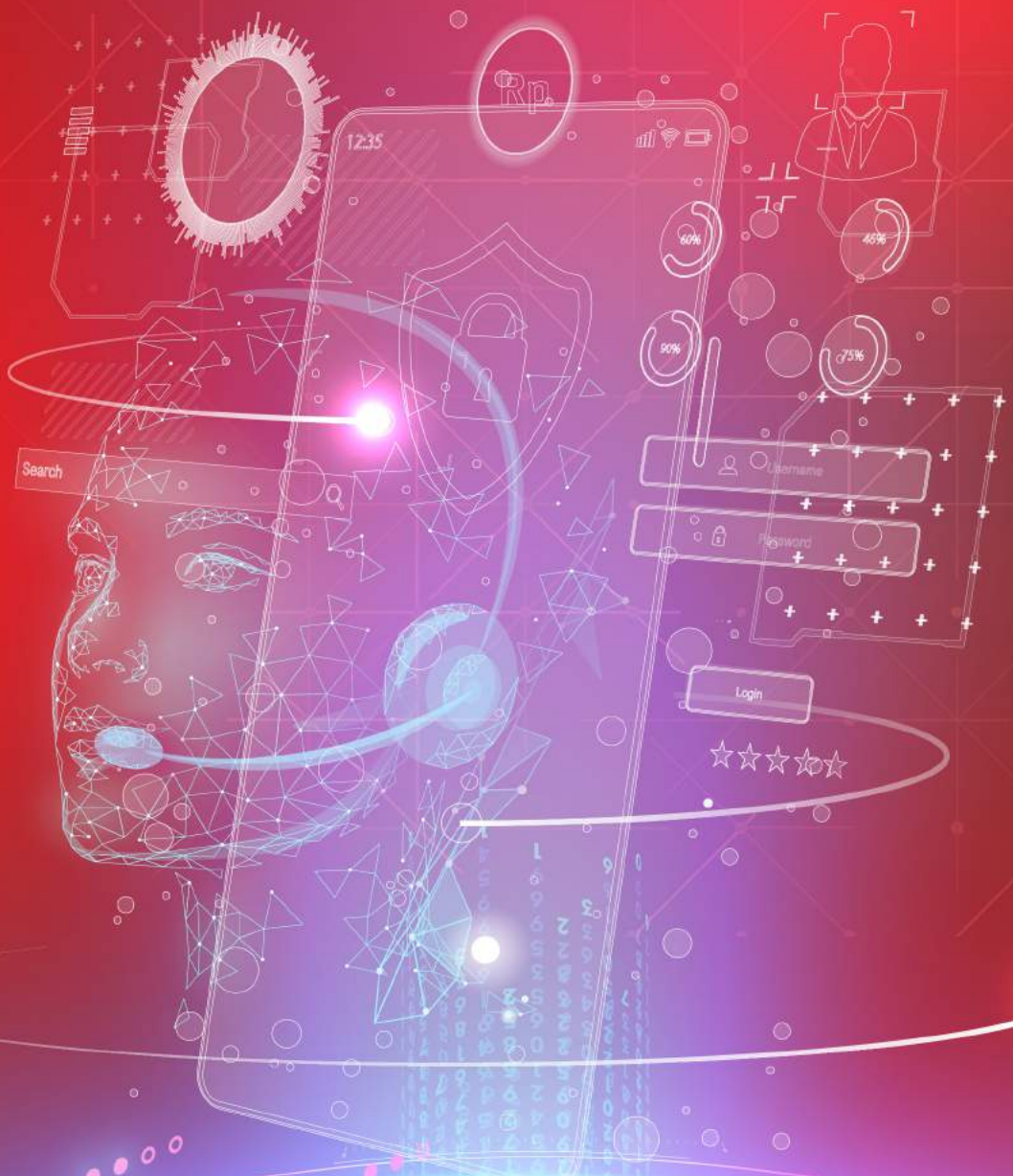
OTORITAS JASA KEUANGAN

CETAK BIRU | TRANSFORMASI DIGITAL PERBANKAN



Every well built house started in the form of a definite purpose plus a definite plan in the nature of a set of blueprints.

(Napoleon Hill)

Daftar Isi

Daftar Gambar

Daftar Grafik

Daftar Tabel

Daftar Singkatan dan Akronim

5G	*Fifth Generation*
AI	*Artificial Intelligence*
API	*Application Programming Interface*
APO	*Align, Plan, and Organize*
AR/VR	*Augmented Reality/Virtual Reality*
AS	Amerika Serikat
ASEAN	Association of Southeast Asian Nations
BAI	*Build, Acquire, and Implement*
Bappenas	Badan Perencanaan Pembangunan Nasional
Bareskrim	Badan Reserse Kriminal
BHI	Berbadan Hukum Indonesia
BI	*Business Intelligence*
BIS	Bank for International Settlements
BSSN	Badan Siber dan Sandi Negara
CDO	*Chief Data Officer*
COBIT	Control Objective for Information and Related Technology
Covid-19	*Corona Virus Disease of* 2019
DBS	Development Bank of Singapore
DFS	*Digital Financial Service*
DII	*Data Integration and Interoperability*
DMAB	*Digital Maturity Assessment for Bank*
DMM	*Digital Maturity Model*
DPIA	*Data Protection Impact Assessment*
DSS	*Deliver, Service, and Support*
EDM	*Evaluate, Direct, and Monitor*
EU GDPR	European Union General Data Protection Regulation

Fintech	*Financial Technology*
HKMA	Hong Kong Monetary Authority
HSBC	Hongkong and Shanghai Banking Corporation
IoT	*Internet of Things*
IP	*Internet Protocol*
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
KOMPAK	Kolaborasi Masyarakat dan Pelayanan untuk Kesejahteraan
KPI	*Key Performance Indicators*
KPMG	Klynveld Peat Marwick Goerdeler
KUB	Kelompok Usaha Bank
LJK	Lembaga Jasa Keuangan
MEA	*Monitor, Evaluate, and Assess*
MPSJKI	Master Plan Sektor Jasa Keuangan Indonesia
NIST	National Institute of Standards and Technology
OECD	Organisation for Economic Co-operation and Development
OJK	Otoritas Jasa Keuangan
OKR	*Objectives and Key Results*
OTP	*One-Time Password*
PIN	*Personal Identification Number*
PKS	Perjanjian Kerja Sama
Polri	Kepolisian Negara Republik Indonesia
PRA	Prudential Regulation Authority
PSD2	Payments Service Directive 2
PwC	PricewaterhouseCoopers
RBS	Royal Bank of Scotland

ROI	*Return of Investment*
RP2I	Roadmap Pengembangan Perbankan Indonesia 2020-2025
SDM	Sumber Daya Manusia
SIM	*Subscriber Identity Module* atau *Subscriber Identification Module*
SJK	Sektor Jasa Keuangan
SLA	*Service Level Agreement*
SME	*Small Medium Enterprise*
Suptech	*Supervisory Technology*
TI	Teknologi Informasi
TM Forum	TeleManagement Forum
TOGAF	The Open Group Architecture Framework
UK	United Kingdom
UMKM	Usaha Mikro, Kecil, dan Menengah
UU PDP	Undang - Undang Pelindungan Data Pribadi

Halaman Ini Sengaja Dikosongkan

Sambutan Kepala Eksekutif Pengawas Perbankan

HERU KRISTIYANA

KEPALA EKSEKUTIF PENGAWAS PERBANKAN

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, Cetak Biru Transformasi Digital Perbankan ini telah selesai kami susun dan dapat kami sajikan kepada para pemangku kepentingan sebagai panduan.

Transformasi digital di sektor perbankan adalah suatu keniscayaan. Selama beberapa tahun belakangan ini, tuntutan akselerasi digital semakin mengemuka didorong perubahan ekspektasi publik akan layanan keuangan yang cepat, efisien, dan aman serta dapat dilakukan dari mana saja. Kondisi demikian mengharuskan perbankan untuk menempatkan transformasi digital sebagai prioritas dan salah satu strategi dalam upaya peningkatan daya saing Bank.

Transformasi digital menuntut perbankan untuk mengubah pola pengelolaan dan operasional yang dilakukan. Pergeseran dari konsep *traditional bank* ke *future bank* mendorong Bank antara lain untuk menyesuaikan strategi bisnis, melakukan penataan ulang jaringan distribusi, mendorong transaksi perbankan melalui *digital channel* (*mobile app* dan internet) termasuk penggunaan perangkat perbankan elektronik terkini, dalam upaya peningkatan *customer experience* (*end-to-end digital solution*).

Seiring dengan berbagai perkembangan dalam bisnis perbankan yang bergerak dalam strategi bisnis digital, Otoritas Jasa Keuangan (OJK) memandang berbagai pengaturan *existing* perlu lebih diperkuat khususnya pengaturan yang terkait dengan teknologi informasi di sektor perbankan. OJK menyadari bahwa perkembangan teknologi yang sedemikian pesat tentunya tidak dapat diimbangi dengan pengaturan dengan pola *rule-based* yang cepat usang dan membatasi ruang gerak

perbankan untuk beradaptasi dengan perkembangan yang terjadi. Untuk itu, pengaturan akan diarahkan pada pola *principle-based*, adaptif terhadap perubahan lanskap dan ekosistem perbankan, serta berorientasi *forward-looking*. Prinsip ini ditujukan untuk memberikan ruang inovasi bagi industri agar lebih berkembang, tentunya tanpa mengkompromikan aspek prudensial.

Dalam Roadmap Pengembangan Perbankan Indonesia 2020-2025, salah satu pilar yang menjadi arah kebijakan adalah akselerasi tranformasi digital perbankan. Pilar ini dijabarkan lebih lanjut melalui Cetak Biru Transformasi Digital Perbankan. Cetak Biru Transformasi Digital Perbankan disusun dengan mengedepankan prinsip keseimbangan antara inovasi digital perbankan dan aspek prudensial untuk menjaga kinerja perbankan dalam kondisi sehat (*prudent, safe and sound banking*). Selain itu, Cetak Biru ini turut mengusung prinsip *technology neutral*, yaitu tidak mengatur aspek teknis terkait teknologi.

Cetak Biru Transformasi Digital Perbankan berisikan 5 (lima) elemen utama yaitu data, teknologi, manajemen risiko, kolaborasi, dan tatanan institusi yang perlu diperhatikan dalam proses transformasi digital perbankan. Cetak Biru Transformasi Digital Perbankan akan memberikan acuan yang lebih konkret akan digitalisasi perbankan ke depan dalam rangka akselerasi transformasi digital, sekaligus merupakan respon kebijakan untuk memitigasi berbagai tantangan dan risiko dari transformasi digital perbankan. Implementasi Cetak Biru ini diharapkan dapat mendorong perbankan nasional lebih memiliki daya tahan (*resilience*), berdaya saing, dan kontributif.

Akhir kata, saya mengucapkan penghargaan sebesar-besarnya kepada seluruh pihak yang telah terlibat dalam memberikan masukan, komentar, serta saran-saran yang sangat berharga dalam penyusunan Cetak Biru Transformasi 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 *resilience*, berdaya saing, dan kontributif.

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

HERU KRISTIYANA

Cetak Biru Transformasi Digital Perbankan: *Quick Facts*

APA ITU CETAK BIRU TRANSFORMASI DIGITAL PERBANKAN?

Cetak Biru Transformasi Digital Perbankan berisikan rancangan kebijakan OJK untuk mendorong percepatan transformasi digital perbankan di Indonesia. Cetak Biru ini diharapkan menjadi landasan dalam mengembangkan digitalisasi di perbankan nasional sehingga lebih *resilience*, berdaya saing, dan kontributif.

APA DASAR PENYUSUNAN CETAK BIRU?

Cetak Biru ini disusun sebagai pengejawantahan lebih lanjut Pilar 3 Master Plan Sektor Jasa Keuangan Indonesia (MPSJKI) 2021-2025 dan Pilar 2 Roadmap Pengembangan Perbankan Indonesia (RP2I) 2020-2025 yang telah mengarahkan perbankan untuk melakukan akselerasi transformasi digital. Penyusunan Cetak Biru ini dilakukan dengan mempertimbangkan beberapa hal antara lain analisis lingkungan strategis perbankan untuk mengetahui peluang dan tantangan digitalisasi perbankan; tingkat kematangan (*maturity level*) digitalisasi perbankan yang diukur dengan *Digital Maturity Assessment for Bank* (DMAB); masukan dari *stakeholders* dalam berbagai *focus group discussion* (FGD) dengan asosiasi, industri perbankan, dan penyedia jasa teknologi informasi; serta studi literatur, *best practices* regulasi di berbagai negara, dan standar internasional di bidang Teknologi Informasi.

PRINSIP APA YANG TERDAPAT DALAM PENYUSUNAN CETAK BIRU?

Cetak Biru ini disusun dengan mengedepankan prinsip utama "Balance" dan "Technology Neutral". *Balance* yaitu menyeimbangkan antara inovasi digital perbankan dan aspek prudensial untuk menjaga kinerja perbankan dalam kondisi sehat (*prudent, safe and sound banking*) serta menjaga kepercayaan masyarakat akan layanan perbankan digital. *Technology Neutral* yaitu tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang.

ASPEK APA SAJA YANG DIATUR DALAM CETAK BIRU?

Cetak Biru ini mencakup aspek *people*, *process*, dan *technology* yang berfokus pada 5 (lima) elemen utama yang akan memberikan kebijakan digitalisasi untuk perbankan yakni meliputi implementasi data, teknologi, manajemen risiko, kolaborasi, dan tatanan institusi pada industri perbankan. Kelima faktor tersebut merupakan langkah strategis untuk mendorong perbankan dalam menciptakan inovasi produk dan layanan keuangan yang dapat memenuhi ekspektasi konsumen dan berorientasi pada kebutuhan konsumen (*customer-centric orientation*).

Overview

Dasar Kebijakan

Arah Pengembangan Perbankan Terkait Akselerasi Transformasi Digital Perbankan

- MPSJKI 2021 – 2025
  Pilar 3: Akselerasi Transformasi Digital Sektor Jasa Keuangan
- RPI21 2020 – 2025
  Pilar 2: Akselerasi Transformasi Digital Perbankan

Current Analysis

- **Kondisi Digitalisasi Perbankan**
  - Analisis Lingkungan Strategis; *Digital Maturity Bank*
- **Harapan *Stakeholder***
  - Aturan yang memfasilitasi percepatan transformasi digital Bank
- **Studi Literatur**
  - Prediksi Perbankan Masa Depan
  - *Best Practices*
  - *International Standards*

Prinsip Penyusunan Cetak Biru

- ***Balance***
  - *Innovation Facilitation*
  - *Prudent, Safe and Sound Banking*
- ***Technology Neutral***
  - Tidak berfokus pada teknologi tertentu
- ***Transformation Element***
  - *People*
  - *Process*
  - *Technology*

Elemen

- Data
- Teknologi
- Manajemen Risiko
- Kolaborasi
- Tatanan Institusi

Akselerasi Transformasi Digital Perbankan

Bab

01

PENDAHULUAN

"The next 5 years will be more disruptive than the last 15. This is not business as usual. A lot of technology that came in three years ago doesn't work anymore."

(Saul Berman, IBM)

Lanskap perbankan di masa depan akan jauh berbeda dengan kondisi pada saat ini. Pesatnya perkembangan teknologi telah membawa perubahan radikal pada lingkungan bisnis perbankan yang terlihat dari perubahan ekspektasi konsumen, peningkatan kualitas produk dan layanan perbankan melalui pemanfaatan data, kemunculan persaingan dan kemitraan baru dengan big-tech *dan* start-up companies, *serta perubahan model operasional menjadi model bisnis digital. Perbankan dihadapkan pada perubahan dinamis terhadap 4 (empat) aspek yaitu data, adopsi teknologi informasi, model bisnis, dan regulasi. Keberhasilan Bank dalam menjaga keberlangsungan usahanya akan sangat ditentukan oleh kemampuan melakukan transformasi digital dengan mengelola keempat aspek tersebut dengan baik.*

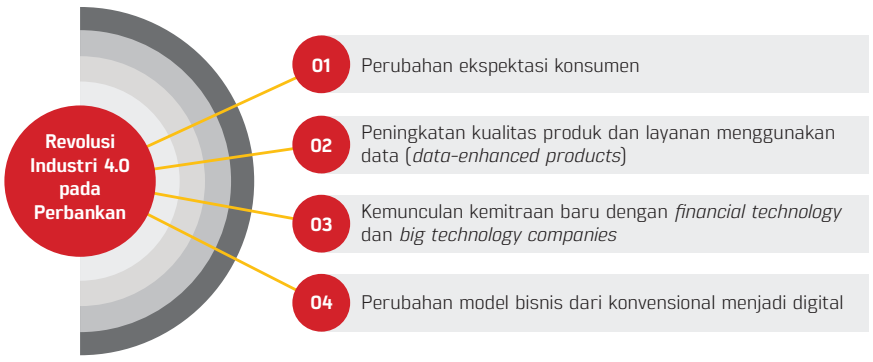
LATAR BELAKANG

Perkembangan teknologi informasi yang cepat telah membawa kehidupan masyarakat dunia memasuki era baru yang sering disebut era revolusi industri 4.0. Era ini ditandai dengan berkembangnya berbagai inovasi teknologi seperti *Internet of Things* (IoT), *Cloud Computing, Artificial Intelligence* (AI), dan *Machine Learning*. Perkembangan dan inovasi teknologi informasi telah banyak mengubah segi kehidupan manusia, mulai dari gaya hidup, dunia kerja, hingga aktivitas ekonomi masyarakat. Di samping itu, perkembangan teknologi telah mendorong munculnya beberapa model bisnis baru dengan basis digital yang jauh lebih efisien dan inovatif sehingga membawa peluang sekaligus tantangan yang perlu dikelola dengan baik.

Revolusi industri 4.0 adalah tentang transformasi digital. Dengan pergerakan digitalisasi tersebut, kegiatan ekonomi dan keuangan masyarakat seakan tidak mengenal batas ruang dan waktu. Transaksi ekonomi dapat dilakukan dimana saja, kapan saja, dan darimana saja. Hal ini telah menuntut perusahaan melakukan perubahan sehingga dapat memenuhi kebutuhan yang timbul akibat transformasi digital dalam kegiatan ekonomi dan keuangan masyarakat, untuk dapat terus bertahan.

Revolusi industri 4.0 juga telah merambah ke sektor perbankan. Revolusi ini menuntut perbankan untuk beradaptasi dan melakukan perubahan. Tuntutan perubahan signifikan di industri perbankan sebagai dampak perkembangan teknologi informasi, secara garis besar dapat diidentifikasi dalam 4 (empat) aspek yaitu perubahan ekspektasi konsumen, peningkatan kualitas produk dan layanan perbankan dengan pemanfaatan data (*data-enhanced products*); kemunculan kemitraan baru dengan *big-tech* dan *start-up companies*; serta perubahan model operasional menjadi model bisnis digital.

Gambar 1
Dampak Revolusi Industri 4.0 pada Perbankan



Perbankan harus mengedepankan nasabah di era ekonomi digital. Saat ini, konsumen perbankan mengharapkan adanya layanan perbankan yang dapat diperoleh dengan cepat melalui berbagai saluran secara aman. Selain itu, konsumen juga semakin menuntut produk dan layanan yang unik, dipersonifikasi,

dan sesuai keinginan mereka dengan berbagai keragaman serta nilai kompetitif tersendiri. Konsumen akan cenderung mengikuti tren terbaru dan mencari berbagai informasi terkait produk dan layanan, terutama melalui media sosial. Perilaku konsumen tersebut menuntut perbankan untuk terus berinovasi dan menciptakan produk dan layanan yang mengedepankan kebutuhan nasabah mereka (*consumer centric*) di era digital.

Perbankan perlu memanfaatkan *big data* dengan baik. Pada beberapa tahun terakhir di era digital, ketersediaan data telah meningkat rata-rata dua kali lipat setiap tahunnya. Volume data diprediksi mencapai kurang lebih 40.000 *exabytes* pada tahun 2020. *Big data* ini perlu digunakan dengan baik oleh perbankan untuk meningkatkan kualitas produk dan layanannya. Penggunaan *big data* menjadi cara yang paling efektif untuk mendapatkan dan menganalisis perilaku para nasabah termasuk para calon nasabah. Selain itu, penggunaan *big data* juga akan membuat perbankan mampu untuk mendeteksi suatu anomali atau perilaku menyimpang, menentukan penyebab suatu masalah atau kegagalan, dan mengambil langkah perbaikan secara cepat dan tepat sehingga dapat meningkatkan efektivitas dan efisiensi pengelolaan perbankan.

Perbankan perlu melakukan kemitraan dengan berbagai pelaku usaha digital lainnya seperti *e-commerce, bigtech, fintech, ride-hailing*, dan *online media*. Kemitraan baru tersebut akan memberikan banyak manfaat baik bagi Bank maupun nasabahnya. Bagi Bank, kemitraan akan memberikan peluang untuk meningkatkan inovasi terhadap produk-produk yang ada, termasuk juga *channel* untuk menyalurkan produk layanan mereka kepada masyarakat yang jauh lebih luas. Bagi nasabah, kemitraan tersebut akan memudahkan mereka untuk memperoleh produk dan layanan perbankan dimana saja dan kapan saja diperlukan.

Gambar 2
Perbedaan *Traditional Banks* dan *New-Age Banks*

Sumber: Capgemini (2020)

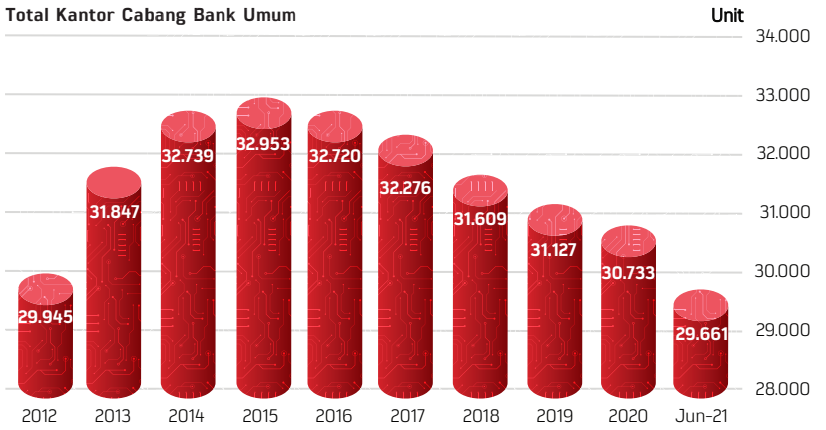
Perbankan perlu melakukan transformasi menjadi Bank Digital. Bank Digital mengedepankan pada proses bisnis yang berbasis platform dan *fully digital* (*fully digital and platform-based*) dengan struktur organisasi yang ramping dan *agile* serta memiliki kapabilitas digital yang lebih maju (*advanced digital capabilities*). Struktur organisasi yang ramping dan *agile* lebih menitikberatkan pada kolaborasi dan integrasi dengan pihak lain seperti memiliki komunitas *marketplace* yang besar dan berorientasi pada konsumen. *Advanced digital capabilities* menitikberatkan pada penggunaan teknologi yang *update* dan *agile* dengan *scalability* yang tinggi, serta bisnis model yang berbasis data dengan proses yang sederhana dan terautomasi dengan mengusung *open-platform*. Bank digital merupakan tren lanskap perbankan di masa depan.

PANDEMI COVID-19 MENDORONG PERCEPATAN DIGITALISASI PERBANKAN

Pandemi Covid-19 telah mendorong percepatan transformasi digital perbankan. Pandemi yang terjadi menyebabkan masyarakat harus beradaptasi dengan digitalisasi, terutama dengan adanya pembatasan aktivitas fisik. Masyarakat dipaksa untuk melakukan transaksi ekonomi mereka melalui platform digital. Seiring dengan hal tersebut, masyarakat juga terdorong untuk melakukan transaksi keuangan secara digital.

Dalam kondisi seperti ini, masyarakat tentunya mengharapkan layanan perbankan digital yang efektif, efisien, dan aman. Akibatnya, Bank mau tidak mau harus mempercepat peningkatan layanan digitalnya jika tidak ingin ditinggalkan nasabah.

Grafik 1 Perkembangan Jumlah Kantor Cabang Bank Umum

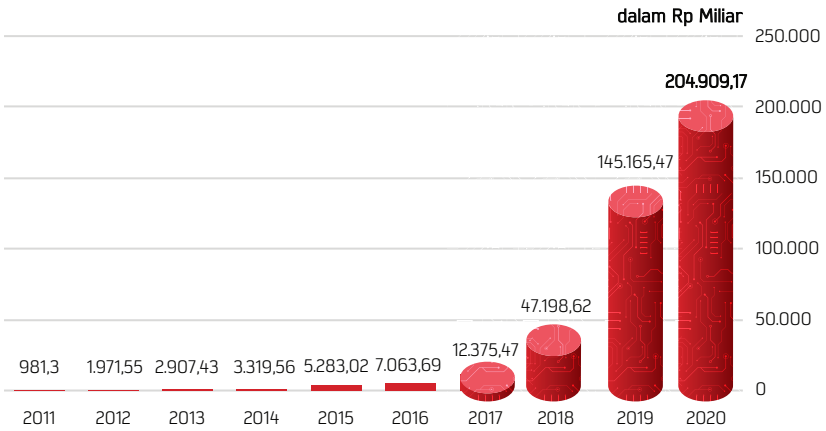


Sumber: Statistik Perbankan Indonesia, OJK (2021)

Inventure (2020) mengidentifikasi sejumlah perubahan transaksi perbankan yang terjadi selama pandemi Covid-19. Pertama, transaksi-transaksi yang awalnya banyak dilakukan di kantor cabang kini dilakukan secara digital melalui *mobile banking*, *internet banking*, ataupun *call center* yang digerakkan oleh *artificial intelligence*. Berdasarkan data statistik pada Grafik 1, dapat terlihat bahwa Bank terus menutup jaringan kantornya.

Kedua, pandemi Covid-19 mendorong konsumen mengurangi transaksi *cash*. Sebelum pandemi, tren transaksi ke arah *cashless transaction* ini sudah meningkat, namun pandemi Covid-19 mempercepat proses tersebut dengan alasan untuk mengurangi potensi penularan virus. Sementara dari sisi produsen, saat ini toko, restoran, hingga hotel mulai menggunakan *cashless transaction* sebagai alat *branding* untuk memulihkan kepercayaan konsumen dan memberikan jaminan keamanan kepada mereka. Tak hanya itu, *smartphone* dan beragam aplikasi di dalamnya kini semakin berfungsi untuk melakukan berbagai transaksi keuangan. Beragam transaksi kini dapat dilakukan melalui *smartphone*, mulai dari berbelanja, menabung, meminjam uang, membayar tagihan, membayar cicilan, dan sebagainya sehingga semakin meningkatkan

Grafik 2
Nilai Transaksi Uang Elektronik 2011-2020 (dalam Rp Miliar)

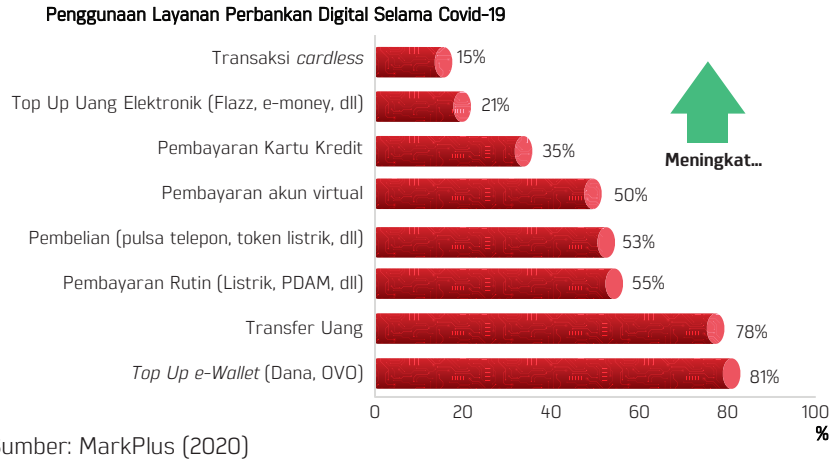


Sumber: Bank Indonesia (2020)

cashless society. Hal ini dapat dilihat dengan semakin meningkatnya transaksi uang elektronik (Grafik 2). Ketiga, selama masa pandemi, nasabah kian menuntut *seamless banking experience* melalui berbagai kanal.

Tuntutan *seamless banking experience* menyebabkan strategi *omnichannel* menjadi faktor kunci dalam memenuhi kebutuhan nasabah. Oleh karena itu, pendekatan *consumer journey*, menuntut para bankir melihat setiap titik persentuhan interaksi (*touchpoint*) sebagai sebuah *journey* yang tak terlepas satu sama lain. Artinya pendekatan yang digunakan bukan lagi *multichannel*, namun *omnichannel*. Paradigma baru ini akan menghasilkan *customer interaction* yang *seamless*.

Grafik 3
Penggunaan Layanan Perbankan Digital selama Covid-19



Sumber: MarkPlus (2020)

KONTEKS KEBIJAKAN OJK

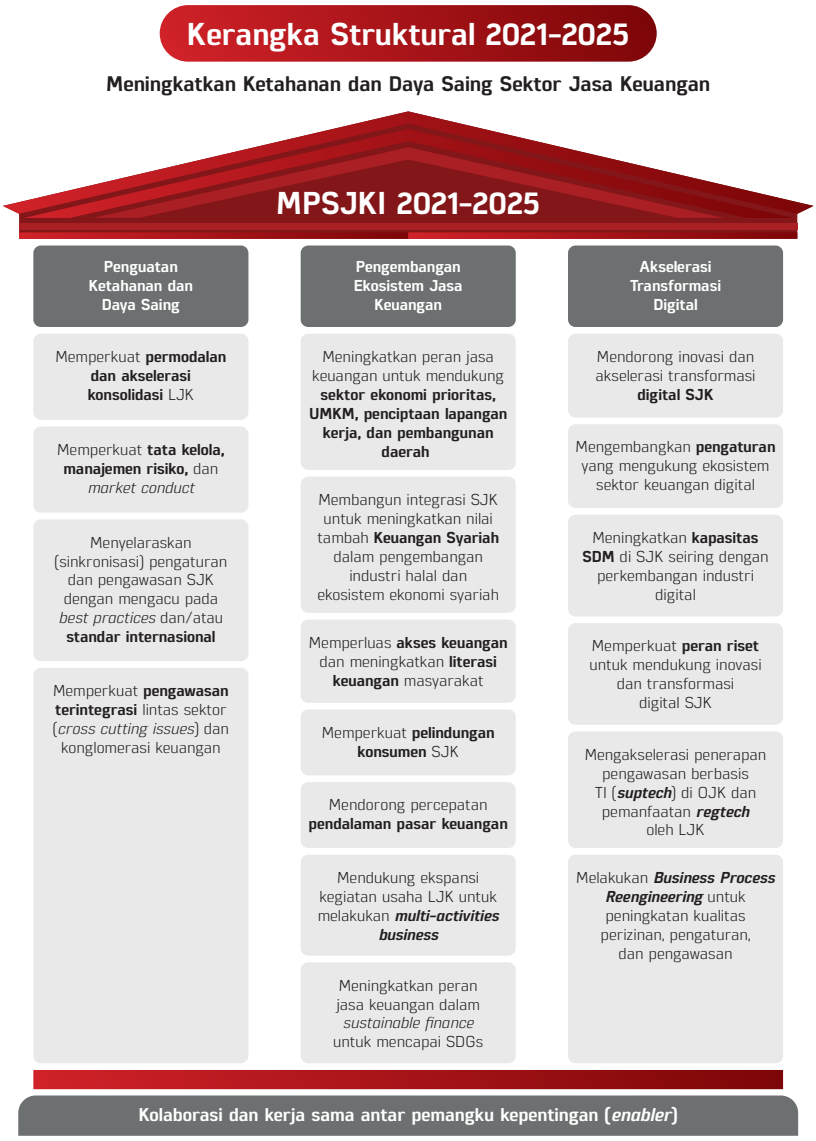
Perbankan adalah urat nadi perekonomian nasional. Perbankan menentukan aliran dana bagi sumber pembiayaan aktivitas perekonomian. Perbankan yang sehat dan stabil merupakan basis utama dalam mendorong pertumbuhan ekonomi dan meningkatkan kesejahteraan masyarakat.

OJK bertanggung jawab secara penuh dalam mengatur dan mengawasi perbankan yang sehat untuk mendukung perekonomian nasional. Revolusi 4.0 menuntut OJK untuk memahami perubahan lanskap perbankan nasional yang terjadi seiring dengan perubahan perilaku ekonomi masyarakat yang semakin ke arah digital. Transformasi digital perbankan dipandang sebagai suatu hal penting di tengah arus digitalisasi yang dapat memicu berbagai peluang bisnis yang perlu dimanfaatkan dan berbagai risiko yang perlu dimitigasi.

OJK mendorong akselerasi transformasi digital perbankan melalui beberapa kebijakan. Pada Januari 2021, OJK telah meluncurkan Master Plan Sektor Jasa Keuangan Indonesia (MPSJKI) 2021-2025 yang memiliki arah pengembangan yaitu

Penguatan Ketahanan dan Daya Saing (Pilar 1), Pengembangan Ekosistem Jasa Keuangan (Pilar 2), dan Akselerasi Transformasi Digital (Pilar 3). Pada pilar 3 MPSJKI, ditekankan bahwa Lembaga Jasa Keuangan (LJK) perlu mengakselerasi transformasi digital di dalam perusahaannya sebagai bagian dari strategi bisnis atau bahkan *core value* LJK. Akselerasi digital Sektor Jasa Keuangan (SJK) akan dicapai melalui 6 (enam) inisiatif, yaitu 1) Mendorong inovasi dan akselerasi transformasi digital SJK, 2) Mengembangkan pengaturan yang mendukung ekosistem sektor keuangan digital, 3) Meningkatkan kapasitas SDM di SJK seiring dengan perkembangan industri digital, 4) Memperkuat peran riset untuk inovasi dan transformasi digital SJK, 5) Mengakselerasi penerapan pengawasan berbasis teknologi informasi (*supervisory technology*) di OJK dan pemanfaatan *regulatory technology* (*regtech*) oleh SJK, dan 6) Melakukan *business process reengineering* untuk peningkatan kualitas perizinan, pengaturan, dan pengawasan.

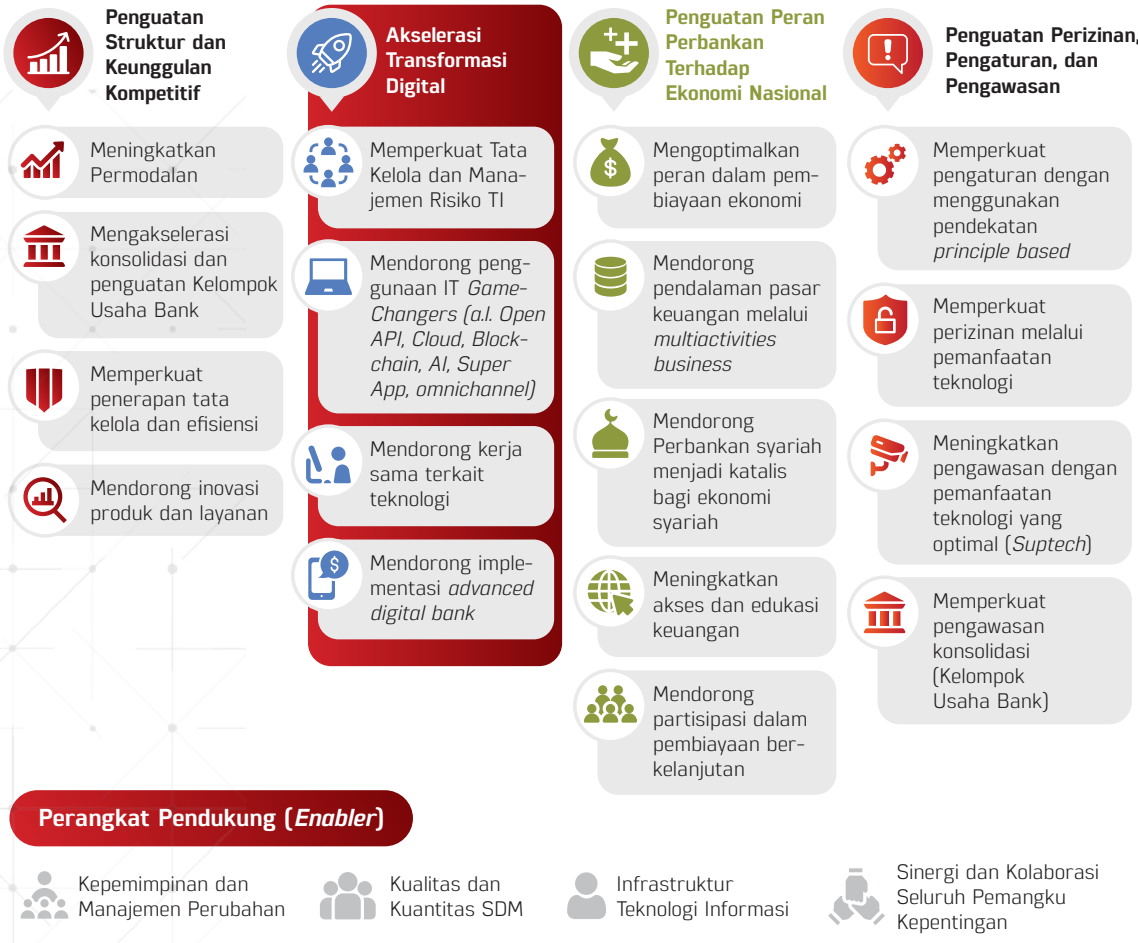
Gambar 3
Master Plan Sektor Jasa Keuangan Indonesia 2021-2025



Sumber: Master Plan Sektor Jasa Keuangan Indonesia 2021-2025

Untuk melengkapi kebijakan dalam MPSJKI, khusus untuk sektor perbankan disusun Roadmap Pengembangan Perbankan Indonesia 2020-2025 (RP2I). RP2I merupakan rancang bangun sektor perbankan sebagai suatu arah dan acuan bagi seluruh pemangku kepentingan sehingga seluruh upaya dan inisiatif dalam pengembangan perbankan ke depan dapat dilakukan dalam satu orkestra yang harmoni. Akselerasi transformasi digital menjadi salah satu arah pengembangan perbankan selama periode 2020-2025. Dalam rangka mempercepat akselerasi transformasi digital pada perbankan, beberapa inisiatif telah menjadi agenda utama untuk pencapaian tersebut. Beberapa inisiatif yang terdapat dalam Pilar 2 yaitu akselerasi transformasi digital adalah 1) Memperkuat Tata Kelola dan Manajemen Risiko Teknologi Informasi (TI), 2) Mendorong penggunaan *Information Technology* (IT) *Game-Changers*, 3) Mendorong kerja sama terkait teknologi, dan 4) Mendorong implementasi *advanced digital bank*. Untuk memberikan gambaran dan acuan yang konkret bagi perbankan, ke empat inisiatif tersebut perlu dijabarkan lebih lanjut dalam Cetak Biru Transformasi Digital Perbankan.

Gambar 4 Roadmap Pengembangan Perbankan Indonesia 2020-2025



Sumber: Roadmap Pengembangan Perbankan Indonesia 2020-2025

PENYUSUNAN CETAK BIRU TRANSFORMASI DIGITAL PERBANKAN

Sebagai bentuk tindak lanjut dari pilar ketiga MPSJKI 2021-2025 yakni akselerasi transformasi digital SJK dan pilar kedua Roadmap Pengembangan Perbankan Indonesia 2020-2025 yakni akselerasi transformasi digital perbankan, OJK mengeluarkan Cetak Biru Transformasi Digital Perbankan. Cetak Biru Transformasi Digital Perbankan ini berisi landasan kebijakan dan pengaturan dalam mendorong akselerasi transformasi digital perbankan.

Cetak Biru Transformasi Digital Perbankan disusun melalui serangkaian tahapan yang cukup panjang serta melibatkan berbagai *stakeholder* terkait perbankan seperti industri perbankan dan asosiasi perbankan. Penyusunan tersebut diawali dengan melakukan studi literatur mengenai lanskap perbankan masa depan, berbagai standar internasional di bidang teknologi informasi serta studi kebijakan dan regulasi terkait digitalisasi perbankan di berbagai negara. Selanjutnya, dilakukan analisis lingkungan strategis dengan memperhatikan faktor pendorong serta berbagai tantangan yang dihadapi oleh perbankan dalam rangka melakukan transformasi digital termasuk mengukur tingkat digitalisasi perbankan nasional dengan menggunakan *Digital Maturity Assessment for Bank*. Hasil studi literatur dan analisis lingkungan strategis kemudian diolah menjadi rancangan Cetak Biru Transformasi Digital Perbankan. Untuk menyempurnakan rancangan Cetak Biru Transformasi Digital Perbankan, secara bersamaan dilakukan serangkaian diskusi dengan *stakeholder* terkait seperti industri perbankan, asosiasi perbankan, *provider* penyedia jasa teknologi informasi, dan regulator terkait untuk menjaring aspirasi dan memperoleh masukan yang kemudian digunakan untuk penyempurnaan dan finalisasi Cetak Biru Transformasi Digital Perbankan sehingga dapat diterbitkan pada akhir 2021.

Gambar 5
Tahapan Penyusunan Cetak Biru Transformasi Digital Perbankan

Cetak Biru Transformasi Digital Perbankan disusun secara sistematis dengan mempertimbangkan beberapa aspek sebagai dasar penyusunan sebagai berikut:

01

STUDI TERKAIT PERBANKAN MASA DEPAN

Di masa depan, perkembangan teknologi informasi diprediksi akan mampu membawa Bank berevolusi dengan sangat cepat untuk dapat mengimbangi perubahan ekspektasi masyarakat dalam menggunakan layanan perbankan. Bank diprediksi akan mengalami evolusi yang cukup pesat pada aspek data, model bisnis, regulasi, dan teknologi.

02

GAMBARAN KONDISI DIGITALISASI PERBANKAN

Salah satu dasar penyusunan Cetak Biru Transformasi Digital Perbankan adalah analisis lingkungan strategis dan analisis tingkat kematangan (*maturity level*) penerapan digitalisasi dan teknologi informasi di industri perbankan Indonesia yang diukur menggunakan DMAB. Hasil analisis lingkungan strategis memberikan informasi mengenai faktor pendorong dan tantangan transformasi digital. Hasil penilaian DMAB dapat memberikan informasi mengenai aspek yang perlu ditingkatkan pada perbankan dalam mengakselerasi transformasi digital.

03

PRINSIP PENYUSUNAN CETAK BIRU TRANSFORMASI DIGITAL PERBANKAN

Cetak Biru ini disusun dengan mengedepankan prinsip utama yaitu "Balance" dan "Technology Neutral". *Balance* diartikan bahwa Cetak Biru ini dimaksudkan untuk menyeimbangkan antara inovasi digital perbankan dan aspek prudensial untuk menjaga kinerja perbankan dalam kondisi sehat (*prudent, safe, and sound banking*). *Technology Neutral* yaitu tidak terfokus pada penggunaan teknologi tertentu sehingga dapat mengikuti perkembangan pada masa yang akan datang.

04

STANDAR INTERNASIONAL

Cetak Biru Transformasi Digital Perbankan disusun dengan memperhatikan implementasi standar internasional, khususnya di bidang Teknologi dan Keamanan Informasi antara lain International Organization for Standardization (ISO), Control Objective for Information and Related Technology (COBIT), National Institute of Standards and Technology (NIST), The Open Group Architecture Framework (TOGAF), Organisation for Economic Co-operation and Development (OECD) *Principle,* dan standar internasional lainnya. Selain mengacu pada standar internasional, penyusunan Cetak Biru Transformasi Digital Perbankan juga mengadopsi regulasi dan *framework* yang diimplementasikan oleh otoritas pengawasan di negara lain seperti Australia dan Uni Eropa dengan tetap menyesuaikan dengan kondisi dan karakteristik perbankan nasional.

05

BEST PRACTICES

Penyusunan Cetak Biru Transformasi Digital Perbankan mengacu pada *international best pratices* industri perbankan untuk mendapatkan gambaran yang lebih luas terkait praktik-praktik terbaik industri perbankan khususnya di negara-negara yang telah berpengalaman dalam transformasi digital industri perbankan dengan memperhatikan kondisi perbankan nasional.

