

**LEMBAGA KETAHANAN NASIONAL
REPUBLIK INDONESIA**



**PENINGKATAN KESIAPAN TEKNOLOGI INFORMASI
DI SEKTOR KEUANGAN DALAM MENGHADAPI BENCANA
DALAM RANGKA
MENJAGA KETAHANAN EKONOMI NASIONAL**

Oleh :

IR. DWI KURNIAWAN, MBA
DIREKTUR TI, OJK

**KERTAS KARYA ILMIAH PERSEORANGAN (TASKAP)
PROGRAM PENDIDIKAN REGULER ANGKATAN LXI
LEMHANNAS RI
TAHUN 2020**

KATA PENGANTAR

Assalamualaikum Wr. Wb.

Dengan memanjatkan puji syukur ke hadirat Tuhan Yang Maha Esa serta atas segala rahmat dan karunia-Na, penulis sebagai salah satu peserta Program Pendidikan Reguler Angkatan (PPRA) LXI telah berhasil menyelesaikan tugas dari Lembaga Ketahanan Nasional Republik Indonesia sebuah Kertas Karya Ilmiah Perseorangan (Taskap) dengan Judul : **“PENINGKATAN KESIAPAN TEKNOLOGI INFORMASI DI SEKTOR KEUANGAN DALAM MENGHADAPI BENCANA DALAM RANGKA MENJAGA KETAHANAN EKONOMI NASIONAL. “**

Penentuan Tutor dan judul taskap ini didasarkan oleh Keputusan Gubernur Lembaga Ketahanan Nasional Republik Indonesia Nomor 81 Tahun 2020 tanggal 8 Juni 2020 tentang Pengangkatan Tutor Taskap kepada para peserta PPRA LXI untuk menulis Taskap dengan memilih judul yang telah ditentukan oleh Lemhannas RI.

Pada kesempatan ini, perkenankanlah Penulis menyampaikan ucapan terima kasih kepada **Bapak Gubernur Lemhannas RI Bapak Letjen TNI (Purn) Agus Widjojo** yang telah memberikan kesempatan kepada penulis untuk mengikuti PPRA LXI di Lemhannas RI tahun 2020. Ucapan terima kasih juga penulis sampaikan kepada Pembimbing atau Tutor Taskap kami yaitu Ibu **Dr. Rosita S. Noer, M.A.** dan **Tim Penguji Taskap** serta semua pihak yang telah membantu serta membimbing Taskap ini sampai terselesaikan sesuai waktu dan ketentuan yang dikeluarkan oleh Lemhannas RI.

Penulis menyadari bahwa kualitas Taskap ini masih jauh dari kesempurnaan akademis, oleh karena itu dengan segala kerendahan hati mohon adanya masukan guna penyempurnaan naskah ini.

Besar harapan penulis agar Taskap ini dapat bermanfaat sebagai sumbangan pemikiran penulis kepada Lemhannas RI, termasuk bagi siapa saja yang membutuhkannya.

Semoga Tuhan Yang Maha Esa senantiasa memberikan berkah dan bimbingan kepada kita semua dalam melaksanakan tugas dan pengabdian kepada Negara dan bangsa Indonesia yang kita cintai dan kita banggakan.

Sekian dan terima kasih. Wassalamualaikum Wr. Wb.

Jakarta, 5 Oktober 2020

Penulis



PERNYATAAN KEASLIAN

1. Yang bertanda tangan di bawah ini :

Nama : Ir. Dwi Kurniawan, MBA
Jabatan : Direktur Strategi Sistem Informasi
Instansi : Otoritas Jasa Keuangan Republik Indonesia
Alamat : JL. Kristal P. Hijau, Blok G 11 A, Jakarta 12210

Sebagai peserta Program Pendidikan Reguler Angkatan (PPRA) LXI Tahun 2020 menyatakan bahwa :

- a. Kertas Karya Ilmiah Perseorangan (TASKAP) yang saya tulis adalah asli.
 - b. Apabila ternyata sebagian atau seluruhnya ulisan Taskap ini terbukti tidak asli atau plagiasi, maka saya bersedia dinyatakan tidak lulus pendidikan.
2. Demikian pernyataan keaslian ini dibuat untuk dapat digunakan seperlunya.

Jakarta, 5 Oktober 2020



IR. DWI KURNIAWAN, MBA
DIREKTUR TI, OJK

DAFTAR ISI

	Halaman
KATA PENGANTAR.....	i
PERNYATAAN KEASLIAN.....	iii
DAFTAR ISI.....	iv
TABEL.....	v
DAFTAR GAMBAR.....	vi
BAB I PENDAHULUAN	
1. Latar Belakang	1
2. Rumusan Masalah.....	5
3. Maksud dan Tujuan	5
4. Ruang Lingkup dan Sistematika.....	6
5. Metode dan Pendekatan.....	7
6. Pengertian.....	7
BAB II TINJAUAN PUSTAKA	
7. Umum.....	9
8. Paradigma Nasional.....	9
9. Peraturan dan Perundang-undangan.....	10
10. Kerangka Teoretis.....	12
11. Data dan Fakta	15
12. Perkembangan Lingkungan Strategis.....	17
BAB III PEMBAHASAN	
13. Umum.....	20
14. Peran Penting Teknologi Informasi di Sektor Keuangan	22
15. Ancaman Gangguan Bencana Terhadap Teknologi Informasi di Sektor Keuangan.....	30
16. Kegiatan Peningkatan Kesiapan Teknologi Informasi di Sektor Keuangan dalam Menghadapi Bencana	41
BAB IV PENUTUP	
17. Simpulan	58
18. Rekomendasi.....	59
DAFTAR PUSTAKA	
DAFTAR LAMPIRAN	
1. ALUR PIKIR	
2. DAFTAR RIWAYAT HIDUP	

LEMBAGA KETAHANAN NASIONAL
REPUBLIC INDONESIA

TABEL

TABEL I. LAYANAN DIGITAL DI PASAR MODAL

TABEL II. LAYANAN DIGITAL DI LJK NON BANK

TABEL III. BENCANA SIBER DARI ASPEK KEBOCORAN DATA

TABEL IV. BENCANA SIBER DARI ASPEK KEUTUHAN DATA

TABEL V. BENCANA SIBER DARI ASPEK KETERSEDIAAN DATA

TABEL VI. ANALISA SWOT TERHADAP KESIAPAN MENGHADAPI BENCANA

TABEL VII. ANALISA TOWS UNTUK MERUMUSKAN KEGIATAN
PENINGKATAN KESIAPAN TEKNOLOGI INFORMASI DALAM
MENGHADAPI BENCANA



LEMBAGA KETAHANAN NASIONAL
REPUBLIC INDONESIA

DAFTAR GAMBAR

GAMBAR 1. TIGA ASPEK PENTING DALAM TRANSFORMASI ORGANISASI

GAMBAR 2. MODEL PDCA SISTEM MANAJEMEN KELANGSUNGAN USAHA

GAMBAR 3. PENGGUNA TELEPON PINTAR DI INDONESIA 2015-2019

GAMBAR 4. NILAI SEKTOR JASA KEUANGAN



BAB I PENDAHULUAN

1. Latar Belakang

Teknologi informasi berkembang dengan sangat pesat. Perkembangan mempengaruhi segala bidang kehidupan masyarakat di segala bidang. Khusus di bidang ekonomi, pengaruh perkembangan teknologi informasi sangat dirasakan. Negara-negara di dunia berlomba-lomba untuk meningkatkan kesiapannya dalam menyongsong era ekonomi digital dan industri 4.0 yang sangat bergantung pada pemanfaatan teknologi informasi.

