sama. Jika demikian, maka prosedur pengendalian masalah yang diterapkan belum cukup memadai dan Bank perlu memperbaiki langsung ke akar permasalahan agar seluruh masalah mendasar dapat terselesaikan.

**B.  
Bertahan  
dan Pulih  
(*Withstand and  
Recover*)**

Tahap *Withstand and Recover* adalah proses yang **menggambarkan kemampuan Bank untuk tetap beroperasi dengan efektif selama insiden keamanan atau gangguan terjadi disertai eksekusi atas prosedur dan kebijakan untuk menangani gangguan/disrupsi**. Tahapan ini berfokus pada pengelolaan dampak serangan dan memulihkan sistem dan fungsi kritis ke keadaan normal setelah terjadi disrupsi/gangguan. Pada tahapan ini dilakukan proses implementasi rencana kelangsungan bisnis yang telah disusun di tahapan *Anticipate*, termasuk pengaturan sumber daya, infrastruktur, dan tim yang diperlukan untuk memulihkan operasional bisnis. Proses ini dapat melibatkan penerapan solusi teknologi, pelatihan staf, dan penerapan prosedur darurat. Tahapan ini diaktivasi ketika



Bank mengalami gangguan atau disrupsi, termasuk ketika menghadapi serangan siber. Beberapa langkah yang perlu dilakukan dalam tahapan ini adalah:

### 1. Penilaian Pelanggaran Keamanan (*Compromise Assessment*)



Proses untuk mendeteksi dan merespon potensi pelanggaran keamanan atau *security compromise* dalam sistem digital bank. *Security compromise* merupakan insiden yang terjadi pada jaringan sistem akibat adanya pelanggaran seperti akses tidak sah, penggunaan data secara ilegal, atau pelaksanaan operasi tanpa izin. Apabila Bank mencurigai suatu aktivitas yang tidak biasa, dilakukan penilaian dengan responsif untuk mengidentifikasi serta mengantisipasi kerentanan pada infrastruktur digital Bank sebelum dieksplorasi lebih lanjut oleh penyerang. Langkah-langkah dasar yang dilakukan dalam *compromise assessment* meliputi:

- a. Identifikasi indikator potensi gangguan melalui pemantauan terhadap aktivitas atau perilaku yang tidak biasa dalam jaringan atau sistem organisasi, seperti upaya *login* yang tidak biasa, lalu lintas jaringan yang tidak biasa, atau upaya akses yang tidak sah.
- b. Pengumpulan data dari berbagai sumber seperti *log system*, lalu lintas jaringan, dan perilaku pengguna untuk membantu mengidentifikasi potensi ancaman.
- c. Analisis data untuk mengidentifikasi potensi pelanggaran atau *security compromise*.
- d. Investigasi aktivitas atau perilaku yang mencurigakan untuk menentukan apakah aktivitas tersebut merupakan pelanggaran atau *security compromise* yang sebenarnya.
- e. Secara responsif melakukan langkah-langkah untuk memulihkan setiap pelanggaran keamanan atau *security compromise* yang teridentifikasi selama asesmen, seperti mengisolasi sistem yang terpengaruh, memperbarui kebijakan keamanan, atau mengatasi jaringan/sistem yang mengalami kerentanan.
- f. Memantau jaringan dan sistem Bank terhadap potensi ancaman atau titik kerentanan baru serta melakukan langkah-langkah keamanan yang diperlukan untuk mengatasi ancaman tersebut.

**2.**  
**Respon atas  
Insiden  
(Incident  
Response)**



Serangkaian proses yang terstruktur untuk merespon insiden/serangan siber yang bertujuan untuk meminimalkan biaya dan gangguan bisnis akibat serangan/insiden siber tersebut. Ketika Bank mengidentifikasi bahwa terjadi serangan/insiden yang cukup mengganggu kegiatan operasional dan bisnis, Bank secara otomatis melakukan aktivasi atas rencana tanggap insiden yang telah disiapkan pada tahap *Anticipate* untuk melakukan stabilisasi insiden sehingga insiden tidak berkembang lebih jauh menjadi krisis. Pada proses ini Bank juga berkomunikasi secara intens dengan internal dan pihak terkait termasuk regulator mengenai dampak yang ditimbulkan dari insiden tersebut serta langkah yang akan dilakukan oleh Bank untuk mengatasi gangguan.

**3.**  
**Manajemen  
Krisis (Crisis  
Management)**



Manajemen krisis adalah proses identifikasi krisis, aktivasi BCP, dan pengelolaan keadaan darurat. Tidak setiap peristiwa memerlukan respons manajemen krisis atau darurat. Bank harus mempertimbangkan dampak krisis atau keadaan darurat terhadap reputasi dan personel Bank. Misalnya, Bank mengaktifkan prosedur tanggap darurat atau krisis selama bencana alam, serangan terhadap jaringan dan sistem informasi, atau peristiwa berdampak signifikan lainnya. Manajemen krisis perlu mencakup koordinasi dengan regulator dan penegak hukum.

Bank perlu menunjuk koordinator yang bertindak sebagai *key personnel* dari departemen/divisi/unit terkait untuk bertindak selama krisis atau situasi darurat. Personel yang ditunjuk harus diberi wewenang untuk membuat keputusan pada waktu yang tepat. *Key personnel* dapat berupa:

- a. Manajemen senior untuk kepemimpinan.
- b. Manajemen yang menangani fasilitas untuk keselamatan dan keamanan fisik/infrastruktur.
- c. Bagian personalia untuk masalah personel, perjalanan, dan relokasi.
- d. *Public relation/media handling* untuk mengelola komunikasi yang baik, khususnya dengan pihak eksternal.
- e. Keuangan dan akuntansi untuk pencairan dana dan keputusan keuangan, termasuk biaya tak terduga.
- f. Hukum dan kepatuhan untuk masalah hukum dan peraturan.