06

MASUKAN STAKEHOLDERS

Dalam proses penyusunan Cetak Biru Transformasi Digital Perbankan, dilakukan pembahasan dan diskusi dengan berbagai pihak dan seluruh pemangku kepentingan terkait, untuk menjaring aspirasi ataupun memperoleh masukan yang konstruktif yang kemudian digunakan untuk penyusunan rancangan awal pokok-pokok Cetak Biru. Selanjutnya, konsep awal Cetak Biru Transformasi Digital Perbankan yang telah disusun tersebut didiskusikan kembali dengan seluruh pemangku kepentingan terkait, untuk memperoleh masukan dalam rangka penyempurnaan dan finalisasi Cetak Biru ini.

07

HARMONISASI KEBIJAKAN/REGULASI OTORITAS TERKAIT

Transformasi digital ekonomi Indonesia khususnya transformasi digital sektor jasa keuangan dan perbankan melibatkan beberapa regulator/otoritas terkait yang memiliki kewenangan sesuai tugas dan tanggung jawabnya. Sebagai contoh, Bank Indonesia memiliki kepentingan dalam menyusun regulasi terkait sistem pembayaran sementara Badan Sandi dan Siber Negara memiliki kepentingan dalam menyusun strategi nasional terkait keamanan siber. Perbankan sebagai bagian dalam ekosistem digital tentunya perlu mematuhi berbagai regulasi yang diterbitkan oleh berbagai regulator/otoritas tersebut. Dengan demikian, harmonisasi kebijakan yang dikeluarkan oleh berbagai regulator/otoritas dengan kebijakan yang akan dituangkan dalam Cetak Biru Transformasi Digital Perbankan menjadi hal yang diperlukan agar implementasi Cetak Biru ini dapat berjalan dengan lancar.

Gmbar 6
Kerangka Penyusunan Cetak Biru Transformasi Digital Perbankan

Boks 1.

LANSKAP PERBANKAN MASA DEPAN

ASPEK PERUBAHAN LANSKAP PERBANKAN

Di masa depan, perbankan akan dihadapkan pada perubahan dinamis yang didorong oleh 4 (empat) aspek yaitu data, model bisnis, regulasi perbankan, dan adopsi teknologi informasi (KPMG, 2019).

Data

Data digunakan sebagai aset Bank untuk mengembangkan analisis prediktif dalam rangka peningkatan produk dan layanan keuangan. Di masa depan, Bank tidak hanya berfungsi sebagai tempat menyimpan uang dengan aman, tetapi juga menjadi salah satu tempat menyimpan data paling aman.

Model Bisnis

Model bisnis berbasis konvensional bergeser menjadi model bisnis berbasis platform yang terkoneksi dengan ekosistem ekonomi digital (platformikasi) melalui teknologi *application programming interface* (API)

Regulasi

Regulasi bergerak ke arah *principle-based* sehingga memberikan ruang kondusif bagi pengembangan perbankan digital dengan menyeimbangkan antara inovasi dan aspek ke hati-hatian. Fokus regulasi beralih dari produk spesifik menjadi pemantauan atas aktivitas dan hasil

Teknologi

Teknologi merupakan pendorong dan penggerak perubahan di sektor perbankan. Penggunaan a*dvanced technology* menjadi hal yang lazim.

TEKNOLOGI DISRUPTIF

Artificial Intelligence **dan** ***Machine Learning***

Distributed Ledger Technology/Blockchain

Biometrics

Cloud Computing

Internet of Things **(IoT)**

Augmented Reality/ Virtual Reality

Quantum Computing

DAMPAK TEKNOLOGI TERHADAP LANSKAP PERBANKAN

Integrasi
Setiap data yang dimiliki akan terhubung satu sama lain

Konsumen Sentris
Penggunaan teknologi untuk peningkatanan layanan pada nasabah

Personalisasi
Personalisasi layanan dengan memanfaatkan teknologi *Artificial Intelligence*

Otomatisasi
Pemanfaatan automasi untuk meningkatkan kepercayaan konsumen dan berintegrasi dengan ekosistem layanan yang lebih luas

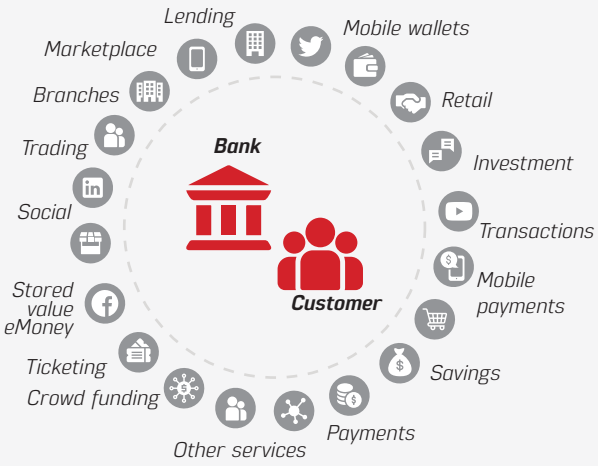
Super-App
Penyediaan platform *Super-App* atau layanan virtual yang menggabungkan intimasi, privasi, dan kontrol akses

Mata Uang DIgital
Penggunaan mata uang digital semakin sering di masa depan dengan harapan dapat meningkatkan inklusi keuangan, transparansi, permrosesan serta penyelesaian transaksi *real-time* yang lebih baik

Cyber Security
Cyber security dibangun berdasarkan analitik prediktif di seluruh perusahaan, kerentanan keamanan, dan pengenalan ancaman

Banking in 2030:
How will banks evolve?

BANKING BECOMES AN INTEGRAL PART OF DAILY LIFE



TRULY INDIVIDUALIZED CUSTOMER-CENTERED BANKING

Gambar 7 Proses Perumusan Cetak Biru Tranformasi Digital Perbankan

Dampak Revolusi Industri 4.0 pada Perbankan

- Perubahan ekspektasi konsumen
- Kemitraan baru dengan ekosistem ekonomi digital
- Pemanfaatan data untuk peningkatan kualitas produk dan layanan (*data-enhanced products and services*)
- Perubahan model bisnis dari konvensional menjadi digital

Pandemi Covid-19 Mendorong Akselerasi Transformasi Digital Perbankan

Digital Behavior
Physical Economy ⟶ Virtual Economy

- *Accelerating Digital Business Process*
- *Going Beyond Innovation*
- *Effective, Efficient, and productive*

Kerangka Penyusunan Cetak Biru

- Studi terkait Perbankan Masa Depan
- Kondisi Digitalisasi Perbankan
- Prinsip penyusunan Cetak Biru (*Balance: Inovasi* dan *prudent, safe and sound*)
- *International Standards*
- *Best Practices*
- Masukkan *Stakeholder*
- Harmonisasi dengan kebijakan/regulasi otoritas terkait

Cetak Biru Transformasi Digital Perbankan

- DATA
- TEKNOLOGI
- MANAJEMEN RISIKO
- KOLABORASI
- TATANAN INSTITUSI

CUSTOMER

Mendorong perbankan nasional lebih memiliki daya tahan (resilience), berdaya saing, dan kontributif.

Halaman Ini Sengaja Dikosongkan

Bab

02

PELUANG DAN TANTANGAN PERBANKAN DI ERA INDUSTRI 4.0

"The shift to a hyperconnected world presents a formidable opportunity–but also risks and challenges."

**(Herve Tourpe,
Chief Digital Advisor,
International Monetary Fund)**

Revolusi industri 4.0 mendorong digitalisasi dan automasi pada semua lini dalam proses bisnis perbankan sehingga di masa depan model bisnis perbankan dapat bertransformasi menjadi model bisnis digital yang menawarkan berbagai inovasi dan efisiensi bagi konsumen. Proses transformasi digital perbankan di Indonesia didukung oleh potensi digital nasional yang masih sangat besar sehingga dapat mendorong akselerasi digital pada perbankan. Namun di sisi lain transformasi digital di era industri 4.0 juga turut menghadirkan sejumlah tantangan dan risiko bagi perbankan yang perlu diantisipasi dan dimitigasi agar transformasi digital perbankan dapat memberikan manfaat yang optimal dalam meningkatkan efisiensi dan produktivitas bisnis.

FAKTOR PENDORONG TRANSFORMASI DIGITAL PERBANKAN

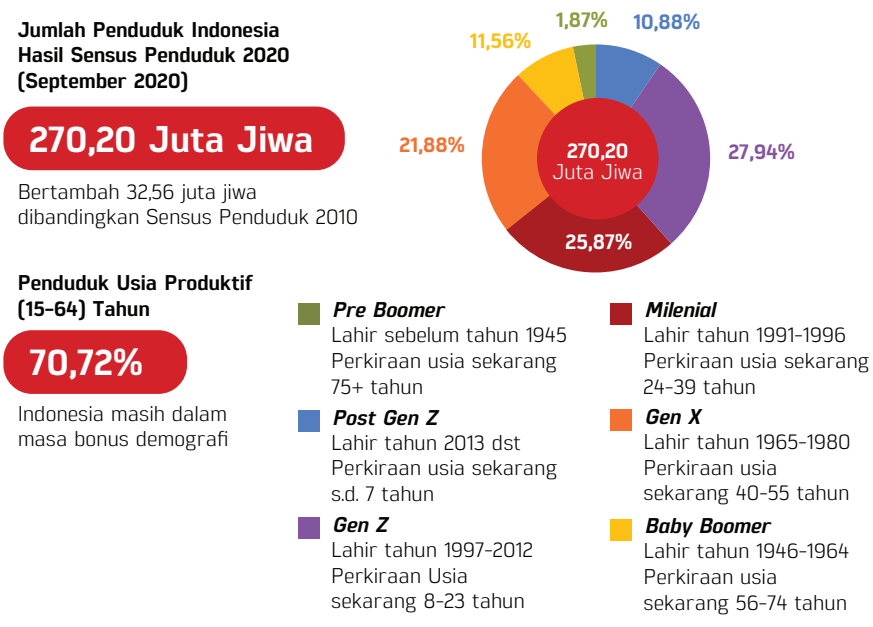
Tuntutan digitalisasi perbankan diperkuat oleh berbagai faktor pendorong pengembangan *digital bank* di Indonesia mengingat Indonesia merupakan perekonomian yang berpotensi besar untuk menyerap arus digitalisasi. Faktor pendorong tersebut tercermin dalam 3 (tiga) aspek utama yaitu peluang digital (*digital opportunity*), perilaku digital (*digital behavior*) dan transaksi digital (*digital transaction*). Peluang digital antara lain meliputi potensi demografis, potensi ekonomi dan keuangan digital, potensi penetrasi penggunaan *internet*, serta potensi peningkatan konsumen. Perilaku digital di antaranya meliputi kepemilikan gawai dan penggunaan aplikasi *mobile* (*mobile apps*). Transaksi digital meliputi transaksi perdagangan *online* (*e-commerce*), transaksi *digital banking*, transaksi uang elektronik, dan penurunan jumlah kantor cabang Bank.

PELUANG DIGITAL (*DIGITAL OPPORTUNITY*)

POTENSI DEMOGRAFIS

Indonesia merupakan negara dengan populasi penduduk terbesar keempat di dunia. Lebih dari 70% populasi penduduk Indonesia berada di rentang usia produktif (15 hingga 64 tahun). Struktur demografi Indonesia didominasi oleh Generasi Z, Generasi Milenial, dan Generasi X sehingga memiliki segmen konsumen paling prospektif. Dominasi ketiga generasi tersebut yang notabene lebih cepat beradaptasi dengan perkembangan teknologi merupakan kesempatan emas bagi Bank untuk bertransformasi menjadi *digital bank* yang diharapkan dapat menawarkan produk dan layanan yang akan memenuhi kebutuhan dan ekspektasi konsumen.

Gambar 8
Struktur Demografis Indonesia

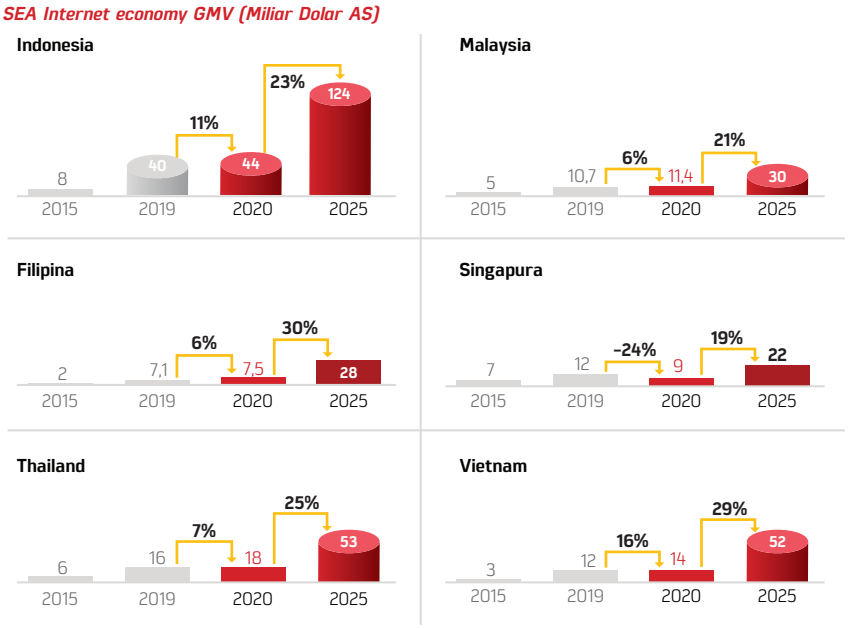


Sumber : Sensus Penduduk 2020 (Badan Pusat Statistik)

POTENSI EKONOMI DAN KEUANGAN DIGITAL

Menurut Bain, Google, dan Temasek (2020), Indonesia berpeluang menjadi negara dengan perkembangan ekonomi digital terbesar di kawasan Asia Tenggara. Nilai transaksi ekonomi digital Indonesia merupakan yang tertinggi di kawasan ASEAN yakni mencapai US$44 miliar dan diprediksi akan mencapai US$124 miliar pada tahun 2025. Potensi ini merupakan peluang yang perlu dimanfaatkan oleh perbankan Indonesia untuk meningkatkan basis konsumen melalui penyediaan produk dan layanan yang berbasis digital.

Grafik 4
Perkembangan Ekonomi Digital di ASEAN

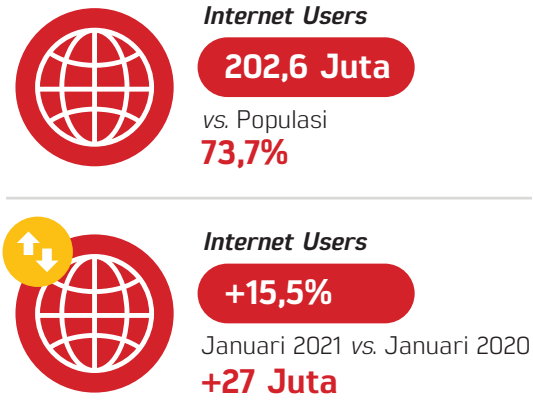


Sumber : Bain, Google, dan Temasek (2020)

POTENSI PENETRASI PENGGUNAAN INTERNET

Arus digitalisasi di Indonesia didukung oleh tingkat penetrasi penggunaan internet yang terus meningkat. Menurut laporan We Are Social dan Hootsuite (2021), penetrasi pengguna internet di Indonesia telah mencapai 202,6 juta jiwa atau 73,7% pada Januari 2021, meningkat 15,5% dari Januari 2020. Hal ini menunjukkan bahwa gelombang digitalisasi terus berkembang di tengah masyarakat Indonesia yang tercermin dari semakin tingginya tingkat pemanfaatan dan penggunaan internet. Potensi ini merupakan peluang yang menjanjikan bagi para pelaku bisnis digital untuk menciptakan produk dan layanan berbasis teknologi informasi. Bagi perbankan, peluang ini menjadi kesempatan sekaligus pengingat agar segera melakukan akselerasi transformasi digital untuk dapat mempertahankan dan memperluas basis konsumen.

Gambar 9
Tingkat Penggunaan Internet di Indonesia

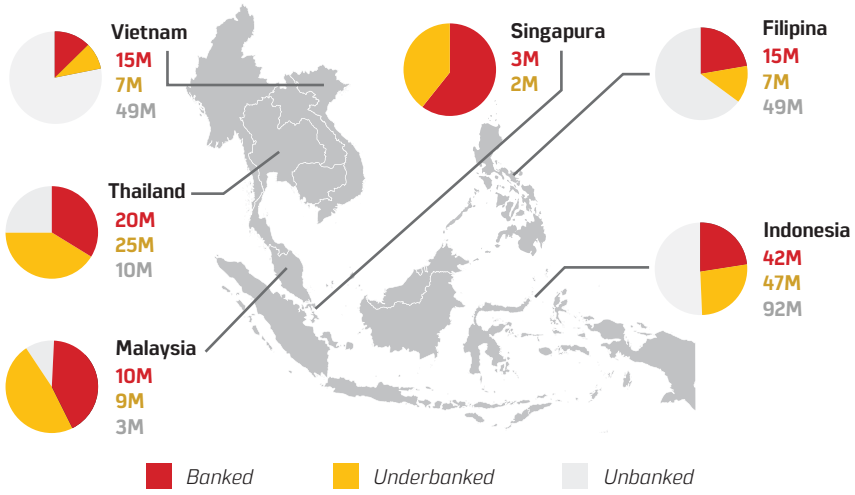


Sumber : We Are Social dan Hootsuite (2021)

POTENSI PENINGKATAN KONSUMEN

Berdasarkan hasil riset Bain, Google, dan Temasek (2019), sebagian besar masyarakat Indonesia belum memiliki rekening di Bank (*unbanked*) dan memiliki keterbatasan akses terhadap layanan keuangan (*underbanked*) dengan jumlah masing-masing mencapai 92 juta jiwa dan 47 juta jiwa. Angka ini merupakan yang terbesar di Kawasan ASEAN. Sementara jumlah masyarakat yang telah memiliki rekening di Bank (*banked*) baru mencapai 42 juta jiwa. Dengan dominasi generasi Z, milenial, dan X dalam struktur kependudukan Indonesia yang lebih menyukai kenyamanan transaksi *online* melalui platform digital, maka kesenjangan yang cukup tinggi antara *banked* dan *underbanked/ unbanked* ini menjadi suatu ceruk yang menjanjikan bagi Bank untuk mengubah strategi pemasaran dari konvensional menjadi digital.

Gambar 10
Komposisi Kelompok *Unbanked, Underbanked,* dan *Banked* di Kawasan ASEAN



Sumber : Bain, Google, dan Temasek (2019)

PERILAKU DIGITAL (*DIGITAL BEHAVIOR*)

KEPEMILIKAN GAWAI

Kepemilikan gawai seperti *mobile phone, smartphone,* laptop, tablet, dan *smartwatch* menjadi salah satu indikator kesiapan masyarakat untuk beralih ke saluran digital mengingat kepemilikan gawai memungkinkan penggunanya untuk dapat melakukan berbagai aktivitas ekonomi dan keuangan secara mandiri melalui perangkat. Menurut laporan We Are Social dan Hootsuite (2021), pengguna internet yang memiliki *mobile phone* di Indonesia telah mencapai 98,3%, adapun presentase pengguna internet yang memiliki gawai lainnya seperti laptop, tablet, dan *smartwatch* masing-masing sebesar 74,7%, 18,5%, dan 13,3%.

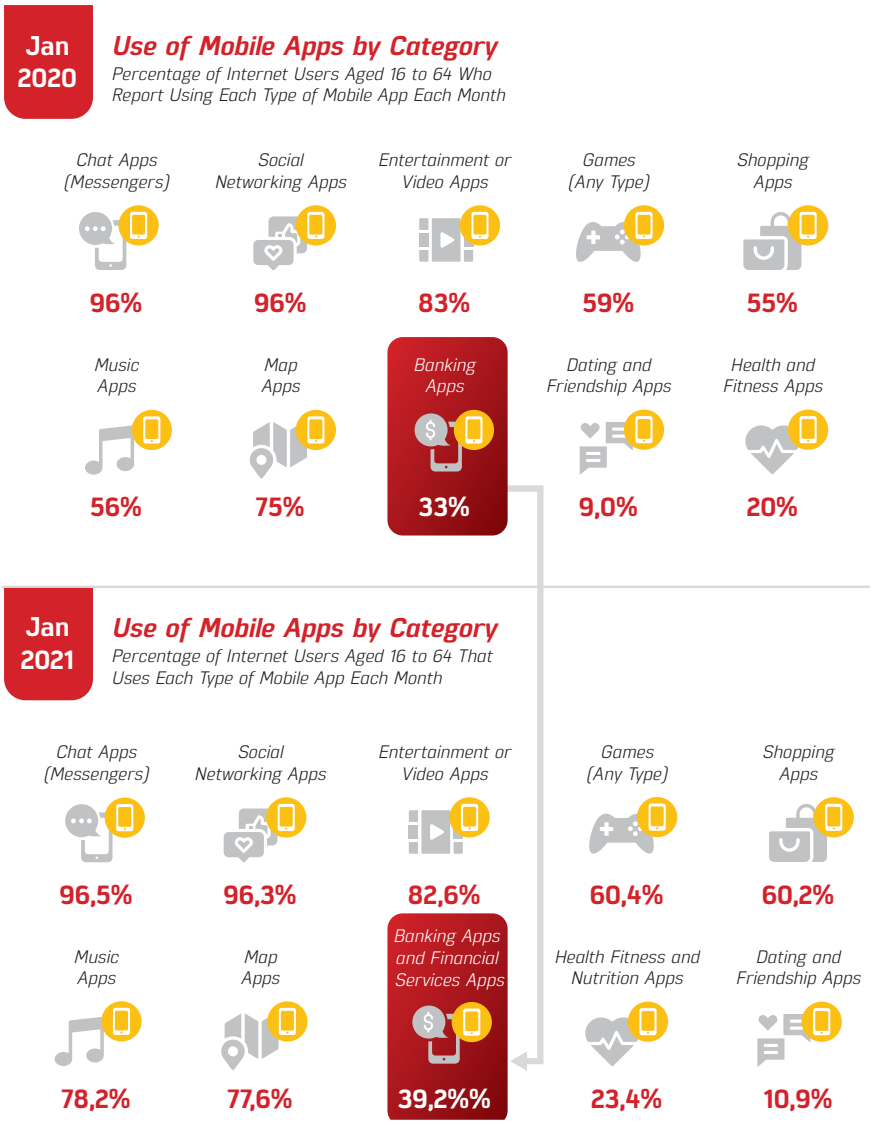
Gambar 11
Kepemilikan Gawai di Indonesia

Sumber : We Are Social dan Hootsuite (2021)

POTENSI PENGGUNAAN APLIKASI MOBILE (*MOBILE APPS*)

Digitalisasi perbankan di Indonesia juga didorong oleh peningkatan penetrasi internet dan penggunaan gawai di masyarakat yang memungkinkan semakin banyak masyarakat mengakses aplikasi daring untuk memudahkan aktivitas sehari-hari, seperti aplikasi *chatting*, media sosial, aplikasi belanja *online* (*shopping apps*), dan aplikasi perbankan (*banking apps*). Menurut laporan We Are Social dan Hootsuite (2021), sebagian besar pengguna internet berusia antara 16 hingga 64 tahun mengakses aplikasi *chatting*, media sosial, dan aplikasi belanja *online* dengan presentase di atas 90%. Sedangkan penggunaan *banking apps* baru sebesar 39,2%. Meskipun demikian, angka ini meningkat dari tahun 2020 yang hanya sebesar 33%. Peningkatan ini menunjukkan bahwa semakin banyak pengguna internet yang mulai beralih menggunakan *banking apps* dalam bertransaksi keuangan. Semakin meningkatnya penetrasi internet dan jumlah pengguna aktif *smartphone* maka jumlah pengguna *banking apps* berpeluang untuk semakin bertambah.

Gambar 12
Tingkat Penggunaan Aplikasi *Mobile* (*Mobile Apps*) di Indonesia

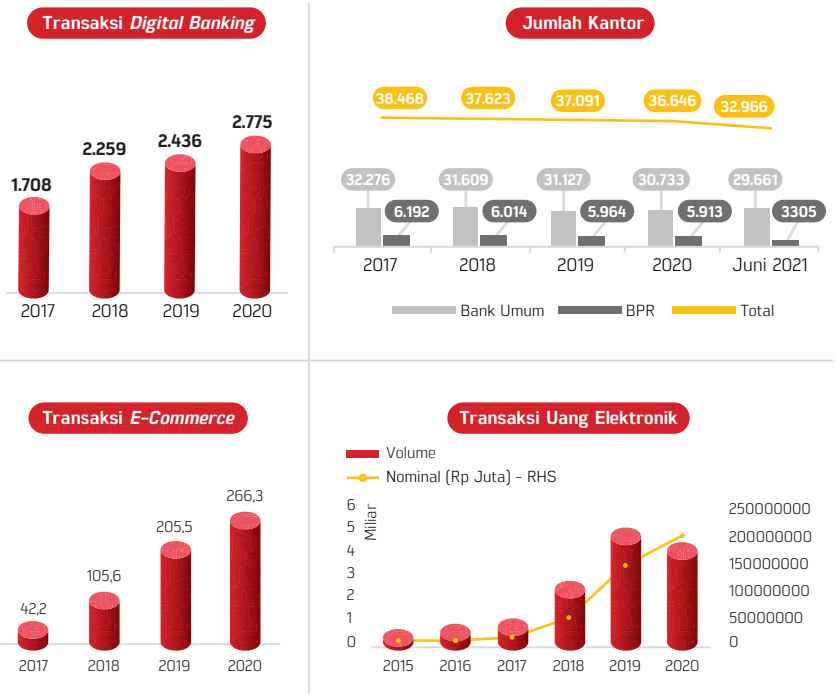


Sumber : We Are Social dan Hootsuite (2021)

TRANSAKSI DIGITAL (*DIGITAL TRANSACTION*)

Dorongan potensi digital dan perilaku digital secara langsung berdampak pada peningkatan tren transaksi digital yang terefleksi dari tren kenaikan transaksi *e-commerce*, *digital banking*, dan uang elektronik dalam beberapa tahun terakhir. Hal ini menunjukkan bahwa masyarakat sudah mulai beralih dari transaksi *offline* menjadi transaksi *online* bahkan sebelum terjadi pandemi Covid-19. Peningkatan transaksi secara digital juga dapat tercermin dari tren penurunan jumlah kantor Bank. Pada Juni 2021, tercatat terdapat 29.661 kantor cabang Bank Umum. Angka ini menurun dari 5 (lima) tahun sebelumnya yang berjumlah 32.276 kantor cabang pada tahun 2017.

Grafik 5
Perkembangan Transaksi Digital di Indonesia



Sumber: Bank Indonesia dan Statistik Perbankan Indonesia OJK (2020)

TANTANGAN TRANSFORMASI DIGITAL PERBANKAN

Di samping membawa peluang yang dapat dimanfaatkan oleh industri perbankan, transformasi digital memunculkan tantangan yang perlu diwaspadai. Beberapa tantangan tersebut mencakup pelindungan data pribadi dan risiko kebocoran data, risiko investasi teknologi yang tidak sesuai dengan strategi bisnis, risiko penyalahgunaan teknologi *artificial intelligence*, risiko serangan siber, risiko alih daya, perlunya dukungan kesiapan tatanan institusi yang berorientasi digital, inklusi keuangan bagi penyandang disabilitas, literasi keuangan digital yang masih rendah, infrastruktur teknologi informasi yang belum merata di Indonesia, dan dukungan kerangka regulasi.

Tantangan

- Pelindungan dan pertukaran data pribadi nasabah yang belum dijamin Undang-Udang
- Risiko strategis, investasi IT yang tidak sesuai strategi bisnis
- Risiko serangan siber
- Kesiapan organisasi dalam mendukung transformasi digital (*talent, leader* digital, budaya, desain organisasi)
- Risiko kebocoran data nasabah
- Risiko penyalahgunaan teknologi (penyalahgunaan *artificial intelligence*)
- Risiko pihak ketiga (*outsourcing*)
- Infrastruktur jaringan komunikasi
- *Regulatory Framework* yang mendukung

PELINDUNGAN DATA PRIBADI DAN RISIKO KEBOCORAN DATA

Pelindungan data pribadi nasabah sangat mempengaruhi perkembangan layanan perbankan digital. Pelindungan tersebut merupakan faktor penentu akan adanya kepercayaan daring (*online trust*) yang menjadi hal penting dalam transaksi digital. Data pribadi nasabah menjadi sebuah hal yang penting karena pengguna dalam jaringan tidak akan melakukan transaksi digital apabila merasa keamanan data pribadi nasabah terancam. Salah satu pelindungan data pribadi tersebut berkenaan dengan bagaimana data nasabah tersebut akan diproses, termasuk data sensitif dari nasabah yang apabila disebarkan atau dipertukarkan kepada pihak yang tidak bertanggung jawab akan berpotensi menimbulkan kerugian finansial bagi nasabah Bank. Ancaman-ancaman yang timbul dari lemahnya pelindungan data pribadi nasabah tersebut memiliki korelasi garis lurus dengan perkembangan layanan perbankan digital.

European Union General Data Protection Regulation (EU GDPR) merupakan sebuah peraturan tentang pelindungan data pribadi yang diterapkan bagi seluruh perusahaan di dunia yang menyimpan, mengolah, dan memproses data pribadi penduduk dari 28 negara yang tergabung dalam Uni Eropa. Regulasi ini memiliki tujuan untuk memberikan pelindungan terhadap kerahasiaan data (*data privacy*) dalam ekonomi digital saat ini dengan memberikan keleluasaan lebih bagi individual terhadap datanya dan memberikan peraturan yang lebih ketat kepada pihak yang mengelola atau menyimpannya. Peraturan ini berlaku tidak hanya bagi perusahaan di Uni Eropa tetapi seluruh perusahaan di dunia yang menyimpan personal data penduduk Uni Eropa. Peraturan tersebut kemudian menjadi model bagi Undang-Undang nasional di luar Uni Eropa.

Perusahaan-perusahaan Eropa yang beroperasi di Indonesia patuh kepada aturan EU GDPR, karena di dalamnya juga diatur terkait kegiatan perusahaan Eropa di luar wilayah Uni Eropa. Namun, sejumlah perusahaan lokal Indonesia justru belum sama sekali mengadopsi kebijakan pelindungan data pribadi dalam kebijakan internalnya (Reynaldi dan Tifana, 2020). Belum tersedianya payung hukum yang mengatur terkait pelindungan data pribadi menjadi alasan utama mengapa perusahaan lokal belum selaras dengan aturan pelindungan data. Dalam konteks industri perbankan ke depan, dengan semakin tingginya dorongan akan integrasi layanan perbankan digital dalam sistem ekonomi digital, adopsi regulasi internasional mengenai pelindungan data pribadi untuk konsumen perbankan menjadi penting. Dengan adanya aturan yang mampu memberikan pelindungan bagi konsumen Bank serta aturan yang mengatur bagaimana Bank mengumpulkan, memproses, dan melakukan

pertukaran data konsumen, diharapkan dapat meningkatkan kepercayaan konsumen dalam menggunakan layanan perbankan digital.

Sebaliknya, ketidakhadiran regulasi yang mengatur pelindungan data akan menimbulkan ancaman terkait privasi dan pengelolaan data pribadi seperti kebocoran data. Ancaman kebocoran data semakin mengemuka seiring dengan semakin berkembangnya ekonomi digital di Indonesia. Sepanjang tahun 2020, telah terjadi serangkaian kasus kebocoran data, baik yang dialami pemerintah maupun perusahaan swasta seperti platform *e-commerce*. Kasus kebocoran data ini terjadi sejak bulan Mei hingga November 2020.

Gambar 13 Rangkuman Kasus Kebocoran Data selama Tahun 2020 - 2021

Tokopedia
Sebanyak 91 juta data pengguna dan lebih dari tujuh juta data merchant Tokopeda dikabarkan dijual di situs gelap (*dark web*). Data pengguna Tokopedia yang dijual mencakup *gender*, lokasi, *username*, nama lengkap pengguna, alamat *e-mail*, nomor ponsel, dan *password*.

BPJS Kesehatan
kebocoran 279 juta data penduduk yang dibobol dari halaman BPJS Kesehatan. Data penduduk yang bocor ini dijual ke forum *online* Raid Forums. Data tersebut berisi NIK, nomor ponsel, *e-mail*, alamat, dan gaji.

Bhinneka.com
Sekelompok peretas dengan nama ShinyHunters mengklaim telah menjual 1,2 juta data pelanggan Bhinneka.com. ShinyHunters kabarnya menjual 1,2 juta pengguna Bhinneka.com tersebut dengan banderol 1.200 dollar AS atau sekitar Rp 17,8 juta pada Mei 2020 lalu.

Daftar Pemilih Tetap (DPT) Pemilu 2014
Jutaan data kependudukan milik warga Indonesia diduga bocor dan dibagikan lewat forum komunitas *hacker*. Data yang dihimpun mencakup sejumlah informasi sensitif, seperti nama lengkap, nomor kartu keluarga, Nomor Induk Kependudukan (NIK), tempat dan tanggal lahir, alamat rumah, serta beberapa data pribadi lainnya.

KreditPlus
Data pribadi milik sekitar 890.000 nasabah milik Kreditplus diduga bocor dan dijual bebas di forum terbuka yang biasanya digunakan sebagai kanal untuk pertukaran *database* hasil peretasan, Raidforums. Adapun *database* ini menghimpun sejumlah data pribadi pengguna yang terbilang cukup sensitif, di antaranya seperti nama, alamat e-mail, kata sandi (*password*), alamat rumah, nomor telepon, data pekerjaan dan perusahaan, serta data kartu keluarga (KK).

Cermati
Sekitar 2,9 juta data pengguna platform *fintech*, Cermati, dikabarkan diretas dan dijual secara bebas melalui forum *hacker* bersama 34 juta data dari 17 perusahaan lain. Data pengguna Cermati yang dijual bebas mencakup nama lengkap, NIK, NPWP, alamat, nomor telepon, rekening, nama ibu kandung pengguna, hingga pekerjaan data pengguna. Cermati tersebut dijual seharga 2.200 dollar AS.

ShopBack
ShopBack mengaku menemukan adanya akses ilegal ke sistem yang memuat data pengguna.

RedDoorz
5,8 juta data pengguna RedDoorz yang dijual seharga 2.000 dollar AS atau sekitar Rp 28,2 juta rupiah pada November 2020 lalu. Data tersebut dijual di situs Raid Forum yang bisa diakses secara terbuka. Data pengguna RedDoorz yang bocor mencakup nama, *e-mail*, *password bcrypt*, foto profil, *gender*, hingga nomor ponsel.

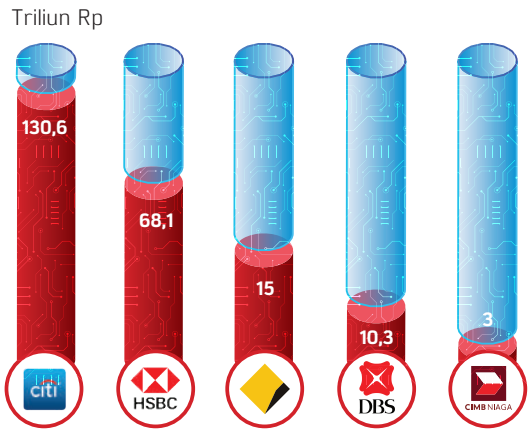
Sumber: http://tekno.kompas.com dan http://nasional.okezone.com (2021)

Ancaman kebocoran data juga dapat terjadi pada perbankan. Perbankan memiliki jutaan data nasabah. Demi keperluan transaksi perbankan, Bank meminta data nasabah atau calon nasabah. Di sisi lain, nasabah tentunya tidak punya pilihan selain memercayakan data kepada Bank. Dengan demikian, sudah seharusnya Bank menjaga kepercayaan tersebut dengan mencegah terjadinya kebocoran data nasabah. Kebocoran data nasabah Bank dapat menyebabkan kerugian keuangan bagi nasabah dan juga kerugian keuangan dan penurunan reputasi Bank. Kebocoran data nasabah dapat disebabkan oleh peretasan sistem Bank atau unsur kesengajaan dalam bentuk penjualan data nasabah oleh pegawai Bank. Banyaknya jumlah data yang dikelola oleh Bank harus diimbangi dengan upaya penguatan dalam pengamanan data agar tidak mudah diretas. Pengelolaan data nasabah juga perlu disertai dengan manajemen dan tata kelola data yang baik untuk menghindari penyebaran data nasabah oleh pegawai Bank.

RISIKO INVESTASI TEKNOLOGI INFORMASI YANG TIDAK SESUAI STRATEGI BISNIS

Digitalisasi adalah suatu keniscayaan yang tidak dapat dihindari sehingga transformasi digital menjadi kunci bagi perbankan untuk dapat bertahan dan bersaing di era revolusi industri 4.0. Penyediaan infrastruktur teknologi informasi untuk mendukung transformasi digital tentunya memerlukan investasi yang tidak sedikit. Sebagai contoh bank-bank besar mengalokasikan belanja modal untuk pengembangan teknologi informasi dalam jumlah besar.

Gambar 14
Belanja Teknologi Beberapa Bank Tahun 2019



Sumber: Laporan Tahunan 2019 masing-masing Bank, diolah

Mengingat besarnya belanja modal untuk teknologi informasi maka Bank perlu menyusun strategi yang tepat dalam mengembangkan teknologi informasi dengan mempertimbangkan *cost and benefit*. Strategi tersebut harus menjadi bagian dalam rencana strategis bisnis Bank secara keseluruhan. Rencana strategis teknologi informasi dan strategi bisnis Bank yang

berjalan secara silo akan berdampak pada ketidaksesuaian produk dan layanan Bank dengan kebutuhan dan ekspektasi pasar sehingga berujung pada kegagalan Bank.

Pengalaman beberapa Bank Digital di UK seperti Bó dan Monzo memberikan pelajaran yang berharga mengenai pentingnya keselarasan antara strategi teknologi informasi dengan strategi bisnis Bank (BNM, 2021). Bó ditutup setelah 6 (enam) bulan diluncurkan dan hanya berhasil merekrut sekitar 11.000 pengguna karena produk dan layanan yang ditawarkan tidak memiliki *uniqe selling point* untuk membedakan dengan produk dan layanan serupa yang ditawarkan oleh Bank Digital lain.

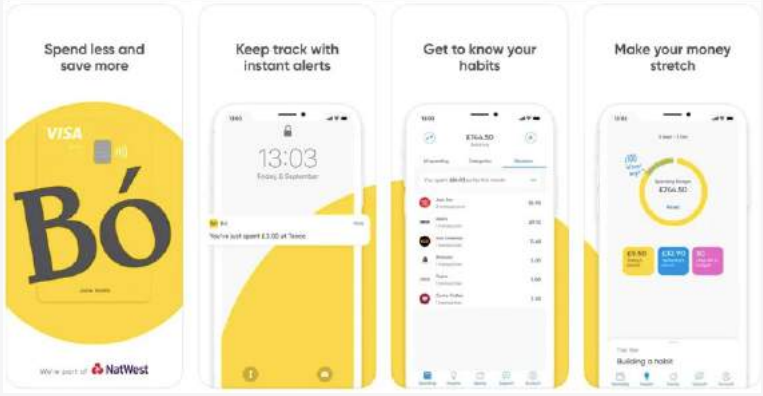
Sedangkan, Monzo mengalami kerugian yang luar biasa karena mengembangkan produk akun premium yang tidak mampu menghasilkan pendapatan sehingga menimbulkan kerugian sebesar US$131 juta. Penyebab kerugian lainnya dari Monzo adalah adanya ekspansi besar ke pasar Amerika Serikat yang tengah mengalami kontraksi hampir 33% pada kuartal kedua tahun 2020 sebagai dampak dari pandemi Covid-19. Dengan demikian, agar tetap bertahan Monzo bergantung pada monetisasi 4,3 juta nasabah yang sudah dimilikinya dibandingkan memperluas pasar baru. Pengalaman tersebut menunjukkan bahwa ekspansi teknologi informasi dalam rangka transformasi digital tidak menjamin profitabilitas bagi Bank apabila tidak diselaraskan dengan strategi bisnis utama Bank dan manajemen risiko yang memadai.

Boks 2.

LESSON LEARNED KEGAGALAN BANK DIGITAL DI INGGRIS

Digitalisasi merupakan suatu keniscayaan. Namun transformasi menjadi Bank Digital tidak menjamin profitabilitas Bank jika tidak disertai dengan *business plan* yang jelas dan manajemen risiko yang baik.

Bo

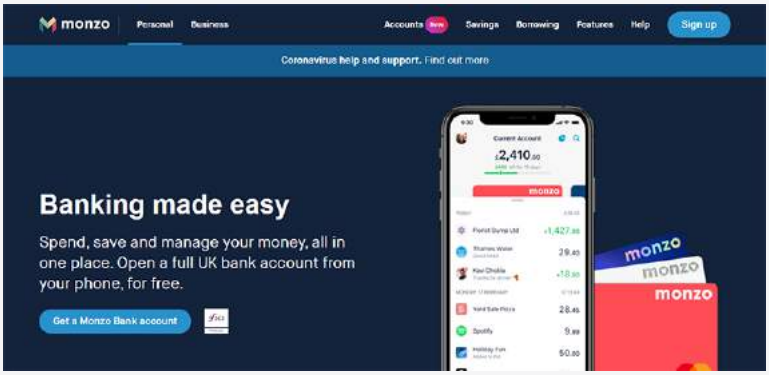


Royal Bank of Scotland (RBS) meluncurkan Bo pada November 2019 sebagai salah satu layanan Bank Digital. Langkah ini bertujuan agar dapat bersaing dengan *financial technology start-up* seperti Monzo, Revolut, dan Starling yang telah memperoleh jutaan nasabah dengan cepat. Bo memiliki fokus memberikan tips "money-saving" bagi nasabah. Sebelum menghentikan kegiatan usahanya, Bo memiliki jumlah nasabah sebanyak 11.000 nasabah. Namun, pada awal 2020, RBS menyatakan bahwa Bo akan menutup usahanya. Kenapa hal tersebut bisa terjadi? Pertama, kurangnya *engagement* Bo dengan nasabahnya. *Engagement* dengan nasabah menjadi poin penting bagi *digital bank*. Di samping itu, Bo tidak memiliki diferensiasi produk dengan *digital bank* lain yang beroperasi di Inggris. Hal ini disebabkan karena persaingan Bank Digital di Inggris yang kompetitif dan ketat membuat ekspektasi nasabah sangat tinggi. Buruknya *engagement* ini terlihat dari *feedback* nasabah yang masih rendah. Ulasan aplikasi Bo di App Store mendapat rating 3.2 dari 5.

Kedua, pengembangan teknologi informasi yang tidak memadai sehingga banyak mengalami permasalahan. Unit IT (*information technology*) pada Bank Bo harus fokus untuk mengatasi *bug* pada sistem IT nya.

Terakhir, pengembangan IT Bo sangat bergantung pada satu orang. Ketika orang tersebut meninggalkan Bo maka pengembangan IT maupun bisnis Bo menjadi terhambat secara keseluruhan.

Monzo



Monzo adalah salah satu *digital bank* pertama yang diluncurkan di Inggris pada tahun 2015. Sejak awal diluncurkan, Monzo memiliki hampir lima juta nasabah. Pada tahun 2020, Monzo mengalami kerugian yang cukup signifikan karena mengembangkan produk akun premium yang tidak mampu menghasilkan pendapatan. Produk akun premium yang ditawarkan oleh Monzo bukan merupakan strategi terbaik untuk mendapatkan pendapatan yang berkelanjutan untuk menutupi biaya yang dikeluarkan Monzo yang berasal dari *hiring*, *marketing*, dan pengembangan produk. Menurut pengamat, Monzo seharusnya berfokus untuk mengembangkan produk pinjaman dan *wealth management service*. Selain itu, keputusan ekspansi besar ke pasar Amerika Serikat juga merupakan salah satu penyebab kerugian yang dialami oleh Monzo, dikarenakan ekonomi Amerika Serikat terkontraksi hampir 33% pada kuartal kedua tahun 2020.

RISIKO PENYALAH-GUNAAN TEKNOLOGI *ARTIFICIAL INTELLIGENCE*

Teknologi diciptakan untuk mempermudah dan membantu berbagai kegiatan yang biasa dilakukan oleh manusia. *Artificial intelligence* diprediksi akan menjadi teknologi kunci di masa depan yang akan menggantikan banyak peran manusia. *Artificial intelligence* bekerja dengan cara menggabungkan sejumlah data spesifik, pengolahan yang berulang, serta algoritma cerdas sehingga *artificial intelligence* memungkinkan perangkat lunak dapat belajar dengan cara otomatis dari pola atau fitur yang ada dalam data. Meskipun *artificial intelligence* diharapkan dapat membawa manfaat signifikan di berbagai bidang kehidupan, namun perdebatan mengenai risiko yang ditimbulkan oleh *artificial intelligence* masih berlangsung hingga saat ini.