Ekonomi digital telah banyak digunakan di Indonesia terutama di sektor keuangan yang meliputi industri perbankan, pasar modal dan industri keuangan nonbank seperti asuransi, dana pensiun, perusahaan pembiayaan, lembaga keuangan mikro dan teknologi keuangan (*financial Technology*) serta *e-commerce*. Peran industri keuangan, yang sarat dengan dukungan teknologi informasi, bagi perekonomian nasional sangat besar. Hal ini terlihat dari total nilai aset industri keuangan untuk industri Perbankan di Indonesia per akhir tahun 2019 sebesar Rp 9.237,158 triliun, total nilai aset di Industri Keuangan Non Bank (IKNB) sebesar Rp 2.557,78 triliun dan total nilai kapitalisasi di pasar modal mencapai Rp7.299,283 triliun pada akhir tahun 2019.¹

Investasi Teknologi Informasi di sektor jasa keuangan juga cukup besar. Sebagai contoh di bidang perbankan, pada tahun 2019 BCA memiliki anggaran investasi teknologi sebesar Rp 5,2 T, Bank Rakyat Indonesia sebesar Rp 3,5T, Bank Mandiri sebesar Rp 3 T, BNI sebesar Rp 1 triliun, dan BTN sebesar Rp 300-400 miliar. Di sisi lain, perkembangan perusahaan pinjam meminjam uang berbasis teknologi informasi (*fintech lending*) juga semakin meningkat, di mana pada bulan Juni 2020 terdapat 158 fintech yang terdaftar atau mendapatkan ijin dari OJK dengan akumulasi penyaluran pinjaman mencapai Rp 113,46 Triliun, akumulasi rekening peminjam (*borrower*) sebesar 25.768.329 entitas, akumulasi rekening pemberi pinjaman

¹ Otoritas Jasa Keuangan. 2019. "Laporan Triwulanan IV-2019". Jakarta:Otoritas Jasa Keuangan

(*lender*) mencapai 659.186 entitas dan nilai *outstanding* pinjaman sebesar Rp 11,77 Triliun.²

Indonesia memang dinilai sebagai salah satu negara yang memiliki pertumbuhan ekonomi digital yang sangat pesat. Untuk layanan *e-commerce* (seperti Tokopedia, Bukalapak, Shopee) jumlah nilai transaksi di 14 *e-commerce* terbesar Indonesia mencapai Rp 265,07 triliun di sepanjang tahun 2019, meningkat pesat dari Rp 80,82 triliun pada tahun 2017 dan Rp 145,95 triliun pada tahun 2018.³ Pada tahun 2022 *pasar e-commerce* Indonesia diproyeksikan akan tumbuh menjadi \$55 miliar hingga \$65 miliar atau tumbuh sebanyak delapan kali lipat dari tahun 2017.⁴

Pemanfaatan teknologi informasi pada digital ekonomi selain diharapkan mampu mendorong pertumbuhan ekonomi, juga diharapkan mampu meningkatkan akses masyarakat di seluruh pelosok Indonesia terhadap produk-produk keuangan. Melalui layanan teknologi informasi baik berupa digitalisasi layanan perbankan maupun layanan *fintech*, masyarakat di pedesaan dan seluruh pelosok Indonesia diharapkan dapat memperoleh akses informasi dan layanan keuangan yang diperlukan.

Pemerintah Indonesia di era presiden Jokowi pun menyadari hal tersebut dan telah mencanangkan berbagai program untuk meningkatkan kesiapan nasional dalam mengembangkan ekonomi digital. Di dalam Peraturan Presiden Peraturan Presiden (Perpres) Nomor 18 Tahun 2020 tentang Rencana Pembangunan Jangka Menengah Nasional (RPJM Nasional) Tahun 2020-2024, tercantum bahwa dari 2 (dua) agenda yang terkait dengan ekonomi digital yaitu “Memperkuat Ketahanan Ekonomi untuk Pertumbuhan yang Berkualitas” dan “Memperkuat Infrastruktur untuk Mendukung Pengembangan Ekonomi dan Pelayanan Dasar”. Di dalam kedua agenda tersebut terdapat target peningkatan kontribusi ekonomi digital dari 3,17% di

² Otoritas Jasa Keuangan. 2020. “Perkembangan Fintech Landing April 2020”. Jakarta:Otoritas Jasa Keuangan.

³ Bidara Pink & Noverius Laoli. 11 February 2020. “BI Sebut Nilai Transaksi *e-commerce* Sepanjang 2019 Meningkatkan Drastis”. <https://nasional.kontan.co.id/news/bi-sebut-nilai-transaksi-e-commerce-sepanjang-2019-meningkat-drastis?> Diunduh 4 Juli 2020 pukul 10:00.

⁴ Kaushik Das, *et al.* 2020. “The Digital Archipelago: How Online Commerce is Driving Indonesia’s Economic Development”. <https://www.mckinsey.com/featured-insights/asia-pacific/the-digital-archipelago-how-online-commerce-is-driving-indonesias-economic-development>. Diunduh 4 Juli 2020 pukul 11:00.

tahun 2019 menjadi 4,66% di tahun 2024, dan target nilai transaksi *e-commerce* dari sekitar Rp. 260 triliun di tahun 2019 menjadi Rp. 600 triliun di tahun 2024.

Dalam kondisi normal, layanan teknologi informasi berjalan sebagaimana seharusnya. Namun apabila terjadi bencana, maka akan dapat berdampak pada berkurang atau terhentinya layanan keuangan yang didukung oleh teknologi informasi.

Bencana adalah peristiwa atau rangkaian peristiwa yang mengancam dan mengganggu kehidupan dan penghidupan masyarakat yang disebabkan baik oleh faktor alam dan/atau faktor non-alam. Berbagai bencana telah terjadi di banyak negara di seluruh dunia. Indonesia sendiri, karena keadaan geografisnya, sering mengalami bencana alam seperti bencana banjir, gunung meletus, penyakit dsb. Badan Nasional Penanggulangan Bencana (BNPB) mencatat terjadinya peningkatan bencana alam di Indonesia dalam tiga tahun terakhir, yaitu 2.862 kali terjadi bencana pada tahun 2017, 3.397 pada tahun 2018 dan 3.768 pada tahun 2019⁵. Nilai kerugian sebagai dampak bencana pada tahun 2019 adalah sebesar Rp 80 Triliun.

Dengan semakin tingginya ketergantungan pada teknologi, bencana non-alam berupa kegagalan teknologi juga semakin mengancam. Bencana kegagalan teknologi, khususnya teknologi informasi, sering dikenal dengan kejahatan di dunia maya (*cyber crime*). Kejahatan di dunia maya ini semakin marak baik dari aspek kerahasiaan data (*confidentiality*), aspek keutuhan data (*integrity*) maupun aspek ketersediaan layanan teknologi informasi (*availability*).

Banyak bencana kegagalan teknologi yang telah dialami di Indonesia. Di aspek kerahasiaan data, contoh bencana yang terjadi pada tahun 2020 adalah bocor dan dijualnya 91 juta pengguna dan 7 juta penjual dari *e-commerce* Tokopedia⁶, 530 ribu akun pengguna Zoom⁷, dan 230 ribu Data Pasien

⁵ Badan Nasional Penanggulangan Bencana. 2020. "Data Bencana di Indonesia". Jakarta: BNPB

⁶ Roy Franedy. 7 Mei 2020. "91 Juta Data Pengguna Bocor, Tokopedia Digugat Rp 100 M". <https://www.cnbcIndonesia.com/tech/20200507083340-37-156876/91-juta-data-pengguna-bocor-tokopedia-digugat-rp-100-m/>. Diakses 18 Juli 2020, pukul 09:00.

⁷ CNBC Indonesia. 16 April 2020. "Kacau, 530.000 Data Akun Zoom Dijual Hacker di Dark Web". <https://www.cnbcindonesia.com/tech/20200416082700-37-152270/kacau-530000-data-akun-zoom-dijual-hacker-di-dark-web>. Diakses 18 Juli 2020, pukul 10:00

Suspek Covid-19⁸. Di aspek keutuhan data sering terjadi tindakan kriminal sebagai akibat pemanfaatan data yang bocor, seperti pembobolan kartu kredit, kartu ATM maupun rekening nasabah. Di aspek ketersediaan layanan, contoh bencana yang pernah terjadi adalah putusnya serat optik telekomunikasi di Palembang sehingga jalur internet Jawa-Sumatera-Kalimantan dan Luar Negeri menjadi terputus, serta gangguan jaringan yang berakibat pada matinya ribuan ATM bank-bank.

Seringnya terjadi bencana sebagaimana tergambar pada data dan fakta di atas serta besarnya dampak kerugian yang dialami menunjukkan bahwa kita, khususnya teknologi informasi di sektor keuangan, belum siap dalam menghadapi bencana.