- g. Fungsi yang menangani TI, termasuk keamanan informasi dan pemulihan sistem/jaringan.

Protokol komunikasi wajib menyertakan daftar kontak dan metode lain untuk menjangkau personel yang berwenang dan/atau stakeholders lain dalam hal keadaan krisis atau peristiwa darurat terjadi. Daftar kontak yang disertakan wajib terverifikasi dan diperbarui berkala, serta harus didistribusikan dan dapat diakses oleh *key personnel*.

Prosedur harus memungkinkan pegawai untuk melaporkan status mereka secara terpusat dan memperoleh informasi terkini. Protokol komunikasi manajemen krisis harus mencakup pula prosedur komunikasi alternatif apabila saluran komunikasi normal tidak dapat beroperasi.

**4. Pemulihan Bencana (Disaster Recovery)**



Aktivitas pemulihan infrastruktur, data, dan sistem TI yang wajib dikembangkan oleh manajemen melalui strategi terkoordinasi seperti dalam hal pemulihan *data centers*, jaringan, *server*, *storage*, *service monitoring*, *user support*, dan jaringan terkait. Rencana pemulihan harus dapat mengakomodir berbagai jenis gangguan (seperti bencana alam, kegagalan infrastruktur, kegagalan teknologi, kekurangan SDM, atau serangan siber), serta memuat pedoman pemulihan aktivitas operasional agar dapat kembali ke normal dengan gangguan seminimal mungkin.

**5. Manajemen Komunikasi Insiden (Incident Communication Management)**



Protokol dan manajemen komunikasi ketika terjadi insiden/serangan/gangguan kepada internal Bank, regulator, dan *stakeholder* termasuk pihak ketiga, nasabah, dan publik.

**Preventif (*Pre-Event*)**

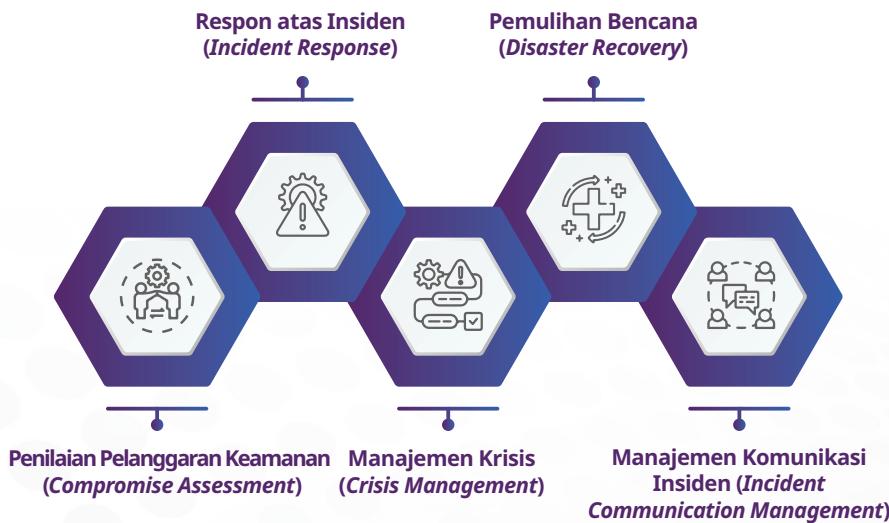
Dalam kondisi normal atau belum terjadi insiden, Bank perlu memperhatikan beberapa hal berikut:

**1. Menetapkan tujuan yang ingin dicapai pasca insiden. Menentukan hal-hal apa saja yang ingin dicapai setelah insiden berakhir, misal :**

- a. Melindungi subjek data
- b. Melindungi pemangku kepentingan utama
- c. Meminimalisir kerusakan reputasi
- d. Menjaga *engagement* nasabah terhadap produk dan layanan bank

- e. Kewajiban hukum
  - f. Menjaga nilai saham (jika Bank merupakan emiten)
- 2. Menentukan *security gaps*.** Mengidentifikasi *security gaps* yang dapat merusak reputasi, antara lain:
- a. Melakukan audit keamanan dan penilaian Risiko
  - b. Menilai *key hygiene factors* antara lain:
    - i. Enkripsi yang *up-to-date* dan *strong*
    - ii. Autentikasi multi faktor (*Multi-factor authentication*)
  - c. Mengutilisasi *threat monitoring* dan *open source intelligence*
- 3. Menetapkan dan mengelola kapabilitas komunikasi krisis**
- a. Menetapkan pengambil keputusan dan tim krisis lintas fungsi
  - b. Memberikan *update* informasi yang akurat kepada pengambil keputusan
  - c. Meninjau secara berkala kapabilitas internal dan merekrut *specialist* terkait keamanan TI jika diperlukan
  - d. Menyiapkan *draft responses* untuk kemungkinan skenario yang terjadi yang terkait dengan pemangku kepentingan utama

**Gambar 19** Langkah-Langkah dalam rangka Bertahan dan Pulih dari Insiden



Sumber: FFIEC (2019), diolah

- e. Menyiapkan media/sarana yang dapat diaktifkan ketika terjadi gangguan/krisis seperti *hotline*, FAQ, dan lain-lain.

#### **4. Koordinasi dengan Pihak Ketiga dan *Supply Chain***

- a. Memastikan perjanjian kerjasama yang disepakati telah memperhitungkan potensi terjadinya kondisi *breach/gangguan*.
- b. Menentukan protokol/mekanisme jika *breach* terjadi dari sisi mitra/*supplier*.
- c. Melibatkan mitra dalam perencanaan dan pelatihan.