Industri perbankan tanah air perlu memahami dengan benar mengenai mekanisme kerja *artificial intelligence* agar dapat dimanfaatkan secara luas dengan tetap mengantisipasi risiko yang dapat ditimbulkan. Di sektor perbankan, *artificial intelligence* telah dimanfaatkan pada beberapa bidang antara lain otomatisasi beberapa pekerjaan (mendeteksi *fraud,* transaksi *money laundering*, atau *decision engine* proses pengajuan kartu kredit). Pemanfaatan *artificial intelligence* tersebut membawa pengaruh positif pada operasional bisnis Bank khususnya peningkatan efisiensi Bank akibat otomatisasi pekerjaan. Namun demikian, potensi penyalahgunaan *artificial intelligence* yang dapat merugikan konsumen Bank cukup tinggi. Beberapa risiko *artificial intelligence* yang teridentifikasi antara lain bias algoritma, *deepfakes*, dan kemampuan membuat keputusan sendiri.

Gambar 15 Risiko Penggunaan *Artificial Intelligence*

Sumber: McKinsey (2019) dan European Parliament Researches Services (2021)

01

Bias Algoritma

Bias algoritma merujuk pada kesalahan algoritma yang terjadi secara sistematik dan berulang sehingga memperoleh hasil yang tidak objektif (*unfair*). Hasil *unfair* dapat diartikan hasil yang secara sistematis memberikan preferensi khusus atau kurang menguntungkan bagi individu/grup/kelompok tertentu sementara tidak terdapat perbedaan yang relevan antara kelompok yang membenarkan preferensi atau kerugian tersebut. Bias algoritma dapat disebabkan oleh 2 (dua) faktor utama. Pertama, bias data. *Dataset* yang tidak mencukupi atau representasi data yang berlebihan pada beberapa kelompok orang daripada yang lain untuk melatih algoritma akan menghasilkan prediksi model yang tidak objektif. Kedua, bias manusia. Manusia sebagai perancang algoritma dapat menuangkan preferensi tertentu pada kriteria atau model yang dibangun sehingga prediksi model yang dihasilkan dapat tidak objektif. Contoh bias algoritma pada perbankan antar lain algoritma untuk penilaian peringkat kredit (*credit rating*) tidak mempertimbangkan kriteria debitur yang relevan atau menggunakan dengan representasi berlebihan pada kelompok debitur tertentu menghasilkan permohonan kredit debitur untuk kelompok tertentu ditolak.

02

DEEPFAKES

Deepfakes merupakan kemampuan untuk menghasilkan gambar, teks, dan audio sintetis untuk meniru identitas orang lain secara *online.* Deepfakes dapat dipergunakan untuk profil seseorang yang tampak sangat nyata. *Deepfakes* dapat disalahgunakan untuk melanggar privasi konsumen dan berakhir pada pembobolan akun konsumen terutama apabila teknologi informasi menggunakan sistem pengenalan wajah (*face recognition*) sebagai metode autentifikasi.

03

KEMAMPUAN MEMBUAT KEPUTUSAN SENDIRI

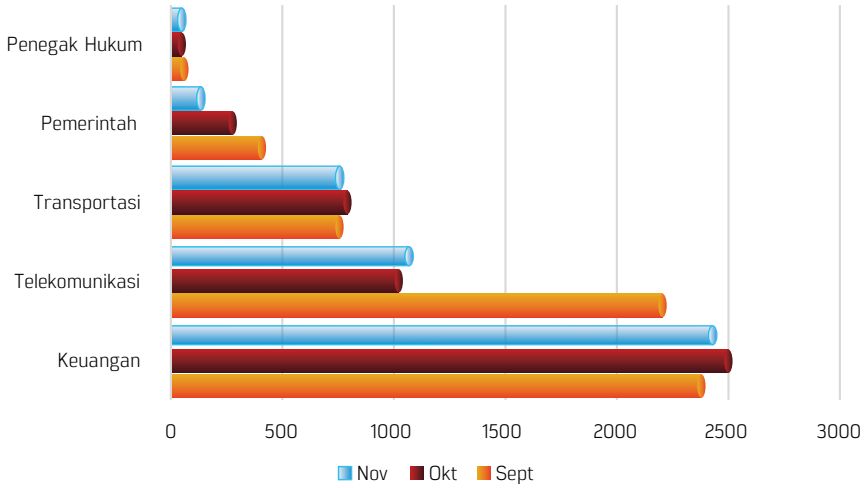
Artificial intelligence cenderung memiliki kemampuan untuk membuat keputusan sendiri dari data masif yang dimilikinya. Keputusan yang dihasilkan *artificial intelligence* dapat tidak sesuai dengan tujuan awal dari pengembangan *artificial intelligence* itu sendiri. Keputusan tersebut dapat berakibat buruk bagi Bank maupun nasabah Bank.

RISIKO SERANGAN SIBER

Serangan siber merupakan salah satu ancaman yang perlu diwaspadai di era industri 4.0. Serangan siber terus meningkat setiap tahunnya dan menyebabkan kerugian yang cukup besar. Data dari Pusat Operasi Keamanan Siber Nasional BSSN menunjukkan bahwa sepanjang tahun 2020 terjadi 495 juta serangan siber atau naik 5 (lima) kali lipat dibanding tahun sebelumnya sebesar 228 juta serangan siber.

Jika dibandingkan dengan berbagai serangan siber yang terjadi, secara global sektor keuangan merupakan sektor yang paling sering terkena insiden siber. Adapun serangan siber yang ditargetkan untuk sektor perbankan memiliki tujuan terhadap motif ekonomi. Berbagai kasus serangan siber di Indonesia kerap terjadi di industri perbankan dengan memanfaatkan *social engineering*, OTP *Fraud*, SIM *Swap*, kelemahan pada sistem Bank, dan *phishing*.

Grafik 6
Serangan Siber Berdasarkan Industri Tahun 2020



Sumber: Pusat Operasi Keamanan Siber Nasional BSSN (2021)

Berdasarkan Laporan Penerapan Strategi *Anti Fraud* periode Semester I 2020 – Semester I 2021, terdapat 7.087 laporan kejadian *fraud* yang dilakukan dengan menggunakan siber, dimana 45% kejadian *fraud* tersebut dilaporkan pada Semester II 2020. Dari jumlah tersebut, mayoritas kejadian *fraud* dengan menggunakan siber (71,6%) dilaporkan terjadi pada Bank Umum milik Pemerintah, disusul oleh Bank Swasta (28%), dan Bank Asing (0,3%). Jenis *fraud* dengan penggunaan siber yang memiliki persentase terbesar adalah jenis Tindakan Lain (48%), yang diikuti dengan Kecurangan (42%).

Jika ditinjau dari pihak yang dirugikan, didominasi oleh Bank dengan 77% dari total kejadian, 20% dialami oleh Nasabah, dan sisanya dialami oleh Pihak Lain sebesar 3%. Kerugian Riil yang dialami Bank Umum dilaporkan sebesar Rp246,5 miliar, *potential loss* sebesar Rp208,5 miliar, dengan nilai *recovery* sebesar Rp302,5

miliar. Kerugian Riil yang dialami nasabah Bank dilaporkan sebesar Rp11,8 miliar, *potential loss* sebesar Rp4,5 miliar, dengan nilai *recovery* sebesar Rp8,2 miliar. Kerugian Riil yang dialami Pihak Lain dilaporkan sebesar Rp9,1 miliar, *potential loss* sebesar Rp3,8 miliar dengan nilai *recovery* sebesar Rp3,8 miliar.

RISIKO ALIH DAYA (*OUTSOURCING*)

Bank seringkali mengalihdayakan teknologi informasi kepada pihak ketiga. Keputusan untuk mengalihdayakan teknologi informasi dilakukan oleh Bank, mengingat implementasi dan operasionalisasi IT *banking system* merupakan hal yang kompleks dan membutuhkan pengkinian informasi yang berkelanjutan sehingga akan lebih efektif dan efisien apabila ditangani oleh pihak yang memiliki keahlian dan kemampuan mumpuni terkait teknologi informasi. Namun demikian, kegiatan alih daya (*outsourcing*) berpotensi meningkatkan risiko yang dihadapi Bank sehingga penyerahan sebagian pelaksanaan pekerjaan tersebut harus dilakukan dengan menerapkan prinsip kehati-hatian dan manajemen risiko yang memadai. Beberapa potensi risiko yang dapat timbul dari kegiatan alih daya antara lain risiko strategis, risiko operasional, risiko regulasi dan kepatuhan, risiko reputasi, serta risiko konsentrasi.

01 RISIKO STRATEGIS

Risiko strategis yang dapat timbul dari kegiatan alih daya (*outsourcing*) antara lain:

a. Pekerjaan yang dilakukan oleh pihak penyedia jasa tidak sejalan dengan tujuan alih daya (*outsourcing*) dan strategi Bank secara keseluruhan.

b. Bank tidak memiliki parameter dan alat evaluasi yang jelas dalam menilai pekerjaan yang dilakukan pihak ketiga sehingga pengawasan dan *monitoring* yang dilakukan Bank tidak efektif.

02 RISIKO OPERASIONAL

Risiko operasional yang dapat timbul dari kegiatan alih daya (*outsourcing*) antara lain:

a. Gangguan atau kerusakan pada sistem/teknologi informasi yang dialihdayakan kepada pihak lain sehingga berdampak pada terhambatnya kegiatan operasional Bank.

b. Kemampuan keuangan Bank tidak memadai untuk memenuhi kewajiban.

03
RISIKO REGULASI DAN KEPATUHAN

Risiko regulasi dan kepatuhan yang dapat timbul dari kegiatan alih daya (*outsourcing*) antara lain:

a. Pihak penyedia jasa tidak memahami ketentuan/regulasi terkait dengan pekerjaan yang diserahkan Bank.

b. Pihak penyedia jasa tidak memiliki sistem kepatuhan dan kontrol internal yang memadai.

04
RISIKO REPUTASI

Risiko reputasi yang dapat timbul dari kegiatan alih daya (*outsourcing*) antara lain:

a. Standar layanan kepada konsumen Bank dari pihak penyedia jasa tidak sesuai dengan standar pelayanan Bank.

b. Layanan yang buruk dari pihak penyedia jasa kepada konsumen sehingga menimbulkan ketidakpuasan konsumen dan menurunkan reputasi Bank.

05
RISIKO KONSENTRASI

Risiko konsentrasi yang dapat timbul dari kegiatan alih daya (*outsourcing*) antara lain:

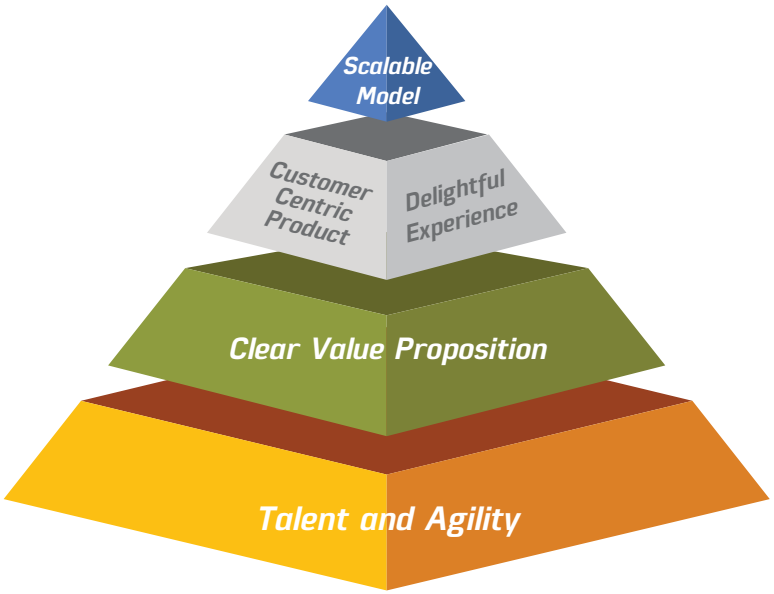
a. Gangguan sistemik yang terjadi akibat beberapa Bank menggunakan pihak penyedia jasa teknologi informasi yang sama.

b. Kegiatan alih daya (*outsourcing*) yang bersifat material terkonsentrasi pada satu perusahaan penyedia jasa sehingga ketika terjadi gangguan pada pihak penyedia jasa, maka kegiatan operasional dan layanan Bank tidak dapat berjalan.

KESIAPAN TATANAN INSTITUSI DI ERA DIGITAL

Transformasi digital tidak hanya membawa perubahan dalam aspek pemanfaatan teknologi informasi tetapi turut mendorong penyesuaian pada aspek tatanan institusi yang lebih berorientasi digital. Tatanan institusi merupakan elemen pendukung yang sangat penting bagi suatu organisasi. Tatanan institusi berperan penting dalam penciptaan nilai perusahaan (*organization value*) yang menjadi arah dan strategi bagi perusahaan dalam menjalankan kegiatan bisnisnya. Dalam konteks transformasi digital perbankan, pemanfaatan teknologi canggih dalam proses bisnis Bank perlu diimbangi oleh transformasi atas tatanan institusi secara keseluruhan, termasuk dari segi manajemen, struktur, kelembagaan, dan kualitas sumber daya manusia. Menurut laporan McKinsey (2021), terdapat beberapa langkah fundamental yang perlu dilakukan dalam membangun bisnis yang berorientasi digital, yang tercermin dalam 5 (lima) *interconnected building blocks* mulai dari langkah paling mendasar sebagai berikut:

Gambar 16
Interconnected Building Blocks untuk Membangun Bisnis Digital



Sumber: McKinsey (2021), dimodifikasi

01

TALENTA DAN *AGILITY* (*TALENT AND AGILITY*)

Dalam membangun bisnis digital, Bank perlu memiliki aset utama (*core asset*) sebagai pondasi awal seperti data, aplikasi/perangkat lunak, infrastruktur teknologi canggih, dan talenta digital (*digital talent*) yang memberikan keunggulan kompetitif. Kepemilikan aset utama tersebut memungkinkan Bank untuk merancang atau mengembangkan produk dan layanan berbasis teknologi informasi yang sesuai dengan tren dan kebutuhan pasar, sehingga meningkatkan keunggulan kompetitif dan daya saing, serta memberikan amunisi bagi Bank agar dapat bertahan di tengah ketatnya persaingan bisnis digital.

02

PROPOSISI NILAI SECARA JELAS (*CLEAR VALUE PROPOSITION*)

Pemanfaatan teknologi canggih dan mutakhir yang tidak diimbangi dengan analisis kebutuhan dan preferensi yang dapat memberikan nilai tambah bagi konsumen tidak dapat menjamin kesuksesan Bank dalam menyediakan layanan jasa keuangan kepada konsumen. Dalam merumuskan strategi bisnis digital, langkah pertama yang perlu dilakukan Bank adalah melakukan identifikasi kebutuhan dari berbagai pemangku kepentingan terkait produk dan layanan jasa keuangan yang sekiranya belum terpenuhi oleh pasar.

03

MENCIPTAKAN PRODUK DAN PENGALAMAN YANG MENYENANGKAN (*DELIGHTFUL PRODUCT AND EXPERIENCE*)

Dalam merancang produk dan layanan keuangan berbasis digital, Bank perlu menghasilkan produk dan layanan yang berorientasi pada pengguna (*human-centered design*) dan dipersonalisasi dengan menyesuaikan pada kebutuhan, kenyamanan, dan karaktersistik konsumen untuk menciptakan *customer engagement* dan *customer experience.* Desain produk dan layanan yang berorientasi pada pengguna merupakan proses yang berkelanjutan sepanjang siklus hidup produk dan layanan tersebut, sehingga Bank dituntut untuk mengadopsi model bisnis yang *agile*, melakukan riset dan pengembangan aplikasi dalam waktu singkat, serta melakukan

pengujian (*testing*) dalam rangka penyesuaian/pengembangan produk dan layanan agar tetap sesuai dengan kebutuhan konsumen yang dinamis.

04

MENCIPTAKAN PRODUK YANG SESUAI KEBUTUHAN KONSUMEN (*CUSTOMER-CENTRIC PRODUCT*)

Produk yang sesuai dengan kebutuhan konsumen merupakan kunci dari keberhasilan Bank dalam menjalankan bisnis digital. Untuk dapat menciptakan produk yang sesuai kebutuhan konsumen, selain melakukan riset mengenai kebutuhan konsumen, Bank perlu melibatkan keahlian dan talenta di bidang teknologi canggih dalam merancang produk dan layanan perbankan. Dengan kata lain, Bank perlu mengadopsi *hybrid model* dalam menciptakan budaya kerja lintas fungsi dengan mengkombinasikan keahlian dan talenta di bidang keuangan serta keahlian dan talenta di bidang teknologi untuk merancang dan menghasilkan produk dan layanan yang *robust* dan sesuai dengan ekspektasi nasabah.

05

MODEL YANG TERUKUR (*SCALABLE MODEL*)

Untuk dapat menyediakan produk dan layanan yang sesuai dengan keinginan pasar yang bergerak secara dinamis, Bank perlu melakukan eksplorasi dari berbagai model bisnis untuk menemukan model bisnis yang paling tepat dan sesuai dengan kebutuhan pasar. Eksplorasi model bisnis memungkinkan Bank untuk melakukan *trial and error* dalam rangka menemukan berbagai opsi dan alternatif agar produk yang ditawarkan Bank lebih bersifat "a must-have" bukannya "nice-to-have".

INKLUSI KEUANGAN BAGI PENYANDANG DISABILITAS

Inklusi keuangan merupakan salah satu kunci keberhasilan pembangunan ekonomi suatu negara. World Bank (2008) mendefinisikan inklusi keuangan sebagai ketiadaan hambatan, baik dalam bentuk harga maupun non-harga, dalam penggunaan layanan keuangan. Oleh karena itu, aksesibilitas sektor keuangan menjadi poin penting untuk mewujudkan sistem keuangan yang inklusif.

Penyandang disabilitas merupakan salah satu kelompok masyarakat yang mengalami kerentanan secara ekonomi karena berbagai keterbatasan yang dialami. Berbagai keterbatasan yang dimiliki oleh penyandang disabilitas berdampak pada

rendahnya tingkat inklusi keuangan penyandang disabilitas. Rendahnya akses penyandang disabilitas terhadap sektor keuangan merupakan salah satu faktor yang dapat menghambat peningkatan perekonomian penyandang disabilitas.

Perkembangan teknologi memberikan kemudahan, tak terkecuali untuk penyandang disabilitas. Beberapa fasilitas yang menggunakan teknologi seharusnya membuat segala sesuatu terintegrasi dan terjangkau bagi siapa saja. Namun, tidak semua layanan berbasis teknologi yang dijumpai sehari-hari ramah bagi penyandang disabilitas. Hasil studi yang dilakukan Bappenas, OJK, KOMPAK, dan DEFINIT (2017) menunjukkan bahwa sebanyak 84,47% lembaga jasa keuangan di tingkat pusat tidak memiliki kebijakan khusus terkait pelayanan keuangan kepada penyandang disabilitas. Selain itu, sebanyak 91,26% lembaga jasa keuangan di tingkat pusat tidak memiliki Petunjuk Teknis Operasional (PTO) khusus terkait pelayanan keuangan kepada penyandang disabilitas. Di tingkat daerah, studi tersebut juga menunjukkan bahwa sebanyak 88,57% lembaga jasa keuangan tidak memiliki kebijakan khusus terkait pelayanan keuangan kepada penyandang disabilitas. Oleh sebab itu, diperlukan langkah konkret untuk meningkatkan layanan perbankan digital bagi penyandang disabilitas.

LITERASI KEUANGAN DIGITAL YANG MASIH RENDAH

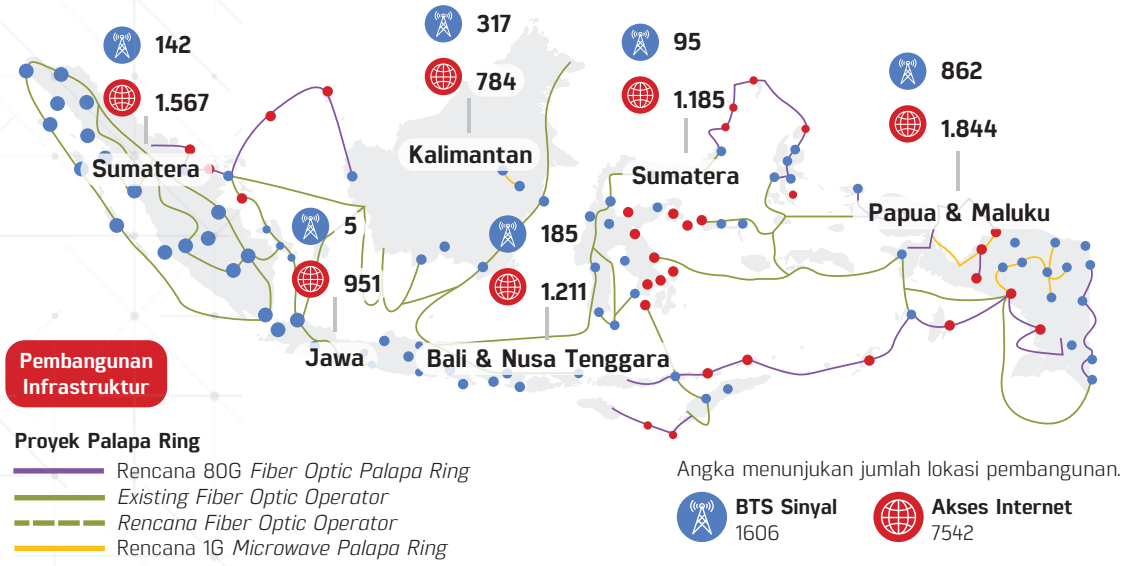
Tingkat literasi keuangan digital konsumen Bank merupakan salah satu faktor pemicu kejahatan siber. Merujuk data Direktorat Tindak Pidana Siber Bareskrim Polri, terdapat 2.259 laporan masyarakat tentang kejahatan digital pada Januari-September 2020. Sebanyak 18 aduan di antaranya tentang peretasan sistem elektronik, 649 penipuan daring, 39 pencurian data atau identitas, dan 71 manipulasi data (CISSREc, 2020). Berdasarkan laporan tersebut terlihat bahwa penipuan daring menjadi aduan tertinggi dan hal ini menunjukkan rendahnya pemahaman masyarakat atas risiko transaksi digital. Rendahnya

literasi keuangan digital masyarakat terkonfirmasi dari data Indeks Literasi Keuangan Digital masyarakat Indonesia yang saat ini baru mencapai 35,5% (Nasution, 2011).

Rendahnya literasi keuangan digital dapat memicu peningkatan kejahatan digital. Berbagai macam jenis kejahatan siber terjadi dikarenakan kurangnya pemahaman konsumen pada proses pengelolaan informasi digital dan kurangnya pemahaman konsumen akan keamanan siber pada aset digital mereka. Hal ini secara tidak langsung dapat mempengaruhi reputasi perbankan khususnya menyangkut tingkat keamanan layanan perbankan pada *digital bank*. Dengan demikian, perbankan juga diharapkan dapat menjadi penggerak utama literasi keuangan digital konsumen.

INFRASTRUKTUR TEKNOLOGI INFORMASI YANG BELUM MERATA

Faktor utama keberhasilan transformasi digital adalah ketersediaan infrastruktur dan jaringan telekomunikasi yang merata di seluruh Indonesia. Implementasi digitalisasi perbankan tidak akan optimal dan menjangkau konsumen secara luas di seluruh wilayah Indonesia jika infrastruktur dan jaringan telekomunikasi khususnya jaringan internet belum memadai, merata, dan berkualitas di seluruh wilayah Indonesia. Pembangunan 22.000 titik belum beroperasi sampai dengan Satelit Satria beroperasi. Sebagian besar wilayah Indonesia kecuali Sumatra, Jawa, dan Bali masih dalam rencana pengembangan infrastruktur teknologi informasi. Infrastruktur yang harus dimiliki oleh Bank antara lain terkait dengan ketersediaan serta kesiapan tempat penyimpanan (*storage*) dan jaringan yang mendukung terselenggaranya transaksi digital yang dapat berupa *server* fisik ataupun pemanfaatan *cloud*, serta sistem keamanan yang memadai.



*Pembangunan 22.000 titik belum beroperasi s/d Satelit Satria beroperasi

Strategi Implementasi Akselerasi Digital

	2020	2021	2022	2023	2024	2025
Layanan BTS 4G (Lokasi)	639	4.200	3.065	-	-	7.904
Akses Internet (Titik Layanan Publik)	7.904	-	22.000	40.000	40.000	109.904

Gambar 17
Peta Sebaran Infrastruktur Teknologi Informasi

Sumber: Proyek Palapa Ring Kementerian Komunikasi dan Informatika (2020)

DUKUNGAN KERANGKA REGULASI

Tidak hanya dari sisi perbankan, regulator juga menghadapi tantangan terkait pemutakhiran peraturan untuk mengakomodasi perkembangan industri di era industri 4.0. Seiring dengan itu, regulator perlu mengeluarkan kebijakan yang dapat mendorong pengembangan layanan berbasis digital secara cepat. Hal ini dilakukan antara lain melalui pemutakhiran kebijakan dan regulasi terkait produk dan kelembagaan dalam penerapan teknologi informasi untuk mendukung percepatan transformasi digital perbankan.

Faktor Pendorong dan Tantangan Transformasi Digital Perbankan

Faktor Pendorong

Digital Opportunity | **Behavior** | **Digital Transaction**

Sumber: We Are Social dan Hootsuite; Badan Pusat Statistik (BPS); Katadata; Bpank Indonesia; OJK, diolah

- Potensi Demografis
- Potensi Ekonomi & Keuangan Digital
- Peningkatan Penetrasi Internet
- Potensi Peningkatan Konsumen

Kepemilikan Perangkat

- *Mobile Phone* **98,3%**
- Laptop **74,7%**
- Tablet **18,5%**
- *Smart watch* **13,3%**

Penggunaan *Mobile Apps*

- *Chat Apps* **96,5%**
- Media Sosial **96,3%**
- *Shopping Apps* **96,3%**
- *Banking Apps* **39,2%**

- Transaksi *E-Commerce*
- Transaksi *Digital Banking*
- Transaksi Uang Elektronik
- Kantor Cabang

Tantangan

- Pelindungan dan pertukaran data pribadi yang belum dijamin Undang-Undang
- Risiko strategis, Investasi TI yang tidak sesuai strategi bisnis
- Risiko serangan siber
- Kesiapan organisasi dalam mendukung transformasi digital (*talent, leader* digital, budaya, desain grafis)
- Risiko kebocoran data nasabah
- Risiko penyalahgunaan teknologi (Penyalahgunaan AI)
- Risiko pihak ketiga (*outsourcing*)
- Infrastruktur jaringan komunikasi
- *Regulatory framework* yang mendukung

Halaman Ini Sengaja Dikosongkan

Bab

03

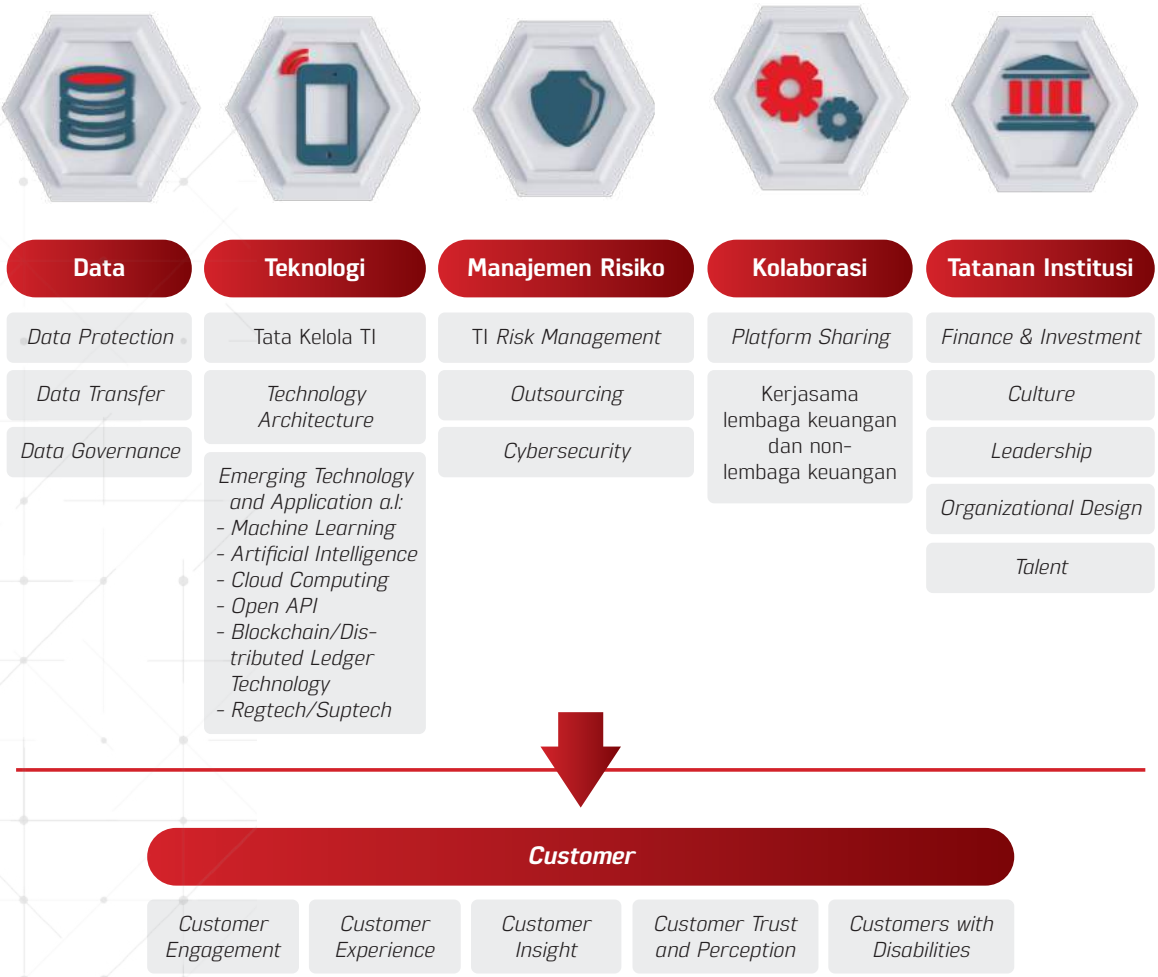
CETAK BIRU TRANSFORMASI DIGITAL PERBANKAN

"It is not the strongest of the species that survives, nor the most intelligent; it is the one most adaptable to change."

(Charles Darwin)

Cetak Biru Transformasi Digital Perbankan disusun sebagai suatu kebijakan dalam upaya mempercepat transformasi digital pada perbankan. Cetak biru ini berfokus pada 5 (lima) elemen utama yang akan memberikan kebijakan digitalisasi untuk perbankan yakni meliputi pedoman implementasi data, teknologi, manajemen risiko, kolaborasi, dan tatanan institusi pada industri perbankan. Kelima elemen tersebut merupakan langkah strategis untuk mendorong perbankan dalam menciptakan inovasi produk dan layanan keuangan yang dapat memenuhi ekspektasi konsumen dan berorientasi pada kebutuhan konsumen (*customer centric orientation*). Beberapa aspek yang perlu diperhatikan yaitu keterlibatan konsumen terhadap layanan perbankan (*customer engangement*), kepuasan konsumen atas layanan perbankan (*customer experience*), kesediaan konsumen dalam mempromosikan layanan perbankan kepada orang lain (*customer insight*), kepercayaan dan persepsi konsumen atas layanan perbankan (*customer trust and perception*), dan kemudahan akses bagi kelompok konsumen dengan disabilitas (*customers with disabilities*).

Gambar 18 Cetak Biru Transformasi Digital Perbankan



Lima elemen dalam Cetak Biru dijabarkan lebih lanjut dalam 16 sub elemen. Implementasi dari seluruh elemen dan sub elemen tersebut akan dilakukan melalui *regulatory approach* dan *facilitative approach*. *Regulatory approach* akan dilakukan melalui penerbitan regulasi yang bersifat *principle-based* sementara *facilitative approach* dilakukan melalui penerbitan panduan terkait transformasi digital perbankan yang diharapkan dapat mendorong perbankan untuk mempercepat transformasi digital. Berbagai penerapan dari elemen dan sub elemen memerlukan komitmen dan kolaborasi erat dari seluruh pemangku kepentingan sehingga perbankan yang kuat (*resilience*), berdaya saing, dan kontributif dapat terwujud.

DATA

Kebijakan pelindungan data, pengaturan pertukaran data, dan tata kelola data pada perbankan merupakan aspek penting yang diperlukan dalam meningkatkan kepercayaan masyarakat terhadap layanan perbankan digital.

Di era digital, data menjadi satu jenis kekayaan baru yang jauh lebih berharga daripada emas atau minyak. Dengan berkembangnya pemanfaatan teknologi informasi maka pengumpulan, pemrosesan, dan pemindahan data akan semakin mudah dilakukan. Pertukaran data akan semakin marak dilakukan seiring perkembangan *open banking* dengan memanfaatkan teknologi API.

Namun demikian, perbankan perlu berhati-hati terhadap data nasabah yang dimilikinya. Perbankan diharapkan dapat berfungsi menjadi tempat penyimpanan data yang aman. Untuk itu, diperlukan perumusan aturan tentang data karena adanya kebutuhan untuk melindungi nasabah perbankan. Pelindungan yang memadai atas data akan mampu memberikan kepercayaan nasabah untuk menyediakan data mereka guna berbagai kepentingan yang lebih besar tanpa disalahgunakan atau melanggar hak-hak pribadi.

Sejumlah elemen krusial terkait data yaitu pelindungan data, pengaturan pertukaran data (*data transfer*) dan tata kelola data pada perbankan menjadi suatu hal penting. Implementasi yang baik atas elemen tersebut akan meningkatkan kepercayaan masyarakat kepada perbankan terutama di era digital.

PELINDUNGAN DATA

Aturan pelindungan data pada dasarnya merupakan skema yang mengatur pengumpulan, pemrosesan dan penyimpanan data konsumen. Dasar dari perumusan norma dan pelaksanaan dalam pelindungan data yakni berdasarkan beberapa asas yang perlu diperhatikan oleh Bank adalah sebagai berikut:

1. Asas pelindungan dimaksudkan untuk memberi pelindungan kepada pemilik data mengenai datanya dan hak-hak atas data tersebut agar tidak disalahgunakan.
2. Asas kepastian hukum dimaksudkan sebagai landasan hukum bagi pelindungan data serta segala sesuatu yang mendukung penyelenggaraannya yang mendapatkan pengakuan hukum di dalam dan di luar pengadilan.
3. Asas kepentingan umum yang menyatakan bahwa dalam menegakkan pelindungan data harus memperhatikan kepentingan umum atau masyarakat secara luas. Kepentingan umum tersebut antara lain kepentingan penyelenggaraan negara serta pertahanan dan keamanan nasional.
4. Asas kemanfaatan menyatakan bahwa pengaturan pelindungan data harus bermanfaat bagi kepentingan nasional, khususnya dalam mewujudkan cita-cita kesejahteraan umum.
5. Asas kehati-hatian dimaksudkan agar para pihak yang terkait dengan pemrosesan dan pengawasan data harus memperhatikan segenap aspek yang berpotensi mendatangkan kerugian.
6. Asas keseimbangan dimaksudkan sebagai upaya pelindungan data untuk menyeimbangkan antara hak-hak atas data di satu pihak dengan hak-hak negara yang sah berdasarkan kepentingan umum.
7. Asas pertanggungjawaban dimaksudkan agar semua pihak yang terkait dengan pemrosesan dan pengawasan data bertindak secara bertanggung jawab sehingga mampu menjamin keseimbangan hak dan kewajiban para pihak yang terkait termasuk pemilik data.

Gambar 19
Asas Pengaturan Pelindungan Data

7 Prinsip Utama

Selain itu, perbankan perlu memenuhi 7 (tujuh) prinsip utama dalam mengumpulkan dan memproses data konsumen yaitu sebagai berikut:

Prinsip 1

ABSAH, ADIL, DAN TRANSPARAN

Data pribadi harus diproses secara sah, adil, dan transparan dalam kaitannya dengan subjek data individu.

Absah memiliki pengertian bahwa Bank memiliki dasar hukum yang sah untuk memproses data pribadi dan menghindari aktivitas ilegal saat memproses data pribadi. Dasar hukum yang sah dalam memproses data pribadi konsumen dapat berupa salah satu dari sebagai berikut:

a. *Consent* yaitu subjek data telah memberikan kewenangan untuk mengolah data pribadi untuk satu atau lebih tujuan khusus.

b. *Contract* yaitu pengolahan data diperlukan untuk pelaksanaan kontrak dengan subjek data menjadi pihak yang akan menandatangani kontrak atau untuk mengambil langkah-langkah atas permintaan subjek data sebelum menandatangani kontrak.

c. *Legal obligation* yaitu pengolahan data diperlukan untuk memenuhi kewajiban Bank untuk tunduk pada hukum.

d. *Protection of vital interests* yaitu pengolahan data diperlukan untuk melindungi kepentingan vital subjek data atau orang perseorangan lainnya.

e. *Public task* yaitu pengolahan data diperlukan untuk pelaksanaan tugas yang dilakukan untuk kepentingan umum atau dalam pelaksanaan kewenangan resmi yang diberikan kepada Bank.

f. *Legitimate interest* yaitu pengolahan data diperlukan untuk tujuan kepentingan sah dari Bank atau pihak ketiga, kecuali jika kepentingan tersebut teranulir oleh kepentingan atau hak dasar dan kebebasan subjek data.

Adil memiliki pengertian bahwa Bank tidak boleh menyalahgunakan data pribadi atau mengumpulkan, menyimpan, dan memproses data dengan cara menipu atau menyesatkan individu sehingga dapat menimbulkan efek negatif bagi seseorang.

Transparan memiliki pengertian bahwa Bank perlu melakukan komunikasi yang jelas, terbuka dan jujur kepada konsumen tentang bagaimana data pribadi mereka digunakan.

Prinsip 2
PEMBATASAN TUJUAN

Pembatasan tujuan memiliki pengertian bahwa data pribadi harus dikumpulkan untuk tujuan yang jelas, eksplisit, dan sah serta tidak diproses lebih lanjut dengan cara yang tidak sesuai dengan tujuan tersebut.

Prinsip 3
MINIMALISASI DATA

Minimalisasi data memiliki pengertian bahwa data pribadi harus memadai, relevan, dan terbatas pada apa yang diperlukan terkait dengan tujuan pemrosesannya atau dengan kata lain Bank hanya dapat mengumpulkan data minimum yang dibutuhkan.

Prinsip 4
AKURAT

Data pribadi harus akurat, jika perlu terus diperbarui. Setiap langkah harus diambil untuk memastikan data pribadi yang tidak akurat, dihapus, atau diperbaiki tanpa penundaan.

Prinsip 5
PEMBATASAN PENYIMPANAN

Data pribadi harus disimpan dalam bentuk yang memungkinkan identifikasi subjek data dan disimpan tidak lebih dari periode yang diperlukan untuk tujuan pemrosesan data pribadi.

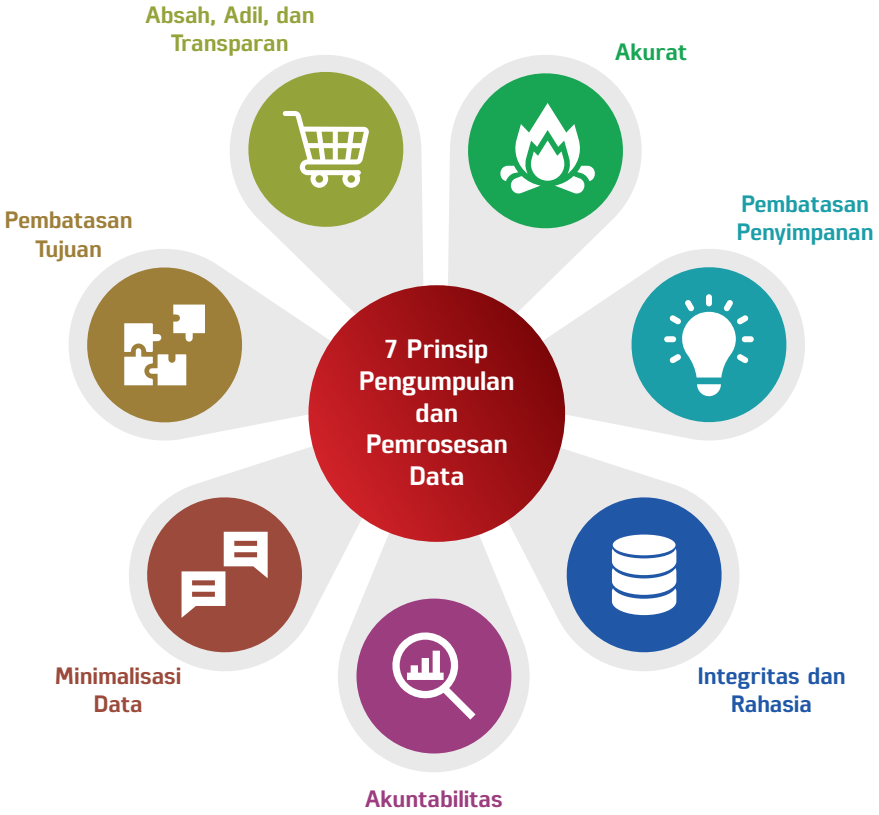
Prinsip 6
INTEGRITAS DAN RAHASIA

Data pribadi harus diproses secara aman, termasuk pelindungan terhadap pemrosesan yang tidak sah atau melanggar hukum serta pelindungan terhadap kehilangan, penghancuran, atau kerusakan yang tidak disengaja.

Prinsip 7
AKUNTABILITAS

Bank sebagai pengontrol data harus bertanggung jawab dan mampu menunjukkan kepatuhan terhadap keseluruhan prinsip-prinsip pengumpulan dan pemrosesan data. Untuk ini Bank perlu memiliki dokumentasi terkait pengumpulan dan pemrosesan data serta mengimplementasikan langkah teknis organisasi dan pelindungan data, termasuk menunjuk *data protection officer.*

Gambar 20 Prinsip Pengumpulan dan Pemrosesan Data



Sumber : EU GDPR (2016)

PERTUKARAN DATA (*DATA TRANSFER*)

Dalam pertukaran data terdapat aspek yang perlu diperhatikan oleh perbankan yaitu aturan jenis data yang dipertukarkan, pihak yang terlibat dalam pertukaran data, dan bagaimana pengaturan pertukaran data.

JENIS DATA

Jenis data pada perbankan diklasifikasikan ke dalam 4 (empat) jenis kategori data yaitu *customer provided data, transaction data, value-added customer data,* dan *aggregated data*.

Gambar 21 Kategori Jenis Data

CUSTOMER PROVIDED DATA

Customer provided data adalah data dan informasi yang diberikan langsung oleh nasabah atau calon nasabah ke Bank. Contoh data yang termasuk dalam kategori ini adalah alamat pribadi dan detail kontak konsumen; informasi tentang situasi keuangan saat pembukaan rekening atau pengajuan pinjaman, dan informasi untuk tujuan melakukan pembayaran seperti daftar penerima pembayaran.

Bank sebagai *data holder* dapat membagikan semua informasi yang diberikan nasabah kepada Bank sepanjang mendapat perintah nasabah untuk mempertukarkan data tersebut. Pengecualian pertukaran data berlaku untuk *customer provided data* yang merupakan data atau informasi pendukung penilaian verifikasi identitas. Bank hanya dapat memberikan data yang merupakan data atau informasi pendukung penilaian verifikasi identitas tersebut kepada nasabah secara langsung. Jika diperintah oleh konsumen, maka Bank sebagai *data holder* berkewajiban untuk membagikan hasil penilaian verifikasi identitas tersebut untuk keperluan pemenuhan undang-undang tertentu seperti anti pencucian uang.

TRANSACTION DATA

Transaction data atau data transaksi adalah data yang dihasilkan sebagai hasil dari transaksi yang dilakukan pada akun atau layanan nasabah. Contoh data yang termasuk kategori ini adalah catatan penyetoran, penarikan, transfer dan transaksi lain yang dilakukan oleh nasabah (seperti transaksi langsung dengan pedagang); saldo akun; bunga yang diperoleh atau dibebankan; serta biaya yang ditanggung oleh nasabah. Bank sebagai *data holder* dapat membagikan semua informasi yang diberikan nasabah kepada Bank sepanjang mendapat perintah dari nasabah untuk mempertukarkan data tersebut.