Ketidaksiapan tersebut juga selaras dengan hasil penilaian dari *International Telecommunication Union* terkait kesiapan untuk menghadapi kegagalan teknologi di dunia maya, yang menempatkan Indonesia pada posisi 41 dari 175 negara berdasarkan *Global Cybersecurity Index (GCI)* pada tahun 2018, dan peringkat 9 di Asia Pasifik di bawah Singapura, Malaysia dan Thailand. Posisi ini meningkat dari tahun sebelumnya, namun masih menunjukkan kelemahan keamanan siber kita di beberapa aspek seperti teknologi, sumber daya manusia dan hukum.⁹

Untuk meminimalkan potensi kejadian dan dampak bencana, Indonesia perlu memastikan kesiapan teknologi informasi dalam situasi tersebut. Layanan keuangan kepada masyarakat harus tetap terlaksana dengan dukungan teknologi informasi yang optimal. Kemandirian dalam teknologi informasi juga perlu ditingkatkan agar kita tidak selalu tergantung pada teknologi dari luar negeri. Kesiapan tersebut diperlukan untuk menghindari gangguan di bidang ekonomi yang dapat menghambat terwujudnya Ketahanan Ekonomi Nasional. Kesiapan teknologi informasi akan menjaga kemampuan Indonesia dalam memelihara stabilitas ekonomi yang sehat dan dinamis serta kemampuan menciptakan kemandirian ekonomi nasional

⁸ CNN Indonesia. 20 Juni 2020. "230 Ribu Data Pasien Covid-19 di Indonesia Bocor dan Dijual". <https://www.cnnindonesia.com/teknologi/20200620083944-192-515418/230-ribu-data-pasien-covid-19-di-indonesia-bocor-dan-dijual>. Diakses 18 Juli 2020, pukul 10:30

⁹ International Telecommunication Union. 2018. "Global Cybersecurity Index 2018". Geneva:ITU

dengan daya saing tinggi dan mewujudkan kemakmuran rakyat yang adil dan merata.

2. Rumusan Masalah

Teknologi Informasi telah menjadi tulang punggung dalam meningkatkan pertumbuhan ekonomi nasional dan kesejahteraan masyarakat. Di sisi lain, kejadian bencana di Indonesia baik alam maupun non-alam, termasuk bencana kegagalan teknologi, menimbulkan dampak yang besar baik bagi masyarakat maupun ketahanan ekonomi nasional. Untuk mengantisipasi dan membantu mengatasi bencana, maka teknologi informasi, khususnya di sektor keuangan, harus memiliki kesiapan yang tinggi.

Berdasarkan uraian di atas, permasalahan yang akan dijawab di dalam penulisan ini adalah “Bagaimana meningkatkan kesiapan Teknologi Informasi di Sektor Keuangan dalam menghadapi bencana dalam rangka menjaga Ketahanan Ekonomi Nasional?”

Di dalam kajian akan dilakukan analisa untuk mendapatkan jawaban dari beberapa pertanyaan sebagai berikut :

- a. Mengapa Teknologi Informasi di Sektor Keuangan Perlu Disiapkan Dalam Menghadapi Bencana?
- b. Bagaimana Bencana Dapat Mengganggu Teknologi Informasi di Sektor Keuangan?
- c. Bagaimana Peningkatan Kesiapan Teknologi Informasi di Sektor Keuangan?

3. Maksud dan Tujuan

- a. Maksud dari penulisan taskap ini adalah untuk memberikan gambaran tentang peran teknologi informasi di bidang keuangan, jenis dan dampak bencana yang menjadi ancaman dan upaya-upaya yang perlu dilakukan agar teknologi informasi di bidang keuangan siap dalam menghadapi bencana .
- b. Tujuan dari penulisan Taskap ini adalah untuk memberikan sumbangan pemikiran kepada para pihak baik pemerintah, bisnis maupun akademisi, agar dapat digunakan sebagai bahan acuan dalam menentukan hal-hal

yang perlu dilakukan untuk meningkatkan kesiapan teknologi informasi di sektor keuangan dalam menghadapi bencana.

4. Ruang Lingkup dan Sistematika

Ruang lingkup tulisan ini dibatasi pada masalah bagaimana meningkatkan kesiapan teknologi informasi di sektor keuangan (perbankan, industri keuangan nonbank dan pasar modal serta *e-commerce*) dalam menghadapi kondisi bencana. Bencana yang akan dibahas adalah bencana non-alam yang berdampak pada teknologi informasi, dengan fokus pada bencana kegagalan teknologi di dunia maya (*cyber security*).

Adapun penulisan makalah ini disusun berdasarkan sistematika sebagai berikut :

a. BAB I : Pendahuluan.

Merupakan bagian awal penulisan, dalam bab ini diuraikan secara singkat tentang latar belakang permasalahan, maksud dan tujuan penulisan, ruang lingkup dan sistematika penulisan, metode dan pendekatan serta pengertian-pengertian yang dianggap relevan dalam materi penulisan.

b. BAB II : Tinjauan Pustaka.

Bab ini membahas teori dan dasar pemikiran yang digunakan sebagai landasan dalam menyusun makalah dan digunakan sebagai instrumental input dalam pemecahan persoalan.

c. BAB III : Pembahasan.

Berisi pembahasan dari pertanyaan-pertanyaan kajian berdasarkan teori beserta aspek yang telah disebutkan dalam bab sebelumnya. Dari hasil pembahasan tersebut didapatkan faktor penyebab masalah dan solusinya.

d. BAB IV : Penutup.

Dalam Bab ini berisi tentang kesimpulan dari keseluruhan pembahasan dan beberapa saran yang dikemukakan.

5. Metode dan Pendekatan

Metode yang digunakan dalam penulisan Taskap ini adalah analisis deskriptif, yakni pengumpulan dan analisa data dan fakta yang berkaitan dengan materi permasalahan berdasarkan metode penelitian literatur (studi pustaka).

Pendekatan yang digunakan dalam penulisan Taskap ini adalah pendekatan perspektif kepentingan ketahanan ekonomi nasional dengan analisa disiplin ilmu teknologi dan manajemen sebagaimana tercantum dalam tinjauan pustaka.

6. Pengertian

Agar menghindari perbedaan persepsi, dalam makalah ini dicantumkan beberapa pengertian sebagai berikut :

- a. **Teknologi Informasi** adalah suatu teknik untuk mengumpulkan, menyiapkan, menyimpan, memproses, mengumumkan, menganalisis, dan/atau menyebarkan informasi.¹⁰
- b. **Sektor Keuangan** adalah sektor yang meliputi lembaga yang melaksanakan kegiatan di bidang Perbankan, Pasar Modal, Perasuransian, Dana Pensiun, Lembaga Pembiayaan, dan Lembaga Jasa Keuangan Lainnya serta *e-commerce*.¹¹
- c. **Bencana** adalah peristiwa atau rangkaian peristiwa yang mengancam dan mengganggu kehidupan dan penghidupan masyarakat yang disebabkan, baik oleh faktor alam dan/atau faktor non-alam maupun faktor manusia sehingga mengakibatkan timbulnya korban jiwa manusia, kerusakan lingkungan, kerugian harta benda, dan dampak psikologis.¹²
- d. **Sistem Manajemen Kelangsungan Usaha** (*Business Continuity Management*) adalah suatu rangkaian proses sistem manajemen yang terencana, terukur, dan menyeluruh, yang mencakup identifikasi dini, pengembangan ketahanan, kemampuan pengendalian setiap potensi

¹⁰ Undang Undang Perubahan Atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang Undang Nomor 19 Tahun 2016. Lembaran Negara RI No. 251 Tahun 2016, Tambahan Lembaran Negara RI No. 5952.

¹¹ Undang Undang Otoritas Jasa Keuangan. Undang Undang Nomor 21 Tahun 2011. Lembaran Negara RI No. 111 Tahun 2011, Tambahan Lembaran Negara RI No. 5253.

¹² Undang-undang Penanggulangan Bencana. Undang-Undang Nomor 24 Tahun 2007. Lembaran Negara RI No. 66 Tahun 2007, Tambahan Lembaran Negara RI No. 4723.

insiden secara efektif, pemulihan kondisi, dan proses penyelenggaraan kegiatan kembali ke normal, untuk menjamin keberlangsungan bisnis perusahaan atau organisasi.¹³

- e. **Ketahanan Ekonomi** adalah kondisi dinamik kehidupan perekonomian bangsa yang berisi keuletan dan ketangguhan yang mengandung kemampuan pengembangan kekuatan nasional dalam menghadapi serta mengatasi segala tantangan, ancaman, hambatan dan gangguan, baik yang datang dari luar maupun dari dalam dan yang langsung atau tidak langsung untuk menjamin kelangsungan hidup perekonomian bangsa dan negara Republik Indonesia berdasarkan Pancasila dan UUD NRI 1945.¹⁴



¹³ The International Organization for Standardization. 2019. "ISO 22301:2019, Security and Resilience – Business Continuity Management Systems – Requirements". Geneva: ISO

¹⁴ Lembaga Pertahanan Nasional. 2020. Bahan Ajar Bidang Studi Geostrategi Indonesia dan Ketahanan Nasional". Jakarta:Lemhannas. hlm 105.