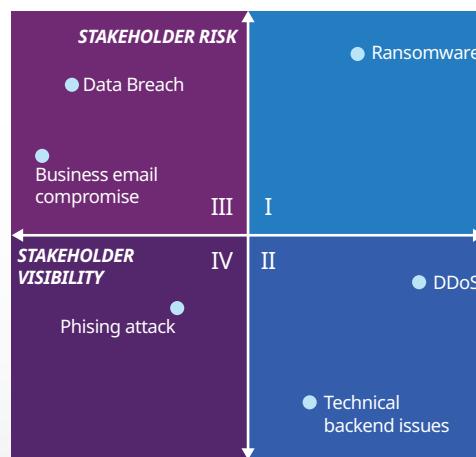
#### **5. Melakukan pelatihan dan *testing* secara berkala**

- a. Mengintegrasikan manajemen komunikasi insiden/krisis dalam BCM.
- b. Melibatkan seluruh pengambil keputusan Utama.
- c. Melakukan latihan dengan skenario yang realistik.
- d. Pertimbangkan skenario jika terjadi *breach* dalam *supply chain*.

#### **Saat Insiden**

Dalam kondisi terjadi insiden, Bank perlu menyiapkan langkah-langkah dalam menyusun pesan atau informasi yang akan disampaikan kepada pihak eksternal/pihak terkait. Dalam menyiapkan informasi yang akan disampaikan kepada pihak eksternal, Bank perlu mempertimbangkan tingkat risiko dan visibilitas dari suatu insiden atau gangguan.

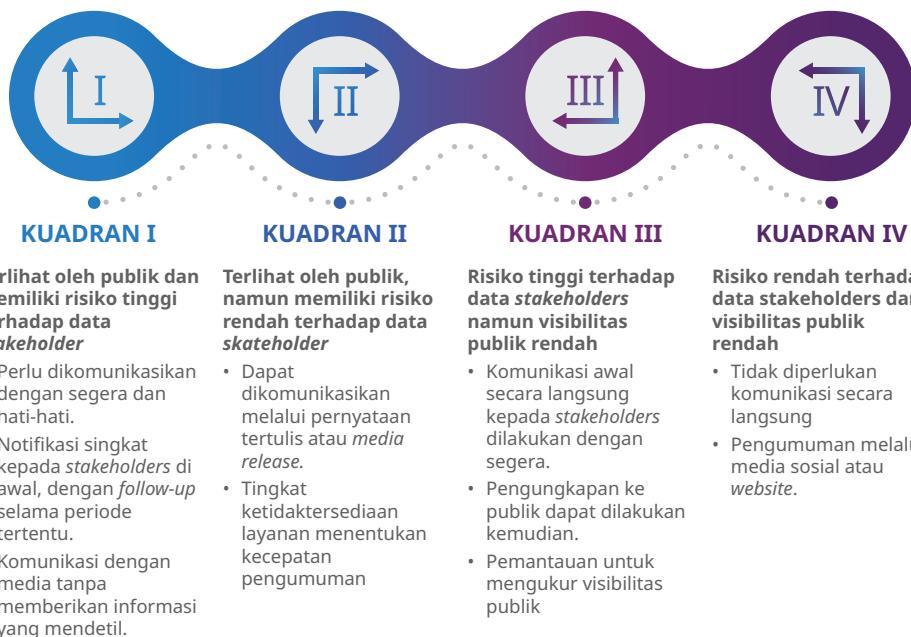
**Gambar 20 | Diagram Stakeholder Risk vs Visibility Matrix**



Sumber: CERT NZ (2023)

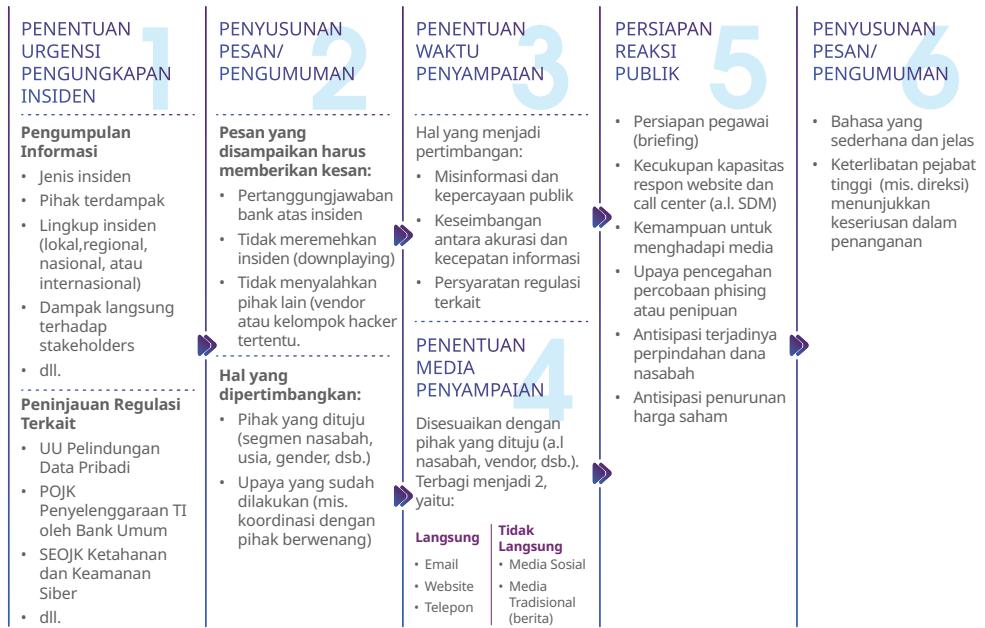
Insiden siber atau gangguan dengan mempertimbangkan risiko pemangku kepentingan (*stakeholder risk*) dan visibilitas pemangku kepentingan (*stakeholder visibility*) dibagi dalam 4(empat) kuadran. **Tingkat risiko (sumbu vertikal)** mengacu pada efek negatif yang dapat ditimbulkan oleh serangan siber kepada *stakeholder*. **Visibilitas (sumbu horizontal)** mengacu pada seberapa terlihat serangan tersebut di publik.