VALUE-ADDED CUSTOMER DATA

Value-added customer data atau data nasabah yang memiliki nilai tambah adalah data yang dihasilkan dari upaya Bank sebagai *data holder* untuk mendapatkan wawasan tentang nasabah. Contoh data yang termasuk kategori data ini adalah data pendapatan/ aset, pemeriksaan verifikasi identitas konsumen, data pelaporan kredit, nilai kredit, data tentang konsumen yang telah dikumpulkan dari seluruh rekening konsumen, serta data perilaku konsumen yang telah dikumpulkan dari *geolocation, e-commerce,* dan lain sebagainya. Data yang dihasilkan dari upaya Bank untuk mendapatkan wawasan tentang nasabah, analisis atau transformasi data oleh Bank dapat dibagikan kepada pihak lain tanpa perlu mendapat persetujuan/*consent* nasabah.

AGGREGATED DATA

Aggregated data adalah data gabungan yang dibuat Bank dengan menggunakan beberapa data nasabah untuk menghasilkan data yang tidak teridentifikasi, kolektif, atau rata-rata di seluruh kelompok atau sub kelompok nasabah. Contoh data yang termasuk kategori data ini adalah saldo akun rata-rata menurut kode pos atau kuintil pendapatan, atau ukuran rata-rata cerukan usaha kecil menurut segmen industri. Atas data yang termasuk kategori data agregat, Bank dapat membagikan informasi kepada pihak lain tanpa perlu mendapat *consent* nasabah.

PARA PIHAK DALAM PERTUKARAN DATA

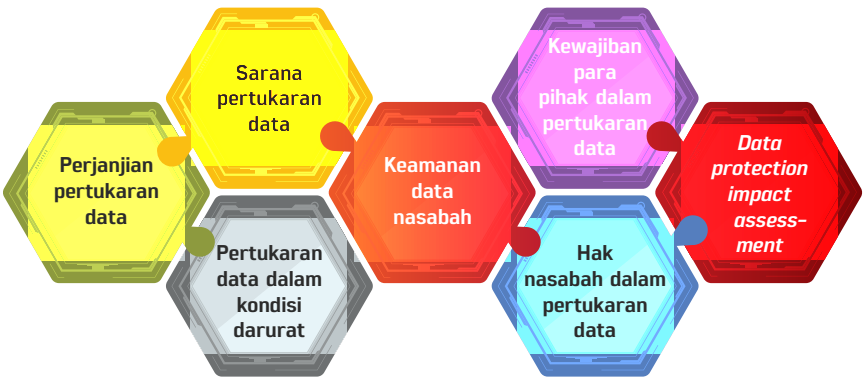
Pihak yang terlibat dalam pertukaran data yaitu:

1. Pihak yang dapat memerintahkan Bank untuk mempertukarkan data individu adalah nasabah pemilik rekening Bank baik nasabah individu, korporasi, atau UMKM.
2. Bank memiliki kewajiban untuk membagikan data atas perintah nasabah.
3. Entitas penerima data berkewajiban membagikan data yang diberikan konsumen kepada entitas tersebut kepada Bank atas perintah konsumen (*reciprocal obligations*).

PENGATURAN PERTUKARAN DATA

Aturan main yang seragam di perbankan terkait pengaturan *data transfer* dapat mendorong kepercayaan perbankan untuk terlibat dalam ekosistem digital ekonomi. Beberapa aspek yang perlu diperhatikan oleh perbankan dalam pertukaran data antara lain perjanjian pertukaran data, sarana pertukaran data, keamanan data nasabah, kewajiban para pihak dalam pertukaran data, *data protection impact assessment*, hak konsumen dalam pertukaran data, dan pertukaran data dalam kondisi darurat.

Gambar 22
Aspek dalam Pertukaran Data



PERJANJIAN PERTUKARAN DATA

Kerja sama/kolaborasi antara perbankan dan pihak ketiga yang menyebabkan terjadinya pertukaran data harus dituangkan dalam perjanjian pertukaran data. Perjanjian pertukaran data - harus memuat setidaknya hal-hal sebagai berikut:

1. Pihak pengendali data pada setiap tahap pertukaran data;
2. Tujuan pertukaran data yang meliputi tujuan khusus, mengapa pertukaran data dibutuhkan dan keuntungan yang diperoleh dari pertukaran data;
3. Pihak ketiga lain yang mungkin terlibat dalam pertukaran data;
4. Data yang akan dipertukarkan;
5. *Lawfull basis* yang dipergunakan yaitu dasar hukum dari para pihak untuk melakukan pertukaran data;
6. Prosedur pemenuhan hak subjek data seperti: akses subjek data terhadap data yang dilakukan proses pertukaran data; dan
7. Pengaturan teknis (misal: rincian *dataset*, *periodic sampling*, *data quality analysis*, format data, *common rules* untuk retensi dan *deletion* data, *security agreement*, prosedur permintaan akses data, dan penghentian pertukaran data).

Perjanjian pertukaran data harus ditinjau secara berkala atau ketika terjadi perubahan yang berdampak pada keluhan konsumen yang signifikan maupun pada saat terjadi pelanggaran keamanan.

SARANA PERTUKARAN INFORMASI

Pertukaran data nasabah diperkenankan menggunakan sarana API.

KEAMANAN DATA NASABAH

Bank harus mengambil langkah-langkah pengamanan untuk melindungi informasi nasabah yang dipertukarkan. Bank perlu memastikan bahwa informasi nasabah yang dipertukarkan tetap akan terlindungi sesuai standar *security* oleh pihak penerima data. Untuk hal ini, pihak penerima data perlu:

1. memahami sifat dan sensitivitas data; dan
2. memastikan bahwa langkah-langkah keamanan dilakukan, terutama untuk memastikan bahwa Bank telah memasukkan serangkaian standar keamanan yang disepakati ke dalam perjanjian pertukaran data.

KEWAJIBAN PARA PIHAK (*LIABILITY ARRANGEMENT*)

Bank perlu mengatur alokasi tanggung jawab pihak yang terlibat dalam pertukaran data. Pada dasarnya pihak yang terlibat dalam pertukaran data bertanggung jawab atas perilaku sendiri, tetapi tidak bertanggung jawab atas kesalahan pihak lain.

Berikut contoh alokasi tanggung jawab antara Bank dan pihak penerima data:

1. Bank harus bertanggung jawab kepada nasabah atas pemberian informasi yang salah kepada penerima data.
2. Bank harus bertanggung jawab kepada nasabah atas pemberian informasi yang tidak sah (*unauthorized sharing information*) kepada penerima data.
3. Bank tidak bertanggung jawab atas kerugian yang diderita nasabah akibat produk yang ditawarkan oleh penerima data.
4. Bank bertanggung jawab kepada nasabah atas koreksi catatan data informasi nasabah.
5. Bank harus bertanggung jawab kepada nasabah atas kerugian yang diderita oleh nasabah akibat kegagalan untuk mentransfer data sesuai perintah nasabah.
6. Penerima data bertanggung jawab kepada nasabah atas kerugian yang diderita nasabah akibat kebocoran data yang diakibatkan penerima data.
7. Bank tidak bertanggung jawab atas kebocoran data yang dialami oleh penerima data.
8. Bank tidak bertanggung jawab atas tindakan yang dilakukan oleh penerima data.

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

DPIA merupakan suatu proses yang perlu dilakukan oleh Bank untuk mengidentifikasi dan meminimalisir risiko terkait proteksi data dari suatu proyek yang akan dilaksanakan Bank. Bank harus melakukan DPIA jika proses pengumpulan dan pemrosesan data yang dilakukan Bank berpotensi membawa risiko tinggi pada nasabah. Kondisi yang mengharuskan Bank melakukan DPIA:

1. Menggunakan teknologi baru;
2. Melakukan pelacakan lokasi atau perilaku individu;
3. Melakukan pengawasan secara sistematis atas tempat yang dapat diakses oleh publik dalam skala besar;

4. Melakukan proses data terkait dengan ras, suku, opini politik, agama atau penganut kepercayaan tertentu; anggota dari perkumpulan dagang; data genetik; data biometrik untuk tujuan identifikasi individu; data kesehatan; dan data kehidupan seksual atau orientasi seksual;

5. Melakukan proses data yang akan digunakan untuk membuat keputusan otomatis terkait individu yang berpotensi memiliki dampak hukum; dan

6. Memproses data yang dapat berdampak buruk pada fisik subjek data jika data bocor.

HAK NASABAH DALAM PERTUKARAN DATA

Nasabah yang terlibat dalam pertukaran data memiliki hak atas hal-hal sebagai berikut:

1. hak untuk mengakses data pribadi yang dipertukarkan;

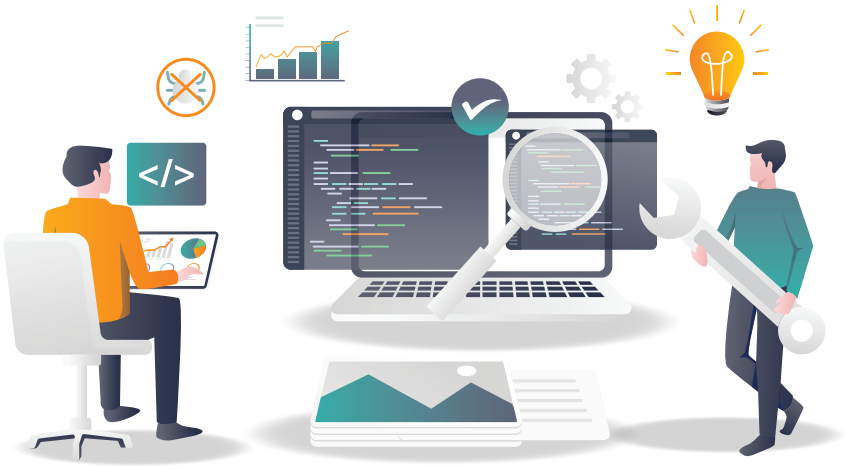
2. hak untuk diberi notifikasi tentang bagaimana dan mengapa data mereka digunakan;

3. hak agar datanya diperbaiki, dihapus atau dibatasi; dan

4. hak untuk tidak tunduk pada keputusan Bank yang didasarkan pada pemrosesan otomatis seperti hasil pemrosesan *big data analytic*.

PERTUKARAN DATA DALAM KONDISI DARURAT

Dalam kondisi darurat, Bank dapat melakukan pertukaran data kepada pihak lain sesuai kebutuhan dan secara proporsional. Contoh keadaan darurat meliputi bencana alam, serangan teroris, pandemi Covid-19, atau kebutuhan mendesak lainnya untuk melindungi keamanan nasional.



TATA KELOLA DATA

Bank merupakan entitas bisnis yang dibangun berdasarkan data, sehingga tata kelola data perlu menjadi perhatian penting dalam bisnis Bank. Tata kelola data merupakan suatu proses penetapan; penerapan; serta pemantauan strategi, kebijakan, dan pengambilan keputusan bersama atas pengelolaan dan penggunaan aset data. Dalam bisnis Bank, tujuan tata kelola data yang utama adalah untuk memungkinkan Bank mengelola data sebagai aset serta mengupayakan ketersediaan data yang andal dan akurat untuk agregasi risiko dan pelaporan termasuk akuntabilitas data dan kemampuan data untuk dapat ditelusuri.

Dalam mencapai tujuan tata kelola data serta mendapatkan manfaat yang optimal dari program tata kelola data, Bank perlu memperhatikan 8 (delapan) prinsip dalam tata kelola data sebagai berikut:

1. Integritas (*Integrity*): Pelaku yang terlibat dalam tata kelola data harus selalu memegang prinsip integritas, kejujuran, serta keterbukaan berkaitan dengan *drivers, constraints*, opsi, dan dampak yang ditimbulkan dari keputusan terkait data.
2. Transparansi (*Transparency*): Proses tata kelola data harus transparan, jelas bagi semua *stakeholders* yang terlibat maupun auditor, serta terdapat kejelasan mengenai bagaimana dan kapan keputusan serta kontrol terkait data dimasukkan ke dalam proses.
3. Kemampuan untuk dapat diaudit (*Auditability*): Keputusan, proses, dan kontrol terkait data yang tunduk pada tata kelola data akan diaudit, sehingga diperlukan dokumentasi dokumen untuk mendukung *compliance-based* dan *operational auditing*.
4. Akuntabilitas (*Accountability*): Akuntabilitas yang jelas untuk keputusan, proses, dan kontrol terkait data yang lintas fungsi.
5. Kepengurusan (*Stewardship*): Akuntabilitas yang jelas untuk aktivitas penatagunaan yang menjadi tanggung jawab kontributor individu, serta akuntabilitas untuk kelompok Pengelola Data.
6. *Checks-and-Balances*: *Check-and-balances* antara Tim Bisnis dan Teknologi Informasi serta antara pembuat/pengumpul, pengelola, pengguna, serta penggagas standar dan persyaratan kepatuhan informasi.
7. Standarisasi (*Standardization*): Adanya standarisasi data yang jelas pada Bank.
8. Manajemen Perubahan (*Change Management*): Program tata kelola data mendukung aktivitas Manajemen Perubahan yang proaktif dan reaktif terkait nilai data referensi serta struktur/ penggunaan data master dan metadata.

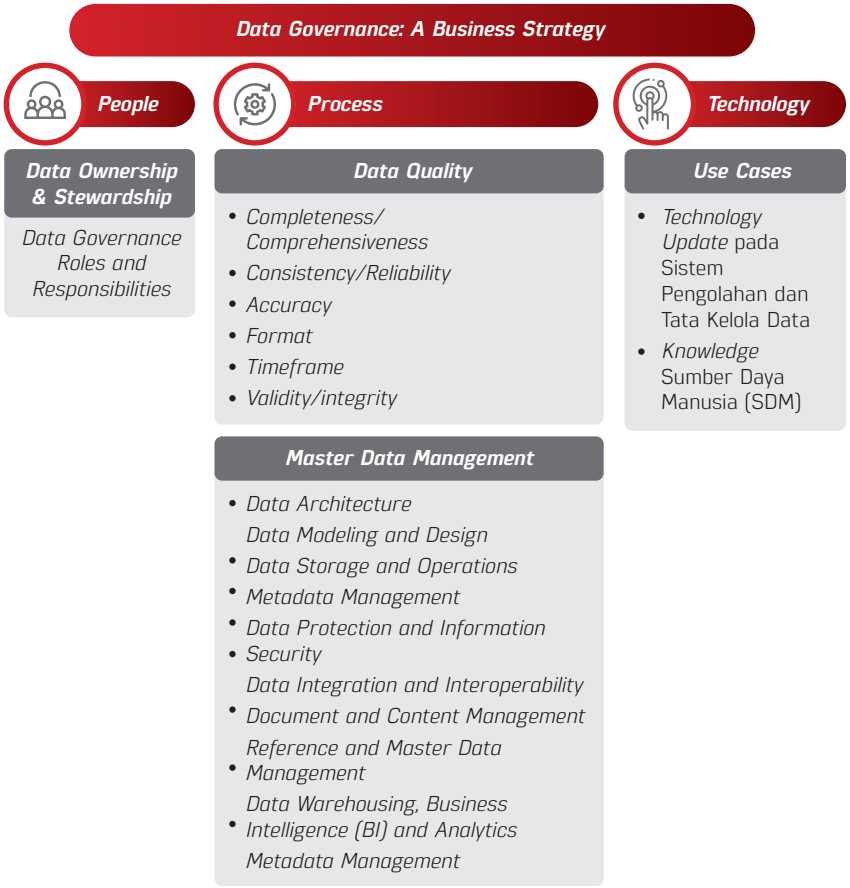
Gambar 23
Prinsip Tata Kelola Data

Sumber: UNSW Australia

IMPLEMENTASI TATA KELOLA

Tata kelola data pada Bank pada prinsipnya adalah suatu inisiatif strategi bisnis. Konsep tata kelola data bukanlah inisiatif program dari bagian (divisi) Teknologi Informasi (TI) Bank dan tidak boleh didorong atau dimotori oleh teknologi informasi. Implementasi tata kelola data diinisiasi oleh satuan kerja bisnis. Satuan kerja bisnis memberikan arahan, inisiatif atau rencana terkait peran divisi TI untuk melakukan eksekusi rencana sehingga implementasi teknis teknologi informasi hanyalah hasil akhir dari program tata kelola data. Proses ini mencakup sumber daya manusia (*people*), proses (*process*), dan teknologi (*technology*) yang diperlukan untuk memastikan bahwa data sesuai dengan tujuan yang dimaksudkan.

Gambar 24
Implementasi Tata Kelola Data



SUMBER DAYA MANUSIA (*PEOPLE*)

Unsur manusia dalam tata kelola data meliputi *data ownership* dan *stewardship* yang di dalamnya menjelaskan mengenai peran serta dan tanggung jawab masing-masing bagian dalam organisasi Bank yang terlibat dalam tata kelola data. Tingkatan pengelolaan data mencakup tingkat strategis, tingkat manajerial, dan tingkat operasional.

TINGKAT STRATEGIS

Pada tingkatan strategis, pemilik dan pengguna data adalah Direksi. Direksi harus merumuskan strategi data, meninjau peristiwa penting yang berkaitan dengan tata kelola data, dan bertanggung jawab penuh atas tata kelola data, termasuk mengatur peran dan tanggung jawab masing-masing bagian (*data ownership* dan *stewardship*) terhadap tata kelola data. Direksi harus menentukan dan memberikan kewenangan kepada departemen yang ditunjuk untuk memimpin dan bertanggung jawab atas sistem tata kelola data, mengawasi mekanisme operasi pengelolaan data, dan menunjuk *Chief Data Officer* (CDO) yang sesuai. CDO diharapkan memiliki perpaduan yang seimbang antara pengetahuan teknis, keterampilan analitis, keahlian dalam masalah hukum dan peraturan serta kompetensi bisnis.

TINGKAT MANAJERIAL

Tingkat manajerial bertanggung jawab untuk mengembangkan dan melaksanakan kebijakan data di tingkat perusahaan dan tingkat lokal. Manajemen senior Bank harus bertanggung jawab untuk menetapkan dan menerapkan sistem tata kelola data, akuntabilitas, insentif, kendali kualitas data, dan harus melapor kepada Direksi secara berkala.

TINGKAT OPERASIONAL

Tingkat operasional tata kelola data terdiri dari *data steward* dan *data user*. *Data steward* merupakan *subject matter expert* pada domain data. *Data steward* memiliki tanggung jawab utama melaksanakan pengelolaan data sesuai kebijakan dan standar pengelolaan data yang telah ditetapkan. Pengelolaan data oleh *data steward* dilakukan pada seluruh siklus hidup data sejak pembuatan, pengumpulan atau akuisisi, pengelolaan akses, penggunaan, pelestarian atau penghapusan data untuk menjaga kualitas, integritas, konsistensi, dan untuk menghindari duplikasi.

PROSES (*PROCESS*)

Dalam lingkup pembahasan proses, tata kelola data meliputi kualitas data (*data quality*) dan *master data management.*

KUALITAS DATA (*DATA QUALITY*)

Ketersediaan data yang andal dan akurat untuk analisis bisnis dan pelaporan risiko termasuk akuntabilitas dan penelusuran data merupakan salah satu tujuan tata kelola data. Data memiliki nilai yang berharga jika data dapat diandalkan dan terpercaya. Dengan kata lain, data tersebut perlu berkualitas tinggi. Dalam mengelola data, Bank perlu untuk memperhatikan 8 (delapan) set dimensi kualitas data sebagai berikut:

1. *Accuracy*: Akurasi mengacu pada kondisi bahwa data telah mewakili kondisi riil atau menggambarkan objek atau peristiwa pada dunia nyata.

2. *Completeness/Comprehensiveness*: Kelengkapan mengacu pada apakah semua data yang diperlukan tersedia.

3. *Consistency/Reliability*: Konsistensi merujuk pada keadaan bahwa nilai sebuah *field* data akan sama semua dalam berkas catatan yang sama (konsistensi tingkat rekaman) atau nilai sebuah *field* data akan sama semua dalam berkas catatan yang berbeda (konsistensi lintas catatan)atau nilai sebuah *field* data akan sama semua dalam berkas catatan yang sama pada titik waktu yang berbeda (konsistensi temporal). Konsistensi juga dapat digunakan untuk merujuk pada konsistensi format.

4. *Integrity*: Integritas mengacu kepada nilai atribut data sesuai dengan batasan yang diperkenankan. Dalam data, integritas mengacu pada integritas referensial (konsistensi antara objek data melalui referensi kunci yang terdapat di kedua objek) atau konsistensi internal dalam kumpulan data, sehingga tidak ada bagian yang hilang.

5. *Reasonability*: Kewajaran data merujuk pada pola data yang telah memenuhi harapan.

6. *Timelineness* (*Timeframe*): Konsep *timeliness* data mengacu pada keterbaharuan data.

7. *Uniqueness/Deduplication* (Format): Keunikan data menyatakan bahwa tidak ada entitas yang ada lebih dari satu kali dalam kumpulan data.

8. *Validity*: Data hanya valid jika sesuai dengan sintaks (format, jenis, rentang) dari definisinya.

MASTER DATA MANAGEMENT

Bank perlu membentuk sistem pengelolaan data (*master data management system*) yang komprehensif dan efektif. Komponen-komponen *master data management* yang perlu diperhatikan Bank adalah sebagai berikut:

01
Data Architecture

Di era *big data* dan *data science*, sangat penting bagi organisasi untuk memiliki arsitektur data yang terpusat dan selaras dengan proses bisnis, arah pertumbuhan bisnis dan kemajuan teknologi. Arsitektur merujuk pada seperangkat aturan, kebijakan, standar dan model yang mengatur dan menentukan jenis data yang dikumpulkan serta bagaimana data itu digunakan, disimpan, dikelola, dan diintegrasikan dalam suatu organisasi dan sistem basis data untuk mendukung strategi organisasi.

02
Data Modelling and Design

Pemodelan dan Desain Data (*Data Modelling and Design*) adalah proses identifikasi, analisis, penyusunan persyaratan data, dan kemudian merepresentasikan serta mengkomunikasikan persyaratan data ke dalam bentuk yang tepat yang disebut model data. Model data menekankan pada kebutuhan, pengaturan, dan operasi data.

03
Data Storage and Operations

Data Storage and Operations merujuk pada proses desain, implementasi, dan penyediaan dukungan atas penyimpanan data untuk meningkatkan nilai data sepanjang siklus hidup data yang dimulai dari tahap penciptaan atau perolehan data hingga pelepasan data.

04
Data Protection and Information Security

Data Protection and Information Security yang dimaksud pada Bank adalah perencanaan, pengembangan, serta pelaksanaan kebijakan dan prosedur keamanan untuk menyediakan otentikasi, otorisasi, akses, dan audit aset data dan informasi yang tepat. Bank harus memastikan bahwa privasi dan kerahasiaan data dijaga, tidak dilanggar, dan data diakses dengan tepat. Bank perlu menetapkan strategi, kebijakan, dan standar keamanan data. Bank wajib melindungi informasi pribadi dan privasi konsumen maupun internal Bank sebagai langkah untuk memitigasi *risks*, *vulnerability,* dan *threats.*

05
Data Integration and Interoperability

Data Integration and Interoperability merujuk pada pengelolaan pergerakan dan konsolidasi data dalam maupun antar aplikasi maupun antar organisasi Bank.

06
Document & Content Management

Manajemen Dokumen dan Konten (*Document and Content* Management) merujuk pada kegiatan perencanaan, implementasi, dan pengendalian untuk pengelolaan siklus hidup data dan informasi yang ditemukan dalam bentuk atau media apa pun.

07

Reference and Master Data Management

Referensi dan Manajemen Data Master (*Reference and Master Data Management*) bagi Bank adalah mengelola data bersama untuk memenuhi tujuan organisasi, mengurangi risiko yang terkait dengan redundansi data, memastikan kualitas yang lebih tinggi, dan mengurangi biaya integrasi data. Bank harus memiliki manajemen referensi data yang efektif untuk memfasilitasi kelancaran arus data sehingga tersedia data yang lengkap, akurat, kini, utuh dan terkonsolidasi.

08

Data Warehousing, Business Intelligence* (BI) *and Analytics

Data Warehousing, Business Intelligence (BI) *and Analytics* merupakan proses perencanaan, implementasi, dan pengendalian untuk menyediakan data pendukung keputusan dan mendukung pengguna data yang terlibat dalam proses pelaporan, pencarian, dan analisis data. *Business Intelligence* pada Bank diperlukan untuk menyediakan *key business data* sehingga Bank dapat dengan cepat dan mudah menyelesaikan permasalahan bisnis (pengambilan keputusan bisnis) dengan data yang akurat dan tepat waktu.

09

Metadata Management

Metadata sangat penting untuk mengelola kualitas data. Manajemen metadata merujuk pada perencanaan, pelaksanaan, dan kegiatan pengendalian sehingga memungkinkan akses ke metadata terintegrasi dan berkualitas tinggi. Manajemen metadata adalah kunci dalam memenuhi tantangan bahwa Bank harus memberikan wawasan tentang proses agregasi data keuangan dan risiko yang dimiliki.

TEKNOLOGI (*TECHNOLOGY*)

Pengelolaan data pada aspek teknologi mencakup pengkinian teknologi termasuk pemanfaatan teknologi *cloud* dan peningkatan sumber daya manusia terkait sistem pengelolaan data.

PENGKINIAN TEKNOLOGI PADA SISTEM PENGOLAHAN DAN TATA KELOLA DATA

Dalam hal pengkinian teknologi, Bank perlu mengevaluasi secara sistematis apakah teknologi yang digunakan telah melindungi kerahasiaan data, memenuhi prinsip integritas, dan ketersediaan datanya cukup untuk mengurangi risiko ke tingkat yang dapat diterima. Bank harus memiliki *awareness* yang tinggi dalam hal mengembangkan/memperbaharui teknologi pengolahan data sebagai langkah *continuous improvement* dalam penerapan *data governance* (prinsip pengkinian teknologi). Pembaharuan teknologi ini ke depan mengarah kepada tiga fokus besar, yakni 1) Peningkatan perlindungan terhadap privasi data, 2) Otomatisasi dan perluasan kontrol tata kelola data dengan menggunakan platform *cloud,* dan 3) Memperluas tata kelola data ke analitik tingkat lanjut.

Kemajuan terbaru dalam *Cloud Computing* telah memperluas batasan baik pengelolaan, penyimpanan, maupun pertukaran data. Oleh karena itu, kebijakan keamanan data perlu meningkatkan standar keamanan data karena pengaplikasian *Cloud Computing*

menyebabkan data Bank berada pada sistem eksternal. Tanggung jawab bersama dalam mendefinisikan data, melacak dan mendefinisikan kepemilikan serta hak perwalian data sangat penting dalam aplikasi *Cloud Computing* pada Bank. Berikut adalah beberapa hal yang perlu diperhatikan oleh Bank dalam *deployment cloud computing*:

1. Bank harus secara jelas menentukan *return of investment* (ROI) untuk proyek berbasis *cloud*. Bank harus memahami manfaat nyata yang tersedia sebelum berinvestasi. Bank harus memilih penyedia layanan dengan keahlian yang telah terbukti dalam manajemen layanan *cloud.*

2. Bank harus menandatangani *service level agreement* dengan *provider cloud.*

3. Lembaga *cloud outsourcing* harus menilai kegiatan mana yang dianggap material sebelum melakukan kegiatan mereka.

4. Lembaga *cloud outsourcing* harus menginformasikan kepada otoritas yang berwenang tentang aktivitas material yang akan dialihdayakan ke penyedia layanan *cloud*.

5. Bank harus memahami kerahasiaan data dan persyaratan regulasi. Bank perlu menyimpan data sensitif di dalam *firewall* untuk memenuhi persyaratan regulasi lokal dan kerahasiaan data konsumen. Untuk pemenuhan peraturan dan kepatuhan, data keuangan untuk konsumen perbankan tetap berada di negara asal dan data tidak dapat dicampur dengan data lain, seperti pada *server* atau basis data bersama. Oleh karena itu, Bank harus memiliki pemahaman yang jelas tentang lokasi data dalam *cloud.*

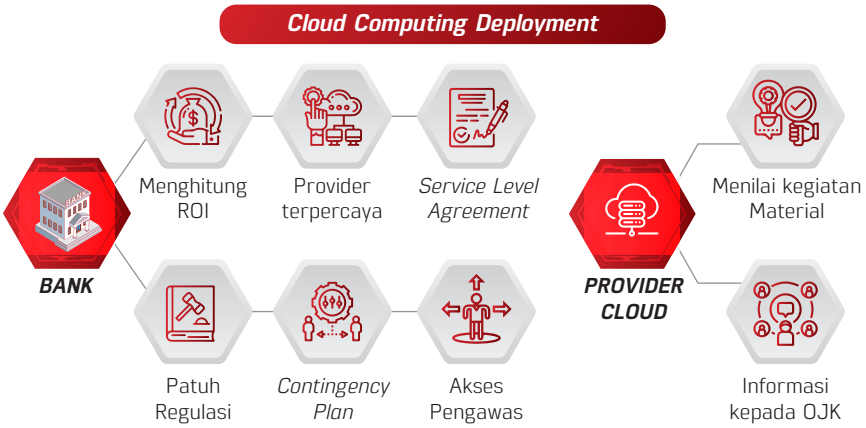
6. Dalam hal kegiatan pengawasan, Bank dan penyedia layanan *cloud* harus mengizinkan dan memastikan bahwa pengawas perbankan dapat menjangkau/mengakses semua komponen *cloud platform* (termasuk *server*, perangkat lunak, pusat data, jaringan, dan lainnya) kapanpun, dalam waktu singkat untuk keperluan audit dan penegakan kepatuhan.

7. Dalam menghadapi potensi gangguan atau kegagalan di *cloud*, Bank harus memastikan bahwa mereka dapat beralih dari *cloud* kembali ke basis data bank.

8. Bank harus menentukan beberapa hal berikut sebelum melakukan alih daya *cloud,* yaitu memutuskan tingkat pelindungan yang sesuai dari kerahasiaan data, kontinuitas aktivitas yang dialihdayakan, dan integritas serta kemampuan data dan sistem untuk dilacak dalam konteks *cloud outsourcing*

yang dimaksud. Bank harus memeriksa apakah tindakan diperlukan untuk skenario tertentu, termasuk data *in transit*, data *in memory*, dan data *at rest*, seperti penggunaan teknologi enkripsi yang dikombinasikan dengan arsitektur manajemen kunci yang sesuai.

Gambar 25
Cloud Computing Deployment



Sumber: Final Report Recommendation on Outsourcing to Cloud Services Provider EBA (2017)

SUMBER DAYA MANUSIA (SDM)

Keberhasilan tata kelola data pada bank tidak terlepas dari kemampuan pemilik dan pengguna data dalam melakukan proses tata kelola data secara keseluruhan. Kemampuan ini turut dipengaruhi oleh kecakapan SDM Bank untuk menggunakan teknologi yang digunakan dalam proses manajemen data. Oleh karena itu, Bank perlu memperhatikan faktor kecakapan SDM nya dalam konteks penggunaan teknologi dalam melakukan aktivitas bisnis. Pengkinian *knowledge* diperlukan dalam hal ini. Program *training* dalam rangka meningkatkan *knowledge* SDM Bank dapat dimasukan ke dalam inisiatif program tata kelola data. Tata kelola data tidak dapat diselesaikan dengan teknologi saja, tetapi organisasi harus memanfaatkan solusi yang akan membantu inisiatif tata kelola yang dimiliki. Teknologi secara umum dapat dikelompokan menjadi dua kategori yaitu investasi teknologi secara kasat mata yang berupa *technological update* yakni teknologi terkini yang digunakan, serta teknologi tidak kasat mata seperti *knowledge* SDM. Teknologi ini dianalogikan sebagai *use cases* karena sifatnya yang secara kontinu berubah menyesuaikan kondisi.

TEKNOLOGI

Adopsi teknologi perlu dilakukan dengan memperhatikan prinsip adopsi teknologi yang bertanggung jawab serta memenuhi prinsip pemilihan, pemanfaatan, dan pengelolaan teknologi yang memadai seperti tata kelola teknologi informasi dan arsitektur teknologi informasi.

Teknologi terus mengalami perubahan seiring dengan perkembangan inovasi yang sedemikian pesat. Hal ini menyebabkan fokus pada suatu teknologi tertentu akan menjadi suatu hal yang cepat usang. Namun demikian, sejumlah aspek yang sangat mempengaruhi pemilihan, pemanfaatan, dan pengelolaan teknologi cenderung tidak banyak mengalami perubahan sehingga perlu diimplementasi secara baik. Aspek tersebut meliputi tata kelola teknologi informasi, arsitektur teknologi informasi, dan prinsip adopsi teknologi informasi terkini.

TATA KELOLA TEKNOLOGI INFORMASI (TI)

Tata kelola teknologi informasi merupakan bagian dari tata kelola perusahaan yang memiliki fokus pada tugas dan tanggung jawab Direksi dalam mengawasi implementasi proses dan mekanisme hubungan dalam organisasi yang memungkinkan unit kerja bisnis dan unit kerja teknologi informasi menjalankan tanggung jawab dalam mendukung penyelarasan strategi bisnis dan investasi teknologi informasi. Tata kelola teknologi informasi dapat menciptakan nilai bisnis dari investasi teknologi informasi. Tata kelola teknologi informasi pada dasarnya berfokus pada nilai yang diperoleh dan mitigasi risiko bisnis yang dihasilkan dari transformasi digital. Lebih khusus, hasil yang diharapkan dari penerapan tata kelola teknologi informasi adalah realisasi keuntungan, optimalisasi risiko dan optimalisasi sumber daya.

Kerangka Tata Kelola Teknologi Informasi COBIT 2019 mendefinisikan komponen dan faktor desain untuk membangun dan mengelola sistem tata kelola yang paling sesuai dengan organisasi. Sistem tata kelola teknologi informasi sesuai COBIT 2019 mengacu kepada 6 (enam) prinsip yaitu:

1. Setiap perusahaan membutuhkan sistem tata kelola untuk memenuhi kebutuhan pemangku kepentingan dan untuk menghasilkan nilai dari penggunaan teknologi informasi. Nilai mencerminkan keseimbangan antara manfaat, risiko, dan sumber daya. Perusahaan memerlukan strategi dan sistem tata kelola yang ditindaklanjuti untuk mewujudkan nilai tersebut.

2. Sistem tata kelola teknologi informasi perusahaan dibangun dari sejumlah komponen yang dapat berasal dari berbagai jenis komponen yang bekerja sama secara holistik.

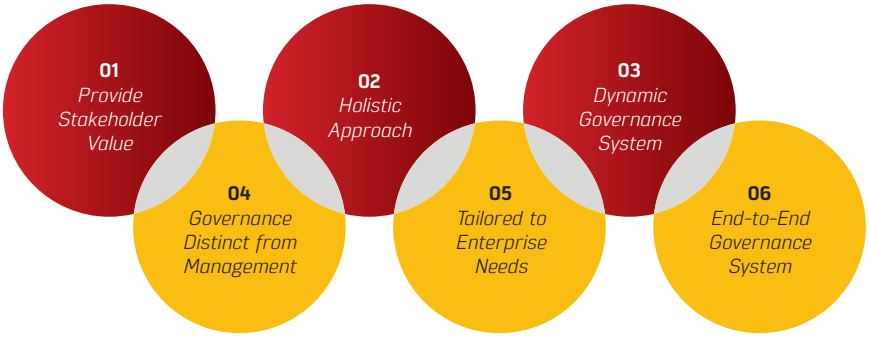
3. Sistem tata kelola teknologi informasi harus dinamis. Hal ini berarti bahwa setiap kali satu atau lebih faktor desain diubah (misalnya, perubahan dalam strategi atau teknologi), dampak dari perubahan ini pada sistem tata Kelola teknologi informasi harus dipertimbangkan.

4. Sistem tata kelola teknologi informasi harus secara jelas membedakan antara kegiatan dan struktur tata kelola dengan manajemen/pengelolaan.

5. Sistem tata kelola harus disesuaikan dengan kebutuhan perusahaan, dengan menggunakan serangkaian faktor desain sebagai parameter untuk menyesuaikan dan memprioritaskan komponen sistem tata kelola.

6. Sistem tata kelola harus mencakup *end to end* perusahaan, dengan fokus tidak hanya pada fungsi teknologi informasi tetapi juga berlaku bagi setiap unit pengguna teknologi informasi.

Gambar 26
Prinsip Sistem Tata Kelola



Sumber: COBIT (2019)

Kerangka Tata Kelola Teknologi Informasi COBIT 2019 membedakan antara tata kelola dan manajemen mengingat kedua hal tersebut mencakup aktivitas, struktur organisasi, dan tujuan yang berbeda. Tata kelola dan manajemen diwujudkan dalam 5 (lima) domain utama (ISACA, 2019). Domain tersebut dinamai dengan kata kerja yang mengekspresikan tujuan kunci dan area aktivitas dari tujuan yang terkandung di dalamnya.

TATA KELOLA

Tujuan tata kelola dikelompokkan ke dalam domain ***Evaluate, Direct,*** *and* ***Monitor*** (EDM). Mengacu kepada domain ini, Dewan Komisaris dan Direksi mengevaluasi pilihan strategi, mengarahkan manajemen senior dalam memilih pilihan strategi dan memonitor pencapaian dari strategi tersebut. Aktivitas Dewan Komisaris dan Direksi dalam domain ini memastikan:

01 PENGATURAN DAN PEMELIHARAAN KERANGKA TATA KELOLA

a. Menganalisis dan mengartikulasikan persyaratan untuk tata kelola teknologi informasi perusahaan.

b. Menerapkan dan mengelola komponen tata kelola dengan kejelasan wewenang dan tanggung jawab pihak yang terlibat untuk mencapai misi, tujuan, dan sasaran perusahaan.

02 PENCAPAIAN MANFAAT

Memaksimalkan manfaat bisnis yang dihasilkan dari investasi teknologi informasi dalam proses bisnis, layanan, dan aset teknologi informasi.

03 OPTIMALISASI RISIKO

Memastikan bahwa selera dan toleransi risiko perusahaan dipahami, diartikulasikan, dan dikomunikasikan sehingga risiko terkait dengan penggunaan teknologi informasi terhadap nilai perusahaan teridentifikasi dan terkelola.

04 OPTIMALISASI SUMBER DAYA

Memastikan kecukupan sumber daya terkait bisnis dan teknologi informasi (sumber daya manusia, proses, dan teknologi) tersedia untuk mendukung tujuan perusahaan secara efektif dan dengan biaya yang optimal.

05 KETERLIBATAN PEMANGKU KEPENTINGAN

Memastikan bahwa seluruh pemangku kepentingan telah teridentifikasi dan dilibatkan dalam sistem tata kelola teknologi informasi serta kinerja, pengukuran kualitas, dan pelaporan kinerja teknologi informasi dilakukan secara transparan, dengan persetujuan pemangku kepentingan terkait tujuan dan metrik pengukurannya serta tindakan perbaikan yang diperlukan.

MANAJEMEN

Tujuan manajemen mencakup aktivitas merencanakan, membangun, menjalankan, dan memantau kegiatan agar selaras dengan arahan yang ditetapkan oleh Direksi untuk mencapai tujuan perusahaan. Tujuan manajemen dikelompokkan ke dalam 4 (empat) domain, yaitu:

01 *ALIGN, PLAN, AND ORGANIZE* (APO)

Align, Plan, *and* ***Organize*** (APO) yaitu membahas keseluruhan penyusunan strategi, dan aktivitas pendukung untuk teknologi informasi yang mencakup aktivitas sebagai berikut:

1-A MENGELOLA KERANGKA MANAJEMEN TEKNOLOGI INFORMASI

i. Merancang sistem manajemen teknologi informasi sesuai tujuan dan faktor desain lainnya.

ii. Menerapkan pendekatan manajemen yang konsisten untuk memenuhi persyaratan tata kelola perusahaan, yang mencakup komponen tata kelola seperti proses manajemen; struktur organisasi; peran dan tanggung jawab; kegiatan yang andal dan berulang; item informasi; kebijakan dan prosedur; keterampilan dan kompetensi; budaya dan perilaku; serta layanan, infrastruktur dan aplikasi.

1-B MENGELOLA STRATEGI

i. Memberikan pandangan holistik tentang kondisi bisnis dan lingkungan teknologi informasi saat ini, arah perusahaan ke depan serta inisiatif yang diperlukan untuk bermigrasi ke lingkungan masa depan yang diinginkan.

ii. Memastikan bahwa tingkat digitalisasi yang diinginkan merupakan bagian integral dari arah masa depan dan strategi teknologi informasi, menilai kematangan digital organisasi saat ini, serta mengembangkan peta jalan untuk menutup kesenjangan menuju tingkat digitalisasi yang diinginkan

iii. Memastikan perusahaan fokus pada proses transformasi di seluruh organisasi.

1-C

MENGELOLA ARSITEKTUR PERUSAHAAN

i. Membangun arsitektur teknologi informasi yang terdiri dari proses bisnis, informasi, data, aplikasi, dan hirarki arsitektur teknologi.

ii. Menyusun model yang menggambarkan arsitektur dasar dan target yang sejalan dengan strategi perusahaan dan teknologi informasi.

iii. Menetapkan persyaratan untuk taksonomi, standar, pedoman, prosedur, format, dan penetapan alat yang berkaitan untuk komponen-komponen tersebut.

iv. Memperbaiki keselarasan, meningkatkan *agility,* dan meningkatkan kualitas informasi serta menghasilkan potensi penghematan biaya melalui inisiatif seperti penggunaan kembali komponen *building block*.

1-D

MENGELOLA INOVASI

i. Mempertahankan kesadaran akan perkembangan teknologi informasi dan layanan terkait serta memantau perkembangan teknologi yang muncul.

ii. Secara proaktif mengidentifikasi peluang inovasi dan merencanakan bagaimana memanfaatkan inovasi dalam kaitannya dengan kebutuhan bisnis dan strategi teknologi informasi yang ditetapkan.

iii. Menganalisis peluang inovasi atau pengembangan bisnis yang dapat diciptakan oleh teknologi, layanan, atau inovasi bisnis yang mendukung teknologi informasi, baik melalui teknologi yang telah dimiliki atau melalui inovasi proses bisnis dan teknologi informasi.

iv. Mempengaruhi perencanaan strategis dan keputusan arsitektur perusahaan.

1-E

MENGELOLA PORTOFOLIO

i. Menjalankan arahan strategis yang ditetapkan untuk investaasi yang sejalan dengan visi arsitektur dan peta jalan teknologi informasi perusahaan.

ii. Mempertimbangkan berbagai kategori investasi dan sumber daya serta kendala pendanaan.

iii. Mengevaluasi, memprioritaskan, dan menyeimbangkan program dan layanan; serta mengelola permintaan dalam batasan sumber daya dan pendanaan, berdasarkan keselarasannya dengan tujuan strategis, nilai perusahaan, dan risiko.

iv. Memantau kinerja keseluruhan portofolio produk, layanan dan program, serta mengusulkan penyesuaian yang diperlukan dalam meningkatkan kinerja program, produk dan layanan, atau mengubah prioritas perusahaan.

1-F

MENGELOLA ANGGARAN DAN BIAYA

i. Mengelola aktivitas keuangan terkait teknologi informasi baik dalam bisnis dan fungsi teknologi informasi, yang mencakup anggaran, manajemen biaya dan manfaat, serta memprioritaskan pengeluaran melalui penggunaan praktik penganggaran formal dan sistem alokasi biaya yang adil dan merata untuk perusahaan.

ii. Melakukan Konsultasi dengan pemangku kepentingan untuk mengidentifikasi dan mengendalikan total biaya dan manfaat dalam konteks rencana strategis dan teknis teknologi informasi.

iii. Memulai tindakan korektif jika diperlukan.

1-G

MENGELOLA SUMBER DAYA MANUSIA

Menyusun pendekatan terstruktur untuk memastikan optimalisasi rekrutmen/akuisisi, perencanaan, evaluasi dan pengembangan sumber daya manusia (baik internal maupun eksternal).