BAB II

TINJAUAN PUSTAKA

7. Umum

Beberapa bahan pustaka akan menjadi rujukan dalam pembahasan. Teori yang akan digunakan adalah Teori Manajemen dan Transformasi Organisasi dari Leavitt. Selain itu akan digunakan rujukan lain berupa standar internasional dan regulasi nasional yang terkait teknologi informasi. Standar internasional ISO 22301 tentang Sistem Manajemen Kelangsungan Usaha berisi petunjuk bagi perusahaan untuk mencegah terjadinya bencana teknologi dan meminimalkan dampaknya. Sedangkan dari sisi regulasi akan digunakan Undang-Undang, Peraturan Pemerintah dan Peraturan Otoritas Jasa Keuangan yang terkait dengan penggunaan teknologi informasi.

8. Paradigma Nasional

Paradigma Nasional adalah acuan dasar dalam melaksanakan upaya untuk mencapai tujuan nasional melalui pembangunan nasional. Paradigma Nasional terdiri dari Wawasan Nusantara, Ketahanan Nasional, dan Kewaspadaan Nasional.

Wawasan Nusantara adalah cara pandang bangsa Indonesia tentang diri dan lingkungan keberadaannya dengan memanfaatkan kondisi dan konstelasi geografi dengan menciptakan tanggung jawab, motivasi, dan rangsangan bagi seluruh bangsa Indonesia untuk mencapai tujuan nasional.

Ketahanan Nasional adalah kondisi dinamik bangsa Indonesia yang meliputi segenap aspek kehidupan nasional 58 Geopolitik Indonesia dan Ketahanan Nasional yang terintegrasi berisi keuletan dan ketangguhan yang mengandung kemampuan mengembangkan kekuatan nasional, dalam menghadapi dan mengatasi segala tantangan, ancaman, hambatan, dan gangguan, baik yang datang dari luar maupun dari dalam, untuk menjamin identitas, integritas, kelangsungan hidup bangsa dan negara, serta perjuangan mencapai tujuan nasionalnya.

Kewaspadaan Nasional adalah suatu sikap dalam hubungannya dengan nasionalisme yang dibangun dari rasa peduli dan rasa tanggung jawab serta

perhatian seorang warga negara terhadap kelangsungan kehidupan bermasyarakat, berbangsa dan bernegaranya dari suatu potensi ancaman.

Paradigma Nasional memiliki landasan berupa 4 (empat) Konsensus Dasar Bangsa yaitu Pancasila, Negara Kesatuan Republik Indonesia dan Bhinneka Tunggal Ika.

Dengan berpedoman pada Paradigma Nasional dan Empat Konsensus Dasar maka pembangunan nasional akan dapat mewujudkan tujuan nasional negara kita yaitu melindungi segenap bangsa Indonesia dan seluruh tumpah darah Indonesia, memajukan kesejahteraan umum, mencerdaskan kehidupan bangsa dan ikut melaksanakan ketertiban dunia yang berdasarkan kemerdekaan, perdamaian abadi, dan keadilan sosial.

9. Peraturan dan Perundangan-Undangan

a. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 19 Tahun 2016

Pasal 15 dari UU ITE ini menyebutkan bahwa setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggung jawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya.

b. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik

Peraturan Pemerintah ini bertujuan untuk memastikan bahwa penyelenggara layanan digital memiliki sistem layanan digital yang komprehensif dan juga aman, standar minimal sistem elektronik serta mengatur mengenai pertanggungjawaban apabila terjadi kebocoran data milik masyarakat pengguna layanan digital. Penyelenggara sistem elektronik yang sebagaimana diamanatkan dalam pasal 4 PP 71/2019 sendiri diwajibkan memiliki sistem elektronik yang memiliki standar minimal seperti dapat menampilkan kembali informasi ataupun dokumen elektronik secara utuh sesuai dengan masa retensi yang ditentukan dalam peraturan perundangan; mampu untuk melindungi ketersediaan, keutuhan, kerahasiaan, keautentikan, dan keteraksesan informasi elektronik; mampu beroperasi sesuai dengan operasi dan petunjuk

dalam penyelenggaraan sistem elektronik tersebut; dilengkapi dengan prosedur atau petunjuk dalam penyelenggaraan sistem elektronik tersebut, dan; ada mekanisme yang berkelanjutan untuk menjaga kebaruan, kejelasan, dan kebertanggungjawaban prosedur atau petunjuk.

Apabila terjadi kegagalan (bencana) dalam perlindungan data yang dimiliki oleh penyelenggara sistem elektronik, penyelenggara pertama harus memberi tahu pemilik data pribadi tersebut akan kegagalan tersebut (pasal 14 ayat (5)). Maka, untuk meminimalisir adanya kegagalan tersebut, penyelenggara sendiri wajib untuk melakukan langkah-langkah yang bersifat mencegah terjadinya kegagalan tersebut. Apabila terjadi kegagalan yang berdampak serius akibat dari adanya intervensi pihak ketiga, maka dalam pasal 24 ayat (3) disebutkan bahwa penyelenggara wajib untuk mengamankan data-data yang dimilikinya serta melaporkan bencana kegagalan tersebut kepada pihak yang berwajib.

c. Peraturan Otoritas Jasa Keuangan (POJK) Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko Penggunaan Teknologi Informasi Oleh Bank Umum.

Pada pasal 2, POJK ini mewajibkan bank agar memiliki kebijakan, standar, dan prosedur penggunaan teknologi informasi. Pasal 8 mewajibkan bank untuk menerapkan kebijakan, standar dan prosedur tersebut secara konsisten dan berkesinambungan. Pasal 12 menyebutkan bahwa sebagai langkah preventif, bank harus memastikan kelangsungan dan kestabilan operasional teknologi informasi yang berpotensi dapat mengganggu kegiatan operasional bank. Pasal 16 mewajibkan bank untuk menyediakan teknologi informasi yang memenuhi prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan ketersediaan (*availability*).

d. Peraturan Otoritas Jasa Keuangan (POJK) Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi.

POJK ini mengatur berbagai hal yang harus ditaati oleh penyelenggara layanan pinjam meminjam uang berbasis teknologi

informasi atau biasa disebut dengan *fintech peer-to-peer lending (P2P lending)*. Tujuan dari ketentuan ini adalah untuk melindungi kepentingan konsumen terkait keamanan dana dan data, serta kepentingan nasional terkait pencegahan pencucian uang dan pendanaan terorisme, serta stabilitas sistem keuangan.

Pasal 25 Peraturan OJK menyebutkan bahwa *fintech* wajib menggunakan pusat data dan pusat pemulihan bencana. Penyelenggara wajib memenuhi standar minimum sistem teknologi informasi, pengelolaan risiko teknologi informasi, pengamanan teknologi informasi, ketahanan terhadap gangguan dan kegagalan sistem, serta alih kelola sistem teknologi informasi.

10. Kerangka Teoretis

a. Teori Manajemen dan Tranformasi Organisasi dari Leavitt

Leavitt menyebutkan bahwa suatu organisasi akan dapat bertransformasi dengan melakukan perbaikan pada 3 aspek yaitu

- manusia (*people*),
- proses (*process : structure and task*)
- teknologi (*technology*).

Untuk mencapai efisiensi dalam pengelolaan organisasi, ketiga aspek tersebut harus dijalankan dengan seimbang.¹⁵



¹⁵ Leavitt, H. J. .1965. "Applied change in Industry: Structural, Technological and Humanistic Approaches". Pennsylvania:Carnegie Institute of Technology

Teori ini akan digunakan untuk menganalisa permasalahan dan menyusun solusi berupa hal-hal yang perlu dilakukan untuk meningkatkan kesiapan Teknologi Informasi.



Gambar 1. Tiga Aspek Penting dalam Transformasi Organisasi

b. Teori SWOT (*Strength, Weakness, Opportunity and Threat*) dari Albert Humphrey

Teori SWOT pertama kali diperkenalkan oleh Albert S Humphrey pada tahun 1960-an di Stanford Research Institute. Teori ini digunakan untuk membantu organisasi dalam mengidentifikasi kekuatan dan kelemahan yang dimiliki serta peluang dan ancaman yang dihadapi dalam rangka menyusun strategi atau rencana perusahaan.