Sebagai contoh, serangan *Distributed Denial of Service* (DDoS) sangat terlihat di publik namun memiliki risiko yang relatif rendah, sementara itu kebocoran data tidak terlihat oleh publik namun memiliki risiko yang tinggi. Pemetaan ini berguna untuk menentukan waktu penyampaian pesan/pengumuman terkait insiden siber serta media yang digunakan sebagai berikut:



Dari pemetaan ini, dapat diidentifikasi jenis insiden atau gangguan yang memerlukan penyampaian informasi kepada pihak eksternal. Dalam proses menyiapkan penyampaian informasi, Bank dapat melakukan langkah-langkah sebagai sebagaimana ilustrasi pada gambar berikut.

Gambar 21 Alur Penyiapan Komunikasi ketika Terjadi Gangguan



Sumber: Knight, R. & Nurse, J.R.C (2020), disesuaikan

### C. Berkelanjutan (*Sustain*)

Tahap *Sustain* merupakan tahapan Bank melakukan evaluasi dan pengembangan (*improvement*) untuk meningkatkan kemampuan dan pengetahuan Bank atas gangguan/disrupsi yang telah terjadi sebagai upaya untuk mengembangkan prosedur ketahanan yang lebih baik dan meminimalisir dampak gangguan/disrupsi di masa depan. Beberapa langkah yang dilakukan dalam tahapan ini mencakup:



## 1. *Root-Cause Analysis (RCA) atas Insiden*



Identifikasi penyebab yang mendasari insiden atau pelanggaran keamanan. Bertujuan untuk membantu bank dalam memahami faktor-faktor yang berkontribusi terhadap insiden, sehingga bank dapat mengembangkan strategi ke depan untuk mencegah insiden serupa terjadi di masa mendatang. Strategi yang dilakukan meliputi:

- a. Identifikasi: mengidentifikasi insiden dan mengumpulkan semua informasi yang tersedia terkait insiden tersebut, termasuk seperti log data, peringatan sistem, laporan pengguna, dan data relevan lainnya.
- b. Analisis: menganalisis data untuk mengidentifikasi akar penyebab insiden tersebut. Hal ini dapat melibatkan analisis forensik dari sistem yang terpengaruh, mewawancara personel yang terkait, dan meninjau kebijakan serta prosedur terkait.
- c. Pelaporan: Temuan proses RCA insiden kemudian didokumentasikan dalam laporan yang mengidentifikasi akar penyebab atau penyebab insiden dan memberikan rekomendasi untuk mencegah insiden serupa terjadi di masa mendatang.
- d. Strategi Ke depan: Berdasarkan temuan proses RCA insiden, Bank mengembangkan strategi ke depan untuk mengatasi akar penyebab atau penyebab insiden. Ini mungkin melibatkan pemutakhiran kebijakan dan prosedur, menerapkan kontrol keamanan baru, dan memberikan pelatihan tambahan kepada personel. Strategi harus dirancang untuk mencegah insiden serupa terjadi di masa depan. Ini harus mengatasi penyebab insiden dan memberikan rekomendasi khusus untuk meningkatkan kontrol keamanan, kebijakan, dan prosedur. Strategi yang disusun juga harus mencakup rencana untuk memantau dan melaporkan keefektifan perubahan yang direkomendasikan untuk memastikan bahwa hasil yang diinginkan dapat tercapai.



**2.  
A Crisis  
After-action  
Review**



Evaluasi efektivitas respon bank terhadap krisis atau situasi darurat. Proses ini melibatkan penilaian komprehensif dari proses manajemen krisis, termasuk tanggapan terhadap insiden awal, proses komunikasi dan pengambilan keputusan, serta efektivitas tanggapan secara keseluruhan. Strategi yang dilakukan meliputi:

- a. Mengumpulkan Informasi: mengumpulkan informasi tentang krisis, termasuk sifat insiden, upaya respons, dan hasilnya.
- b. Menilai Tanggapan: menilai tanggapan Bank terhadap krisis yang terjadi, termasuk keefektifan upaya tanggapan, proses komunikasi dan pengambilan keputusan, serta tingkat kesiapsiagaan secara keseluruhan.
- c. Mengidentifikasi Kekuatan dan Kelemahan: Berdasarkan penilaian, tim mengidentifikasi kekuatan dan kelemahan dari upaya respons terhadap krisis yang telah dijalankan.
- d. Mengembangkan Strategi Peningkatan: Setelah kekuatan dan kelemahan diidentifikasi, tim mengembangkan strategi untuk meningkatkan kemampuan respons krisis organisasi. Hal ini termasuk pula kebijakan dan prosedur, peningkatan protokol komunikasi, atau peningkatan upaya pelatihan dan kesiapsiagaan.
- e. Menerapkan Perubahan: Langkah terakhir adalah menerapkan perubahan yang direkomendasikan agar kemampuan respons krisis Bank dapat ditingkatkan.

**3.  
Pelatihan dan  
Peningkatan  
Kesadaran  
(Training and  
Awareness)**



Memberikan pelatihan kepada pegawai mengenai prosedur kelangsungan bisnis kritikal, berikut peran dan tanggung jawab masing-masing, yang dilakukan secara berkelanjutan melalui reviu berkala dan pengkinian *business continuity program*. Strategi yang dilakukan dapat meliputi:

- a. Program pelatihan harus sejalan dengan strategi perusahaan dan menggunakan pendekatan yang komprehensif, *risk-based, multi-year approach*, termasuk *interrelated programs* (e.g. pemulihan bencana dan manajemen risiko pihak ketiga).
- b. Frekuensi pelatihan bergantung pada ukuran dan kompleksitas dari entitas dan elemen dari program pelatihan itu sendiri, risiko, serta iterasi pengujian program, yang seluruhnya tercakup dengan tepat waktu.