1-H **MENGELOLA HUBUNGAN**	i. Mengelola hubungan dengan pemangku kepentingan bisnis dengan cara yang formal dan transparan untuk memastikan rasa saling percaya dan bersama-sama fokus untuk mencapai tujuan strategis dalam batasan anggaran dan toleransi risiko ii. Mendasarkan hubungan pada komunikasi yang terbuka, transparan, dan bersedia untuk mengambil tanggung jawab serta akuntabilitas atas keputusan penting bagi kedua belah pihak. iii. Bisnis dan teknologi informasi harus bekerja sama untuk mencapai *outcome* terbaik dalam mendukung tujuan perusahaan.
1-I **MENGELOLA PERJANJIAN KERJA SAMA**	Menyelaraskan produk dan layanan serta tingkat layanan teknologi informasi yang mendukung dan sesuai dengan kebutuhan dan harapan perusahaan, termasuk identifikasi, spesifikasi, desain, penerbitan perjanjian, pemantauan produk dan layanan teknologi informasi, tingkat layanan, dan indikator kinerja.
1-J **MENGELOLA PENYEDIA JASA LAYANAN/ VENDOR**	Mengelola produk dan layanan terkait teknologi informasi yang disediakan oleh semua penyedia jasa/vendor agar dapat memenuhi kebutuhan perusahaan. Hal ini mencakup pencarian dan pemilihan vendor, mengelola hubungan, mengelola kontrak, dan meninjau dan memantau kinerja vendor dan ekosistem vendor (termasuk rantai pasokan hulu) telah berjalan dengan efektif.
1-K **MENGELOLA KUALITAS**	Menetapkan dan mengkomunikasikan persyaratan kualitas dalam semua proses, prosedur, dan *outcome* terkait. Mengaktifkan kontrol, pemantauan berkelanjutan, dan penggunaan praktik dan standar yang telah terbukti dalam upaya peningkatan dan efisiensi berkelanjutan.
1-L **MENGELOLA RISIKO**	Senantiasa mengidentifikasi, mengukur, dan mengurangi risiko terkait teknologi informasi dalam tingkat toleransi yang ditetapkan perusahaan.

1-M **MENGELOLA KEAMANAN**	Menentukan, mengoperasikan, dan memantau sistem manajemen keamanan informasi.
1-N **MENGELOLA DATA**	Mencapai dan mempertahankan pengelolaan aset data perusahaan yang efektif di seluruh siklus hidup data, mulai dari pembuatan hingga pengiriman, pemeliharaan, dan pengarsipan.
02 ***BUILD, ACQUIRE, AND IMPLEMENT* (BAI)**	***Build, Acquire***, *and* ***Implement*** (BAI) mencakup aktivitas akuisisi dan implementasi dari solusi teknologi informasi serta integrasinya pada proses bisnis sebagai berikut:
2-A **MENGELOLA PROGRAM**	i. Mengelola semua program dari portofolio investasi sesuai dengan strategi perusahaan secara terkoordinasi. ii. Merencanakan, mengontrol, dan menjalankan program, dan memantau hasil yang diharapkan dari program.
2-B **MENGELOLA KRITERIA KEBUTUHAN**	i. Identifikasi solusi dan analisis kebutuhan sebelum akuisisi atau pengembangan untuk memastikan bahwa solusi tersebut selaras dengan kebutuhan strategis perusahaan yang mencakup proses bisnis, aplikasi, informasi/data, infrastruktur, dan layanan ii. Melakukan analisis berbagai pilihan yang layak bagi pemangku kepentingan terkait, termasuk biaya dan manfaat, analisis risiko, serta persetujuan kebutuhan dan solusi yang diusulkan.

2-C

MENGELOLA IDENTIFIKASI SOLUSI DAN PENGEMBANGAN

i. Menyusun dan memelihara produk dan layanan yang teridentifikasi (teknologi, proses bisnis, dan alur kerja) sesuai dengan kebutuhan perusahaan yang mencakup desain, pengembangan, pengadaan/sumber, dan kemitraan dengan vendor.

ii. Mengelola konfigurasi, persiapan pengujian, pengujian dan pemeliharaan proses bisnis, aplikasi, informasi/data, infrastruktur, dan layanan.

2-D

MENGELOLA KETERSEDIAAN DAN KAPASITAS

i. Menyeimbangkan kebutuhan saat ini dan masa depan terkait ketersediaan, kinerja, dan kapasitas dengan penyediaan layanan yang hemat biaya.

ii. Menilai kemampuan saat ini, memprediksi kebutuhan masa depan berdasarkan kebutuhan bisnis, analisis dampak bisnis, dan penilaian risiko untuk merencanakan dan mengimplementasikan tindakan yang diperlukan untuk memenuhi persyaratan yang diidentifikasi.

2-E

MENGELOLA PERUBAHAN ORGANISASI

Maksimalkan kemungkinan keberhasilan penerapan perubahan organisasi yang berkelanjutan dengan cepat dan dengan risiko yang lebih rendah.

2-F

MENGELOLA PERUBAHAN TEKNOLOGI INFORMASI

Mengelola semua perubahan secara terkendali yang mencakup perubahan standar dan pemeliharaan darurat yang berkaitan dengan proses bisnis, aplikasi, dan infrastruktur termasuk standar dan prosedur perubahan, penilaian dampak, prioritas dan otorisasi, perubahan darurat, pelacakan, pelaporan, penutupan, dan dokumentasi.

2-G

MENGELOLA AKSEPTASI PERUBAHAN DAN TRANSISI TEKNOLOGI INFORMASI

Pengelolaan akseptasi perubahan dan transisi teknologi informasi yang meliputi perencanaan implementasi, konversi sistem dan data, pengujian akseptasi, persiapan rilis, perpindahan ke pengembangan/produksi proses bisnis dan layanan teknologi informasi baru atau perubahan, dukungan pengembangan/produksi, dan tinjauan pasca-implementasi.

2-H

MENGELOLA PENGETAHUAN

i. Menjaga ketersediaan pengetahuan dan informasi yang relevan, terkini, tervalidasi, dan andal untuk mendukung semua aktivitas proses serta untuk memfasilitasi pengambilan keputusan terkait tata kelola dan manajemen teknologi informasi perusahaan.

ii. Merencanakan identifikasi, pengumpulan, pengorganisasian, pemeliharaan, penggunaan, dan penghentian pengetahuan.

2-I

MENGELOLA ASET

i. Mengelola aset teknologi informasi sepanjang siklus hidupnya untuk memastikan bahwa penggunaannya memberikan nilai/manfaat dengan biaya optimal, beroperasi sesuai dengan tujuan, dan dilindungi secara fisik.

ii. Memastikan bahwa aset-aset yang penting untuk mendukung kemampuan layanan dapat diandalkan dan tersedia.

iii. Mengelola lisensi perangkat lunak untuk memastikan bahwa jumlah optimal dapat diperoleh, dipertahankan, dan digunakan sehubungan dengan keperluan penggunaan bisnis, dan perangkat lunak yang dipasang sesuai dengan perjanjian lisensi.

2-J

MENGELOLA KONFIGURASI

Menetapkan dan memelihara/mempertahankan deskripsi dan hubungan di antara sumber daya dan kemampuan utama yang diperlukan untuk memberikan layanan yang mendukung TI, termasuk mengumpulkan informasi konfigurasi, menetapkan *baseline*, memverifikasi dan mengaudit informasi konfigurasi, serta memperbarui repositori konfigurasi.

2-K

MENGELOLA PROYEK

Mengelola semua proyek yang telah diinisiasi oleh perusahaan sesuai dengan strategi perusahaan dan dengan cara yang terkoordinasi berdasarkan pendekatan standar manajemen proyek termasuk merencanakan, mengontrol dan melaksanakan proyek, serta menutup dengan tinjauan pasca implementasi.

03

***DELIVER, SERVICE, AND SUPPORT* (DSS)**

Deliver, Service, *and* ***Support*** (DSS) mencakup aktivitas membahas operasional penyampaian dan dukungan layanan teknologi informasi, termasuk keamanan.

3-A

MENGELOLA OPERASIONAL

Mengkoordinasikan dan melaksanakan kegiatan dan prosedur operasional yang diperlukan untuk memberikan layanan teknologi informasi secara internal dan alih daya termasuk pelaksanaan prosedur operasi standar yang telah ditetapkan dan kegiatan pemantauan yang diperlukan.

3-B

MENGELOLA PERMINTAAN DAN INSIDEN LAYANAN

Memberikan respon yang tepat waktu dan efektif terhadap permintaan pengguna dan resolusi semua jenis insiden termasuk layanan normal; merekam dan memenuhi permintaan pengguna; serta merekam, menyelidiki, mendiagnosis, mengeskalasi, dan menyelesaikan insiden.

3-C

MENGELOLA MASALAH

Mengidentifikasi dan mengklasifikasikan masalah dan akar penyebabnya, memberikan resolusi tepat waktu untuk mencegah insiden berulang serta memberikan rekomendasi untuk perbaikan

3-D

MENGELOLA KELANGSUNGAN BISNIS (*BUSINESS CONTINUITY*)

Menetapkan dan memelihara rencana untuk memungkinkan bisnis dan organisasi teknologi informasi merespons insiden dan beradaptasi dengan cepat terhadap gangguan.

3-E

MENGELOLA KEAMANAN LAYANAN

Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. Menetapkan dan memelihara keamanan informasi dan hak akses serta melakukan pemantauan keamanan.

3-F

MENGELOLA KONTROL PROSES BISNIS

i. Menetapkan dan menjaga kontrol proses bisnis yang tepat untuk memastikan bahwa informasi yang terkait dengan dan diproses oleh proses bisnis internal atau alih daya memenuhi semua persyaratan kontrol informasi yang relevan.

ii. Mengidentifikasi persyaratan pengendalian informasi yang relevan.

iii. Mengelola dan mengoperasikan *input, throughput*, dan *output* (kontrol aplikasi) yang memadai untuk memastikan bahwa informasi dan pemrosesan informasi memenuhi persyaratan.

04

***MONITOR, EVALUATE, AND ASSESS* (MEA)**

Monitor, Evaluate, *and* ***Assess*** (MEA) mencakup aktivitas pemantauan kinerja dan kesesuaian teknologi informasi dengan target kinerja internal, tujuan pengendalian internal, dan persyaratan eksternal. Aktivitas dalam domain ini mencakup:

4-A

MENGELOLA PEMANTAUAN KINERJA

i. Mengumpulkan, memvalidasi, dan mengevaluasi keselarasan kinerja dengan tujuan perusahaan.

ii. Memantau proses dan praktik yang berjalan agar sesuai dengan sasaran kinerja yang telah disepakati dan tujuan perusahaan

iii. Memberikan pelaporan yang sistematis dan tepat waktu.

4-B

MENGELOLA SISTEM PENGENDALIAN INTERNAL

i. Memantau secara berkelanjutan dan mengevaluasi lingkungan pengendalian, termasuk melakukan *self-assesments* dan *self-awareness*.

ii. Memungkinkan manajemen untuk mengidentifikasi kekurangan dan ketidakefisienan lingkungan pengendalian dan melakukan tindakan perbaikan.

iii. Merencanakan, mengatur dan memelihara standar penilaian pengendalian internal dan efektivitas pengendalian proses.

4-C

MENGELOLA KEPATUHAN TERHADAP KETENTUAN EKSTERNAL

i. Mengevaluasi bahwa proses teknologi informasi dan proses bisnis yang didukung teknologi informasi patuh terhadap undang-undang, peraturan, dan persyaratan perjanjian

ii. Memperoleh *assurance* bahwa persyaratan telah diidentifikasi dan dipatuhi; mengintegrasikan kepatuhan teknologi informasi dengan kepatuhan perusahaan secara keseluruhan.

4-D

MENGELOLA *ASSURANCE*

i. Merencanakan, dan melaksanakan inisiatif *assurance* untuk mematuhi persyaratan internal, undang-undang, peraturan, dan tujuan strategis.

ii. Memungkinkan manajemen untuk memberikan jaminan yang memadai dan berkelanjutan di perusahaan dengan melakukan tinjauan dan kegiatan independen *assurance*.

Gambar 27 COBIT *Core Model*

Sumber: COBIT (2019)

KOMPONEN DARI SISTEM TATA KELOLA

Untuk memenuhi tujuan tata kelola dan manajemen, setiap perusahaan perlu menetapkan, menyesuaikan, dan mempertahankan sistem tata kelola yang dibangun dari sejumlah komponen. Komponen adalah faktor yang secara individual dan kolektif, berkontribusi pada operasi yang baik dari sistem tata kelola perusahaan atas teknologi informasi. Komponen saling berinteraksi satu dengan lainnya, memberikan hasil dalam suatu sistem tata kelola teknologi informasi yang holistik. Komponen dapat berupa beberapa tipe yang berbeda. Komponen dari sistem tata kelola antara lain meliputi struktur organisasi, kebijakan dan prosedur, item informasi, budaya dan perilaku, kemampuan dan kompetensi, serta layanan, infrastruktur, serta aplikasi.

Gambar 28
Komponen COBIT pada Sistem Tata Kelola

Sumber: COBIT (2019)

1. ***Processes*** menggambarkan suatu kumpulan terorganisir dari praktik dan aktivitas untuk mencapai tujuan yang ada dan prosedur dari kumpulan hasil yang mendukung pencapaian dari semua tujuan teknologi informasi yang saling berhubungan.
2. ***Organizational structures*** adalah entitas pembuat keputusan utama dalam suatu perusahaan.
3. ***Principles, policies, and frameworks*** menerjemahkan perilaku yang diinginkan ke dalam panduan praktis untuk manajemen sehari-hari.
4. ***Information*** harus tersampaikan ke seluruh organisasi dan mencakup semua informasi yang dihasilkan dan digunakan oleh perusahaan.

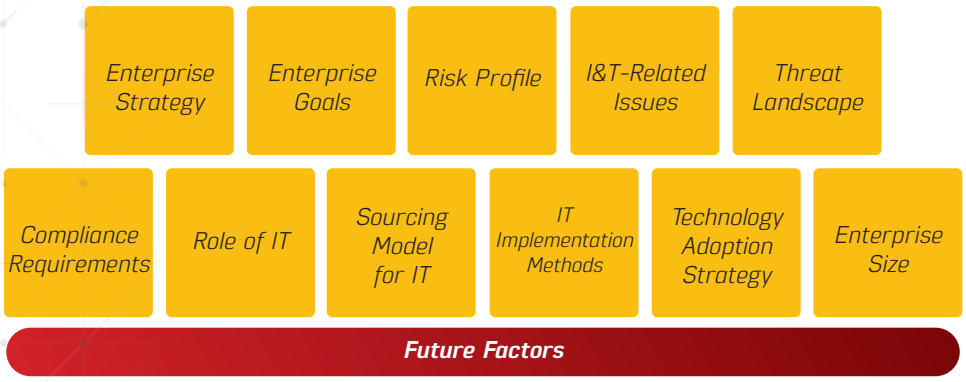
5. ***Culture, ethics, and behavior*** dari individu-individu dan dari perusahaan sebagai faktor keberhasilan kegiatan tata kelola dan manajemen.
6. ***People, skills, and competencies*** dibutuhkan untuk pemilihan yang tepat untuk eksekusi dari tindakan koreksi dan berhasil menyelesaikan semua permasalahan.
7. ***Services, infrastructure, and applications*** meliputi infrastruktur, teknologi, dan aplikasi yang menyediakan perusahaan dengan sistem tata kelola untuk proses teknologi informasi

FAKTOR DESAIN

Faktor desain adalah faktor-faktor yang dapat mempengaruhi desain dari sistem tata kelola perusahaan dan posisinya untuk kesuksesan dalam penggunaan teknologi informasi. Faktor desain terkandung dalam kombinasi dari beberapa hal berikut:

1. Strategi Perusahaan (*Enterprise Strategy*)
2. Tujuan Perusahaan (*Enterprise Goals*)
3. Profil Risiko (*Risk Profile*)
4. Isu Terkait TI (IT *related issues*)
5. Lanskap Ancaman (*Threat Landscape*)
6. Persyaratan Kepatuhan (*Compliance requirements*)
7. Peran dari TI (*Role of* IT)
8. Model Sumber Daya TI (*Sourcing Model for* IT)
9. Metode Implementasi TI (IT *Implementation Methods*)
10. Strategi Penerapan Teknologi (*Technology Adoption Strategy*)
11. Ukuran Perusahaan (*Enterprise Size*)

Gambar 29 Faktor Desain COBIT



Sumber: COBIT (2019)

ARSITEKTUR TEKNOLOGI INFORMASI

Transformasi digital dapat secara maksimal memberikan manfaat bagi Bank jika adopsi teknologi informasi yang dilakukan oleh Bank sesuai dengan kebutuhan proses bisnis Bank; sesuai dengan kebutuhan dan karakteristik konsumen Bank serta mampu mendukung arah, tujuan dan strategi bisnis Bank. Untuk dapat memperoleh manfaat maksimal tersebut, sebelum membangun infrastruktur teknologi informasi, Bank perlu melakukan perancangan arsitektur teknologi informasi sebagai bentuk transformasi digital yang dilakukan Bank.

Arsitektur teknologi informasi adalah cetak biru yang menerjemahkan strategi organisasi menjadi rencana sistem informasi. Arsitektur teknologi informasi disusun berdasarkan pemahaman atas strategi organisasi yang kemudian menjadi landasan dalam mengatur, merencanakan dan menentukan teknologi informasi dalam mendukung proses bisnis organisasi. TOGAF (*The Open Group Architecture Framework*) merupakan kerangka standar global untuk membangun arsitektur teknologi informasi sebuah organisasi yang menyediakan pendekatan secara komprehensif dalam mendesain, merencanakan, mengimplementasi, dan melakukan kontrol atas arsitektur teknologi informasi.

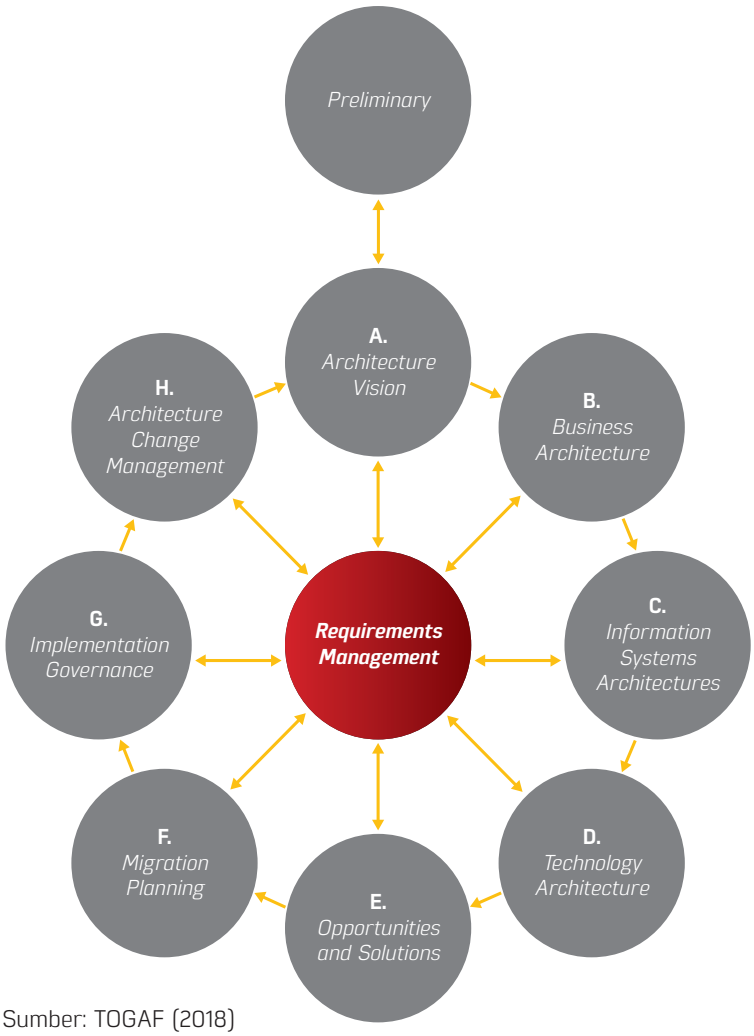
Perancangan Arsitektur teknologi informasi sesuai TOGAF dipandu oleh prinsip-prinsip strategis dan prinsip *best practices* pemilihan teknologi. Prinsip strategis diturunkan dari konsep solusi strategis teknologi informasi yang mengharuskan teknologi yang diimplementasikan organisasi mendukung dan selaras dengan solusi strategis kebutuhan organisasi. Perancangan arsitektur teknologi juga memperhatikan prinsip pemanfaatan aset teknologi yang sudah dimiliki organisasi agar dapat meminimalkan risiko migrasi teknologi. Selain kebutuhan prinsip-prinsip strategis, prinsip-prinsip *best practice* diperlukan untuk memandu pilihan teknologi, yaitu penyeragaman teknologi di seluruh organisasi; penerapan *open standard;* duplikasi komponen-komponen kritis; modularisasi komponen-komponen sistem dan maksimalisasi penggunaan ulang (*reuse*)/penggunaan bersama (*sharing*).

Gambar 30
Prinsip Arsitektur Teknologi Informasi

Sumber: TOGAF (2018)

TOGAF terdiri dari siklus yang bersifat iterasi yang artinya seluruh fase yang ada pada TOGAF dikerjakan secara berulang-ulang sesuai dengan kebutuhan arsitektur untuk mencapai tujuan organisasi. TOGAF terdiri dari 9 fase yaitu *Preliminary*, *Architecture Vision, Business Architecture, Information System Architecture, Technology Architecture, Opportunities and Solutions, Migration Planning, Implementation Governance,* dan *Architecture Change Management.*

Gambar 31
Siklus TOGAF



Sumber: TOGAF (2018)

***PRELIMINARY PHASE* (FASE PENDAHULUAN)**

Fase ini merupakan fase perumusan landasan solusi teknologi informasi bagi organisasi baik di tingkat strategis maupun operasional. Fase ini mencakup aktivitas persiapan untuk menyusun kapabilitas arsitektur termasuk kustomisasi TOGAF; mendefinisikan prinsip-prinsip arsitektur serta menspesifikasikan *what, who, where, when, why* dan *how* dari arsitektur itu sendiri. Tahapan-tahapan yang akan dilakukan pada fase ini adalah:

a. Menentukan prinsip-prinsip sebagai acuan perencanaan arsitektur organisasi.

b. Menentukan cakupan dari apa yang akan dibuat (*What*).

c. Menentukan siapa saja aktor yang akan bertanggung jawab untuk mengerjakan perencanaan arsitektur organisasi (*Who*).

d. Menentukan lokasi di mana perencanaan arsitektur organisasi dilakukan (*Where*).

e. Menentukan waktu mulai dan kapan target penyelesaian perencanaan arsitektur organisasi ini selesai dikerjakan (*When*).

f. Merumuskan alasan mengapa perencanaan arsitektur organisasi perlu dilakukan (*Why*).

g. Menjelaskan bagaimana perencanaan arsitektur organisasi ini dilakukan (*How*).

***PHASE A – ARCHITECTURE VISION* (GAMBARAN ARSITEKTUR)**

Fase ini merupakan tahap menetapkan gambaran umum bagaimana teknologi diterapkan untuk mendukung strategi bisnis organisasi. Fase ini merupakan fase inisiasi dari siklus pengembangan arsitektur yang mencakup pendefinisian ruang lingkup, identifikasi *stakeholders,* dan penyusunan visi arsitektur untuk memulai pengembangan arsitektur.

Tahapan-tahapan yang akan dilakukan pada fase ini adalah sebagai berikut:

a. Mendefinisikan visi, misi, dan tujuan organisasi.

b. Menentukan seluruh aktivitas dalam organisasi, meliputi aktivitas utama dan aktivitas pendukung.

c. Menentukan hubungan *stakeholder* dengan aktivitas utama dan pendukung menggunakan *stakeholder viewpoint* untuk memetakan kepentingan setiap aktor pada visi perusahaan.

***PHASE B – BUSINESS ARCHITECTURE* (ARSITEKTUR BISNIS)**

Fase ini merupakan tahap mendefinisikan dekomposisi (struktur) aktivitas dalam proses-proses bisnis organisasi. Pada fase ini dilakukan analisis terhadap proses bisnis yang sedang berjalan saat ini. Tahapan yang dilakukan mencakup:

a. Melakukan analisis terhadap proses bisnis saat ini.

b. Menentukan target arsitektur bisnis yang mendukung visi arsitektur.

c. Melakukan analisis kesenjangan (*Gap Analysis*) terhadap proses bisnis. Analisis kesenjangan dilakukan terhadap kesenjangan bisnis, data, aplikasi, dan teknologi.

Fase ini menghasilkan usulan proses bisnis yang diajukan untuk memperbaiki proses bisnis saat ini dan mendukung pencapaian visi pembangunan arsitektur.

***PHASE C – INFORMATION SYSTEM ARCHITECTURE* (ARSITEKTUR SISTEM INFORMASI)**

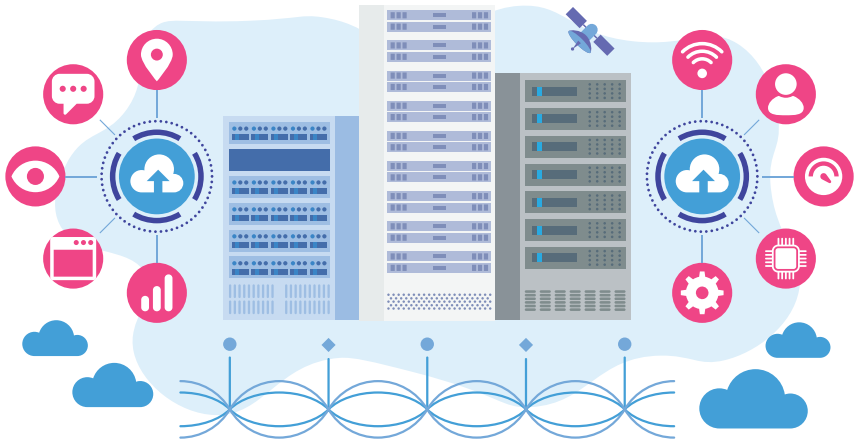
Fase ini mendeskripsikan sistem-sistem aplikasi dan perannya dalam mendukung proses-proses bisnis. Fase ini menentukan bagaimana membangun arsitektur sistem informasi yang meliputi arsitektur data dan arsitektur aplikasi yang akan digunakan.

a. *Data Architecture* (Arsitektur Data)

Arsitektur data akan mengidentifikasi seluruh komponen data yang digunakan oleh aplikasi untuk menghasilkan informasi yang dibutuhkan organisasi. Tahapan untuk membuat arsitektur data mencakup:

i. Mengidentifikasi struktur aliran informasi yang saat ini berjalan di organisasi.

ii. Membuat pemodelan arsitektur data usulan.



b. *Aplication Architecture* (Arsitektur Aplikasi)

Arsitektur aplikasi digunakan untuk merancang suatu aplikasi yang telah didefinisikan pada arsitektur bisnis (aktivitas tugas pokok dan fungsi). Tahapan-tahapan yang digunakan pada fase ini adalah:

i. Menganalisis aplikasi yang saat ini berjalan pada organisasi.

ii. Menentukan dan mendefinisikan aplikasi-aplikasi yang dibutuhkan organisasi.

iii. Membuat pemodelan aplikasi-aplikasi yang dibutuhkan tersebut dan hubungannya satu dengan yang lainnya.

***PHASE D – TECHNOLOGY ARCHITECTURE* (ARSITEKTUR TEKNOLOGI)**

Konfigurasi infrastruktur dibutuhkan untuk menjalankan aplikasi-aplikasi pada Arsitektur Sistem Informasi. Fase ini menggambarkan struktur teknologi yang dibutuhkan untuk menunjang operasional aplikasi yang telah dimodelkan pada arsitektur aplikasi. Tahapan-tahapan untuk membuat arsitektur teknologi mencakup:

a. Memodelkan konfigurasi jaringan awal pada organisasi.

b. Menentukan dan mendefinisikan infrastruktur teknologi yang dibutuhkan organisasi.

c. Mendefinisikan kebutuhan infrastruktur teknologi informasi untuk mendukung aplikasi.

***PHASE E – OPPORTUNITIES AND SOLUTIONS* (PELUANG DAN SOLUSI)**

Fase ini merupakan fase analisis gap antara arsitektur saat ini dan masa depan. Fase ini akan menguraikan hasil analisis gap mulai dari arsitektur bisnis sampai arsitektur teknologi dan perhitungan estimasi biaya investasi pada organisasi.

***PHASE F – MIGRATION PLANNING* (RENCANA MIGRASI)**

Pada fase ini akan dilakukan persiapan dan perencanaan migrasi untuk implementasi arsitektur aplikasi baru yang dibangun pada fase sebelumnya. Tahapan-tahapan pada fase ini mencakup:

a. Membuat rencana migrasi dan urutan prioritas pengimplementasian aplikasi.

b. Menetapkan dan menggambarkan *roadmap* aplikasi.

***PHASE G – IMPLEMENTATION GOVERNANCE* (IMPLEMENTASI TATA KELOLA)**

Fase ini merupakan fase pengawasan kepatuhan proyek-proyek yang dilakukan terhadap arsitektur yang telah dibangun.

***PHASE H – ARCHITECTURE CHANGE MANAGE* (MANAJEMEN PERUBAHAN ARSITEKTUR)**

Fase ini merupakan fase (Re)evaluasi relevansi arsitektur yang telah dibangun dan tren teknologi terkini. Pada tahap ini dilakukan penetapan rencana manajemen arsitektur dari sistem yang baru dengan cara melakukan pengawasan terhadap perkembangan teknologi dan perubahan lingkungan organisasi, baik internal maupun eksternal serta menentukan apakah akan dilakukan siklus penambangan arsitektur organisasi berikutnya.

***REQUIREMENT MANAGEMENT* (MANAJEMEN KEBUTUHAN)**

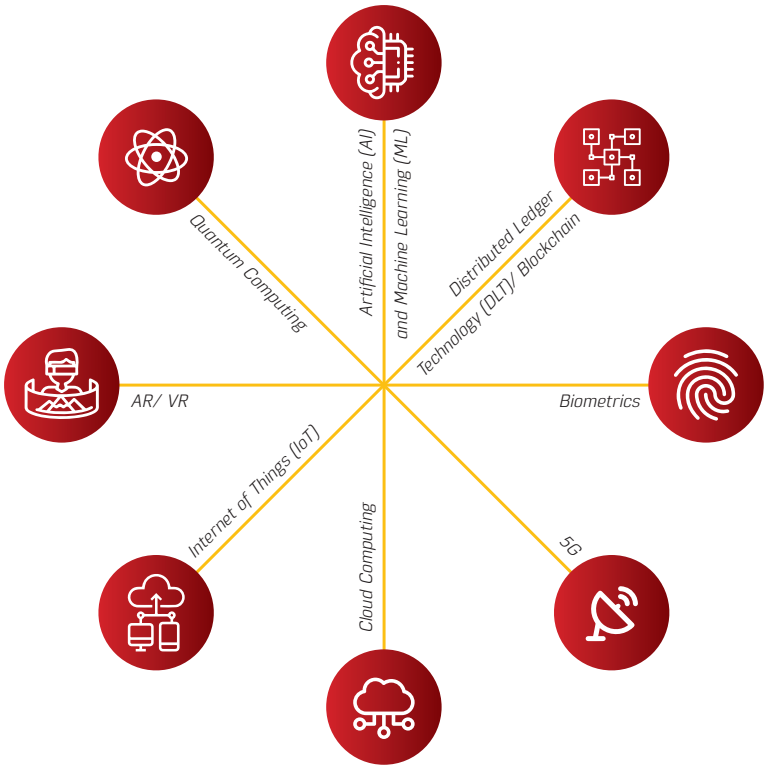
Pada fase ini dilakukan analisis kebutuhan objek dan kebutuhan pengguna sistem. Tujuan dari fase ini yaitu untuk melakukan analisis dan mengelola kebutuhan arsitektur terhadap seluruh tahapan. Langkah-langkah yang dilakukan pada fase ini mencakup:

a. Mengidentifikasi permasalahan yang ada pada objek.

b. Mempersiapkan solusi aktivitas atas permasalahan yang telah teridentifikasi.

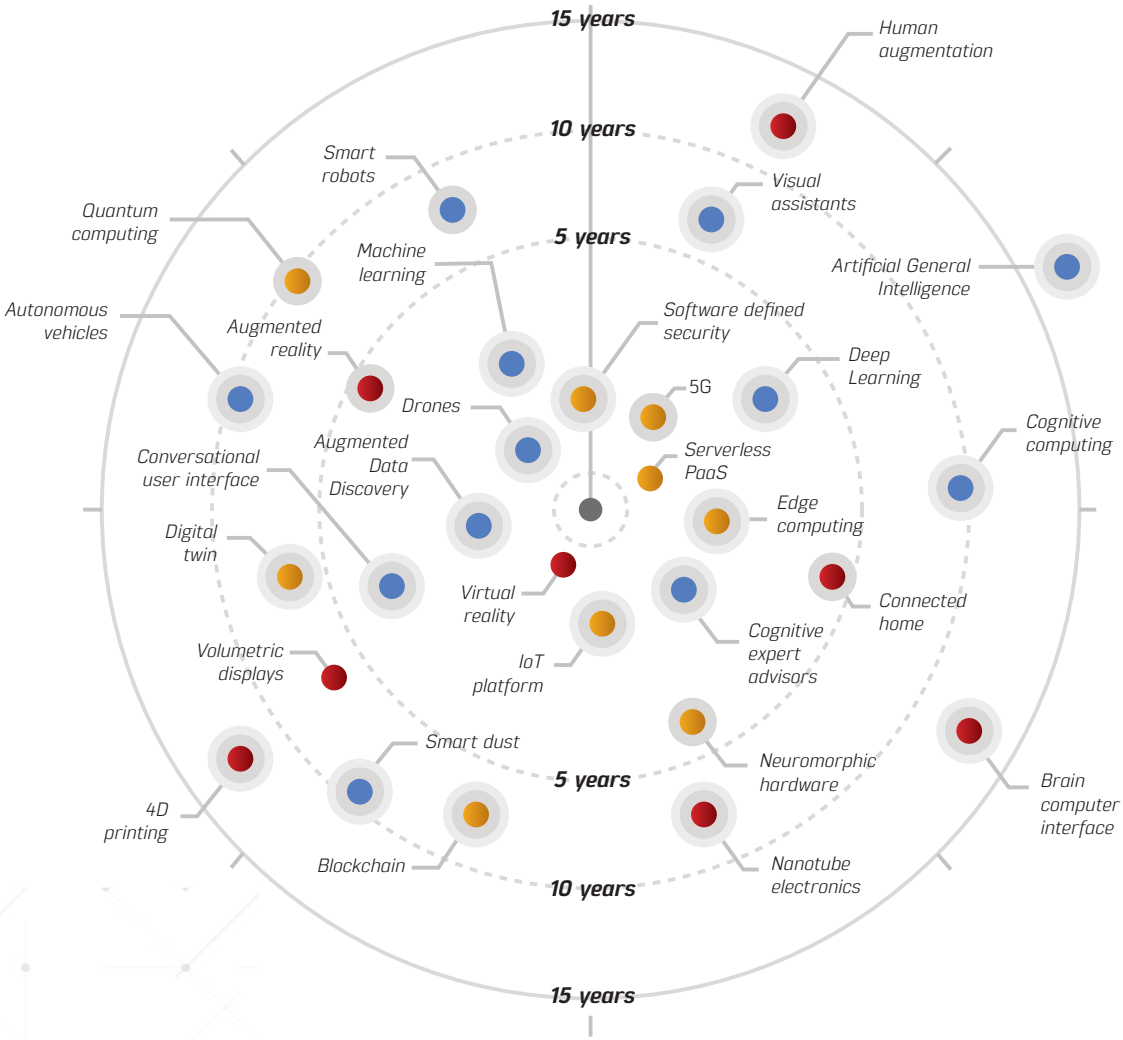
c. Mempersiapkan solusi sistem informasi atas permasalahan yang telah teridentifikasi.

ADOPSI TEKNOLOGI INFORMASI TERKINI



Teknologi akan membuat perbankan lebih personal dan ada di mana-mana di seluruh perangkat dan aplikasi. Masa depan ini akan dimungkinkan oleh sejumlah inovasi yang beralih dari *emerging technology* menjadi *transformative technology.* Teknologi tersebut akan menyebabkan aspek perbankan menjadi tidak dapat dikenali dari apa yang kita alami saat ini. Teknologi mampu mengubah saluran, layanan, dan peran Bank dalam kehidupan sehari-hari. Menurut KPMG (2019) dalam 15 tahun ke depan perkembangan dan kapabilitas dari 8 (delapan) teknologi yaitu *Artificial intelligence, Blockchain, Biometrics,* 5G, *Cloud Computing, Internet of Things,* AR/VR, dan *Quantum Computing* akan membawa manfaat besar bagi perbankan. Teknologi ini tidak bekerja secara terpisah, dan sering kali penggunaan teknologi tersebut secara bersamaan dapat membawa potensial terbesar pada hubungan Bank dan konsumen ke depan. Untuk itu perbankan Indonesia didorong untuk dapat mempersiapkan diri untuk mengadopsi teknologi tersebut.

Gambar 32 Teknologi Informasi pada Perbankan ke Depan



Sumber: KMPG (2019)

Salah satu jenis emerging technology adalah *Artificial Intelligence* (AI) atau kecerdasan buatan yang merupakan teknologi yang telah berhasil diciptakan oleh manusia untuk membantu dan memudahkan berbagai kegiatan yang seharusnya dikerjakan oleh manusia itu sendiri. AI kemudian digadang-gadang akan menjadi teknologi kunci di masa depan. Meskipun AI digadang-gadang membawa manfaat signifikan di berbagai bidang kehidupan, namun, banyak yang menganggap terdapat bahaya yang tersimpan dari teknologi ini. AI yang sedang tren saat ini bagai pisau bermata dua. Dampak AI dapat menjadi bencana besar dan buruk bagi peradaban manusia, kecuali perkembangannya yang cepat dikontrol secara ketat dan etis.

Mempertimbangkan potensi risiko yang menyertai dalam implementasi *emerging technology* seperti potensi risiko dalam konteks AI, maka dalam mengadopsi berbagai e*merging technology and application* termasuk teknologi informasi, Bank perlu menerapkan prinsip adopsi teknologi informasi yang bertanggung jawab (*Responsible Adoption Principles*) sebagai berikut :

1. Adopsi teknologi informasi harus memberi manfaat bagi pertumbuhan inklusif, pembangunan berkelanjutan, dan kesejahteraan umat manusia.

2. Teknologi informasi khususnya yang berbasis AI harus dirancang dengan cara yang menghormati aturan hukum, hak asasi manusia, nilai-nilai demokrasi dan keragaman, serta harus mencakup pengamanan yang sesuai seperti memungkinkan intervensi manusia jika diperlukan dan lain sebagainya.

3. Transparansi dan pengungkapan yang bertanggung jawab atas teknologi informasi untuk memastikan bahwa konsumen memahami output yang dihasilkan.

4. Bank yang mengembangkan, menerapkan, atau mengoperasikan teknologi informasi harus bertanggung jawab atas fungsinya.

5. Teknologi informasi harus berfungsi dengan kokoh dan aman sepanjang siklus hidupnya serta potensi risiko yang dapat ditimbulkan oleh sistem tersebut harus terus diukur dan dikelola.

Gambar 33 Prinsip Adopsi *Emerging Technology*

Sumber: OECD (2019), dimodifikasi

MANAJEMEN RISIKO

Pemanfaatan dan penggunaan teknologi informasi perlu didukung oleh penerapan manajemen risiko yang efektif untuk memitigasi berbagai potensi risiko termasuk risiko alih daya dan risiko keamanan siber.

Pemanfataan teknologi informasi membawa suatu risiko tersendiri bagi perbankan. Beberapa risiko yang biasanya muncul pada saat penggunaan teknologi informasi yaitu adanya serangan siber yang dapat mengganggu kinerja dari teknologi informasi, serangan *cracker* yang dapat mengacaukan sistem bahkan sampai mencuri data rahasia suatu perusahaan, kesalahan dan kerusakan sistem pendukung seperti jaringan listrik putus, dan lain sebagainya. Untuk itu, perbankan perlu menerapkan secara efektif manajemen risiko teknologi informasi guna memitigasi berbagai risiko tersebut. Sejalan dengan ini, perbankan perlu juga menerapkan keamanan siber secara memadai. Selain itu, perbankan juga perlu menerapkan manajemen alih daya (*outsourcing*) yang baik dalam hal menggunakan pihak ketiga untuk menyediakan teknologi informasi.

MANAJEMEN RISIKO TEKNOLOGI INFORMASI

Manajemen Risiko Teknologi Informasi (MRTI) adalah penerapan dari prinsip-prinsip manajemen risiko terhadap perusahaan yang memanfaatkan teknologi informasi dengan tujuan untuk dapat mengelola risiko-risiko yang berhubungan dengan perusahaan tersebut. Risiko-risiko yang dikelola meliputi kepemilikan, operasional, keterkaitan, dampak, dan penggunaan dari teknologi informasi pada sebuah perusahaan.

Teknologi informasi merupakan aset yang berharga bagi Bank sehingga pengelolaannya bukan hanya merupakan tanggung jawab unit kerja penyelenggara teknologi informasi namun juga seluruh pihak yang menggunakan. Penerapan manajemen risiko harus dilakukan secara terintegrasi dalam setiap tahapan penggunaan Teknologi Informasi sejak proses perencanaan, pengadaan, pengembangan, operasional, pemeliharaan hingga penghentian, dan penghapusan sumber daya teknologi informasi. Penerapan manajemen risiko teknologi informasi paling sedikit mencakup:

1. Pengawasan aktif Direksi dan Dewan Komisaris;
2. Kecukupan kebijakan, standar, dan prosedur penggunaan teknologi informasi;
3. Kecukupan proses identifikasi, pengukuran, pemantauan dan pengendalian risiko penggunaan Teknologi Informasi; dan
4. Sistem pengendalian intern atas penggunaan teknologi informasi.

01

IDENTIFIKASI RISIKO TI BERDASARKAN *ENTERPRISE RISK POSTURE AND APETITE* (*IDENTIFY RISK*)

Proses Manajemen Risiko Terkait Teknologi Informasi mencakup:

Risiko teknologi informasi termasuk kegagalan perangkat keras dan perangkat lunak, kesalahan manusia (seperti persoalan *network control access*, perlakuan data, kebocoran kata sandi), *spam*, virus, kebocoran dan kehilangan data, serangan berbahaya (*malicious attacks* termasuk *cyberattacks*), serta bencana alam. Penilaian risiko teknologi informasi yang efektif meliputi mengidentifikasi risiko berdasarkan kemungkinan bahwa risiko akan terjadi, biaya dampak bisnis dan pemulihan (*business impact analysis and recovery plan*). Identifikasi risiko harus dilakukan pada seluruh level tata kelola dan perusahaan dan merupakan bagian dari hasil *continuous auditing*. Metodologi Penilaian (*Assessment*) Risiko teknologi informasi meliputi:

a. *Asset Identification*
b. *Threat Identification: Threat - Source Identification, Motivation and Threat Actions*
c. *Vulnerability Identification*
d. *Control Analysis*
e. *Risk Assessment: Risk Identification and Measurement*
f. *Risk Acceptance Criteria*

Bank harus memastikan kecukupan proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko penggunaan Teknologi Informasi yang diimplementasikan.

02

MENGELOLA RISIKO TI MELALUI IMPLEMENTASI PROSES DAN KONTROL (*MANAGE RISK*)

Dalam hal penerapan Manajemen Risiko Teknologi Informasi, Bank perlu menetapkan Rencana Strategis Teknologi Informasi, kebijakan, standar dan prosedur secara konsisten dan berkesinambungan sebagai langkah dalam mengelola risikoteknologi informasi melalui implementasi proses dan kontrol. Bank perlu memastikan kecukupan kebijakan, standar, dan prosedur penggunaan teknologi informasi; serta sistem pengendalian internal atas penggunaan teknologi informasi. Mengelola risiko teknologi informasi adalah proses terstruktur yang melibatkan serangkaian aktivitas yang dirancang untuk:

1. mengidentifikasi risiko
2. menilai risiko
3. mengurangi risiko
4. mengembangkan rencana respons
5. meninjau prosedur manajemen risiko (sistem pengendalian internal atas penggunaan teknologi informasi)

Dalam pengelolaan risiko terdapat dua proses yang terlibat yakni analitik dan prediksi pemodelan dari data-data yang didapatkan.

03

PERLAKUAN TERKAIT ISU MAUPUN KEKURANGAN TI PERUSAHAAN (*MITIGATE RISK*)

Dalam hal memitigasi risiko dan penanganan isu terkait teknologi informasi, Bank perlu melakukan sejumlah prosedur. Bank dapat menangani (perlakuan) risiko dengan beberapa metode meliputi:

a. Mitigasi Risiko
b. Transfer Risiko
c. Penghindaran Risiko
d. Penerimaan Risiko

Dalam mitigasi risiko terdapat dua proses yang terlibat yakni prediksi pemodelan yang masih berlangsung dan proses *remote auditing*.