SWOT dapat digunakan sebagai alat untuk mengevaluasi posisi strategis suatu organisasi dari berbagai jenis baik perusahaan bisnis maupun non bisnis seperti pemerintahan.

Dengan melakukan analisa berdasarkan SWOT maka dapat diidentifikasi 4 (empat) aspek berbeda dari suatu perusahaan :

- Kekuatan: karakteristik bisnis atau kegiatan yang memberikan keunggulan dibandingkan dengan perusahaan lain.
- Kelemahan: karakteristik bisnis atau kegiatan yang kurang menguntungkan dibandingkan dengan perusahaan lain.

- Peluang: unsur-unsur di lingkungan bisnis atau kegiatan yang dapat dimanfaatkan oleh perusahaan untuk keuntungannya.
- Ancaman: unsur-unsur di lingkungan bisnis atau kegiatan yang dapat menimbulkan masalah bagi perusahaan.

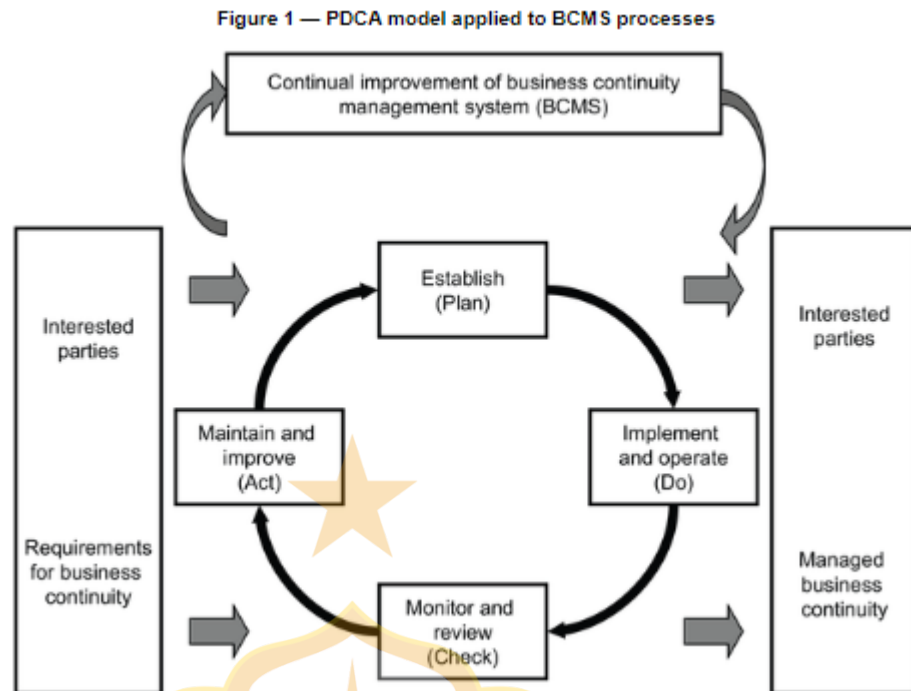
c. Sistem Manajemen Kelangsungan Usaha (*Business Continuity Management*)

Perusahaan atau organisasi perlu mempersiapkan diri dalam menghadapi bencana yang dapat mengakibatkan hilangnya kemampuan perusahaan dalam melakukan proses bisnis secara normal. Proses bisnis yang kritical harus dilindungi dari ancaman bencana sehingga tetap bisa berjalan agar tidak menimbulkan dampak operasional, ekonomi, hukum maupun reputasi perusahaan.

ISO 22301:2019 tentang Sistem Manajemen Kelangsungan Usaha berisi standar untuk mempersiapkan dan mengelola secara efektif suatu Sistem Manajemen Kelangsungan Usaha (SMKU) dalam menghadapi bencana.

Adapun proses Standard internasional ini menerapkan model PDCA (*Plan - Do – Check - Act*), yang dipopulerkan oleh Dr. W. Edwards Deming, untuk merencanakan, mengimplementasikan, meninjau dan meningkatkan efektivitas secara terus menerus SKMU organisasi atau perusahaan.





Gambar 2. Model PDCA Sistem Manajemen Kelangsungan Usaha

11. Data dan Fakta

a. Data dan Fakta tentang Pentingnya Teknologi Informasi di Sektor Keuangan.

Penggunaan Teknologi Informasi di sektor keuangan semakin meningkat, mendorong pertumbuhan ekonomi dan kesejahteraan masyarakat.

Besarnya dukungan teknologi informasi ini dapat dilihat dari beberapa data. Total nilai aset industri keuangan untuk industri Perbankan di Indonesia per akhir tahun 2019 sebesar Rp 9.237,158 triliun, total nilai aset di Industri Keuangan Non Bank (IKNB) sebesar Rp 2.557,78 triliun dan total nilai kapitalisasi di pasar modal mencapai Rp7.299,283 triliun pada akhir tahun 2019.¹⁶

Untuk perusahaan *fintech peer-to-peer lending*, pada bulan Juni 2020, terdapat 158 perusahaan *fintech P2P* yang terdaftar atau mendapat ijin dari OJK dengan akumulasi penyaluran pinjaman mencapai Rp 113,46 Triliun. Akumulasi rekening peminjam (*borrower*)

¹⁶ Otoritas Jasa Keuangan. 2019. "Laporan Triwulanan IV-2019". Jakarta:Otoritas Jasa Keuangan

sebesar 25.768.329 entitas, akumulasi rekening pemberi pinjaman (*lender*) mencapai 659.186 entitas dan nilai *outstanding* pinjaman sebesar Rp 11,77 Triliun.

Di sub sektor perdagangan on-line, jumlah nilai transaksi di 14 *e-commerce* terbesar Indonesia diestimasi mencapai Rp 265,07 triliun di sepanjang tahun 2019. Jumlah nilai transaksi ini meningkat pesat dari nilai transaksi di keseluruhan tahun 2017 yang sebesar Rp 80,82 triliun dan keseluruhan nilai transaksi di sepanjang tahun 2018 yang mencapai Rp 145,95 triliun.¹⁷

b. Data dan Fakta tentang Bencana Yang Mengancam Teknologi Informasi di Sektor Keuangan

Namun demikian, seiring dengan semakin maraknya penggunaan teknologi informasi, semakin meningkat pula ancaman bencana non-alam berupa kegagalan teknologi.

Beberapa contoh bencana tersebut adalah bocornya data 91 pengguna di salah satu *e-commerce*. Kebocoran ini juga menyebabkan gugatan dari Komunitas Konsumen Indonesia sebesar Rp. 100 Miliar atas dasar kegagalan penyelenggara sistem elektronik dalam menyimpan serta melindungi kerahasiaan data pribadi dan hak privasi dari pengguna situs tersebut.¹⁸

Bencana non-alam berupa kegagalan teknologi dapat pula disebabkan oleh bencana alam seperti banjir dan gempa bumi. Kejadian bencana gempa bumi berskala besar akan menyebabkan kerusakan infrastruktur teknologi informasi. Bencana alam ini sering terjadi di Indonesia akibat letak geografis Indonesia. Secara geografis Indonesia merupakan negara kepulauan yang terletak pada pertemuan 4 (empat) lempeng tektonik besar yaitu lempeng Benua Asia, Benua Australia, lempeng Samudera Hindia dan Samudera Pasifik. Sabuk vulkanik (*volcanic arc*) berada di Indonesia memanjang mulai dari Pulau

¹⁷ Pink, Bidara & Laoli, Noverius. 11 Februari 2020. "BI Sebut Nilai Transaksi *e-commerce* Sepanjang 2019 Meningkat Drastis". <https://nasional.kontan.co.id/news/bi-sebut-nilai-transaksi-e-commerce-sepanjang-2019-meningkat-drastis?page=all>. Diakses 25 Juli 2020, pukul 21:00

¹⁸ CNN Indonesia. 2020. "13 Juta Data Bocor Bukalapak Dijual di Forum Hacker". <https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker>. Diakses 1 Agustus 2020 pukul 08:00

Sumatera, Pulau Jawa, Nusa Tenggara sampai dengan Pulau Sulawesi. Kondisi geografis tersebut menyebabkan Indonesia menjadi daerah rawan bencana alam. Tingkat kejadian gempa di Indonesia termasuk tertinggi di dunia, lebih dari 10 kali lipat tingkat kegempaan di Amerika Serikat. Pada tahun 2020 ini BNPT mencatat telah terjadi 11 kali gempa bumi di Indonesia.