- c. Manajemen harus menginventarisir *skill sets* yang dimiliki, kemudian mengidentifikasi serta menanggulangi *gaps* yang ada.
- d. Program pelatihan dapat memuat elemen antara lain:
  - i. Pelatihan;
  - ii. *Current risks;*
  - iii. *Future risks;*
  - iv. *recent failures;*
  - v. *New programs/technologies;*
  - vi. *Organizational changes;* dan
  - vii. *Lesson learned* terdahulu.

Secara umum, pelatihan akan memberikan pemahaman konseptual dari aspek kelangsungan bisnis itu sendiri (metode dan hasil pengujian, serta fungsi bisnis kritikal). Pelatihan yang diberikan disusun dengan tujuan untuk memvalidasi rencana dan asumsi yang telah disusun dengan menguji interaksi *people, process, dan technology*, risiko serta kerentanan (*vulnerabilities*) lainnya tanpa menimbulkan konsekuensi.

#### **4. Pengembangan (*Continuous Improvement*)**



Bank perlu melakukan review secara berkala dan melakukan pengkinian *business continuity program* sesuai dengan perkembangan lingkungan terkini mengingat risiko dan teknologi dapat dengan cepat berubah. Hal ini memungkinkan Bank untuk menyelaraskan *business continuity process* dengan tujuan bisnis. Informasi yang diperoleh dari hasil peninjauan dapat digunakan Bank untuk menentukan prioritas dan fokus terhadap perbaikan dan penyempurnaan proses dan sistem. Hal-hal yang memicu perlunya pemeliharaan dan peningkatan atas *business continuity program* antara lain meliputi:

- a. Perubahan strategi perusahaan.
- b. Produk, jasa, atau infratruktur yang baru atau yang dikonfigurasi ulang.
- c. Perubahan pada produk dan jasa yang disediakan oleh penyedia jasa pihak ketiga.
- d. Kekurangan yang teridentifikasi pada *business continuity process* penyedia jasa pihak ketiga.
- e. Peraturan perundang-undangan yang baru, persyaratan ketentuan, dan praktik ketahanan.

- f. Hasil analisis *metric* operasional (misalnya indikator risiko utama, indikator kinerja utama).
- g. Indikator peringatan dini yang mengidentifikasi potensi kejadian, krisis, dan insiden (seperti bencana alam, peningkatan serangan siber, dan lain-lain).
- h. Selisih antara beban *business continuity* yang dianggarkan dan *actual*.
- i. Hasil *exercises, testing*, dan *lesson learned*.
- j. Perubahan lanskap ancaman (misalnya kemampuan baru, *intent of threat actors*).
- k. Hasil rekomendasi (misalnya dari audit, penilaian kerentanan dan *penetration test*).

*Business continuity program* harus direview untuk keakuratan dan kelengkapannya secara berkala. Beberapa area yang mungkin perlu disesuaikan antara lain:

- a. Persyaratan operasional.
- b. Persyaratan keamanan.
- c. Prosedur teknis.
- d. *Hardware, software*, dan peralatan lain.
- e. Informasi kontak anggota tim.
- f. Informasi kontak vendor.
- g. Persyaratan fasilitas alternatif dan diluar lokasi.
- h. Catatan penting (*vital records*).

Gambar 22 | Langkah-Langkah dalam rangka Ketahanan Berkelanjutan



Sumber: Diolah dari berbagai sumber

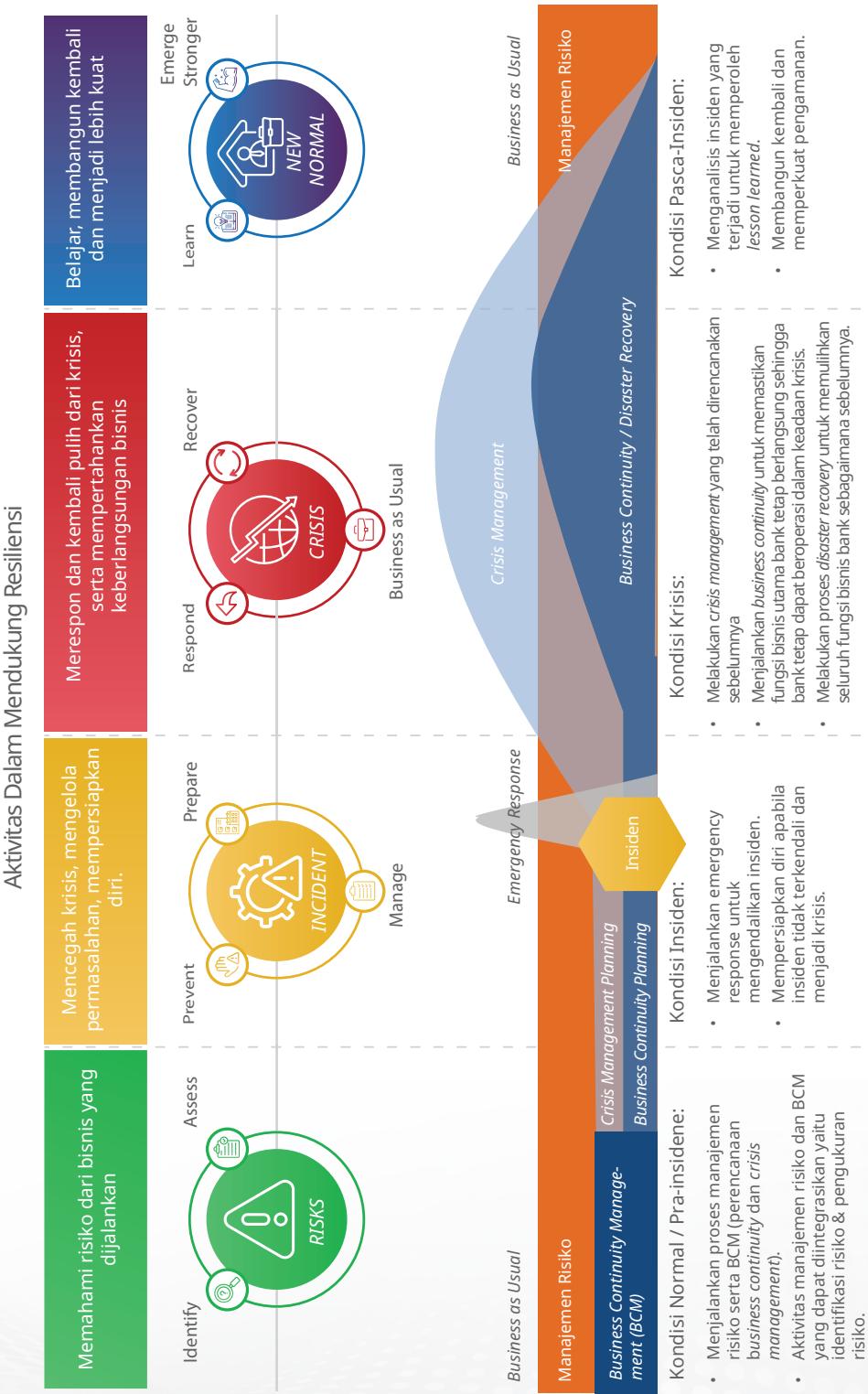
Ketika melakukan pengkinian *business continuity program*, Bank perlu mendokumentasikan semua perubahan yang terjadi kemudian melakukan analisis dan menentukan *lesson learned* dari kejadian yang merugikan (*adverse event*). Hal ini penting bagi Bank untuk dapat mempersiapkan diri menghadapi *adverse event* di masa depan. Dokumentasi tersebut antara lain mencakup:

- a. Identifikasi penyebab kejadian.
- b. Evaluasi potensi/alternatif solusi.
- c. Implementasi tindakan perbaikan secara tepat waktu.
- d. Mencatat dan mereviu tindakan perbaikan yang dilakukan.

Untuk menentukan sejauh mana perubahan *business continuity program*, SDM yang bertanggung jawab atas *business continuity program* perlu berkomunikasi secara berkala dengan tim teknis untuk menilai dampak perubahan terhadap bisnis, struktur, sistem, *software*, *hardware*, SDM, dan fasilitas.



Gambar 23 Aktivitas dalam Mendukung Resiliensi



Sumber: Deloitte (2020), diolah dan dimodifikasi

# 03

## RESILIENSI NASABAH DI ERA DIGITAL



*Customer Incident Management*



*Customer Incident Recovery*



*Customer Post-Recovery Services*



## Resiliensi Nasabah di Era Digital

Serangan siber kepada industri perbankan dilakukan melalui beberapa cara, baik secara langsung, maupun tidak langsung. Serangan siber tidak langsung dapat dilakukan menggunakan *social engineering* atau *reverse social engineering* melalui konsumen/nasabah Bank yang merupakan titik terlemah dari jaringan Bank. Tidak peduli sekuat apapun pertahanan keamanan teknologi informasi yang dimiliki Bank, serangan siber masih dapat menembus pertahanan Bank melalui nasabah. Oleh sebab itu, selain melakukan langkah-langkah untuk memperkuat resiliensi digital di internal Bank melalui peningkatan keamanan sistem maupun aktivasi rencana kelangsungan bisnis yang komprehensif, Bank perlu membekali nasabah dengan pemahaman terkait dengan bagaimana melakukan kegiatan keuangan di ruang digital, termasuk terkait keamanan siber dan keamanan dalam melakukan transaksi digital untuk meningkatkan resiliensi konsumen terhadap serangan digital yang menargetkan dirinya.

Untuk meningkatkan resiliensi konsumen, Bank perlu melakukan kebijakan berupa 1) *Customer Incident Management* sebagai langkah antisipasi terhadap serangan digital yang ditujukan kepada konsumen; 2) *Customer Incident Recovery* sebagai langkah penanggulangan atas insiden/serangan digital yang dialami konsumen dan strategi pemulihannya; dan 3) *Customer Post-Recovery Services* sebagai upaya evaluasi atas serangan digital yang terjadi pada konsumen dan langkah agar konsumen tidak mengalami serangan yang serupa di masa depan.

**A. Manajemen Insiden bagi Konsumen (*Customer Incident Management*)**

Serangkaian kebijakan/mekanisme oleh Bank yang bertujuan untuk memberikan pemahaman kepada konsumen mengenai risiko saat beraktivitas di ruang digital dan menyadari ketika dirinya berada dalam risiko/serangan digital. Kebijakan ini diharapkan dapat meningkatkan ketahanan konsumen dan nasabah Bank ketika menggunakan layanan/jasa keuangan digital atau saat melakukan transaksi digital. Untuk meningkatkan ketahanan konsumen terhadap serangan digital, Bank dapat melakukan beberapa langkah sebagai berikut:



- a. Melakukan edukasi dan sosialisasi kepada konsumen mengenai jenis-jenis risiko saat berada di ruang digital dan bagaimana cara mengelola risiko tersebut.
- b. Memberikan pemahaman mengenai penggunaan internet secara positif, tindakan yang dapat mengancam kebocoran data pribadi, dan kewajiban menjaga informasi pribadi seperti OTP, PIN, dan *password*.
- c. Memiliki ekosistem pendukung yang memadai seperti kebijakan dan prosedur terkait mekanisme pelaporan bagi konsumen yang mengalami serangan digital.
- d. *Dedicated reporting channel* bagi konsumen untuk melaporkan *fraud* dan penipuan *online*, melakukan penginventaris dan pengkinian data *fraud* dan *scam* serta melakukan koordinasi dengan otoritas dan penegak hukum dalam rangka *law enforcement*.
- e. Layanan dan format pelaporan yang *user-friendly* sesuai dengan usia konsumen.