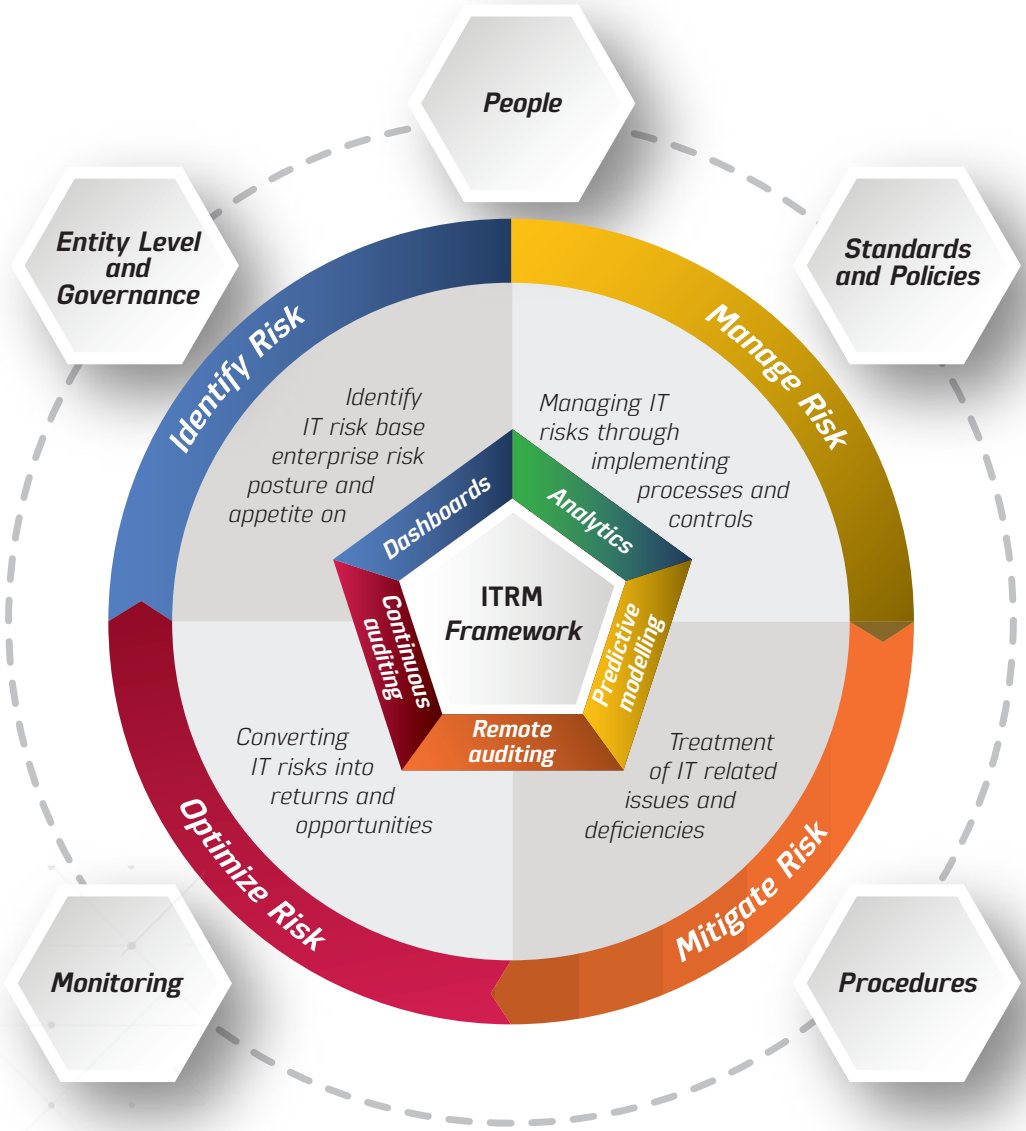
04

MENGUBAH RISIKO TI MENJADI *RETURN* DAN *OPPORTUNITES* (*OPTIMIZE RISK–MONITORING & REVIEW*)

Bank harus memastikan bahwa Teknologi Informasi yang digunakan Bank dapat mendukung perkembangan usaha Bank, pencapaian tujuan bisnis Bank dan kelangsungan pelayanan terhadap konsumen. Oleh karena itu, *Bank remote* dan *continuous auditing* sangat berperan penting dalam mengoptimalisasi risiko sehingga optimasi *return* dan *opportunities* bagi pertumbuhan dan perkembangan bisnis dapat dicapai. Dalam hal *optimizing risk* (*optimizing information technology and information security*), penting bagi Bank untuk memperhatikan aspek-aspek berikut ini:

a. *Confidentiality*: informasi hanya dapat diakses oleh mereka yang memiliki hak atau kebutuhan untuk melihatnya.
b. *Integrity*: informasinya akurat, valid, dan dapat diandalkan.
c. *Availability*: informasi, sumber daya, dan layanan tersedia saat dibutuhkan.
d. *Accountability*: setiap tindakan transaksi dapat dikaitkan dengan individu yang bertanggung jawab.
e. *Provenance*: setiap bagian informasi (atau setiap item data) diketahui dan didefinisikan dengan baik.

Gambar 34 Proses Manajemen Risiko Teknologi Informasi



Sumber: KPMG (2019)

ALIH DAYA (*OUTSOURCING*)

Dalam melakukan kegiatan penyerahan pekerjaan kepada pihak lain (alih daya/*outsourcing*) khususnya di bidang Teknologi Informasi, Bank menghadapi berbagai risiko yang dapat timbul seperti risiko strategis, risiko operasional, risiko regulasi dan kepatuhan, risiko reputasi, dan risiko konsentrasi. Untuk meminimalisir berbagai potensi risiko tersebut, Bank perlu menerapkan manajemen risiko terhadap kegiatan alih daya terutama dengan memperhatikan secara seksama prinsip alih daya serta proses dan tahapan alih daya dengan baik.

PRINSIP ALIH DAYA

Bank dapat melakukan kegiatan alih daya secara optimal dengan tetap memenuhi prinsip kehati-hatian dan manajemen risiko yang memadai. Prinsip alih daya teknologi informasi meliputi 8 (delapan) elemen sebagai berikut:

01 TATA KELOLA (*GOVERNANCE*)

a. Strategi: Bank harus memiliki strategi alih daya yang konsisten dengan strategi teknologi informasi Bank yang relevan, antara lain kesesuaian dengan strategi teknologi informasi dan komunikasi, strategi keamanan informasi, strategi manajemen risiko operasional, serta kebijakan dan prosedur internal Bank, termasuk alokasi tanggung jawab, sumber daya, dan pemantauan atas kegiatan alih daya.

b. Akuntabilitas: Direksi dan Dewan Komisaris memastikan akuntabilitas dari kebijakan dan kegiatan alih daya.

c. Penilaian Risiko: Direksi dan Dewan Komisaris harus memastikan bahwa potensi risiko telah diidentifikasi melalui penilaian risiko secara komprehensif sebelum perjanjian alih daya dilakukan. Penilaian risiko antara lain mencakup:

   i. Identifikasi fungsi kritikal dan penting (*critical and important functions*) yang akan dialihdayakan kepada pihak lain.

   ii. Analisis manfaat dan biaya (*cost and benefit analysis*).

   iii. Identifikasi potensi risiko dari kegiatan alih daya antara lain terkait teknologi komunikasi (*communication technology*), keamanan informasi (*information security*), kelangsungan bisnis (*business continuity*), aspek hukum dan kepatuhan (*legal and compliance*), risiko reputasi (*reputational risks*), risiko operasional (*operational risks*), risiko konsentrasi (*concentration risk*), dan bagaimana dampaknya terhadap profil risiko Bank.

d. Manajemen Risiko: Bank melakukan pengelolaan risiko antara lain mencakup pengawasan aktif Direksi dan Dewan Komisaris, kecukupan kebijakan dan prosedur, kecukupan proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko, serta sistem informasi manajemen risiko dan sistem pengendalian intern.

02

UJI KELAYAKAN (*DUE DILIGENCE*)

a. Bank perlu melakukan uji kelayakan (*due diligence*) dan memiliki prosedur yang sesuai dalam menentukan perusahaan penyedia jasa alih daya. Selain mempertimbangkan faktor biaya dan kualitas layanan, dalam memilih perusahaan penyedia jasa (*provider*) alih daya, Bank perlu memperhatikan beberapa aspek antara lain:

i. kondisi kesehatan keuangan (*financial soundness*)

ii. reputasi

iii. keahlian manajemen

iv. kemampuan teknis

v. kapasitas dan kemampuan operasional

vi. kesesuaian dengan budaya perusahaan dan strategi pengembangan Bank ke depan

vii. memiliki pemahaman yang memadai terkait industri jasa keuangan khususnya perbankan

viii. memiliki kapasitas untuk dapat beradaptasi dengan inovasi pasar

b. Dalam hal terdapat kemungkinan penyedia jasa melakukan *sub-outcourcing* (pengalihdayaan kembali) yang material, Bank perlu memperhatikan dampak/potensi risiko yang mungkin terjadi dari kompleksitas *sub-outsourcing* terhadap ketahanan operasional Bank.

c. Bank melakukan pemantauan secara berkala untuk memantau kinerja penyedia jasa. Dalam melakukan pemantauan, Bank memperhatikan aspek *materiality* dan *criticality* dari kegiatan yang dialihdayakan kepada *provider*.

d. Penilaian ulang materialitas (*materiality reassessment*) perlu dilakukan ketika terjadi perubahan organisasi yang signifikan pada penyedia jasa (termasuk penyedia jasa *sub-outsourcing*) seperti perubahan kepemilikan atau kondisi keuangan penyedia jasa, yang secara material dapat mengubah sifat, skala, dan kompleksitas risiko yang melekat pada kegiatan alih daya.

---

03 PERSYARATAN KONTRAK (*CONTRACTUAL REQUIREMENT*)

a. Kegiatan alih daya didasarkan atas perjanjian/kontrak tertulis yang mengikat secara hukum antara Bank dan perusahaan penyedia jasa alih daya.

b. Rincian perjanjian disesuaikan dengan aspek *materiality* dan *criticality* dari kegiatan yang dialihdayakan terhadap bisnis Bank.

c. Perjanjian antara Bank dan penyedia jasa harus menetapkan secara jelas jenis dan cakupan layanan yang disediakan oleh penyedia jasa serta hak dan kewajiban dari penyedia jasa, termasuk apabila penyedia jasa akan melakukan *sub-outsourcing* untuk pekerjaan yang material.

d. Bank perlu meninjau isi perjanjian secara berkala untuk mengidentifikasi klausul yang perlu dinegosiasikan dan diperbaharui kembali, disesuaikan dengan standar terkini dan perubahan strategi bisnis Bank.

04

KEAMANAN INFORMASI (*INFORMATION SECURITY*)

a. Bank harus menetapkan persyaratan keamanan informasi dalam kebijakan dan prosedur internal serta dalam perjanjian kerja sama dan melakukan pemantauan berkala atas kepatuhan persyaratan tersebut.

b. Keamanan informasi yang ditetapkan mencakup antara lain keamanan informasi organisasi (*information security organization*), pengelolaan akses (*access management*), manajemen enkripsi dan sandi (*encryption and key management*), keamanan jaringan dan operasi (*operations and network security*), antarmuka pemrograman aplikasi (*application programming interfaces*), lokasi data (*data location*), dan kerahasiaan data pribadi konsumen (*customer data confidentiality*).

c. Bank harus melindungi kerahasiaan data pribadi konsumen dengan memastikan bahwa penyedia jasa menjaga dan memperhatikan persyaratan kerahasiaan data pribadi konsumen. Beberapa upaya yang dapat dilakukan Bank antara lain:

   i. memastikan penyedia jasa beserta pegawai/staf penyedia jasa yang menjadi penanggung jawab mematuhi ketentuan terkait kerahasiaan dan pelindungan data konsumen sesuai ketentuan dan perundang-undangan yang berlaku.

   ii. melakukan tindakan tegas jika terjadi pelanggaran kerahasiaan data konsumen oleh penyedia jasa.

   iii. memastikan penyedia jasa melakukan pemisahan atau *compartmentalisation* (*segregation/compartmentalisation*) data konsumen Bank dengan data konsumen Bank/ perusahaan lain yang menjadi klien penyedia jasa.

   iv. pemberian hak akses atas data konsumen Bank kepada pegawai/staf penyedia jasa yang berwenang dilakukan sesuai kebutuhan.

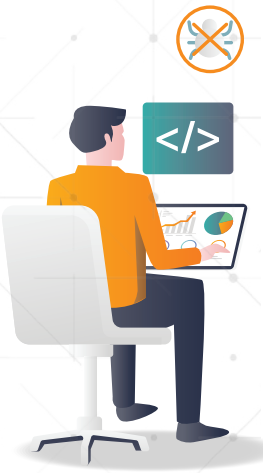
d. Bank harus menginformasikan kepada konsumen mengenai kemungkinan data konsumen dialihdayakan kepada penyedia jasa.

e. Bank perlu memastikan lokasi data dapat diketahui setiap saat termasuk *data-at-rest*, *data-in-use*, dan *data-in-transit*.

f. Dalam hal terjadi pemutusan perjanjian alih daya dengan penyedia jasa, Bank harus memastikan bahwa semua data konsumen telah dikembalikan dari penyedia jasa atau dimusnahkan.

05

PEMANTAUAN DAN KONTROL (*MONITORING AND CONTROL*)



a. Bank harus memiliki prosedur pemantauan dan kontrol yang efektif untuk memantau kinerja penyedia jasa dan mengelola risiko terkait kegiatan yang dialihdaya, terutama jika kegiatan alih daya yang bersifat material terkonsentrasi pada satu perusahaan penyedia jasa. Cakupan aspek yang dilakukan pemantauan dan dikontrol antara lain:

   i. kinerja penyedia jasa sesuai yang disepakati dalam perjanjian;

   ii. masalah yang bersifat material yang dialami oleh penyedia jasa;

   iii. kondisi keuangan dan profil risiko dari penyedia jasa;

   iv. rencana kontijensi (*contingency plan*) dari penyedia jasa, hasil pengujian (*testing*) atas aplikasi, data dan sistem, serta cakupan perbaikan (*scope of improvement*).

b. Bank memiliki prosedur pelaporan atas hasil pemantauan penyedia jasa terkait kegiatan alih daya yang dilakukan sehingga bila terjadi permasalahan dapat segera dieskalasi kepada manajemen Bank dan manajemen dari penyedia jasa

c. Prosedur pemantauan dan kontrol atas perjanjian alih daya perlu ditinjau (*review*) secara berkala oleh satuan kerja audit internal Bank.

d. Dalam hal dilakukan *sub-outsourcing* atas pekerjaan yang material, Bank perlu memastikan penyedia jasa mengelola *sub-outsourcing* secara memadai.

06

RENCANA KELANGSUNGAN BISNIS (*BUSINESS CONTINUITY PLAN*)

a. Bank harus memastikan kelangsungan bisnis (*business continuity*), termasuk menyusun rencana kontijensi (*contingency plan*), recana pemulihan bencana (*disaster recovery plan*), *cloud resiliency,* dan menguji fasilitas cadangan (*backup facilities*) secara berkala.

b. Bank harus memastikan penyedia jasa memiliki *contingency plan* sebagai antisipasi apabila terjadi kegagalan sistem dari penyedia jasa.

c. Dalam menyusun *contingency plan,* Bank harus memperhatikan antara lain alternatif penyedia jasa lain atau opsi untuk mengelola kembali secara *in house* kegiatan yang dialihdaya.

07 HAK AKSES DAN AUDIT (*ACCESS AND AUDIT RIGHTS*)

Bank harus memastikan bahwa informasi relevan terkait kegiatan yang dialihdayakan dapat diakses oleh regulator, auditor, dan Bank sendiri mencakup akses data, sistem TI, dan informasi SDM perusahaan penyedia jasa yang berkaitan dengan tugas-tugas yang dialihdayakan.

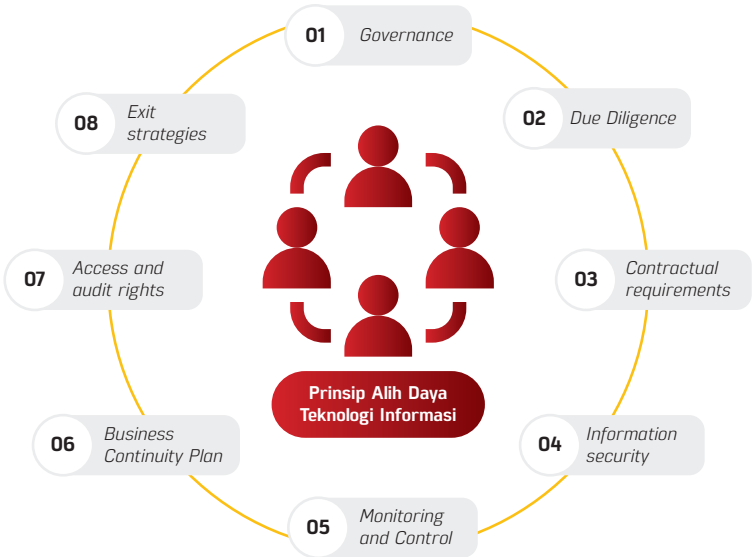
08 STRATEGI PENGAKHIRAN (*EXIT STRATEGIES*)

a. Bank memiliki *exit plan* apabila terjadi gangguan pada kegiatan alih daya dan melakukan penilaian atas ketahanan layanan dan data yang dialihdayakan serta pengujian/simulasi terhadap kelangsungan bisnis.

b. Dalam melakukan simulasi dan menetapkan skenario, Bank dapat mempertimbangkan insiden sebelumnya yang pernah terjadi dan potensi gangguan di masa depan. Skenario dapat bervariasi bergantung pada ukuran dan kompleksitas dari kegiatan Bank.

c. Bank memiliki klausul terkait terminasi kegiatan alih daya dalam perjanjian/kontrak dengan perusahaan penyedia jasa. Dalam hal perjanjian berakhir, Bank perlu memastikan tidak terjadi gangguan pada aktivitas bisnis dan layanan kepada konsumen, termasuk aspek kerahasiaan, integritas, dan ketersediaan data.

Gambar 35
Prinsip Alih Daya Teknologi Informasi



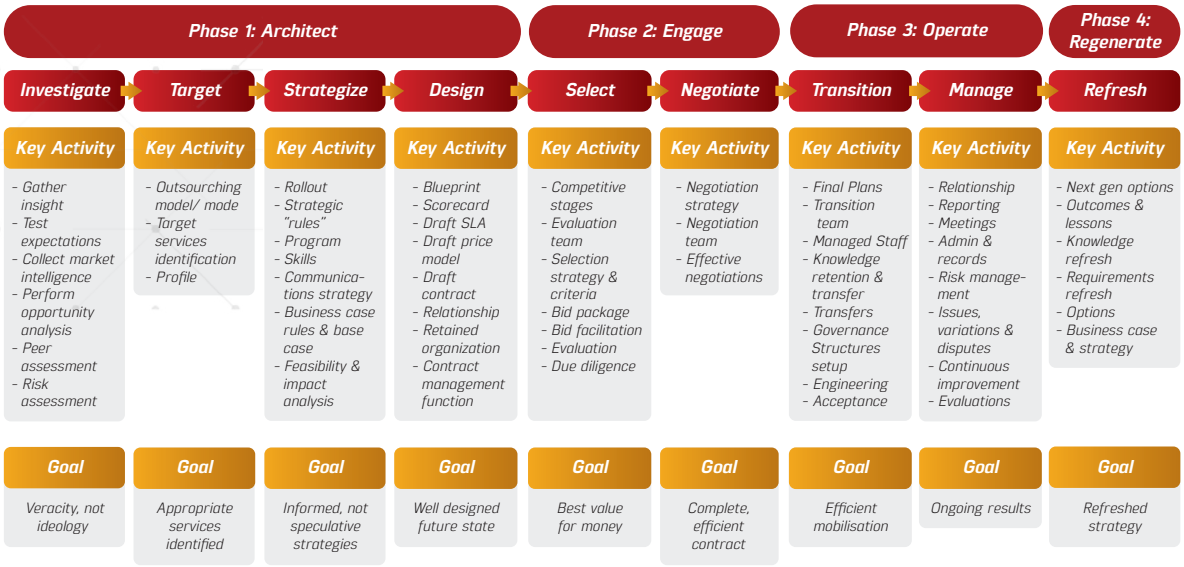
Sumber: IOSCO (2020), ESMA (2020), HKMA, PRA (2021) dimodifikasi

Implementasi prinsip alih daya teknologi informasi diharapkan dapat memberikan manfaat dan keuntungan bagi proses bisnis Bank antara lain efisiensi dalam upaya pemanfaatan Teknologi Informasi, mengurangi biaya teknologi informasi, fokus pada bisnis utama, *update* dengan teknologi terbaru, dan meningkatkan produktivitas.

PROSES DAN TAHAPAN ALIH DAYA

Dalam melakukan kegiatan alih daya teknologi informasi, Bank perlu melakukan pengelolaan, pemantauan dan pengukuran secara berkala atas kualitas pekerjaan yang dialihdayakan dalam rangka meminimalisasi risiko operasional dan memastikan standar pelayanan kepada konsumen tetap terjaga selama periode alih daya. Bank juga perlu memastikan pekerjaan yang dialihdayakan tidak bertentangan dengan strategi dan tujuan alih daya. Oleh karena itu, tahapan proses kegiatan alih daya perlu dilakukan secara sistematis dan terukur dari mulai proses identifikasi, pemilihan, pelaksanaan, dan evaluasi kegiatan Alih Daya. Untuk menyediakan kerangka kerja sistematis dalam proses tahapan alih daya teknologi informasi, dalam Cetak Biru ini disusun proses dan tahapan alih daya dengan mengacu kepada *Outsourcing Lifecycle Model*.

Gambar 36 Tahapan Alih Daya sesuai *Outsourcing Lifecycle Model*



Sumber : Cullen 2006, KPMG 2020 dimodifikasi kembali

Proses dan tahapan alih daya terdiri dari 4 (empat) fase yaitu *Architect, Engage, Operate*, dan *Regenerate*.

Fase 1
ARCHITECT

Fase ini merupakan fondasi awal bagi Bank dalam melakukan keputusan alih daya teknologi informasi yang terdiri atas 4 (empat) tahapan yaitu *investigate, target, strategize*, dan *design*. Dari fase ini diharapkan Bank dapat memahami seberapa besar kebutuhan alih daya, potensi risiko yang timbul, kesesuaian dengan strategi organisasi, dan merancang pengelolaan kegiatan alih daya secara optimal. Adapun aktivitas pada fase ini antara lain :

01
INVESTIGATE

a. Bank menentukan tujuan dan ekspektasi yang ingin dicapai dari kegiatan alih daya teknologi informasi.

b. Bank mengumpulkan informasi menyeluruh terkait pengalaman alih daya teknologi informasi mengingat kegiatan alih daya perlu disesuaikan dengan keadaan, karakteristik, dan strategi dari Bank.

c. Bank melakukan observasi mengenai pihak penyedia jasa alih daya yang potensial.

d. Bank melakukan *peer group analysis* dengan membandingkan performa alih daya yang dicapai oleh Bank lain yang bergerak di segmen pasar sejenis yang melakukan alih daya pada pekerjaan yang sama.

02
TARGET

a. Bank mengidentifikasi kriteria dan jenis pekerjaan yang akan dialihdayakan beserta target yang ingin dicapai.

b. Bank menentukan model alih daya yang akan digunakan dan sesuai dengan kondisi organisasi.

03
STRATEGIZE

a. Bank menentukan strategi alih daya dan memastikan strategi tersebut sejalan dengan strategi teknologi informasi secara keseluruhan.

b. Bank menyusun tahapan dan proses siklus alih daya dari mulai proses pemilihan pihak penyedia jasa hingga evaluasi.

c. Bank menyusun *staffing strategy* untuk menentukan SDM yang diperlukan untuk mengelola dan memantau kegiatan alih daya.

d. Bank melakukan analisis terkait kelayakan, risiko, dan pengukuran dampak dari kegiatan alih daya terhadap operasional dan proses bisnis Bank.

04
DESIGN

a. Bank menyusun *tools* atau parameter untuk menilai dan mengukur kinerja dari pekerjaan yang dialihdayakan seperti *scorecard* atau *score metrics* yang terdiri atas beberapa komponen penilaian.

b. Bank menyiapkan dokumen pendukung antara lain konsep *Service Level Agreement* (SLA), *pricing framework*, dan kontrak perjanjian.

c. Bank merancang struktur internal antara lain mencakup pembagian kewenangan dan peran unit kerja/SDM yang akan bertanggung jawab atas pelaksanaan kegiatan alih daya.

Fase 2
ENGAGE

Fase ini merupakan tahapan saat Bank mulai melakukan seleksi/pemilihan dan negosiasi dengan pihak penyedia jasa alih daya. Fase ini terdiri dari 2 (dua) tahapan yaitu *select* dan *negotiate.*

01
SELECT

a. Bank menentukan kriteria dan standar penilaian dalam pemilihan pihak penyedia jasa alih daya.

b. Bank melakukan *due diligence* atas calon penyedia jasa alih daya dengan memperhatikan beberapa aspek antara lain kinerja perusahaan, kinerja keuangan, harga yang ditawarkan, pengetahuan pihak penyedia jasa atas kondisi pasar dan kebutuhan konsumen, keandalan teknologi, dan keamanan teknologi.

02 *NEGOTIATE*

Bank menyiapkan strategi negosiasi dan menyusun skala prioritas atas aspek yang akan dinegosiasikan serta melakukan negosiasi secara efektif dengan tetap mengacu pada strategi dan parameter yang telah dirancang sebelumnya pada Fase 1.

Fase 3 *OPERATE*

Fase ini merupakan tahapan saat Bank dan pihak penyedia jasa alih daya yang terpilih melaksanakan hal-hal yang telah disepakati sesuai kontrak atau perjanjian kerja sama. Fase ini terdiri dari 2 (dua) tahap yaitu *transition* dan *manage*.

01 *TRANSITION*

a. Bank melakukan koordinasi dan komunikasi yang efektif dengan pihak penyedia jasa alih daya mengenai aspek-aspek yang telah disepakati dalam kontrak/perjanjian kerja sama untuk memastikan kedua belah pihak memiliki pemahaman yang sama dan pihak penyedia jasa memahami dan mematuhi hal-hal yang diperjanjikan.

b. Bank melakukan *transfer knowledge* terkait area pekerjaan yang dialihdayakan kepada pihak penyedia jasa melalui komunikasi yang efektif.

02 *MANAGE*

a. Bank melakukan pemantauan dan *monitoring* atas performa pekerjaan yang dialihdayakan dan kinerja pihak penyedia jasa dengan mengacu pada *scorecard/score metrics*, SLA, kontrak kerja sama yang telah disusun.

b. Bank melakukan pertemuan secara berkala dengan pihak penyedia jasa alih daya.

c. Bank melakukan dokumentasi dan administrasi dokumen yang terkait dengan pekerjaan yang dialihdayakan.

d. Bank melakukan pengelolaan risiko dan melakukan penyelesaian masalah jika terjadi gangguan.

e. Bank melakukan penilaian dan evaluasi atas pekerjaan yang dialihdayakan termasuk menilai tingkat kepuasan konsumen atas layanan yang disediakan.

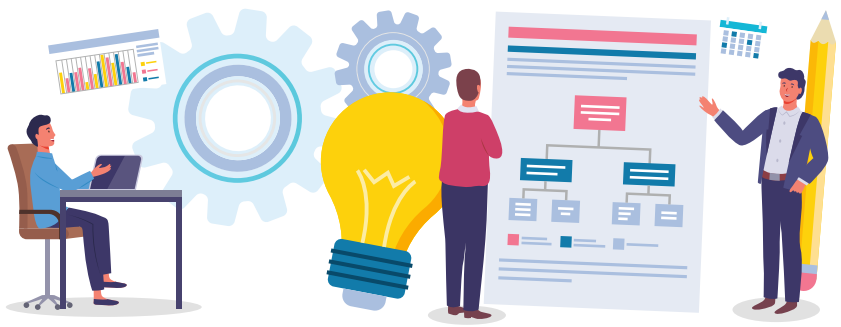
Fase 4
REGENERATE

Fase ini merupakan tahapan akhir saat Bank menentukan keputusan atas kegiatan alih daya berdasarkan hasil evaluasi dan penilaian kinerja atas pekerjaan yang dialihdayakan dan memperbaharui strategi alih daya yang sudah disesuaikan dengan hasil evaluasi. Tahapan di fase ini adalah *refresh,* yaitu Bank melakukan pembaharuan strategi alih daya sesuai hasil evaluasi atas pekerjaan alih daya sebelumnya.

KEAMANAN SIBER

Perkembangan digitalisasi di sektor perbankan meningkatkan timbulnya risiko terhadap keamanan siber bagi Bank. Maraknya serangan siber telah mendorong kebutuhan untuk meningkatkan ketahanan siber (*cyber resilience*) melalui penguatan keamanan siber (*cyber security*). Penguatan keamanan siber telah mengarah kepada berbagai insiatif di berbagai sektor industri tak terkecuali sektor perbankan untuk mengatasi risiko siber (*cyber risk*) oleh para regulator di berbagai negara. Terlebih lagi, sektor keuangan termasuk perbankan merupakan sektor yang menjadi target serangan siber paling tinggi baik secara global maupun di Indonesia. Berdasarkan catatan Bank for International Settlements (BIS), regulator perbankan di beberapa negara telah memiliki kebijakan khusus terkait keamanan siber. Beberapa *best practices* di berbagai negara yang bertujuan untuk meningkatkan keamanan siber antara lain mencakup kebijakan terkait pengelolaan keamanan siber, kewajiban penilaian risiko siber, kewajiban pengujian kerentanan teknologi informasi Bank, penilaian tingkat maturitas siber, dan pelaksanaan pengujian keamanan siber Bank. *Best practices* tersebut patut juga dipertimbangkan untuk diimplementasikan pada perbankan Indonesia agar Bank dapat melakukan mitigasi potensi ancaman dan kerentanan siber di era digitalisasi perbankan.

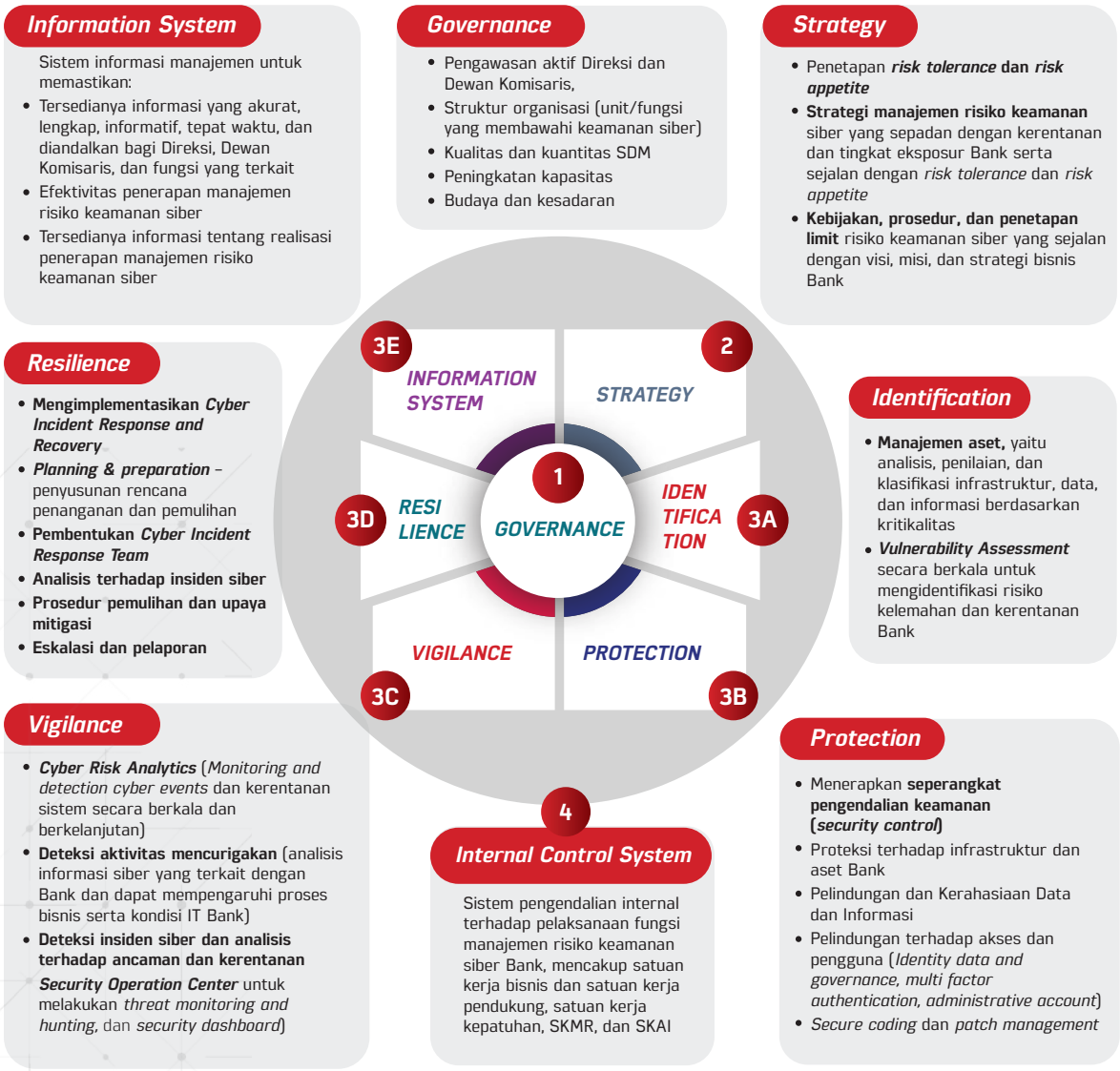
Mengacu pada standar internasional dan *best practices* dari berbagai negara, disusun *framework* penguatan kerangka keamanan siber sektor perbankan yang terdiri atas *Cyber Security Management, Cyber Security Exercise,* dan *Cyber Security Reporting.*



CYBER SECURITY MANAGEMENT

Cyber security management memberikan gambaran dan panduan bagi Bank dalam mengelola risiko siber yang merujuk pada standar dan *best practices* internasional antara lain National Institute of Standards and Technology (NIST) Framework for Improving Cyber Secucity, NIST Risk Management Framework, ISO 27001 – Information Security Management Standard, ISO 27032 – Guidelines for Cybersecurity, dan Financial Stability Board Cyber Incident Response and Recovery Toolkits. Kerangka pengelolaan risiko siber terdiri dari 4 (empat) pilar yang saling berkesinambungan.

Gambar 37 *Cyber Security Management*



Pilar 1 adalah ***governance*** (tata kelola), yang merupakan bentuk dari peranan Direksi dan Dewan Komisaris dalam menerapkan manajemen keamanan siber Bank, yang antara lain terdiri atas perlunya peran Direksi dan Dewan Komisaris untuk membangun pemahaman dan kesadaran terhadap risiko siber, memastikan struktur organisasi yang memadai dalam pengelolaan keamanan siber, menetapkan tugas dan tanggung jawab yang jelas pada fungsi keamanan siber, dan memastikan kecukupan kuantitas serta kapabilitas sumber daya manusia untuk mendukung manajemen keamanan siber secara efektif.

Pilar 2 yaitu ***strategy*** (strategi), yang dituangkan dalam suatu pedoman yang memuat tentang penetapan *risk tolerance* dan *risk appetite* terkait risiko keamanan siber, strategi manajemen risiko keamanan siber yang sepadan dengan kerentanan dan tingkat eksposur Bank serta sejalan dengan *risk tolerance* dan *risk appetite Bank*, dan kecukupan kebijakan dan prosedur manajemen risiko keamanan siber yang sejalan dengan visi, misi, dan strategi bisnis Bank.

Pilar 3 adalah terkait dengan proses utama manajemen risiko keamanan siber yang terdiri atas 5 (lima) tahapan, yaitu kecukupan proses ***identification*** (identifikasi), ***protection*** (pelindungan), ***vigilance*** (ketanggapan), dan ***resilience*** (daya tahan), serta tersedianya **sistem informasi** manajemen risiko yang memadai. Tahapan pertama adalah *identification*, yaitu proses identifikasi terhadap risiko keamanan siber yang dilakukan dengan analisis, penilaian, dan klasifikasi infrastruktur data dan informasi berdasarkan kritikalitas, serta proses *vulnerability assessment* secara berkala untuk mengidentifikasi risiko, kelemahan, dan kerentanan Bank. Tahapan kedua adalah *protection*, Bank perlu

menerapkan seperangkat pengendalian keamanan untuk melakukan pelindungan atau proteksi antara lain terhadap infrastruktur dan aset Bank, kerahasiaan data dan informasi, aplikasi, dan identitas serta *access control*. Tahapan ketiga, yaitu *vigilance* merupakan aksi dan ketanggapan bank dalam melakukan pemantauan atas kerentanan sistem dan potensi ancaman siber. Tahapan ini meliputi pula *cyber risk analytics* yaitu kegiatan memonitor dan mendeteksi *cyber event* dan kerentanan dalam sistem, *cyber threat intelligence* untuk mendeteksi aktivitas mencurigakan yang dapat mempengaruhi proses bisnis Bank, deteksi insiden siber dan analisis terhadap ancaman dan kerentanan Bank. Dalam melakukan tahapan *vigilance* Bank dapat membentuk *security operation center* yang bertugas untuk melakukan pemantauan ancaman (*threat monitoring and hunting*) serta mengelola *security dashboard* dan *security design*.

Tahapan keempat, yaitu *resilience* atau ketahanan yang memuat proses Bank dalam merespon dan melakukan pemulihan terhadap insiden siber atau *cyber incident response and recovery*. Beberapa aspek yang harus diperhatikan adalah perencanaan penanganan dan pemulihan, pembentukan *cyber incident response team* yang bertanggung jawab atas penanganan terhadap insiden, proses analisis, prosedur pemulihan dan upaya mitigasi, serta eskalasi dan pelaporan baik dalam internal bank maupun kepada otoritas dan lembaga atau *stakeholders* terkait. Tahapan terakhir adalah kecukupan sistem informasi manajemen risiko yang disesuaikan dengan karakteristik, kegiatan, dan kompleksitas kegiatan usaha bank. Sistem informasi manajemen risiko ini bertujuan untuk memastikan tersedianya informasi yang akurat, lengkap, informatif, tepat waktu, dan dapat diandalkan bagi Direksi, Dewan Komisaris, dan fungsi lain yang terkait; memastikan efektivitas penerapan manajemen risiko keamanan siber; dan tersedianya informasi tentang realisasi penerapan manajemen risiko keamanan siber.

Pilar 4 adalah **sistem pengendalian intern** yang bertujuan untuk memastikan seluruh proses manajemen keamanan siber diimplementasikan sesuai dengan kebijakan dan prosedur Bank. Dalam hal ini termasuk pula mengenai tugas dan tanggung jawab dari satuan kerja bisnis dan pendukung termasuk satuan kerja kepatuhan, serta satuan kerja manajemen risiko, dan satuan kerja audit internal dalam hal manajemen risiko keamanan siber.

CYBER SECURITY EXERCISE

Cyber security exercise merujuk pada praktik pengujian/tes penetrasi (*penetration testing*) yang bertujuan untuk menguji fungsi penting (*critical function*) Bank serta kemampuan SDM dan infrastruktur yang mendukung fungsi penting tersebut (*people, process and technology*). Hal tersebut mencakup penilaian dari aspek teknis berupa kecukupan dan efektivitas infrastruktur serta keamanan sistem, kemampuan dan kapasitas SDM dalam merespon insiden atau ancaman, dan juga pelaksanaan proses simulasi secara keseluruhan. Pelaksanaan *cyber security exercise* dapat dilakukan secara berkala sesuai dengan kebutuhan dan profil risiko siber Bank.

CYBER SECURITY REPORTING

Cyber security reporting bertujuan untuk mendukung penguatan ketahanan dan keamanan siber bank dengan memberikan gambaran mengenai insiden dan ancaman siber yang terjadi kepada otoritas, yang antara lain terdiri atas laporan insiden siber, laporan hasil penilaian penerapan manajemen risiko keamanan siber Bank, dan laporan hasil pengujian pertahanan keamanan siber.

KOLABORASI

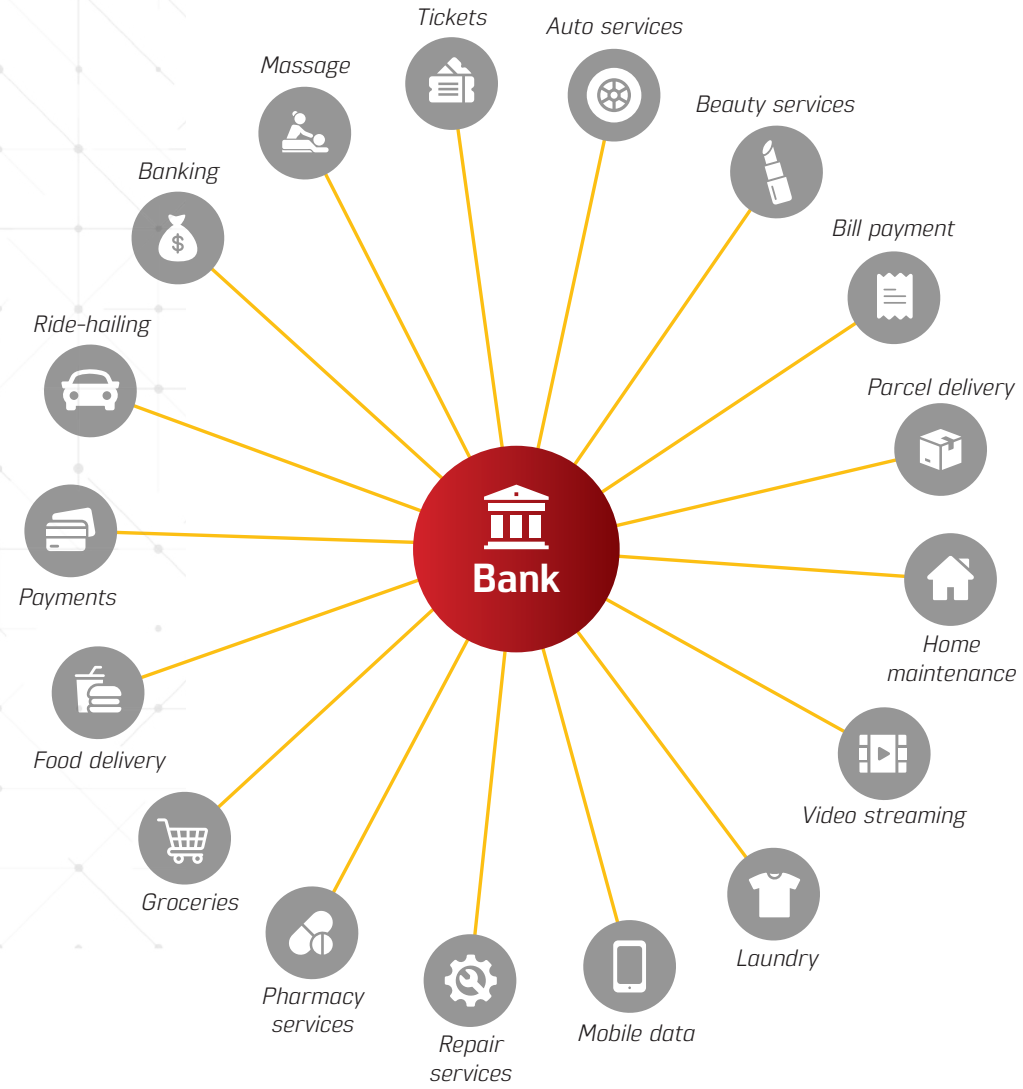
Kolaborasi Bank dalam ekosistem digital mendorong suatu bisnis model baru yang dapat dilakukan melalui *platform sharing*, *infrastructure sharing*, dan kerjasama dalam distribusi produk dan layanan.

Kolaborasi dalam ekosistem digital sangat diperlukan sebagai suatu bisnis model baru perbankan. Pembentukan kemitraan/kolaborasi antara perbankan dengan institusi lain baik institusi Bank, institusi keuangan non-bank, institusi non keuangan seperti perusahaan teknologi finansial atau *fintech* dapat dilakukan melalui beberapa bentuk yaitu:

01

PLATFORM SHARING (SUPER APP)

Bank bertindak sebagai penyedia *platform* melalui satu aplikasi *mobile*. Mitra Bank dapat memanfaatkan *platform Bank* untuk memberikan layanan kepada konsumen bank. Nasabah dapat mengakses berbagai layanan melalui layanan digital milik Bank. Hal tersebut dapat mempermudah konsumen dalam menjelajah ekosistem digital dalam satu genggaman aplikasi perbankan.