Di dunia internasional, ketidaksiapan Indonesia dalam menghadapi bencana dunia maya nampak dalam Laporan *Global Cybersecurity Index (GCI)* pada tahun 2018. Laporan tersebut menempatkan Indonesia di peringkat 41 dari 175 negara di dunia dan peringkat 9 di Asia Pasifik di bawah Singapura, Malaysia dan Thailand. Posisi ini meningkat dari tahun sebelumnya, namun masih menunjukkan kelemahan keamanan siber kita di beberapa aspek. Laporan lain yaitu *World Risk Report 2018* yang dikeluarkan oleh ReliefWeb, menilai Indonesia belum mampu meminimalkan dampak negatif dari bencana.¹⁹

12. Perkembangan Lingkungan Strategis

a. Global.

Seiring dengan semakin meningkatnya ketergantungan pada teknologi informasi, ancaman dunia maya (*cyber security*) semakin meningkat secara global. Berdasarkan survey kepada para pimpinan perusahaan di dunia, serangan terhadap dunia maya menjadi ancaman terbesar bagi perkembangan ekonomi (yang sangat tergantung pada teknologi informasi) di dunia abad ini.²⁰ Hal ini juga ditunjukkan dengan semakin meningkatnya kejadian bencana non-alam berupa kegagalan teknologi di dunia maya (*cyber crime*) ini. Sebagai contoh di Amerika, FBI menerima 467,361 laporan serangan di dunia maya di Amerika di tahun 2019 dengan kerugian sebesar \$3.5 billion atau sebesar Rp 49 Triliun pada kurs \$1=Rp 14.000,-. Nilai kerugian tersebut merupakan kenaikan 3 kali lipat dari nilai kerugian pada tahun 2015 sebesar \$1.1 billion.²¹

¹⁹ Mucke, P., et. al. 2018. "World Risk Report 2018". Jerman: Naldo Gruden.

²⁰ <https://www.cnbc.com/2019/07/09/cybersecurity-biggest-threat-to-world-economy-ceos-say.html>. Diakses 9 Agustus 2020, pukul 07:00

²¹ <https://www.fbi.gov/news/stories/2019-internet-crime-report-released-021120>. Diakses 9 Agustus 2020, pukul 08:00

Perkembangan global ini menunjukkan bahwa teknologi informasi berdampak positif bagi perkembangan ekonomi, namun di sisi lain berdampak negatif karena meningkatkan ancaman dunia maya, termasuk ancaman serangan ke layanan digital di Indonesia.

b. Regional.

Indonesia menjadi bagian dari ASEAN yang memiliki tiga komunitas, yakni ASEAN Security Community (ASC), ASEAN Economic Community (AEC) dan ASEAN Socio-Culture Community (ASCC). ASEAN Security Community merupakan upaya bersama untuk meningkatkan kerjasama keamanan regional, salah satunya mengenai keamanan di dunia maya. Pada pertemuan ASEAN Security Community ke-20 di Thailand, dibahas penguatan kerja sama dalam bidang keamanan siber yang semakin penting dalam mendukung perekonomian negara-negara di ASEAN. Disepakati bahwa sangat diperlukan kerjasama antar negara ASEAN mengingat bencana kejahatan dunia siber semakin meningkat dan tidak mengenal batas negara.

Tidak hanya di forum ASEAN, negara lain di kawasan regional seperti Australia, *menyadari* pentingnya kerjasama antar negara. Oleh karena itulah pada tahun 2018, Australia menandatangani *Memorandum of Understanding* (MOU) dengan Indonesia tentang kerjasama di bidang *cyber security*.²² Di dalam MOU itu kedua negara sepakat untuk bekerjasama *sharing* informasi dan standar internasional, pendidikan dan pelatihan, ekonomi digital dan *cyber crime*.

c. Nasional.

Penggunaan Teknologi Informasi di sektor keuangan telah mendorong pertumbuhan ekonomi dan meningkatkan akses masyarakat kepada layanan keuangan di Indonesia. Perkembangan pesat layanan digital terjadi baik yang disediakan oleh perbankan, *fintech* maupun *e-commerce*. Namun demikian bencana kegagalan teknologi di dunia maya juga meningkat. Contoh terbaru adalah kasus bocornya data-data

²² <https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/mou-indonesia-australia-cyber-cooperation>. Diakses 9 Agustus 2020, pukul 08:20

pengguna *e-commerce*, pembobolan kartu kredit dan rekening pada tahun 2020 ini.

Secara nasional, pemerintah menyadari pentingnya keamanan dunia maya dengan pembentukan beberapa instansi yang menangani keamanan dunia siber. Kementerian Komunikasi dan Informasi (Kominfo) bertugas untuk menyusun kebijakan terkait teknologi informasi dan keamanan dunia maya. Kebijakan tentang keamanan teknologi informasi telah ditetapkan yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 19 Tahun 2016. Selain Kominfo, Badan Siber dan Sandi Negara yang dibentuk pada tahun 2017 bertugas untuk melaksanakan keamanan siber secara efektif dan efisien.

Pembentukan instansi dan penetapan regulasi terkait keamanan dunia maya berdampak positif terhadap daya tahan teknologi informasi di sektor keuangan dalam menghadapi bencana. Namun makin sering terjadinya bencana berupa serangan terhadap teknologi informasi menunjukkan bahwa dampak negatif yaitu ketidaksiapan penggunaan teknologi informasi dalam menghadapi bencana perlu segera ditangani dengan lebih optimal.



BAB III

PEMBAHASAN

13. Umum

Saat ini, kita berada dalam sebuah era yang sarat dengan teknologi informasi. Perkembangan teknologi informasi telah membawa perubahan drastis dan mendasar dalam banyak lapangan kehidupan. Dalam kehidupan sehari-hari, kita tidak bisa lepas dari penggunaan teknologi baik dari untuk kebutuhan pribadi maupun dalam kaitannya dengan pekerjaan. Penggunaan teknologi dalam kehidupan sehari pun tidak terlepas dari penggunaan internet. Di era informasi teknologi sendiri semua hal terkait dengan internet, baik itu televisi, telepon seluler, dan komputer.

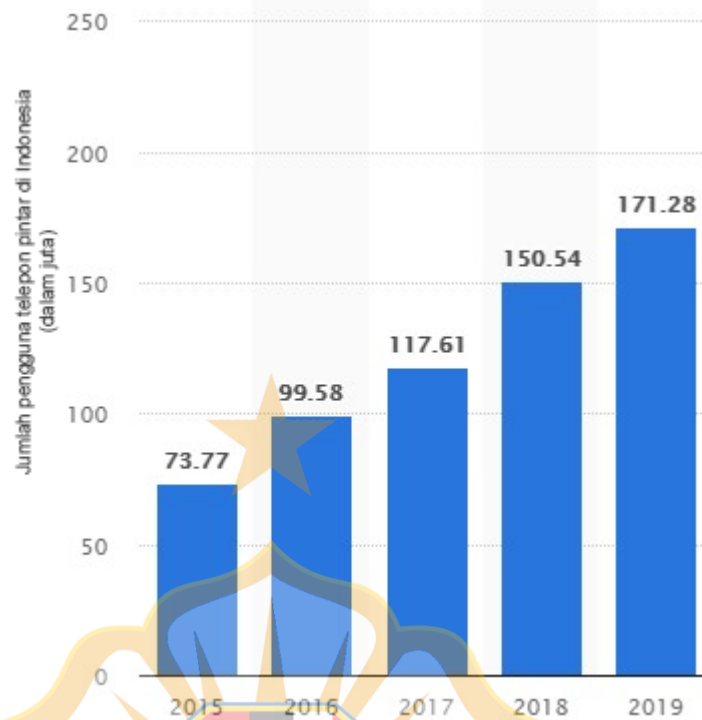
Pemakaian internet di Indonesia pun meningkat dengan pesat. Berdasarkan laporan survei Asosiasi Penyedia Jasa Internet Indonesia (APJII), pengguna internet di Indonesia pada tahun 2019 berjumlah 171,17 juta jiwa dari total penduduk Indonesia sebesar 264,16 juta orang.²³ Angka ini meningkat setiap tahunnya di mana pada tahun 2015 jumlahnya sebesar 110,2 juta jiwa, tahun 2016 sebesar 143,26 juta jiwa, dan tahun 2017 sebesar 143,26 juta jiwa.