**B.  
Pemulihan  
Insiden bagi  
Konsumen  
(Customer  
Incident  
Recovery)**

Serangkaian kebijakan/prosedur yang bertujuan untuk memberikan panduan dan mekanisme yang jelas kepada konsumen mengenai bagaimana konsumen harus bertindak ketika mereka mengalami risiko di ruang digital atau mendapatkan serangan digital. Untuk membantu konsumen yang mengalami serangan digital, Bank dapat melakukan beberapa langkah sebagai berikut:

- a. Memberikan panduan dan dukungan kepada konsumen mengenai cara bertindak / merespon serangan digital.
- b. Memberikan panduan lebih lanjut kepada konsumen mengenai pihak-pihak mana saja yang perlu dihubungi terkait serangan / risiko yang dihadapi dan memandu konsumen untuk melaporkan insiden yang dialami kepada otoritas penegak hukum.



- c. Memberikan bantuan dan pendampingan kepada konsumen yang mengalami serangan digital dengan kerugian yang signifikan.

**C.  
Layanan  
Pasca-  
Insiden bagi  
Konsumen  
(Customer  
Post-Recovery  
Services)**

Layanan pendukung bagi konsumen yang bertujuan untuk memberikan edukasi mengenai risiko-serangan digital yang dialami oleh konsumen dan membantu konsumen lebih berhati-hati agar tidak mengulangi kesalahan sebelumnya sehingga konsumen dapat terhindar dari serangan digital di masa mendatang. Bank dapat melakukan beberapa upaya sebagai berikut:

- a. Menyediakan layanan informasi bagi konsumen untuk meningkatkan pengetahuan/kemampuan menggunakan aplikasi/layanan *online* untuk mengantisipasi jika konsumen mengalami serangan/ancaman *online* di masa depan.
- b. Memberikan bantuan kepada konsumen yang pernah mengalami serangan digital dan melakukan pelaporan kepada bank, melalui notifikasi/pengingat secara berkala terkait bahaya/risiko di ruang digital dan perlunya kewaspadaan dalam bertransaksi digital.
- c. Bank melakukan rekapitulasi hasil pelaporan yang dilakukan konsumen terkait serangan digital yang dialami dan melakukan evaluasi serta menyusun strategi edukasi dan sosialisasi berdasarkan hasil analisis laporan tersebut agar konsumen dapat terhindar dari serangan serupa di masa mendatang.





*Ransomware* merupakan perangkat lunak jahat yang dirancang untuk mengenkripsi data di dalam sistem atau perangkat yang dapat menghalangi pemiliknya mengakses data tersebut. Setelah berhasil mengenkripsi data, penyerang akan menampilkan pesan tebusan yang meminta pembayaran dalam bentuk mata uang kripto, seperti Bitcoin, sebagai imbalan untuk pemulihian akses ke data yang dienkripsi. Jika tebusan tidak dibayar, data tersebut mungkin hilang secara permanen atau dapat diperjualbelikan oleh penyerang.

*Ransomware* memiliki berbagai bentuk yang dapat menyerang perangkat atau sistem. Dari sekian banyak jenis *ransomware*, terdapat 2 (dua) jenis *ransomware* utama yang cukup berbahaya dan paling sering digunakan oleh para pelaku kejahatan siber, yaitu:

1. **Leakware**, jenis *ransomware* ini menjalankan aksinya dengan mempublikasikan atau membocorkan data penting milik seseorang jika orang tersebut tidak ingin menebusnya. Jenis ini paling banyak digunakan untuk menyerang perusahaan-perusahaan besar hingga pemerintahan. Perusahaan atau lembaga yang diserang oleh virus ini biasanya bergerak di bidang layanan masyarakat yang pastinya memiliki ratusan hingga ribuan data sensitif pengguna di dalamnya. Data tersebut dapat dijadikan jaminan sekaligus ancaman bagi perusahaan apabila tidak memberikan tebusan sesuai yang diinginkan oleh pelaku.
2. **Lockers**, jenis *ransomware* ini tidak mengenkripsi data seperti yang dilakukan pada umumnya. Jenis *lockers* hanya mengunci layar perangkat pengguna dari akses ke dalam data dengan memberikan peringatan untuk menebus sejumlah uang jika ingin membuka kunci tersebut. *Lockers* merupakan bentuk tahap awal ancaman kepada

pengguna untuk melihat respons mereka. Jika tidak dipenuhi, para pelaku bisa saja melanjutkan aksinya dengan mengenkripsi data penting pengguna.

Agar terhindar dari serangan siber berupa *ransomware*, Bank perlu membangun pertahanan sistem yang kuat dan memadai. Langkah-langkah yang dapat dilakukan sebagai berikut:

1. Mengupayakan penggunaan *multi-factor authentication* untuk semua layanan, terutama untuk email web, VPN, dan akun yang mengakses sistem penting.
2. Menerapkan prinsip *least privilege* pada semua sistem dan layanan sehingga pengguna hanya memiliki akses yang diperlukan untuk melakukan pekerjaannya.
3. Menjalankan *best practice* dan mengaktifkan pengaturan keamanan yang terkait dengan lingkungan *cloud*, seperti Microsoft Office 365.
4. Mengembangkan dan melakukan update secara berkala atas diagram jaringan yang menggambarkan sistem dan aliran data dalam jaringan organisasi.
5. Menerapkan segmentasi jaringan (secara *logic* atau fisik) untuk memisahkan berbagai unit bisnis atau sumber daya TI departemen dalam organisasi serta untuk menjaga pemisahan antara TI dan teknologi operasional.
6. Memastikan organisasi memiliki manajemen aset yang komprehensif (contoh: memahami data dan sistem yang kritikal).
7. Membatasi penggunaan PowerShell untuk pengguna tertentu berdasarkan kasus per kasus. Umumnya, hanya pengguna atau administrator yang mengelola jaringan atau OS Windows yang diizinkan menggunakan PowerShell.
8. Melakukan pengamanan terhadap *Domain Controller* (DC). Pelaku ancaman sering kali menargetkan dan menggunakan DC sebagai titik awal untuk menyebarkan ransomware ke seluruh jaringan.
9. Menyimpan dan mengamankan log secara memadai dari perangkat jaringan dan *host* lokal. Hal ini mendukung triase dan remediasi peristiwa keamanan siber.
10. Membuat *baseline* dan menganalisis aktivitas jaringan selama beberapa bulan untuk menentukan pola perilaku sehingga aktivitas jaringan normal dapat lebih mudah dibedakan dari aktivitas jaringan anomali.

## DAFTAR PUSTAKA

- Bank Indonesia. 2024. "Laporan Perekonomian Indonesia Tahun 2023". *Departemen Kebijakan Ekonomi dan Moneter*, Jakarta.
- Bank of England. 2022. "Operational Resilience: Critical Third Parties to The UK Financial Sector". London.
- Brinker, Scott, and Jason Baldwin. 2020. "MARTECH 2030: Five Trends in Marketing Technology for the Decade of the Augmented Marketer." *chiefmartec.com* and WPP, Oxford.
- Capgemini Digital Transformation Institute. 2018. "The Digital Culture Challenge: Closing the Employee-Leadership Gap". *Capgemini Digital Transformation Institute*, Paris.
- CERTNZ. 2023. "Public Communications for Cyber Security Incidents: A Framework for Organisations". *New Zealand Government*, Wellington.
- Deloitte. 2020. "Tying the Knot: Integrating ERM and BCM to Improve Resiliency". *Deloitte Indonesia*, Jakarta.
- Deloitte. 2023. "Digital Resilience and Enterprise Recovery: Would your business survive a catastrophic cyber attack?". *Deloitte*, London.
- Digitaleurope. 2023. "The Digital Front Line: 15 actions to boost Europe's Digital Resilience". *Digitaleurope*, Brussels.
- Digital Government Authority of Saudi Arabia. 2023. "Guideline of The Emerging Technology Adoption". *Digital Government Authority*, Riyadh.
- Federal Financial Institutions Examinations Council (FFIEC). 2019. "Business Continuity Management". *FFIEC Information Technology Examination Handbook*. *Federal Financial Institutions Examinations Council*, Virginia.
- Garside, Debbie. 2018. "Digital Resilience – A Step Up from Cybersecurity". CSO, tersedia pada <https://www.csoonline.com/article/565945/digital-resilience-a-step-up-from-cybersecurity.html>.

- Institute for Strategy Resilience & Security University College London, and Shearwater Group. 2018. "Digital Resilience: Understanding the Challenges of Resilience in Digital Environments". *Institute for Strategy Resilience & Security University College London, and Shearwater Group*, London.
- Knight, R. & Nurse, J.R.C. 2020. "A Framework for Effective Corporate Communication after Cyber Security Incidents". *Computers & Security* (99). Elsevier.
- Monetary Authority of Singapore. 2022. "Business Continuity Management Guidelines". *Monetary Authority of Singapore*, Singapore.
- Otoritas Jasa Keuangan. 2021. "Cetak Biru Transformasi Digital Perbankan". *Departemen Penelitian dan Pengaturan Perbankan*, Jakarta.
- Perera, T. & Higgins, D. 2017. "Theoretical Overview of Known, Unknown and Unknowable Risks for Property Decisions Making. *23rd Annual Pacific Rim Real Estate Society Conference*, Sydney.
- Russell Reynolds Associates, "Digital Pulse 2018 : Organizational Structure." *Russell Reynolds Associates*, London.
- The European Parliament and The Council of The European Union. 2022. Regulation (EU) 2022/2554 on Digital Operational Resilience for the Financial Sector.
- UK Council for Internet Safety. 2019. "Digital Resilience Framework". *UK Council for Internet Safety*, London.
- Wavestone. 2020. "Navigating through the Resilience frameworks: How to Identify the Right Frameworks to Use". *Wavestone*, tersedia pada <https://www.wavestone.com/en/insight/navigating-through-the-resilience-frameworks-how-to-identify-the-right-frameworks-to-use/>.
- We are Social. 2023. "Digital 2023: Indonesia". *We are Social*, tersedia pada <https://datareportal.com/reports/digital-2023-indonesia>.
- World Economic Forum. 2024. "The Global Risk Report 2024 19<sup>th</sup> Edition". *Insight Report*. World Economic Forum, Geneva.
- World Economic Forum. 2021. "Digital Culture: The Driving Force of Digital Transformation". *Digital Culture Guidebook*. World Economic Forum, Geneva.

# **TIM PENYUSUN**

## **Pengarah**

Dian Ediana Rae  
Kepala Eksekutif Pengawas Perbankan

## **Koordinator**

Eddy Manindo Harahap  
Kepala Departemen Pengaturan dan  
Pengembangan Perbankan

## **Tim Perumus**

Mohamad Miftah | M. Zulkifli Salim  
| Citra Christina | Irawan Muhamad  
| Muhammad Radhi | Nurani Pertiwi  
Ekaputri | Norkolis Dwi Atmoko | Annisa  
Dwi Ramadhania Nasura





## Otoritas Jasa Keuangan

Menara Radius Prawiro,  
Kompleks Perkantoran Bank Indonesia  
Jl. M. H. Thamrin No. 2 Jakarta 10350