Gambar 38
Bank sebagai Penyedia *Super App*

Sumber: Techinasia.com (2020) dan Financial Times (2019)

Menurut Robosoft Technology (2020), beberapa pertimbangan dalam membangun *Super App* antara lain:

a. Memperkuat *core product* yang memiliki *engagement* konsumen tinggi, kemudian menambah fitur lainnya yang dibutuhkan oleh pengguna.

b. Mengidentifikasi target pasar yang dituju. Misalnya Go-Jek menargetkan jasa *ride-hailing* sebagai target pasar, WeChat menargetkan pengguna aplikasi *messenger*, dan lain sebagainya.

c. Memahami kebutuhan pengguna, ekspektasi pasar, dan kondisi ekonomi sebelum memperluas layanan.

d. Membangun kerja sama dan ekosistem yang mendukung pengembangan layanan *Super App.*

02

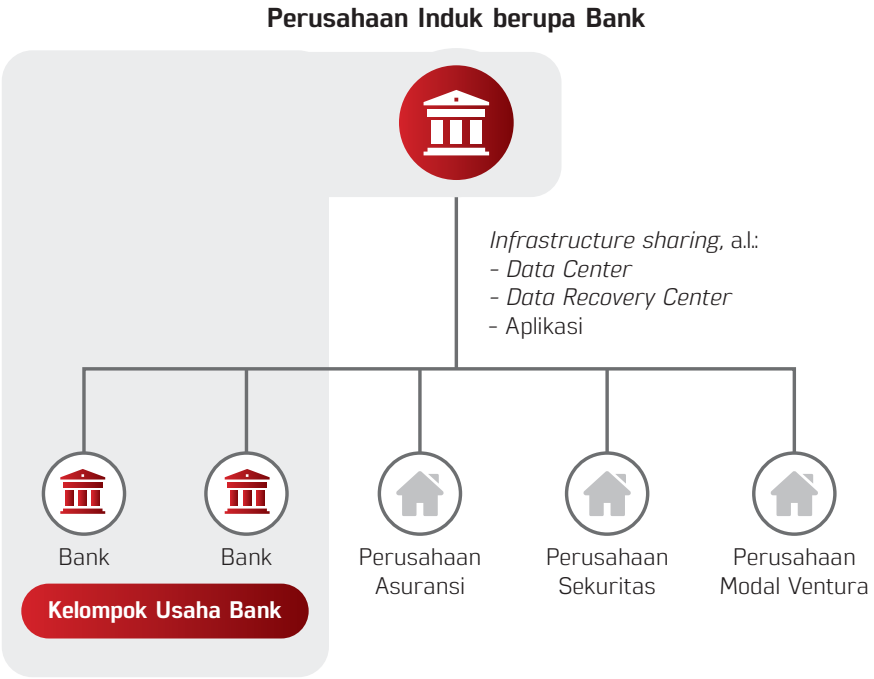
KERJA SAMA DENGAN INSTITUSI KEUANGAN/ INSTITUSI NON KEUANGAN

Bentuk kerja sama dibedakan menjadi *sharing service* (*infrastructure sharing*) bagi Kelompok Usaha Bank dan distribusi produk dan layanan.

a. Sharing service (infrastructure sharing) bagi Kelompok Usaha Bank

Salah satu bentuk sinergi yang dapat dilakukan adalah melalui *infrastructure sharing* bagi Kelompok Usaha Bank (KUB) yang bertujuan untuk mendorong efisiensi operasional. Sinergi Bank Berbadan Hukum Indonesia (BHI), sebagai perusahaan induk atau pelaksana perusahaan induk, yang tergabung dalam KUB dapat dalam bentuk pemanfaatan infrastruktur teknologi seperti aplikasi, *data center*, atau *data recovery center*.

Gambar 39
Sharing Service bagi Kelompok Usaha Bank



b. Distribusi dan Penawaran Produk

Bentuk kerja sama dalam hal distribusi dan penawaran produk dilakukan untuk memperluas akses konsumen terhadap produk Bank, termasuk bank yang memiliki kegiatan usaha terbatas. Berikut bentuk distribusi dan penawaran produk:

i. Skema *Channeling*

Melalui skema ini, Lembaga Jasa Keuangan (LJK) terlibat dalam distribusi dan penawaran produk Bank. LJK juga wajib melakukan *monitoring* terhadap konsumen.

ii. Skema *Referral*

Skema ini memungkinkan LJK untuk memberikan data calon konsumen kepada Bank sesuai persetujuan calon konsumen sehingga LJK tidak terlibat lebih lanjut setelah pemberian data.

iii. Skema Sistem Pembayaran

Bagi bank yang belum dapat berpartisipasi dalam sistem pembayaran, kerja sama dengan LJK yang memiliki izin dalam sistem pembayaran dapat dilakukan.

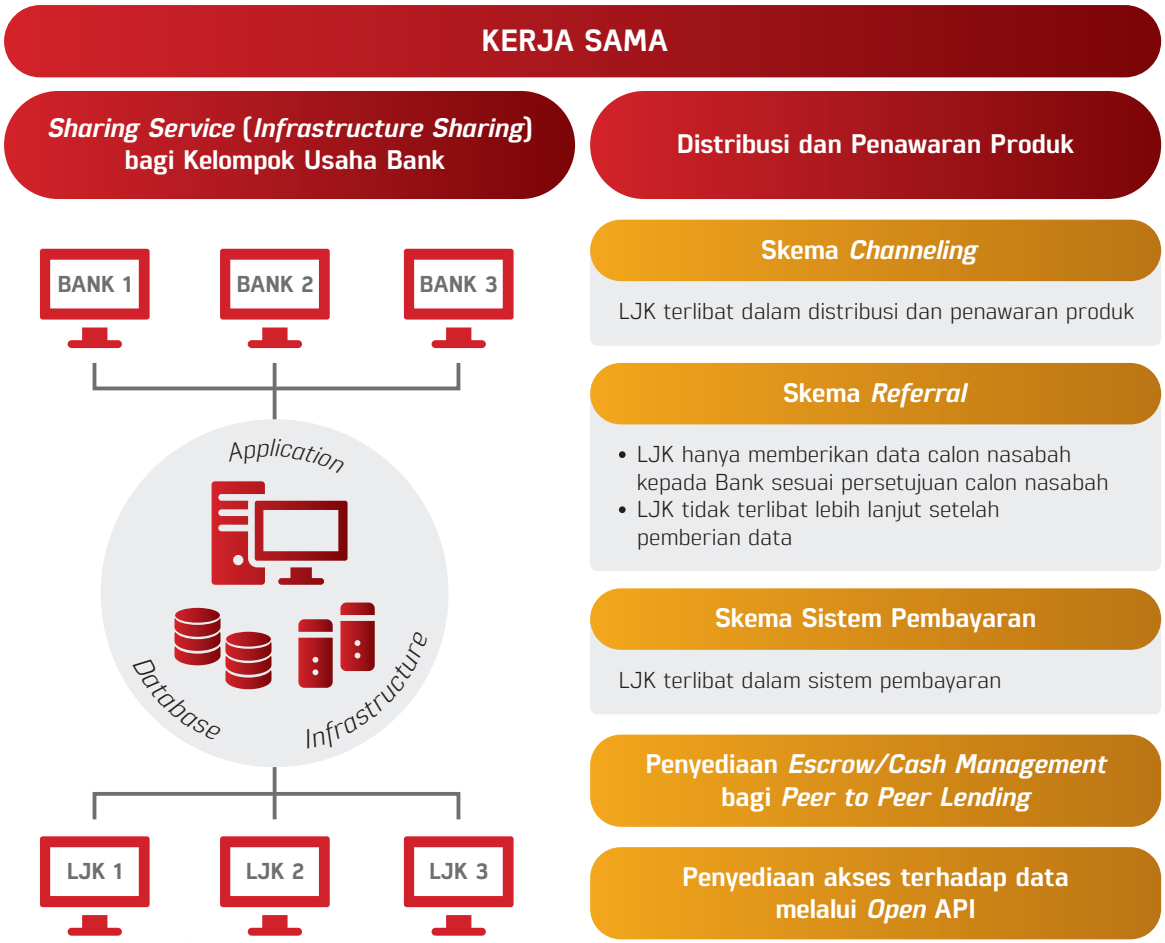
iv. Penyediaan *Escrow/Cash Management* bagi *Peer to Peer Lending*

Rekening penampungan (*escrow account*) merupakan suatu akun yang disediakan oleh pihak ketiga untuk dapat menampung serta menyalurkan uang antara pihak dalam proses penyelesaian transaksi bagi perusahaan *Peer to Peer Lending*. Rekening penampungan dimanfaatkan untuk meningkatkan sistem keamanan dalam transaksi *online*

Di samping itu, Bank dapat menawarkan sistem *cash management*, antara lain berupa fasilitas *automatic payment* dan *automatic posting*, atau yang biasa dikenal dengan *Host-to-Host service* kepada *Peer to Peer Lending*.

v. Penyediaan Akses terhadap data melalui *Open* API

Kerja sama antara Bank dengan mitra dapat berupa penyediaan akses data Bank melalui API yang meliputi antara lain data konsumen, data transaksi dan data finansial lain yang dikelola oleh institusi keuangan Bank dan Non-Bank kepada mitra penyedia layanan keuangan.



Pelaksanaan kolaborasi atau pembentukan mitra perlu dituangkan dalam suatu perjanjian kerja sama (PKS) secara tertulis antar kedua belah pihak. Aspek yang diatur dalam PKS minimal mencakup antara lain 1) pihak yang melakukan PKS, 2) tujuan dan ruang lingkup PKS, dan 3) jangka waktu PKS. Lebih lanjut, hak dan kewajiban setiap pihak, antara lain mengenai:

a. kewajiban kedua belah pihak untuk menjaga kerahasiaan dan keamanan informasi, termasuk informasi konsumen (*Non-Disclosure Agreement*/Perjanjian Kerahasiaan);

b. tanggung jawab atas kerugian yang muncul (misalkan terjadi kegagalan sistem, penipuan, atau faktor eksternal);

c. mitigasi risiko dalam hal terjadi penghentian kerja sama sebelum jatuh tempo sebagai upaya untuk memastikan keberlangsungan operasional dalam hal terjadi penghentian PKS;

d. penanganan pengaduan konsumen;

e. aspek alih pengetahuan SDM; dan

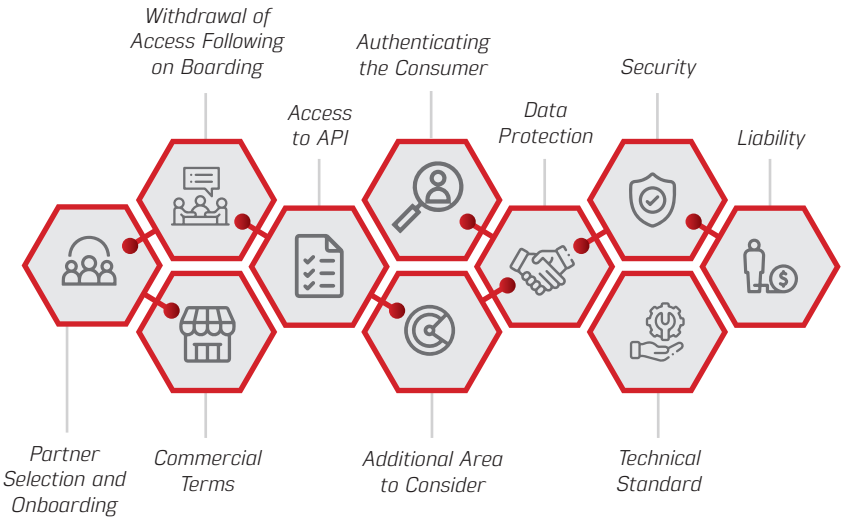
f. pengelolaan dan pemeliharaan dokumentasi/bukti transaksi dari aktivitas/ruang lingkup yang dilakukan kerja sama (untuk kepentingan audit).

Bank telah mengumpulkan berbagai data terkait konsumen, produk, ataupun operasional. Namun, bagaimana Bank memanfaatkan data tersebut untuk meningkatkan loyalitas konsumen serta menjadikan alternatif pemasukan baru bagi Bank masih belum terlalu diperhatikan. Dalam ekosistem digital saat ini, industri perbankan perlu didorong untuk mengolah informasi berdasarkan sumber data yang melimpah menggunakan teknologi terkini. Integrasi Bank dengan ekosistem digital menyebabkan bank memiliki sumber data yang dapat digunakan untuk meningkatkan efisiensi, menawarkan layanan yang bersifat konsumen sentris, dan membuka alternatif pemasukan baru bagi Bank.

API dapat dimanfaatkan oleh Bank untuk menciptakan model bisnis baru dengan cara kolaborasi dengan mitra/ pihak ketiga. Menurut survei yang dilakukan oleh Google dan Oxford Economics (2020) menunjukkan bahwa 51% responden yang merupakan *Chief Information Officer* dari perusahaan-perusahaan berpendapat bahwa API merupakan hal penting dalam melakukan kemitraan dan ekosistem yang dimiliki semakin produktif dan berharga. Lebih lanjut, lebih dari setengah dari total responden survei tersebut menyampaikan bahwa API penting dalam konteks hubungan dengan pengembang aplikasi (*developers*) dan konsumen.

Menurut CGAP (2020), terdapat beberapa hal yang perlu diperhatikan dalam melakukan kolaborasi dalam konteks penggunaan API.

Gambar 40
Hal-Hal yang Perlu Diperhatikan dalam Implementasi Kolaborasi



Sumber: CGAP (2020)

01 PEMILIHAN REKANAN (*ON-BOARDING*)

Proses *on-boarding* dengan rekanan dilakukan sebelum melakukan kerja sama. Bank perlu menguji kelayakan mitra terkait aspek antara lain pengecekan *financial soundness*, pengecekan terkait anti pencucian uang, *business continuity*, dan *disaster recovery plan*.

02 PENARIKAN AKSES MITRA

Akses terhadap API (*application programming interface*) dapat ditangguhkan atau dihentikan ketika terdapat transaksi mencurigakan (misalnya terdapat keraguan terhadap otentikasi dan kecurigaan penyalahgunaan API). Hal tersebut harus tercantum dalam kontrak API. Beberapa kewenangan Bank untuk menangguhkan atau menghentikan akses API sebagai berikut.

a. Hak untuk tidak melakukan perintah diperlukan jika Bank memiliki kekhawatiran mengenai keamanan atau transaksi penipuan, khususnya terkait transaksi pembayaran, Bank berhak untuk menangguhkan atau menghentikan akses API.

b. Hak untuk mengakhiri diperlukan jika mitra tidak memenuhi 1) kriteria yang dipersyaratkan oleh Bank, 2) mitra memberikan ancaman terkait teknologi ke sistem Bank, dan 3) mitra Bank dimiliki oleh kompetitor Bank.

c. Hak untuk menangguhkan akses diperlukan jika mitra mengalami *security breach* atau akses tidak sah ke sistem mitra yang memiliki akses ke Bank.

03 AKSES API

Bank perlu memperhatikan keamanan data konsumen ketika membuka akses API bagi mitra. Mitra dapat menggunakan dua pendekatan yaitu melibatkan konsumen secara aktif dan tidak melibatkan konsumen (independen) dalam proses akses API. Keterlibatan aktif konsumen terwujud dalam pemberian kredensial untuk mengakses layanan sehingga mitra tidak dapat melakukan aktivitas apa pun tanpa persetujuan konsumen. Apabila konsumen telah mengizinkan akses kepada mitra di awal proses maka untuk proses yang sama selanjutnya tidak diperlukan proses yang sama dari konsumen.

04 PROSES OTENTIKASI KONSUMEN

Proses ini bertujuan untuk mencegah penipuan dengan memastikan bahwa seseorang yang memberikan instruksi sebenarnya adalah konsumen serta memastikan bahwa instruksi pembayaran itu valid. Terdapat empat metode otentikasi (*strong customer authentication*) yang dapat digunakan:

a. *Redirection:* konsumen diarahkan ke aplikasi atau *website* Bank oleh mitra dan konsumen tidak diwajibkan untuk membuka data privasinya kepada mitra.

b. *Embedded:* konsumen melakukan proses otentikasi melalui *interface* mitra namun *background process* otentikasi dilakukan oleh Bank. Mitra tidak menyimpan data konsumen dan Bank dapat mengontrol seluruh proses otentikasi.

c. *Decoupled:* proses otentikasi melibatkan penggunaan perangkat atau saluran terpisah, seperti aplikasi khusus.

d. *Delegated*: Bank mendelegasikan proses otentikasi kepada mitra sehingga mitra melakukan otentikasi melalui platform mitra. Untuk itu, di dalam kontrak Bank dengan mitra perlu disebutkan: 1) kewajiban mitra untuk melakukan otentikasi atas nama Bank sesuai dengan proses otentifikasi yang disepakati dan 2) penentuan liabilitas dari setiap pihak.

05 PELINDUNGAN DATA

Aspek pelindungan data dalam tahapan ini tidak berbeda dengan prinsip pelindungan data yang telah dijelaskan pada bagian sebelumnya. Sehubungan dengan data pribadi konsumen, setiap pemrosesan, pengungkapan, transmisi, dan penyimpanan data harus dilakukan sesuai dengan undang-undang pelindungan data yang berlaku. Hukum yang berlaku di setiap negara mungkin mengharuskan data pribadi diproses hanya dengan persetujuan konsumen. Meskipun tidak diatur dalam hukum pelindungan data, Bank dapat memproses terkait data pribadi apabila memiliki izin pengguna.

06 KEAMANAN

Ketika Bank memberikan akses informasi akun konsumen kepada mitra serta mengizinkan mitra untuk melakukan transaksi, terdapat risiko penipuan melalui akses, penggunaan informasi, dan inisiasi transaksi yang tidak sah. Meskipun Bank telah memiliki prosedur untuk melindungi data konsumen, namun data pribadi konsumen berisiko akan terungkap ketika mitra mengalami *data breach* sehingga konsumen berpotensi mengalami kerugian. Untuk memitigasi risiko ini, aspek keamanan dapat mencakup cara untuk melindungi kerahasiaan dan integritas kredensial keamanan konsumen; standar yang kuat untuk komunikasi antara Bank dan mitra; dan tindakan teknis yang dimiliki oleh mitra untuk melindungi data konsumen.

07 KEWAJIBAN (*LIABILITY*)

Pertimbangan utama bagi Bank adalah pembagian kewajiban antara Bank dan mitra apabila terdapat penyalahgunaan terkait API. Untuk itu, para pihak harus mempertimbangkan: 1) pihak yang paling bertanggung jawab, 2) pihak yang paling mampu mengendalikan risiko, dan 3) pihak mana yang paling mampu untuk mengurangi kerugian yang timbul dari risiko tersebut yang mencakup mitigasi operasional (penutupan akses layanan) maupun mitigasi keuangan (pelindungan asuransi pada konsumen).

08 STANDAR TEKNIS

Bank akan menentukan dan mendokumentasikan standar teknis API yang tersambung dengan mitra. Spesifikasi teknis minimal mencakup bagaimana mitra akan mengidentifikasi API Bank dan keamanan komunikasi antara para pihak. Selanjutnya, apabila terdapat perubahan API, Bank harus mempertimbangkan pemberitahuan perubahan pada spesifikasi kepada mitra dan waktu minimal untuk implementasi perubahan API tersebut oleh mitra.

09 AREA TAMBAHAN UNTUK DIPERTIMBANGKAN

Beberapa area yang perlu dipertimbangkan dalam kolaborasi antara lain lisensi, prosedur penyelesaian perselisihan (perselisihan antar pihak dan perselisihan dengan konsumen), dan kelangsungan bisnis (*business continuity*).

10

ISTILAH KOMERSIAL (*COMMERCIAL TERMS*)

Beberapa aspek komersial yang perlu dipertimbangkan dalam kontrak API antara Bank dan mitra antara lain sebagai berikut:

a. Penetapan Harga (*Pricing*): Sebagian besar Bank tidak memungut biaya untuk akses ke layanan melalui API. Hal tersebut juga didukung oleh ketentuan negara yang mengatur *open banking* (misalnya di Eropa). Melalui ketentuan *Payments Service Directive* 2 (PSD2), Bank dan bank lain di Eropa harus mengizinkan penyedia layanan mitra mengakses akun konsumen dan Bank tidak diizinkan untuk menagih penyedia layanan mitra untuk akses akun konsumen melalui API. Di sisi lain, apabila Bank memilih untuk mengenakan biaya untuk akses API-nya, pengubahan harga API yang disesuaikan selama jangka waktu kontrak dapat menjadi pertimbangan sebagai cara untuk menyesuaikan dengan keadaan pasar.

b. Jangka Waktu Keberlakuan Kontrak: Terdapat dua jenis periode kontrak yaitu *fixed term* dan *evergreen.* Kontrak *fixed term* memiliki jangka waktu kontrak dengan periode tertentu. Kontrak *evergreen* akan tetap ada sampai kontrak tersebut diakhiri atau kontrak tersebut memiliki jangka waktu namun secara otomatis akan diperbarui ketika jangka waktu kontrak berakhir.

c. Ketersediaan dan *Service Level Agreement* (SLA): Setiap Bank perlu mempertimbangkan apakah bersedia menyediakan tingkat layanan (termasuk ketersediaan data melalui API) dan memberikan jaminan kualitas data yang disediakan oleh Bank.

   Beberapa level layanan minimum yang perlu menjadi pertimbangan mencakup: 1) penghitungan level layanan minimum, 2) pemantauan dan frekuensi dari kinerja SLA, dan 3) ganti rugi yang didapatkan oleh mitra apabila Bank tidak dapat memenuhi SLA.

d. Kualitas Data: Jika Bank menyediakan data untuk mitra, maka data yang diberikan tersebut bersifat "as-is" atau Bank bersedia menerima tanggung jawab apa pun atas kualitas data. Sebagian besar Bank tidak bersedia memberikan jaminan terkait kualitas data, terutama jika Bank tidak mengenakan biaya untuk akses ke data tersebut. Namun, apabila Bank bersedia memastikan kualitas data maka perlu mempertimbangkan konsekuensi yang bersedia diterima oleh Bank jika kualitas data tidak dapat dipertanggungjawabkan.

e. Pelindungan Hak Milik: Bank perlu memperhatikan *property right* (termasuk *intellectual property right*) yang ada apabila terdapat penyalahgunaan API. Di dalam kontrak API perlu memperhatikan ketentuan yang berhubungan dengan kepemilikan dan penggunaan API (spesifikasi dan dokumentasi), penyediaan data oleh Bank kepada mitra, dan turunan data yang disediakan.

f. Kontrak Pengguna API: Kontrak pengguna API bertujuan untuk memetakan kembali risiko kerugian konsumen yang timbul dari aktivitas yang berada dalam kendali mitra (misalnya, mitra dapat melakukan ganti rugi untuk setiap kerugian konsumen yang ditimbulkan karena kegagalan layanan mitra).

TATANAN INSTITUSI

Transformasi digital perlu didukung oleh kesiapan tatanan institusi Bank meliputi sumber pendanaan dan investasi teknologi informasi, *digital leader*, desain organisasi, budaya digital, dan *digital talent*.

Perubahan yang terjadi seiring dengan transformasi digital perlu diikuti dengan kesiapan tatanan institusi bank. Tatanan institusi tersebut meliputi antara lain pendanaan dan investasi, kepemimpinan, desain organisasi, budaya digital, serta talenta digital.

PENDANAAN DAN INVESTASI (*FINANCING AND INVESTMENT*)

Transformasi digital di sektor perbankan tentunya perlu didukung oleh kemampuan Bank dalam memelihara sumber pendanaan dan melakukan investasi di bidang teknologi informasi.

BANK MEMILIKI SUMBER PENDANAAN YANG JELAS DAN MEMADAI

Sumber pendanaan Bank berasal dari permodalan. Permodalan yang memadai merupakan aspek kritikal dalam kegiatan bisnis Bank. Selain berfungsi sebagai bantalan (*cushion*) untuk menyerap

risiko dan kerugian yang tidak terduga (*unexpected losses*), permodalan juga memberikan sumber dukungan keuangan dalam pelaksanaan aktivitas lembaga jasa keuangan baik untuk ekspansi usaha maupun penyediaan infrastruktur yang memadai, termasuk infrastruktur teknologi informasi. Kemampuan permodalan yang kuat dapat memberikan kesempatan bagi Bank untuk menyediakan layanan keuangan yang sesuai dengan kebutuhan masyarakat saat ini dengan cepat, sejalan dengan dominasi generasi milenial. Hal tersebut mendorong perbankan perlu menyesuaikan produk dan layanan dalam memenuhi kebutuhan generasi milenial untuk mempertahankan eksistensi bisnis Bank. Jika perbankan Indonesia tidak memiliki kapasitas permodalan yang memadai dalam menyediakan infrastruktur teknologi informasi, maka peluang dari berkembangnya ekonomi digital tentunya tidak akan dapat ditangkap oleh perbankan Indonesia.

BANK MEMILIKI KOMITMEN DALAM MENDANAI PENYEDIAAN INFRASTRUKTUR

Penyediaan infrastruktur teknologi informasi untuk mendukung transformasi digital tentunya memerlukan investasi yang tidak sedikit. Bank harus melakukan keputusan investasi yang tepat dengan mempertimbangkan aspek-aspek yang terkait agar investasi yang dilakukan memberikan manfaat dan keuntungan bagi proses bisnis Bank ke depannya, serta didukung oleh komitmen penuh dari jajaran pengurus Bank. Dalam melakukan investasi untuk penyediaan infrastruktur teknologi informasi, Bank dapat memperhatikan beberapa aspek sebagai berikut:

01

PRIORITIZING HIGH-VALUE INVESTMENTS

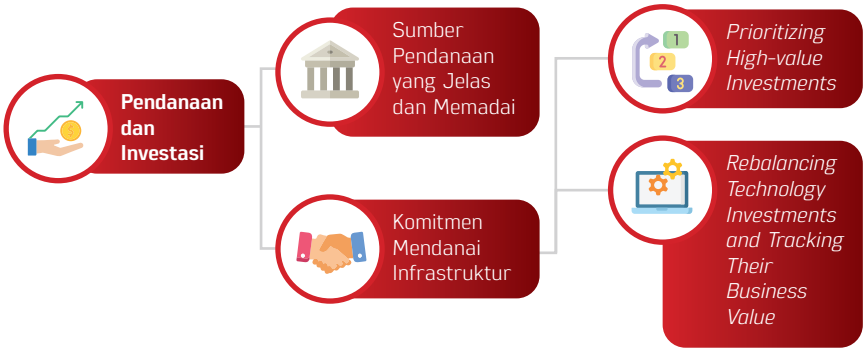
Bank dapat dihadapkan pada kondisi saat rencana investasi infrastruktur/teknologi melebihi anggaran yang dimiliki, sehingga Direksi harus memiliki komitmen untuk memprioritaskan investasi yang menghasilkan nilai tinggi (*high-value investment*) dengan tidak hanya mengukur tingkat pengembalian dari investasi teknologi, tetapi juga mengalokasikan kembali modal ke peluang yang menjanjikan.

02

REBALANCING TECHNOLOGY INVESTMENTS AND TRACKING THEIR BUSINESS VALUE

Bank menyeimbangkan kembali investasi teknologi dan mengukur nilai bisnis dari investasi tersebut, misalnya dengan menyiapkan indikator penilaian berupa *key performance indicators* (KPI) dan *objectives and key results* (OKR) untuk mengukur seberapa besar nilai bisnis yang dihasilkan dari investasi. Dari hasil penilaian tersebut Bank dapat memutuskan melakukan investasi tambahan hanya untuk investasi yang menunjukkan hasil yang positif.

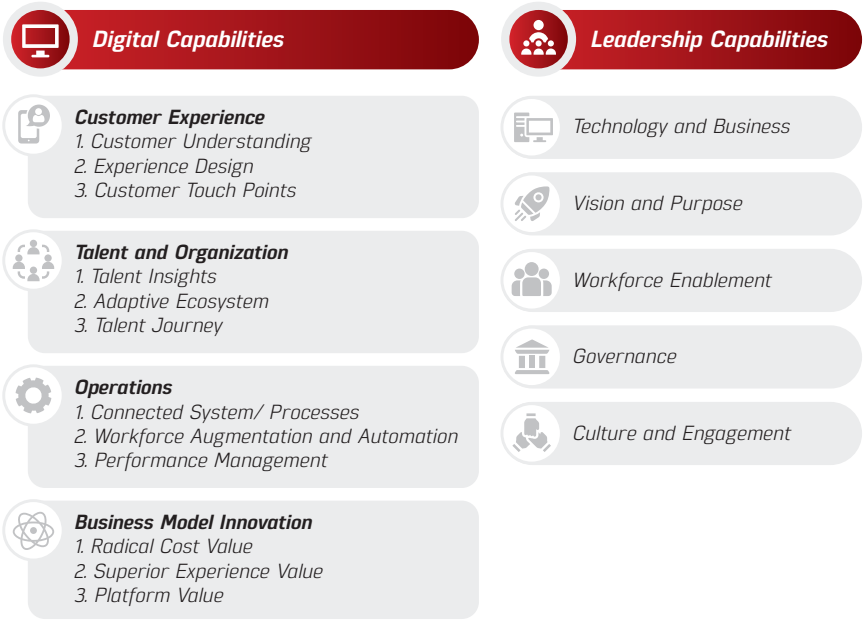
Gambar 41
Kebutuhan Pendanaan dan Komitmen Investasi Teknologi



KEPEMIMPINAN (*LEADERSHIP*)

Dalam rangka transformasi digital perbankan, Bank harus memiliki kepemimpinan digital (*digital leadership*) yang diartikan sebagai 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*). *Digital capabilities* meliputi kemampuan dalam penggunaan teknologi untuk mengubah proses bisnis Bank antara lain dalam hal interaksi Bank dengan konsumen (*customer experience*), pengembangan talenta dan organisasi (*talent and organization*), operasionalisasi proses internal (*operations*), serta perumusan model bisnis (*business model innovation*). Sementara *leadership capabilities* meliputi kemampuan untuk menggerakkan dan memimpin transformasi digital dalam hal teknologi dan bisnis, visi dan tujuan, pemberdayaan tenaga kerja, tata kelola, serta budaya dan keterlibatan.

Gambar 42
Kapasitas Digital dan Kapasitas Kepemimpinan



Sumber : Capgemini (2018)

Disrupsi teknologi telah menuntut Bank untuk bergerak secara agresif dalam merespons kebutuhan pasar dan memenuhi ekspektasi konsumen. Dengan demikian kepemimpinan digital memainkan peranan yang sangat penting dalam menjaga dan mempertahankan eksistensi Bank di tengah ketatnya persaingan dengan pemain lain di sektor jasa keuangan seperti *fintech* dan *bigtech*, serta mendorong inovasi berkelanjutan untuk meningkatkan keunggulan kompetitif Bank.

DESAIN ORGANISASI (*ORGANIZATIONAL DESIGN*)

Transformasi digital tentunya berdampak pada perlunya dilakukan transformasi desain organisasi bank yang lebih sesuai. Dalam hal ini, Bank perlu menyesuaikan berbagai macam aspek, mulai dari tempat kerja (*workplace*), struktur organisasi, kewenangan, dan pemberdayaan tenaga kerja (*workforce enablement*) agar sesuai dengan kebutuhan dan lingkungan bisnis yang telah berubah di era digital ini.

Gambar 43 Desain Organisasi yang Mendukung Transformasi Digital

Sumber: Martech (2021) dan Russel Reynold (2017), diolah kembali

KANTOR (*WORKPLACE*)

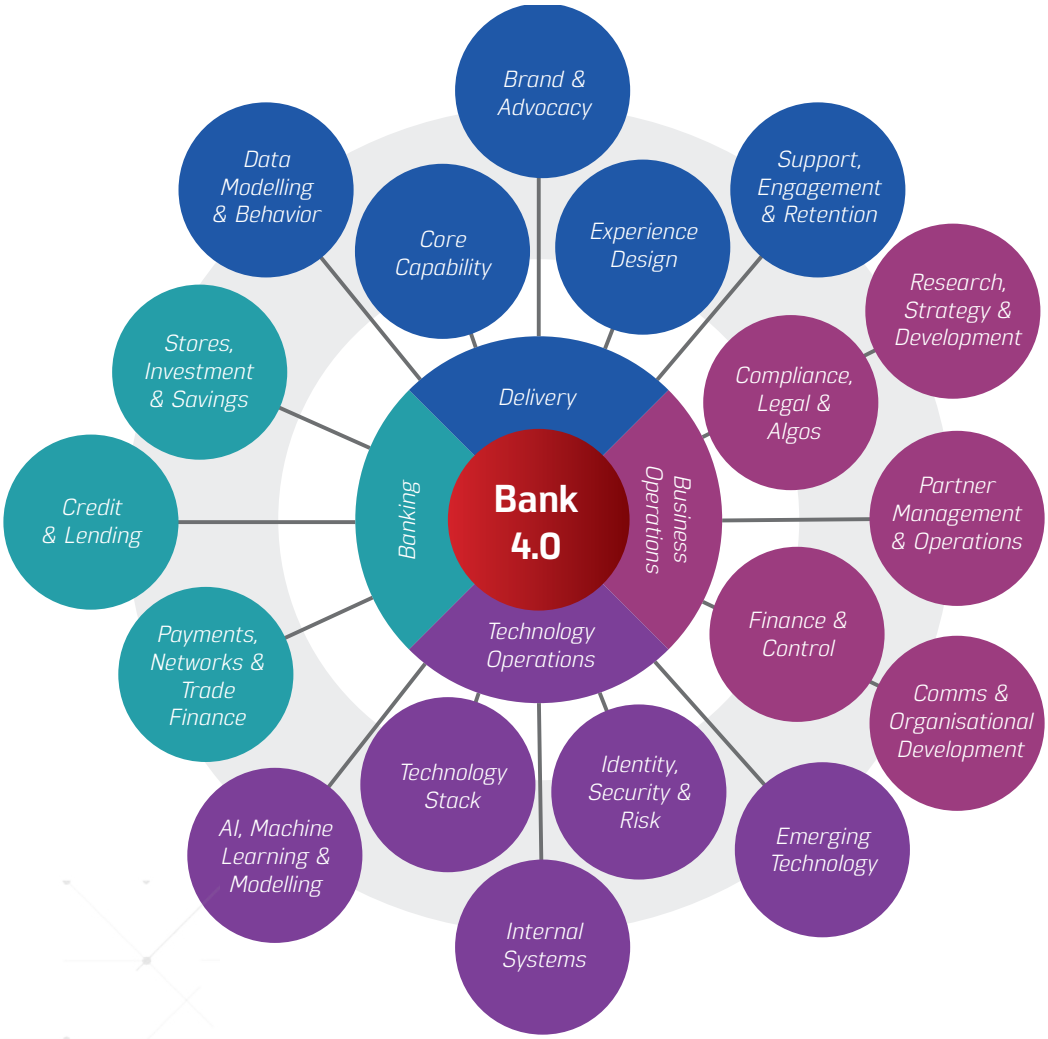
Dalam menjalankan model bisnis *full digital*, Bank dapat mengandalkan infrastruktur berupa teknologi canggih dan perangkat lunak dalam melakukan operasional bisnis sehingga mengurangi kebutuhan penyediaan jaringan kantor secara fisik dalam melayani konsumen. Untuk itu, Bank diperkenankan memiliki satu kantor fisik yang berfungsi sebagai kantor pusat (*principal/ head office*), sedangkan kantor cabang tidak diperlukan. Kantor pusat difungsikan sebagai titik penghubung antara Bank dengan seluruh pemangku kepentingan (*stakeholder)*, termasuk sebagai titik pusat (*central hub)* dalam melayani komplain konsumen dan pusat penyediaan layanan konsumen (*customer service centre*), serta menjadi *homebase* bagi jajaran manajemen dan unit-unit operasional pendukung. Kantor pusat tidak menyediakan produk dan layanan Bank kepada konsumen karena produk dan layanan ditawarkan melalui aplikasi yang diakses secara digital.

STRUKTUR ORGANISASI (*ORGANIZATIONAL STRUCTURE*)

Digitalisasi menuntut struktur organisasi Bank menjadi lebih dinamis dalam rangka menyediakan produk dan layanan yang inovatif sesuai dengan kebutuhan konsumen. Struktur organisasi tradisional yang berprinsip pada susunan hierarki menjadi tidak relevan untuk diterapkan pada organisasi yang menjalankan bisnis digital. Bank perlu menyesuaikan struktur organisasi menjadi lebih kolaboratif yang memungkinkan adanya interaksi yang lebih luas antar unit kerja melalui pemanfaatan teknologi terdistribusi seperti *blockchain* atau teknologi berbasis IP. Dengan demikian, akan menghindari timbulnya unit kerja yang bersifat silo.

Menurut Brett King (2018), struktur organisasi Bank 4.0 berbeda dengan struktur organisasi Bank tradisional yang merupakan sebuah bagan yang menunjukkan unit-unit bisnis strategis secara terpisah. Struktur organisasi Bank 4.0 lebih menitikberatkan pada bagan yang terdiri dari kompetensi inti di organisasi tersebut yang saling berhubungan satu sama lain (*frictionless*). Struktur ini bertujuan agar proses bisnis Bank berjalan lebih *agile* dalam melayani beragam segmen konsumen baik ritel, usaha kecil menengah, korporasi, dan konsumen lainnya, serta mendukung orientasi bisnis digital yang berfokus pada hubungan kemitraan (Bank-Nasabah) dan *costumer centricity*.

Gambar 44 Bagan Kompetensi Inti dari Bank 4.0



Sumber : Brett King (2019)

KEWENANGAN (*AUTHORITY*)

Struktur organisasi yang *frictionless* memungkinkan proses pengambilan keputusan dapat dilakukan dengan lebih cepat melalui kewenangan yang terdesentralisasi di 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 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.

PENGGERAK TENAGA KERJA (*WORKFORCE ENABLEMENT*)

Transformasi bank menjadi Bank Digital perlu didukung oleh perubahan tempat kerja (*workplace*) menjadi *digital workplace*. Berdasarkan laporan Deloitte (2021), *digital workplace* terdiri dari 4 (empat) aspek utama yaitu:

1. **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.

2. **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.

3. **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.

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

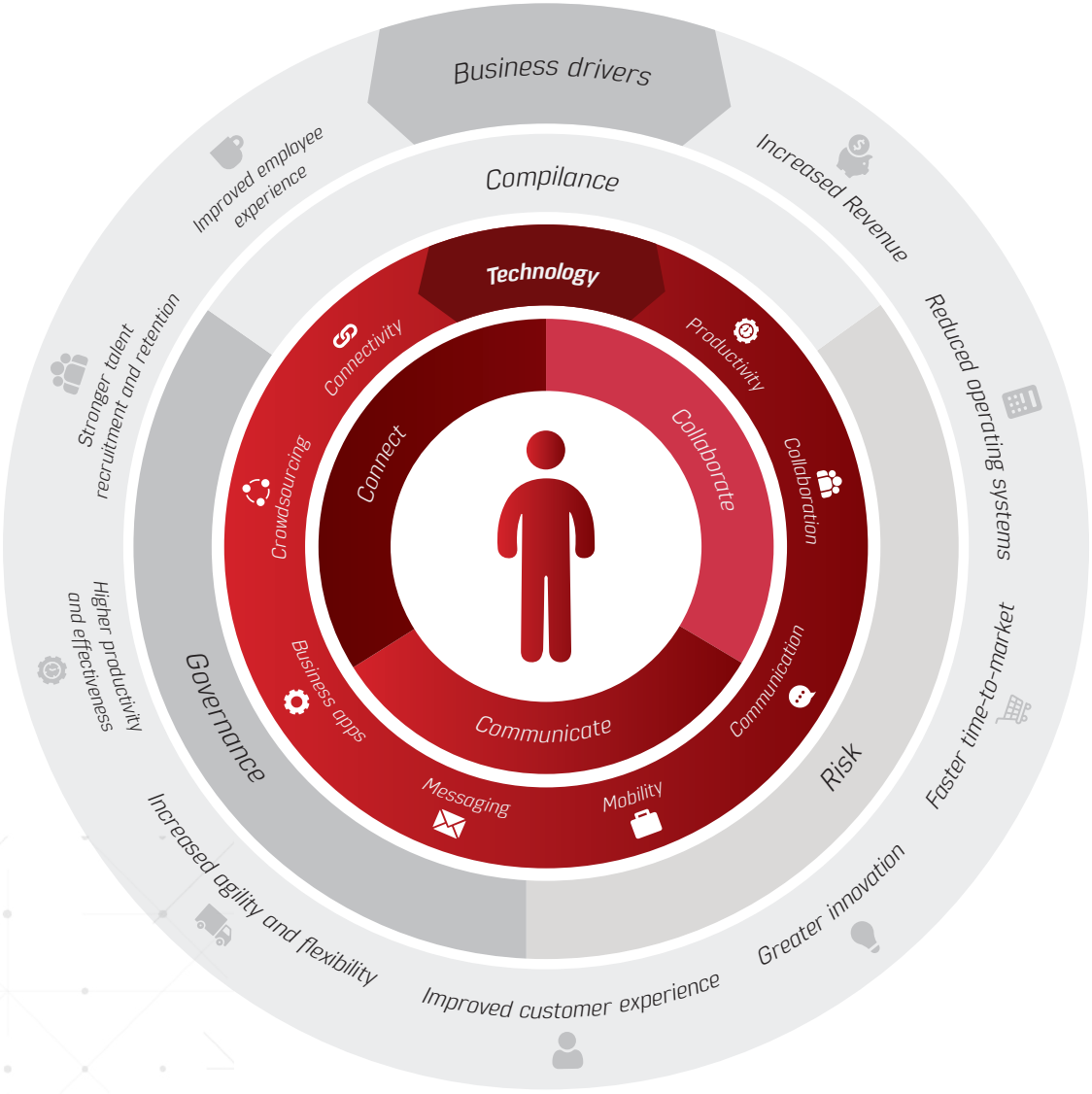
Lebih lanjut, berdasarkan laporan Capgemini (2018), kriteria *digital workplace* yang efektif sebagai berikut:

1. 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*;

2. 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

3. memungkinkan adanya tenaga kerja digital berupa tim robot perangkat lunak yang dapat bekerja bersama karyawan untuk menyelesaikan tugas dan proses yang berulang.

Gambar 45 Aspek Utama dalam Mewujudkan Digital Workplace



Sumber: Deloitte (2021)

BUDAYA DIGITAL (*DIGITAL CULTURE*)

Bank perlu mengembangkan budaya digital sebagai fondasi yang kuat untuk mengubah pola pikir dan pemahaman baik pengurus Bank maupun pegawai Bank agar berorientasi pada visi digital untuk mendukung transformasi digital perusahaan. Budaya digital setidaknya terdiri atas beberapa aspek sebagai berikut:

1. Inovasi (*Innovation*): perilaku yang mendukung pengambilan risiko, pemikiran disruptif dan eksplorasi ide-ide baru.
2. Pengambilan Keputusan berdasarkan Data (*Data-driven Decision-Making*): penggunaan data dan analisis untuk membuat keputusan bisnis.

3. Kolaborasi (*Collaboration*): penciptaan tim yang bersifat lintas fungsi dan lintas departemen untuk mengoptimalkan kemampuan perusahaan.

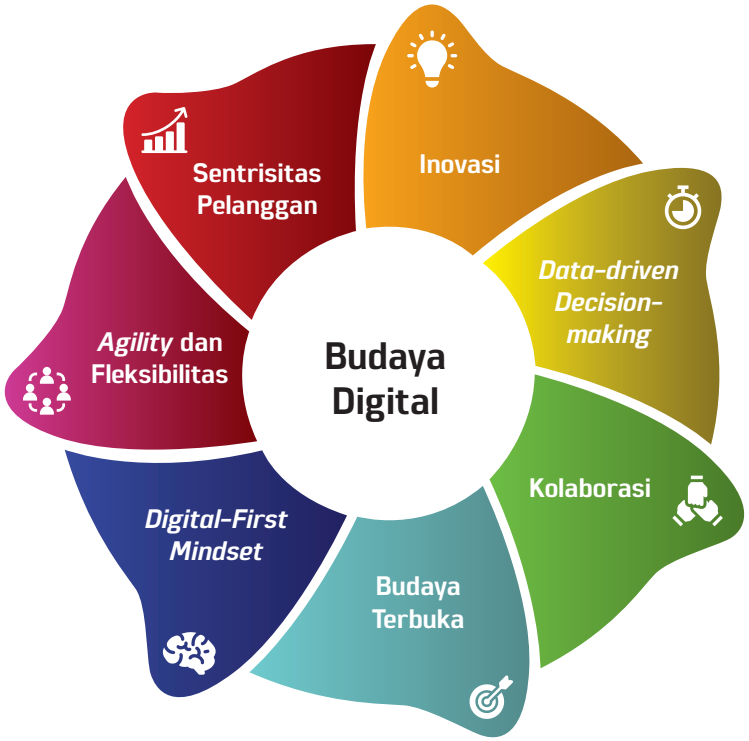
4. Budaya Terbuka (*Open Culture*): perluasan kerja sama dengan pihak eksternal seperti vendor pihak ketiga, perusahaan rintisan, dan konsumen.