Pertumbuhan internet ini juga berbanding lurus dengan jumlah penggunaan teknologi komunikasi informasi seperti telepon seluler hingga komputer. Berdasarkan data yang dimiliki oleh *Statista Research*, pengguna telepon seluler pintar (*smartphone*) pada tahun 2019 berjumlah 171,28 juta jiwa. Angka ini merupakan peningkatan yang terus dialami sejak tahun 2015 yaitu sejumlah 73,77 juta jiwa; tahun 2016 sejumlah 99,58 juta jiwa; tahun 2017 sejumlah 117,61 juta jiwa, dan; tahun 2018 sejumlah 150,54 juta jiwa.²⁴

²³ APJII. 2019. "Laporan Survei Penetrasi dan Profil Pengguna Internet Indonesia Tahun 2018". Jakarta: APJII

²⁴ Müller, J. 2020. "Indonesia Smartphone Users". <https://www.statista.com/statistics/266729/smartphone-users-in-indonesia/>. Diakses 19 Juli 2020, pukul 08.00

Data tersebut disajikan dalam gambar berikut:



Gambar 3. Pengguna Telepon Pintar di Indonesia Tahun 2015-2019

Peningkatan pengguna internet dan *gadget* tersebut juga seiring dengan peningkatan penggunaan teknologi informasi di sektor keuangan. Nilai investasi teknologi semakin meningkat, demikian pula jenis-jenis layanan digital yang tersedia di sektor keuangan.

Namun di sisi lain, ancaman berupa bencana di Indonesia semakin tahun semakin meningkat. Bencana tersebut dapat berupa bencana alam, bencana non-alam maupun bencana kegagalan teknologi. Bencana tersebut berdampak kepada berbagai aspek kehidupan masyarakat. Contoh bencana alam yang berdampak besar adalah bencana Tsunami Aceh pada tahun 2004. Sedangkan contoh bencana non-alam yang berdampak besar adalah wabah penyakit pandemi Covid-19 yang saat ini melanda negara kita dan seluruh dunia. Selain pandemi Covid-19, karena ketergantungan masyarakat yang besar terhadap teknologi, maka bencana non-alam lainnya yang sering terjadi adalah bencana kegagalan teknologi. Kegagalan teknologi ini bisa terjadi di bidang transportasi, industri dan juga di sektor teknologi keuangan.

Bencana-bencana tersebut menimbulkan dampak kerugian yang besar, baik secara individu maupun bagi negara. Produktivitas masyarakat akan turun sehingga pertumbuhan ekonomi terganggu yang akan berdampak pada turunnya ketahanan ekonomi nasional.

Upaya untuk meningkatkan kesiapan teknologi informasi di sektor keuangan dalam menghadapi bencana perlu dirumuskan dengan melakukan analisa terhadap beberapa pertanyaan kajian yaitu peran Teknologi Informasi di sektor keuangan, jenis dan dampak bencana, kondisi kesiapan bencana dan upaya meningkatkan kesiapan teknologi informasi di sektor keuangan dalam menghadapi bencana.

14. Peran Penting Teknologi Informasi di Sektor Keuangan

Dalam era perkembangan teknologi dan digitalisasi, kebutuhan masyarakat akan kegiatan di sektor jasa keuangan yang mudah, cepat dan fleksibel pun meningkat. Kebutuhan masyarakat ini mendorong para pelaku jasa keuangan untuk terus melakukan inovasi dan transformasi dari transaksi secara tradisional ke dalam bentuk digital. Kegiatan dalam sektor jasa keuangan, seperti mendatangi bank untuk melakukan transaksi, bertemu dengan agen penjual langsung untuk mendaftarkan diri sebagai konsumen asuransi, atau mendatangi perusahaan sekuritas bagi masyarakat yang ingin berinvestasi, mulai digantikan dengan proses yang lebih singkat, mudah, dan terjangkau dengan adanya platform digital.²⁵

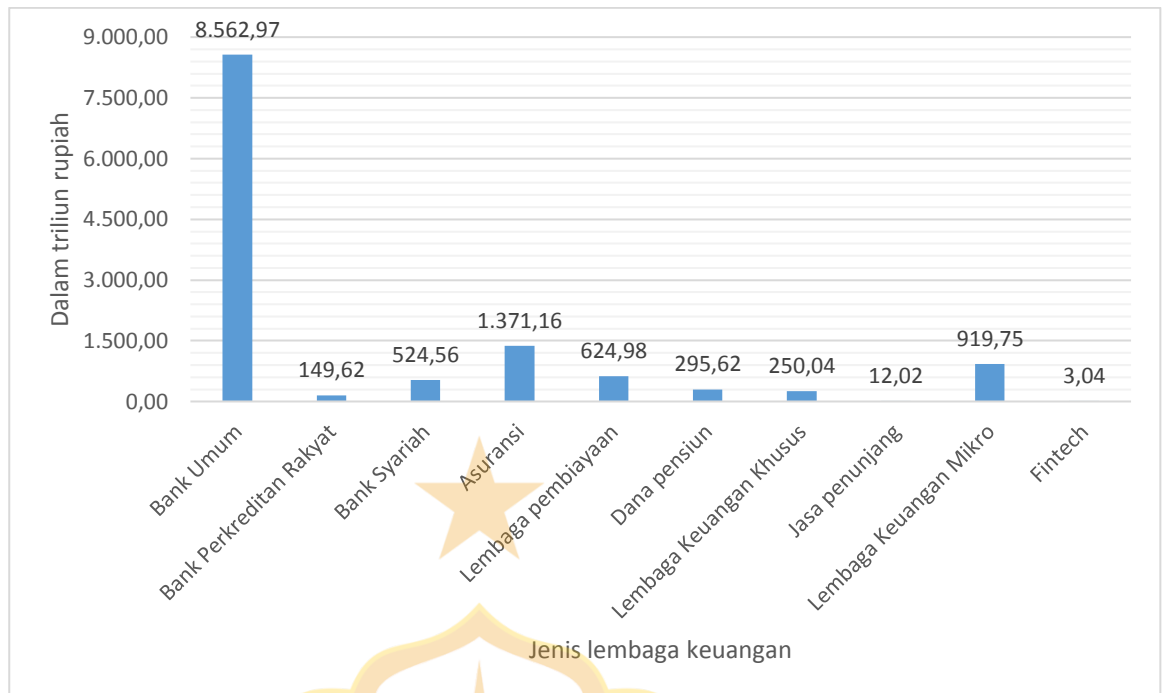
Teknologi informasi di sektor keuangan perlu disiapkan dalam menghadapi bencana karena memiliki peran penting dan merupakan tulang punggung perekonomian nasional. Hal ini dapat dilihat dari nilai layanan teknologi informasi di Indonesia dan beragamnya jenis layanan teknologi informasi di sektor keuangan.

²⁵ Otoritas Jasa Keuangan. 2017. "Kajian Perlindungan Konsumen Sektor Jasa Keuangan: Perlindungan Konsumen Pada Fintech."
<https://konsumen.ojk.go.id/MinisiteDPLK/images/upload/201807131451262.%20Fintech.pdf>.
 Diakses 19 Juli 2020, pukul 12:00

a. **Nilai Layanan Teknologi Informasi di Indonesia**

Untuk mendapatkan gambaran seberapa penting peran teknologi informasi di sektor keuangan, kita dapat melihatnya dari beberapa angka:

- Pagu Anggaran Pendapatan dan Belanja Negara di tahun 2019 adalah sebesar Rp. 2.461,1 triliun, dengan realisasi belanja Rp 2.310 Triliun, dan penerimaan Rp 1.957 Triliun.
- Total nilai aset industri keuangan untuk industri Perbankan di Indonesia per akhir tahun 2019 adalah sebesar Rp 9.237,158 triliun. Nilai ini terdiri dari total aset dari Bank Umum dan Bank Perkreditan Rakyat dengan nilai masing-masing sebesar Rp 8.562,974 triliun dan Rp 149,62 triliun. Total aset Perbankan Syariah sendiri yakni sebesar Rp 524,564 triliun.
- Total nilai aset di Industri Keuangan Non Bank (IKNB) adalah sebesar Rp 2.557,78 triliun. Nilai tersebut terdiri dari Rp.1.371,16 triliun di industri asuransi, Rp624,98 triliun di industri lembaga pembiayaan, Rp295,62 triliun di industri dana pensiun, Rp250,04 triliun di industri Lembaga Keuangan LKK, Rp12,02 triliun di industri Jasa penunjang, Rp919,75 miliar di industri LKM dan Rp3,04 triliun di industri *fintech* yang menitikberatkan penggunaan teknologi informasi.
- Total nilai kapitalisasi di pasar modal mencapai Rp7.299,283 triliun pada akhir tahun 2019.
- Estimasi jumlah nilai transaksi di 14 e-commerce terbesar Indonesia mencapai Rp 265,07 triliun di sepanjang tahun 2019.