5. Pola Pikir Mengedepankan Digital (*Digital-First Mindset*): pemikiran bahwa digitalisasi adalah solusi.

6. Agilitas dan Fleksibilitas (*Agility and Flexibility*): kecepatan dan dinamisme pengambilan keputusan dan kemampuan organisasi untuk beradaptasi dengan tuntutan dan teknologi yang berubah.

7. Sentrisitas Konsumen (*Customer Centricity*): penggunaan solusi digital untuk memperluas basis konsumen, mengubah pengalaman konsumen, dan bersama-sama menciptakan produk baru.

Gambar 46
Tujuh Aspek Budaya Digital



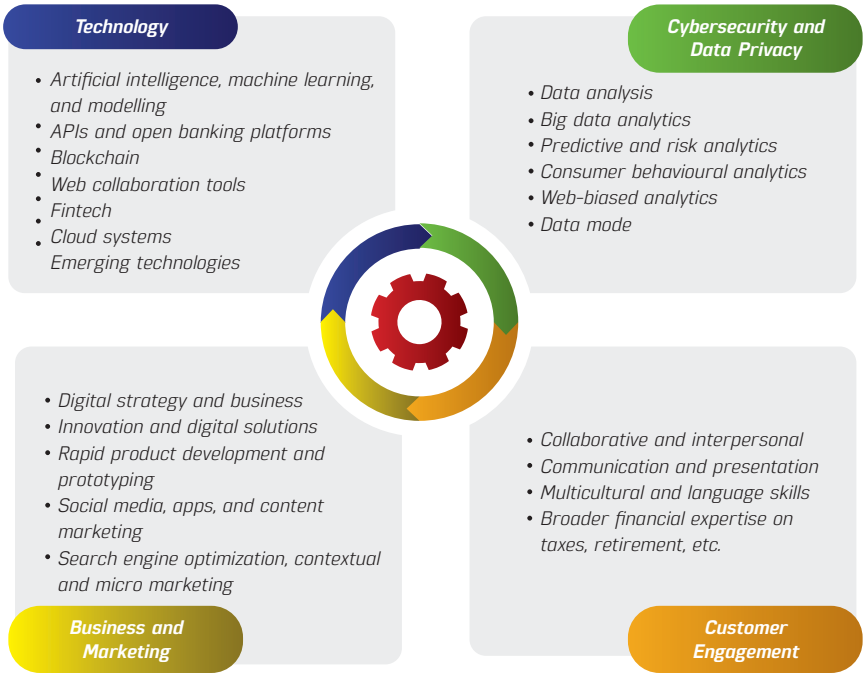
Sumber : Capgemini (2018)

Penerapan budaya digital yang efektif diharapkan dapat memberikan manfaat bagi Bank antara lain meningkatkan kemampuan Bank untuk melihat ancaman dan peluang digital, mendukung ruang lingkup tindakan/aksi yang dapat diambil oleh Bank dalam menanggapi digitalisasi, dan mendorong koordinasi yang erat di seluruh fungsi, departemen, dan unit bisnis.

TALENTA DIGITAL (*DIGITAL TALENT*)

Pemanfaatan teknologi pada proses bisnis Bank dalam rangka transformasi digital perlu diimbangi dengan pembangunan kualitas sumber daya manusia (SDM) yang memiliki pemahaman memadai terkait teknologi informasi sehingga penggunaan teknologi dapat berjalan efektif dan optimal karena didukung oleh SDM yang tepat. Dengan demikian, Bank memerlukan pengembangan talenta digital (*digital talent*) sebagai bagian dari transformasi digital. Menurut Capgemini (2018), talenta digital meliputi *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.

Gambar 47
Skill Set yang Dibutuhkan Untuk Mendukung Transformasi Digital



Sumber : Roubini ThoughtLab 2017, Brett King 2019 (dimodifikasi)

Dalam perbankan tradisional, Bank lebih banyak merekrut SDM dengan latar belakang keahlian terkait perbankan seperti bidang akuntansi, kredit, investasi, sistem pembayaran, dan keuangan. Sebaliknya, dalam Bank 4.0 Bank perlu meningkatkan proporsi SDM yang memiliki keahlian di bidang Teknologi Informasi dan bisnis inovatif. Lebih lanjut, dalam rangka meningkatkan kualitas talenta digital, Bank dapat menyelenggarakan pelatihan atau sertifikasi di bidang Teknologi Informasi seperti pelatihan mengenai risiko teknologi dan keamanan siber untuk Direksi sehingga Direksi dapat secara efektif menjalankan fungsi pengawasan keamanan teknologi informasi.

Tabel 1
Contoh Sertifikasi di Bidang Teknologi Informasi pada Bidang IT *Security Operations and Delivery*, IT *Risk Management and Control*, dan IT *Audit*

	First Line of Defence	*Second Line of Defence*	*Third Line of Defence*
Recognised Certificates	***IT Security Operation and Delivery***	***IT Risk Management and Control***	***IT Audit***
Core Level			
CSX Fundamentals Certificate	✓	✓	✓
CSX Practitioner Certificate (CSX-P)	✓	✓	✓
GIAC Information Security Professional (GIAC GISP)	✓	✓	
GIAC Security Essentials (GSEC)	✓	✓	✓
ISC² Systems Security Certified Practitioner (SSCP)	✓		
Professional Level			
CSX Specialist Certificate (CSX-S)	✓	✓	✓
CSX Expert Certificate (CSX-E)	✓	✓	✓
ISACA Certified Informastion Systems Auditor (CISA)	✓	✓	✓
ISACA Certified Information Security Manager (CISM)	✓	✓	✓
ISACA Certified in Risk and Informations Systems Control (CRISC)		✓	
ISACA Certified in the Governance of Enterprise IT (CGEIT)	✓	✓	✓
ISC² Certified Information Systems Security Professional (CISSP)	✓	✓	✓
ISC² Certified Cloud Security Professional (CCSP)	✓	✓	

Sumber : HKMA (2016)

Di samping pengembangan kompetensi dan kapasitas SDM, transformasi digital perbankan perlu didukung oleh pemahaman terkait produk dan layanan keuangan serta literasi digital masyarakat dalam memanfaatkan penggunaan teknologi informasi untuk bertransaksi. Hal ini bertujuan agar perkembangan teknologi informasi di industri perbankan dapat meningkatkan efektivitas transaksi layanan keuangan sehingga mendorong kesejahteraan masyarakat dan menghindarkan masyarakat dari dampak negatif seperti penipuan dan penyalahgunaan informasi. Untuk itu, Bank perlu melakukan edukasi dan literasi kepada masyarakat antara lain mengenai produk dan layanan keuangan yang ditawarkan termasuk fitur, manfaat dan risiko, hak dan kewajiban terkait produk dan jasa keuangan, serta keterampilan dalam menggunakan produk dan jasa keuangan. Selain itu untuk meningkatkan literasi digital, Bank perlu melakukan sosialisasi dan edukasi terkait aspek keamanan dalam bertransaksi secara digital seperti kerahasiaan *personal identification number* (PIN) dan kode *one time password* (OTP), dan pentingnya menjaga data dan informasi pribadi.

CUSTOMER

Di samping *customer centric orientation services*, Bank juga perlu memperhatikan ketersediaan layanan perbankan bagi seluruh lapisan masyarakat.

Transformasi digital bertujuan untuk memberikan produk dan layanan yang sesuai dengan kebutuhan konsumen atau mencapai *customer centric orientation services*. Mengacu kepada kerangka *digital maturity TM Forum*, tingkat kematangan digitalisasi organisasi pada aspek *customer* diukur dari 4 (empat) hal yaitu *customer engagement, customer experience, customer insight* dan *customer trust and perception* (TM Forum, 2021). Bank perlu memperhatikan ke empat hal tersebut dalam perjalanan transformasi digital untuk mencapai *customer centric orientation services*. Di samping *customer centric orientation services*, Bank juga perlu memperhatikan ketersediaan layanan perbankan bagi seluruh lapisan masyarakat. Bank perlu memastikan bahwa layanan perbankan secara digital dapat diakses oleh seluruh lapisan masyarakat dalam rangka meningkatkan inklusi keuangan, termasuk bagi kaum disabilitas yang berpotensi termarginalkan akibat perkembangan teknologi.

Gambar 48
Aspek Penting dalam Mencapai Sentrisitas Konsumen

KETERLIBATAN KONSUMEN (*CUSTOMER ENGAGEMENT*)

Dalam konteks layanan perbankan digital, keterlibatan konsumen (*customer engagement*) merujuk kepada keterikatan atau ketergantungan konsumen terhadap layanan perbankan digital. Hal itu dapat terjadi melalui suatu interaksi, reaksi, efek, atau pengalaman yang dirasakan konsumen secara keseluruhan terhadap produk atau layanan jasa yang mereka pilih. Perkembangan perbankan digital menyebabkan produk Bank yang ditawarkan kepada masyarakat bersifat konsumen sentris sehingga masyarakat cenderung mencari Bank yang menawarkan produk yang bersifat *personalized*. Keterlibatan konsumen menjadi bermanfaat bagi Bank karena produk digital Bank akan memiliki karakteristik yang berbeda untuk setiap konsumen sehingga loyalitas konsumen meningkat. Hubungan yang terjalin dengan baik antara produsen dan konsumen akan mengikat konsumen untuk terus memilih produk atau layanan jasa kita secara berkala.

PENGALAMAN KONSUMEN (*CUSTOMER EXPERIENCE*)

Pada dasarnya, pengalaman konsumen atau *customer experience* adalah suatu indikator kesuksesan layanan yang diberikan oleh perusahaan. Pada layanan perbankan digital, *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. Akselerasi transformasi digital berupa penggunaan *advanced technology* untuk personalisasi konsumen dapat menjadi solusi untuk meningkatkan *customer experience*. Microsoft dan PSFK (2017) menyebutkan bahwa *customer experience* dapat diperoleh dengan memperdalam pemahaman dari setiap konsumen dengan mengolah data konsumen sehingga dapat memberikan pengalaman yang kontekstual dan *personalized*. Data yang diolah menggunakan *artificial intelligence* dapat berasal dari data internal Bank maupun data lain dari konsumen misalkan data media sosial atau data belanja.

WAWASAN 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. Bagi Bank, *customer insight* bertujuan untuk meningkatkan penjualan produk Bank secara cepat dan mudah

melalui data yang diolah dengan *tools* analisis tertentu. Pada akhirnya, apabila Bank dapat menemukan produk dan cara pemasaran yang tepat bagi setiap konsumen, loyalitas konsumen akan semakin meningkat sehingga konsumen tidak ragu untuk merekomendasikan layanan perbankan digital kepada orang lain.

KEPERCAYAAN DAN PERSEPSI KONSUMEN (*CUSTOMERS TRUST AND PERCEPTION*)

Di era digital semua hal terhubung satu sama lain, sehingga aspek keamanan memegang peranan penting dalam pengembangan perbankan digital. Hal tersebut berpengaruh terhadap kepercayaan (*trust*) dan persepsi (*perception*) konsumen terhadap layanan perbankan digital. Perkembangan teknologi internet yang dimulai sejak 1990-an menyebabkan peluang *internet security breach* berkurang (Suh dan Han, 2003). Untuk itu, Bank perlu memperhatikan *customer trust and perception* mengingat pentingnya hal tersebut dalam industri jasa keuangan. Studi Tham dkk. (2017) di Malaysia menunjukkan bahwa dalam menarik konsumen Bank untuk menggunakan layanan perbankan virtual, Bank perlu memperkuat keamanan dan keandalan layanan perbankannya. Hasil serupa ditunjukkan oleh Vejačka dan Stofa (2017) bahwa keamanan yang dirasakan oleh konsumen menjadi faktor yang penting dalam membangun kepercayaan di bidang layanan perbankan elektronik yang mempengaruhi sikap dalam menggunakannya.

KONSUMEN PENYANDANG DISABILITAS (*CUSTOMERS WITH DISABILITIES*)

Aksesibilitas sektor keuangan merupakan hal yang krusial untuk mewujudkan sistem keuangan yang inklusif. Penyandang disabilitas merupakan salah satu kelompok masyarakat yang mengalami kerentanan secara ekonomi karena berbagai keterbatasan yang dialami. Berbagai keterbatasan yang dimiliki oleh penyandang disabilitas berdampak pada rendahnya tingkat inklusi keuangan penyandang disabilitas. Rendahnya akses penyandang disabilitas ke dalam sektor keuangan merupakan salah satu faktor yang dapat menghambat peningkatan perekonomian penyandang disabilitas. Pemerintah telah berkomitmen untuk memenuhi hak-hak penyandang disabilitas dengan memasukkan penyandang disabilitas sebagai subjek dalam pembangunan Indonesia. Sebagai sektor yang memiliki peran penting dalam perekonomian Indonesia, tentunya perbankan dituntut untuk berpartisipasi dalam upaya meningkatkan inklusi keuangan bagi penyandang disabilitas.

Perkembangan teknologi informasi bertujuan memudahkan, tak terkecuali bagi penyandang disabilitas. Kaum disabilitas memiliki keterbatasan dalam berkomunikasi, berinteraksi, mengakses informasi, dan berpartisipasi dalam aktivitas sipil. Penggunaan teknologi digital dalam aktivitas kaum disabilitas dapat mengatasi keterbatasan tersebut karena teknologi memungkinkan beragam bentuk komunikasi dengan menggunakan berbagai media seperti suara, teks, dan gestur sehingga mengurangi hambatan bagi kaum disabilitas dalam beraktivitas. Namun, tidak semua layanan berbasis teknologi yang dijumpai sehari-hari ramah bagi penyandang disabilitas sehingga diperlukan dukungan dalam hal penyediaan layanan yang ramah bagi penyandang disabilitas. Dalam rangka partisipasi perbankan dalam rangka meningkatkan inklusi keuangan, Bank ke depan perlu memperhatikan kebutuhan konsumen penyandang disabilitas dan menyediakan layanan perbankan yang ramah bagi penyandang disabilitas.

Tabel 2
Contoh Solusi *Information and Communication Technology* (ICT) yang Dapat Diterapkan Bagi Kaum Disabilitas Sesuai Jenis Disabilitas

Visual Disability (Includes total blindness or low vision)	***Hearing Disability (Includes total blindness or low vision)***	***Speech Impairments***
- *Text-to-speech rendition and speech/voice output* - *Braille displays* - *Screen and text magnification* - *Voice recognition* - *Audio description of graphic and visual media* - *Electronic audio signage* - *GPS-facilitated navigation* - *Optical character or image recognition* - *Changing screen brightness, color contrast*	- *Closed and open captioning, subtitles for videos, TV programming SMS, text messaging* - *Text Telephone or Telecommunication Device for the Deaf (TTY/TDD) which allow text messaging over the phone line* - *Telecommunications Relay Services which allow text to speck conversions through an operator* - *Use of vibrations/text alerts instead of audio alerts*	- *SMS, text messaging* - *Synthesized voice output, text to speech functionality* - *Use of virtual picture board and communication solutions*
Physical Disability	***Cognitive Disability***	***Psychosocial Disability***
- *Voice Recognition* - *Adapted and virtually keyboard* - *Joystick and adapted mouse* - *Use of eye-gaze and gesture to control device* - *Remote and online access to work, education, and other services*	- *Text-to-speech rendition and speech/voice output* - *Touch screen devices* - *Mobile apps and online resources that mimic Augmentative and Alternative Communication (AAC) devices, electronic picture boards for communication* - *Organization and memory aid tools such as online calendars, note taking, alerts GPS-facilitated navigation* - *Use of multimedia to aid comprehension e.g., videos, graphics*	- *Use of online communication, documentation, work tools to aid with flexible scheduling* - *Organization and memory aid tools such as online calendars, note taking, alerts*

Sumber: World Bank (2016): Bridging the Disability Divide through Digital Technologies

Cetak Biru Transformasi Digital Perbankan

Data	Teknologi	Manajemen Risiko	Kolaborasi	Tatanan Institusi
Data Protection	Tata Kelola TI	IT *Risk Management*	*Platform Sharing*	*Finance & Investment*
Data Transfer	*Technology Architecture*	*Outsourcing*	Kerjasama lembaga keuangan dan non-lembaga keuangan	*Culture*
Data Governance	*Emerging Technology and Application a.l:* - *Machine Learning* - *Artificial Intelligence* - *Cloud Computing* - *Open API* - *Block Chain/ Distributed Ledger Technology* - *Regtech/ Suptech*	*Cybersecurity*		*Leadership*
				Organizational Design
				Talent

Customer

Customer Engagement	*Customer Experience*	*Customer Insight*	*Customer Trust and Perception*	*Customers with Disabilities*

Boks 3.

DIGITALISASI PERBANKAN BERDASARKAN *DIGITAL MATURITY ASSESSMENT FOR BANK* (DMAB)

"This is the digital age - Everything about business is transforming. Before you can know where to go, you need to understand where you are. We call that digital maturity"

(Deloitte, 2019)

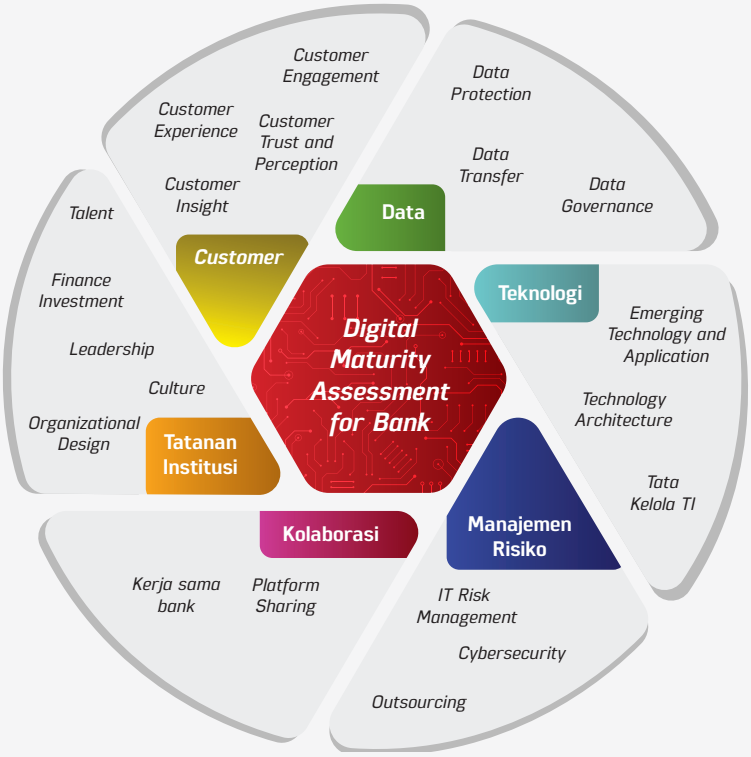
Transformasi digital dalam industri perbankan akan menjadi momen perubahan yang sangat penting. OJK selaku regulator perbankan perlu mengawal transformasi digital yang dilakukan perbankan sekaligus mengarahkan dan memfasilitasi percepatan transformasi digital yang dilakukan oleh perbankan. Untuk mencapai tujuan tersebut, kondisi digitalisasi pada perbankan perlu diketahui; agar OJK dapat menentukan kerangka kerja, pedoman dan strategi sebagai landasan dalam pembuatan kebijakan dalam rangka akselerasi transformasi digital perbankan; serta kondisi digitalisasi perbankan tersebut perlu dipantau perkembangannya secara kontinu.

Kesuksesan transformasi digital perbankan bergantung pada kombinasi dari 3 (tiga) unsur yakni Sumber Daya Manusia (SDM) Bank (*people*), bagaimana Bank mengeksekusi strategi untuk melakukan transformasi bisnis (*process*) dan teknologi yang menciptakan nilai tambah bagi organisasi dan nasabah Bank. Ketiga unsur transformasi digital perbankan tersebut diturunkan dalam bentuk Cetak Biru Transformasi Digital Perbankan yang meliputi 5 (lima) elemen utama yakni meliputi pedoman implementasi data, teknologi, manajemen risiko, kolaborasi, dan tatanan institusi pada industri perbankan. Kelima elemen tersebut merupakan langkah strategis yang bertujuan untuk mendorong perbankan dalam menciptakan inovasi produk dan layanan keuangan yang dapat memenuhi ekspektasi konsumen serta berorientasi pada kebutuhan konsumen (*customer centric orientation*). Kelima elemen utama serta tujuan akhir Cetak Biru (*building blocks*) tersebut kemudian dibuat menjadi tolok ukur tingkat kematangan digital (*digital maturity*) pada Bank. Tolok ukur tersebut disusun menjadi suatu model yakni *Digital Maturity Model* (DMM) yang digunakan sebagai alat penilaian tingkat digitalisasi pada Bank, sehingga dapat diketahui kondisi digitalisasi perbankan dan dilakukan *monitoring* terhadap perkembangan transformasi digital yang dilakukan oleh Bank. Alat penilaian (DMM) tersebut kemudian dinamai *Digital Maturity Assessment for Bank* (DMAB).

DMAB memberikan panduan komprehensif untuk menentukan, menilai, dan mengevaluasi tingkat digitalisasi Bank saat ini. Lebih lanjut, DMAB akan dapat dipergunakan sebagai alat untuk mengukur pencapaian (*monitoring*) digitalisasi perbankan dan pelaksanaan Cetak Biru Transformasi Digital Perbankan. OJK mengembangkan DMAB bagi sektor perbankan melalui kolaborasi lintas *stakeholders* yakni dengan melibatkan industri perbankan, asosiasi perbankan, serta *stakeholders* eksternal lainnya. DMAB kemudian dapat dipergunakan baik bagi Bank dan pengawas dalam menilai sejauh mana tingkat digitalisasi yang telah dilakukan oleh bank. DMAB mengevaluasi tingkat kematangan digital bank dalam 6 (enam) dimensi untuk menciptakan pandangan holistik tentang kematangan digital di seluruh level organisasi Bank.

Penilaian tingkat kematangan digital telah dilakukan OJK pada seluruh Bank Umum baik konvensional dan Syariah. Tingkat kematangan digital yang tinggi mencerminkan kesuksesan transformasi digital yang dilakukan oleh Bank pada 6 (enam) dimensi penilaian DMAB. Semakin tinggi level *score* hasil penilaian DMAB (level 1 – 3) maka dapat disimpulkan bahwa Bank tersebut memiliki nilai maturitas digital yang semakin tinggi. Hasil penilaian tingkat kematangan digital pada perbankan Indonesia menunjukkan bahwa nilai tingkat kematangan digital rata-rata Bank di Indonesia berada dalam kategori level 1, hanya sejumlah kecil bank yang telah masuk dalam kategori level 2 atau level 3. Hasil ini mengindikasikan bahwa terdapat kebutuhan untuk memfasilitasi transformasi digital perbankan agar dapat mendorong sebagian besar Bank di Indonesia dalam melakukan transformasi digital. Dengan demikian, perbankan nasional dapat lebih siap menghadapi tantangan digitalisasi dan melakukan transformasi digital dengan lebih cepat.

Gambar 49
Digital Maturity Assessment for Bank

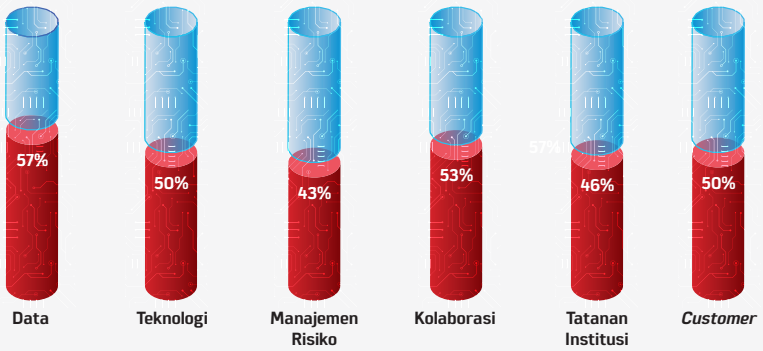


Tingkat kematangan digital tertinggi merupakan proksi tingkat kematangan digital yang dimiliki oleh Bank *fully digital*. Rasio rata-rata nilai tingkat kematangan digital Bank di Indonesia dibandingkan dengan nilai tingkat kematangan digital Bank *fully digital* menunjukkan sejauh mana pencapaian transformasi digital yang dilakukan oleh perbankan Indonesia. Berdasarkan hasil penilaian rata-rata tingkat kematangan digital Bank di Indonesia pada masing-masing dimensi DMAB, tingkat kematangan digital perbankan Indonesia pada dimensi data dan kolaborasi menunjukkan rasio di atas 50%. Dimensi

data memiliki tingkat kematangan digital sebesar 57% terkait pengelolaan, pengolahan, dan analisis data (pemanfaatan data untuk kepentingan *market intelligence* dan kemampuan Bank dalam memanfaatkan data untuk menyediakan informasi secara *real time*), sedangkan dimensi kolaborasi menunjukkan tingkat kematangan digital sebesar 53% yang menunjukan level *interconnectedness* perbankan di Indonesia dalam ekosistem ekonomi dan keuangan digital baik melalui *platform sharing* dan kerja sama bank dengan institusi lain.

Hasil tersebut mencerminkan bahwa tingkat kematangan digital pada aspek data dan kolaborasi rata-rata Bank di Indonesia dinilai cukup memadai walaupun belum optimal. Sementara itu, tingkat kematangan digital pada dimensi teknologi dan konsumen menunjukkan rasio sebesar 50% (Gambar 50). Hasil tersebut menunjukkan bahwa level tata kelola teknologi perbankan di Indonesia seperti terkait telah memiliki strategi digitalisasi dan mengadopsi teknologi terkini dalam layanan dan produk Bank, serta terkait bank dapat memenuhi ekspektasi konsumen (*customer engagement*, *customer experience*, *customer insight,* dan *customer trust and perception*) dinilai sudah cukup baik meskipun belum sepenuhnya optimal. Namun demikian, penilaian tingkat kematangan digital rata-rata Bank di Indonesia pada dimensi manajemen risiko dan tatanan institusi masih berada di bawah 50% (Gambar 50).

Gambar 50
Rasio Rata-Rata Nilai Tingkat Kematangan Digital Bank di Indonesia terhadap Nilai Tingkat Kematangan Digital Maksimal



Sumber: Hasil Penilaian DMAB OJK, 2021

Hasil tersebut menunjukkan bahwa strategi digitalisasi perbankan yang diikuti dengan adopsi *emerging technology*, konektivitas dalam ekosistem digital dan pengelolaan data dalam layanan dan produk Bank masih belum didukung oleh kapasitas organisasi dan budaya digital serta manajemen risiko yang memadai dalam rangka mendukung transformasi digital. Dimensi tingkat kematangan digital yang masih memiliki penilaian rendah dibandingkan dimensi lainnya kemudian akan menjadi perhatian utama OJK ke depan dalam rangka mendorong perbankan Indonesia untuk melakukan percepatan transformasi digital.

Glosarium

Application Programming Interface	Seperangkat rutin (*routine*), protokol, dan alat untuk membangun aplikasi perangkat lunak yang menentukan tata cara interaksi komponen perangkat lunak tersebut.
Artificial intelligence	Analisis dan teknik berbasis logika untuk menginterpretasikan peristiwa, mendukung dan mengotomatisasi proses pengambilan keputusan dan aksi.
Big Data	Data bervolume besar, frekuensinya tinggi dan tidak terstruktur, yang dihasilkan menggunakan teknologi digital dan sistem informasi.
Big Data Analytic	Teknik analisis lanjutan (*advanced*) 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*).
Bigtech	Perusahaan besar yang bergerak di bidang TI yang melebarkan sayap bisnisnya pada penyediaan layanan keuangan, baik secara langsung ataupun melalui produk yang mirip produk keuangan.
Biometrics	Studi dan penerapan metode ilmiah dan/atau teknologi yang dirancang untuk mengukur, menganalisis, dan/atau mencatat karakteristik fisiologis atau perilaku unik manusia.
Blockchain	Teknologi yang digunakan sebagai sistem penyimpanan data digital yang terhubung melalui kriptografi.
Business Impact Analysis	Alat bantu untuk menganalisis bagaimana suatu peristiwa risiko dapat mempengaruhi aktivitas operasional organisasi dan mengidentifikasi kapabilitas apa yang dibutuhkan untuk mengelola peristiwa risiko tersebut.
Cloud Computing	Layanan bisnis yang menyediakan akses jaringan ke sumber daya komputer (*server, database storage,* aplikasi, *services*) yang dapat dikonfigurasi dan digunakan sesuai permintaan, disediakan secara cepat dengan interaksi yang minimal (US NIST).

Cyberattacks	Serangan yang digunakan oleh negara, individu, kelompok, atau organisasi yang menargetkan sistem informasi komputer, infrastruktur, jaringan komputer, dan/atau perangkat komputer pribadi dengan berbagai cara tindakan berbahaya yang biasanya berasal dari sumber anonim untuk mencuri, mengubah, atau menghancurkan target yang ditentukan dengan cara meretas sistem yang rentan.
Data Science	Disiplin ilmu yang mempelajari tentang cara pemrosesan *Big Data.*
Deepfakes	Video rekayasa atau materi digital yang dibuat oleh *artificial intelligence* yang canggih hingga menghasilkan gambar dan suara yang terlihat dan terdengar asli.
Delivery Channel	Fasilitas pelayanan yang diberikan kepada nasabah untuk memberikan kemudahan dan kenyamanan dalam bertransaksi.
Digital Banking	Layanan perbankan elektronik yang dikembangkan dengan mengoptimalkan pemanfaatan data nasabah dalam rangka melayani nasabah secara lebih cepat, mudah, dan sesuai dengan kebutuhan serta dapat dilakukan secara mandiri sepenuhnya oleh nasabah dengan memperhatikan aspek pengamanan.
E-Commerce	Satu set teknologi, aplikasi-aplikasi, dan proses bisnis yang dinamis untuk menghubungkan perusahaan, konsumen, dan masyarakat melalui transaksi elektronik dan pertukaran barang, pelayanan, dan informasi yang dilakukan secara elektronik.
Emerging Technology	Pengembangan, kombinasi, atau integrasi dari beberapa teknologi yang sudah ada sebelumnya.
Escrow Account	Rekening giro di Bank atas nama Penyelenggara yang merupakan titipan dan digunakan untuk tujuan tertentu yaitu penerimaan dan pengeluaran dana dari dan kepada pengguna jasa penyelenggara pinjam meminjam uang berbasis teknologi informasi.
Fintech	Inovasi teknologi jasa keuangan yang menghasilkan model bisnis, aplikasi, proses, dan/atau produk baru.

Firewall	Sistem keamanan jaringan komputer untuk membantu mencegah dari ancaman akses ilegal dari koneksi luar.
Generasi Milenial	Penduduk yang lahir pada periode 1981-1996
Generasi X	Penduduk yang lahir pada periode 1965-1980
Generasi Z	Penduduk yang lahir setelah tahun 1996
Internet of Things	Digitalisasi atas dunia/aplikasi fisik.
Machine Learning	Bentuk dari *artificial intelligence* yang memungkinkan suatu sistem untuk belajar dari data ketimbang dari proses pemrograman yang eksplisit.
Omnichannel	Interaksi yang mulus dan konsisten antara pelanggan dan penyedia layanan keuangan yang memanfaatkan multi-saluran.
Open Banking	Sistem yang menyediakan pengguna dengan jaringan data lembaga keuangan melalui penggunaan antarmuka pemrograman aplikasi atau *Application Programming Interface* (API).
Phishing	Jenis serangan manipulasi psikologis yang sering digunakan untuk mencuri data pengguna gawai.
Quantum Computing	Alat untuk memproses informasi yang menggunakan prinsip mekanika kuantum.
Regulatory Technology	Pemanfaatan teknologi untuk *regulatory compliance* secara efektif dan efisien.

SIM *Swap*	Modus penipuan dengan mengambil alih nomor ponsel (SIM *Card*) seseorang oleh pelaku kejahatan dan dijadikan sebagai sarana untuk meretas akun perbankan seseorang.
Social Engineering	Teknik manipulasi yang memanfaatkan kesalahan manusia untuk mendapatkan akses pada informasi pribadi atau data-data berharga.
Super-App	Platform yang menawarkan berbagai macam layanan dalam satu aplikasi.
Supervisory Technology	Penggunaan teknologi inovatif oleh lembaga pengawas untuk mendukung implementasi fungsi pengawasan.
Wearable Devices	Sensor dan alat yang menempel di tubuh dimana pengunaannya mengacu pada teknologi elektronik atau komputer yang digabungkan di dalam pakaian.

Daftar Pustaka

Accenture Interactive. 2014. "Digital Transformation Re-Imagine from the Outside-In." *Point of View Series*. *Accenture Interactive,* Dublin.

Anand, Ambrish, and Prakash Suman. 2019. "Global and Industry Frameworks for Data Governance." *PricewaterhouseCoopers Private Limited*, Singapore.

Boston Consulting Group. 2018. "Understanding the Path to Digital Marketing Maturity." *The Boston Consulting Group*, Boston.

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.

BNM (2021) dan https://www.kapronasia.com/research/blog/why-is-monzo-struggling-more-than-revolut.html

Capgemini, and Altran. 2019. "Create a Global Digital Transformation Leader." *Capgemini Worldwide. Capgemini*, Amstelveen.

Capgemini. 2010. "Data Governance & Stewardship." *Convergent Media and Privacy*. Paris.

Capgemini Digital Transformation Institute. 2018. "The Digital Culture Challenge: Closing the Employee-Leadership Gap". *Capgemini Digital Transformation Institute,* Paris.

CISSREc. 2020. Pentingnya literasi digital untuk tangkal kejahatan siber diunduh di https://www.cissrec.org/news/detail/838/Pentingnya-literasi-digital-untuk-tangkal-kejahatan-siber.html pada 2 Juli 2021.

Cullen, Sara, Peter Seddon, and Leslie P Willcocks. 2006. "Managing Outsourcing: The Lifecycle Imperative." Department of Information Systems London School of Economics and Political Science, *MIS Executive*. Vol. 44. London.

Deloitte Canada. 2021. "The Digital Workplace: Think, share, do". *Deloitte*, Quebec.

Deloitte. 2018. "Digital Maturity Model." *Deloitte*. London.

Deloitte. 2018. "The Deloitte Global Outsourcing Survey 2018." *Deloitte,* London.

ESMA. 2020. "Final Report: Guidelines on Outsourcing to Cloud Service Provider," *European Securities and Market Authorities,* Paris.

European Parliament Research Services. 2021. "Tackling Deepfakes in European Policy" Study Panel for the Future Science and Technology.

Gökşen, Haluk, and Yılmaz Gökşen. 2021. "A Review of Maturity Models Perspective of Level and Dimension." *Proceedings 2021 Vol* 74 No2, pp: 2-6.

Google Cloud dan Oxford Economics. 2020. *How digital business ecosystems drive efficiency and innovation in a new era*. Oxford Economics.

Grebe, Michael, Michael Rüßmann, Michael Leyh, and Marc Roman Franke. 2018. "Digital Maturity Is Paying Off." *The Boston Consulting Group*, Boston.

Hernandez, Emilio. 2019. "Agent Networks at the Last Mile: A Guide for Digital Finance to Reach Rural Customers." *CGAP Technical Guide. CGAP/World Bank,* Washington.

HKMA. 2016. "Guide to Enhanced Competency Framework on Cybersecurity". *Hong Kong Monetary Authority*, Hong Kong.

HKMA. 2001. "Supervisory Policy Manual SA-2: Outsourcing". *Hong Kong Monetary Authority*, Hong Kong.

International Organization for Standardization. 2020. ISO/IEC 27005:2018 Information technology-Security techniques-Information security risk management, ICS: 35.030 IT Security (2018).

Inventure Knowlegde. 2020. "15 Banking Customer Megashift."

IOSCO. 2020. "Principles on Outsourcing: Consultation Report". *International Organization of Securities Commissions,* Madrid.

Jeník, Ivo, Mark Flaming, and Arisha Salman. 2020. "Inclusive Digital Banking: Emerging Markets Case Studies." *Consultative Group to Assist the Poor, World Bank*, Washington DC.

King, Brett. 2018. "Bank 4.0: Banking Everywhere, Never at a Bank". Wiley, New York.

KPMG Australia. 2019. "The Future of Digital Banking." *KPMG International Cooperative*, Adelaide.

KPMG International. 2017. "The Route to Digital Business Leadership." *KPMG International Cooperative,* Amstelveen.

KPMG AG. 2020. "Outsourcing Advisory Services for Banks". *KPMG AG*. Zurich.

Krishnan, Mahesh. 2013. "Data Governance for Financial Institutions." *Capgemini,* Paris.

Lee, Nicol Turner, Paul Resnick dan Genie Barton. 2019. "Algorithmic bias detection and mitigation: Best practices and policies to reduce consumer harms" The Brookings Institution. https://www.brookings.edu/research/algorithmic-bias-detection-and-mitigation-best-practices-and-policies-to-reduce-consumer-harms/.

Lim, Tristan, and Patrick Thng. 2021. "Outsourcing Life Cycle Model for Financial Services in the FinTech Era." *Proceedings of the International Conference on Industrial Engineering and Operations Management*, pp: 1–11.

Martin Vejačka dan Tomáš Štofa. 2017. Influence of Security and Trust on Electronic Banking Adoption in Slovakia. https://core.ac.uk/download/pdf/295589125.pdf

McKinsey. 2019. "Digital Maturity Scan McKinsey Digital Quotient (DQ)." McKinsey Digital Quotient; Fastfwd, New York.

McKinsey. 2019. "Tackling Bias in Artificial intelligence."

Microsoft dan PSFK. 2017. Digital Banking Playbook. http://info.microsoft.com/rs/157-GQE-382/images/Digital%20Banking%20Playbook%20Final%20.pdf

MIT Center for Digital Business and Capgemini Consulting. 2011. "Digital Transformation: A Road-Map for Billion-Dollar Organizations." MIT Center for Digital Business and Capgemini. London.

Nasution, Ameidyo N. 2021. "Literasi Keuangan Digital Rendah, Jokowi Minta Fintech Perluas Peran" diunduh di https://katadata.co.id/ameidyonasution/berita/5fac4a1893be8/literasi-keuangan-digital-rendah-jokowi-minta-fintech-perluas-peran pada 2 Juli 2021

Newman, Mark. 2017. "Digital Maturity Model (DMM): A Blueprint for Digital Transformation." *TM Forum White Paper*. New Jersey.

Otoritas Jasa Keuangan. 2016. Peraturan Otoritas Jasa Keuangan Nomor 38 /POJK.03/2016 Tentang Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum. LNRI 2016/267. TLNRI 5963 (2016).

Peters, Kasper, and Gerry Pelgrims. 2021. "Interbank Ecosystems Accelerating the Transformation of Banking Services." Deloitte, Belgium.

Petrella, Andy. 2020. "What Is Data Governance? Understanding the Business Impact." *O'Reilly,* Sebastopol.

Pickens, Mark, David Porteous, and Sarah Rotman. 2009. "Scenarios for Branchless Banking in 2020." *Focus Note 57. CGAP, World Bank,* Washington, D.C.

Prudential Regulation Authority (PRA). 2021. "Policy Statement PS7/21 Outsourcing and Third Party Risk Management". *Prudential Regulation Authority.* United Kingdom.

PwC Singapore. 2018. "Fundamentals of Data Governance." *PricewaterhouseCoopers Singapore,* Singapore.

Rasmus, Russ Blanchet Max McKinney Jeff. 2020. "The Race for Digital Operations Transformation: The Time for Experimenting Is Over." *Accenture,* Dublin.

Reynaldi, F., & Tifana, N. 2020. Urgensi Pelindungan Data Pribadi dalam Menjamin Hak Privasi: Sebuah Telaah RUU Pelindungan Data Pribadi. Universitas Padjajaran Press tersedia pada https://fh.unpad.ac.id/urgensi-pelindungan-data-pribadi-dalam-menjamin-hak-privasi-sebuah-telaah-ruu-pelindungan-data-pribadi/

Ritter, Jeffrey, Mary K. Pratt, and Jeff Jenkins. 2015. "Data Governance Strategies for the Digital Age." *SearchCompliance.com e-Publication. TechTarget,* Newton.

Robosoft Technology. 2020. https://www.robosoftin.com/blog/how-to-create-super-apps

Roubini Thoughtlab. 2016. "The Path to Digital Leadership." Vol. 63. *RoubiniThoughtlab and Global Coalition Organization,* Philadelphia.

Roubini Thoughtlab. 2018. "Wealth and Asset Management 2022: The Path to Digital Leadership." *RoubiniThoughtlab and Global Coalition Organization,* Philadelphia, 2017.

Russell Reynolds Associates, "Digital Pulse 2018 : Organizational Structure." *Russell Reynolds Associates,* London.

Stouffer, Keith, Timothy Zimmerman, CheeYee Tang, Michael Pease, Joshua Lubell, and Jeffrey Cichonski. 2020. "Cybersecurity Framework Version 1 . 1 Manufacturing Profile." *National Institute of Standards and Technology.* Gaithersburg, 2020.

Strauß, Ralf, Kerstin Clessienne, and Kerstin Pape. "Marketing Tech Monitor 2020." Statista *Content & Information Design,* Hamburg.

Suh, Bomil, and Ingoo Han. 2003. The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. *International Journal of Electronic Commerce/ Spring*, vol. 7 No.3, pp: 135–161.

Tham, Jacquline, Mohd Shukri Ab Yazid, Abdol Ali Khatibi, S.M. Ferdous Azam. 2017. "Customer Perception of Trust towards Virtual Banking Adoption in Malaysia." *European Journal of Business and Management,* 9(14).

The European Parliament And The Council Of The European Union. 2016. EU General Data Protection Regulation, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, Pub. L. No. Directive 95/46/EC.

The Open Group Standard. 2018. "The TOGAF® Standard, Version 9.2." *The Open Group*.

The OECD, 2019 "The OECD AI Principles" diunduh dari https://www.oecd.org/going-digital/ai/principles pada 30 Juni 2021

The Treasury of Australian Government. 2019. "Consumer Data Right.". *Commonwealth of Australia,* Parkes.

UNSW Sydney. 2017. "Data Governance Policy." *University of New South Wales,* Sydney.

Veenstra, Jennifer, and Timothy Murphy. 2020. "2021 Global Marketing Trends." *Deloitte*. London.

Vejačka, Martin, and Tomáš Štofa. 2017. "INFLUENCE OF SECURITY AND TRUST ON ELECTRONIC BANKING ADOPTION IN SLOVAKIA." *E+M: Ekonomie a* Management 20, no. 4, pp: 135–50. https://doi.org/10.15240/tul/001/2017-4-010.

Westerman, George, Maël Tannou, Didier Bonnet, Patrick Ferraris, and Andrew McAfee. 2012. "The Digital Advantage: How Digital Leaders Outperform Their Peers in Every Industry." *MIT Sloan Management Review; Capgemini*, Paris.

Wray, Pauline, Ian Loh, Yang Yu, Selin Suntay, Jason Han, and Alex Walker. 2020. *"Southeast Asia: Coming of the Digital Challenger Banks," Singapore Fintech Association, BCG, Expand, Finastra.*

Yuen, Arthur. 2016*. "Guide to Enhanced Competency Framework on Cybersecurity." Hong Kong Monetary Authority* (*HKMA*) Vol. 17. Hongkong.

Tim Penyusun

PENGARAH

Heru Kristiyana | Kepala Eksekutif Pengawas Perbankan

Teguh Supangkat | Deputi Komisioner Pengawas Perbankan I

KOORDINATOR

Anung Herlianto E.C. | Kepala Departemen Penelitian dan Pengaturan Perbankan

TIM PERUMUS

Mohamad Miftah | Tony | Citra Christina | Elsa Ryan Ramdhani | Muhammad Radhi | Nurani Pertiwi Ekaputri | Aulia Yuliyanti Wulandari | Aninda Nusratina | Yenny Yorisca

Halaman Ini Sengaja Dikosongkan

DEPARTEMEN PENELITIAN DAN PENGATURAN PERBANKAN
OTORITAS JASA KEUANGAN

GEDUNG BANK INDONESIA
MENARA RADIUS PRAWIRO
JL. M.H. THAMRIN NO. 2
JAKARTA 10110
TEL. 62 21 296 00000