Gambar 4. Nilai Sektor Jasa Keuangan

Dari angka-angka di atas, tampak bahwa sektor keuangan memiliki porsi yang sangat besar dalam ekonomi nasional.

Pertanyaan selanjutnya adalah berapa nilai dari investasi teknologi informasi di sektor keuangan? Tidak terdapat informasi resmi atau akurat yang dapat diperoleh tentang hal ini. Secara umum dapat kita sebutkan bahwa mengingat industri jasa keuangan merupakan andalan dalam operasional, maka nilai total aset dan kapitalisasi di atas dapat memberikan gambaran mengenai nilai yang diolah dengan menggunakan teknologi informasi.

Secara lebih spesifik terdapat beberapa data tambahan seperti jumlah biaya investasi teknologi informasi di beberapa bank dan perusahaan telekomunikasi. Pada tahun 2019, BCA memiliki anggaran investasi teknologi sebesar Rp 5,2 T, Bank Rakyat Indonesia sebesar Rp 3,5T, Bank Mandiri sebesar Rp 3 T, BNI sebesar Rp 1 triliun, dan BTN sebesar Rp 300-400 miliar.

Anggaran investasi yang sangat besar tersebut digunakan oleh bank-bank untuk :

- Mengembangkan program/aplikasi teknologi informasi untuk melayani nasabah seperti aplikasi *e-banking*, *phone banking*
- Membangun infrastruktur teknologi informasi seperti jaringan komputer, peralatan *video conference*, *ip-phone*, *server*, *storage*
- Membangun pusat data (*data center*) untuk mengoperasikan infrastruktur dan program/aplikasi dengan spesifikasi bangunan yang berstandar tinggi guna mencegah bencana
- Mengoperasikan helpdesk teknologi informasi untuk membantu nasabah yang mengalami masalah terkait teknologi informasi
- Menyiapkan perangkat keras dan perangkat lunak yang khusus digunakan untuk meningkatkan pengamanan teknologi informasi seperti *firewall*, *intrusion prevention system*, *anti virus*, *anti malware*.
- Mengembangkan teknologi terkini seperti *Big Data*, *Artificial Intelligence*, *Internet of Things* dan *Cloud* untuk meningkatkan kemampuan bank dalam menganalisa data. Analisa ini ditujukan untuk menyusun strategi agar dapat meningkatkan jumlah nasabah, kepuasan nasabah dan meningkatkan keunggulan kompetitif bank.

Upaya di atas menggambarkan keseriusan dari bank-bank dalam menggunakan dan memastikan kehandalan serta keamanan teknologi informasinya.

Selain itu, untuk menunjang kegiatan ekonomi digital, diperlukan adanya perusahaan yang bertindak sebagai penyedia infrastruktur bidang telekomunikasi. Salah satu perusahaan tersebut adalah PT. Telkom, Tbk. Pada Kuartal III 2019, Telkom telah menyerap belanja modal sebesar Rp22,2 triliun, atau 21,6% dari total pendapatannya.²⁶

b. **Jenis Layanan digital di Sektor Keuangan**

Sejalan dengan perkembangan teknologi informasi, layanan yang disediakan Bank mengalami evolusi yang mengarah kepada layanan

²⁶ Boyke P. Siregar. 1 November 2019. "Telkom Serap 21,6% Belanja Modal Hingga Kuartal III ". <https://www.wartaekonomi.co.id/read254465/telkom-serap-216-belanja-modal-hingga-kuartal-iii>. Diakses 25 Juli 2020, pukul 12:30

perbankan digital (*digital Banking*). Layanan ini lebih berorientasi kepada pemenuhan kebutuhan nasabah dengan memanfaatkan sepenuhnya teknologi digital melalui perangkat (*device*) dan aplikasi (*software*) sebagai *delivery channel*. Selain itu, layanan perbankan digital dapat diakses kapan saja dan di mana saja, serta meminimalkan interaksi secara langsung dengan pegawai Bank. Hal ini bertujuan juga untuk meningkatkan efisiensi kegiatan operasional dan mutu pelayanan Bank kepada nasabahnya.²⁷ Perkembangan ini juga mendukung Bank untuk meningkatkan pelayanan kepada nasabah secara aman, nyaman, dan efektif.

Berbagai jenis layanan berbasis teknologi informasi telah disediakan oleh bank seperti ATM, Electronic Data Capture (Kartu Kredit, Kartu Debit), Internet Banking, SMS Banking, Mobile Banking, e-Money dll. Berbagai fitur layanan tersedia secara online seperti informasi (rekening, kurs valuta asing, suku bunga), tranfer, pengajuan pinjaman, pembukaan rekening, portofolio investasi, pembelian (pulsa, tiket), pembayaran (telepon, pulsa, internet, asuransi, listrik, air, pajak, kartu kredit, cicilan, zakat), dan update/topup saldo (e-money, gopay)

Besarnya peran perbankan di dalam perekonomian nasional mendorong Otoritas Jasa Keuangan mengeluarkan peraturan terkait yaitu Peraturan Otoritas Jasa Keuangan (POJK) Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko Penggunaan Teknologi Informasi Oleh Bank Umum. Sebagaimana disebutkan dalam Tinjauan Pustaka, di dalam peraturan tersebut mewajibkan bank untuk meningkatkan kesiapan teknologi informasi dalam menghadapi bencana. Kesiapan tersebut berupa kelengkapan kebijakan, standar dan prosedur keamanan teknologi yang diterapkan secara konsisten dan berkesinambungan.

Pasar modal merupakan sarana pendanaan bagi perusahaan dan pemerintah, dan sebagai sarana kegiatan berinvestasi bagi pemilik dana. Dengan demikian, pasar modal memfasilitasi berbagai sarana dan

²⁷ Otoritas Jasa Keuangan. 2016. "Panduan Penyelenggaraan Digital Branch oleh Bank Umum". Jakarta:Otoritas Jasa Keuangan.

prasarana kegiatan jual beli dan kegiatan terkait lainnya.²⁸ Pasar modal memegang dua peranan sekaligus yakni mempertemukan dua kepentingan yaitu pihak yang memiliki kelebihan dana (investor) dan pihak yang memerlukan dana (issuer/emiten) serta memberikan kesempatan memperoleh imbalan (return) bagi pemilik dana, sesuai dengan karakteristik investasi yang dipilih.

Perusahaan	Layanan Digital
Bursa Efek Indonesia	<i>Jakarta Automated Trading System (JATS)</i>
PT Kliring Penjaminan Efek Indonesia (KPEI)	<i>Electronic Clearing and Guarantee System (e-Clear)</i>
PT Kustodian Sentral Efek Indonesia (KSEI)	<i>Central Depository and Book Entry Settlement (C-BEST)</i>

Tabel 1. Layanan Digital di Pasar Modal

Dalam pelaksanaannya, pasar modal pun tidak terlepas dari pengaruh digitalisasi pelayanan. Saat ini dikenal suatu sistem yang disebut *Scriptless Trading* atau perdagangan efek tanpa warkat. *Scriptless trading* adalah suatu sistem perdagangan efek tanpa warkat yang dilakukan secara otomatis melalui jaringan komputer di Bursa Efek, yaitu penyelesaian transaksi perdagangannya dilaksanakan melalui proses pemindahbukuhan secara elektronik (*book entry settlement*). Jadi dalam perdagangan efek ini penyelesaian transaksinya tidak lagi menggunakan penyerahan surat saham secara fisik.

Terdapat beberapa sistem penunjang dalam pelaksanaan *Scriptless Trading*. Pertama ialah JATS atau *Jakarta Automated Trading System*. JATS adalah sistem perdagangan Efek yang berlaku di Bursa untuk perdagangan yang dilakukan secara otomatis dengan menggunakan sarana komputer²⁹. Penggunaan JATS mampu

²⁸ Otoritas Jasa Keuangan.2017. "Pasar Modal: Seri Literasi Keuangan Perguruan Tinggi" (Ser. 3). Jakarta:Otoritas Jasa Keuangan, hlm 2.

²⁹ PT Bursa Efek Indonesia. 2020. " Surat Keputusan Direksi PT Bursa Efek Indonesia perihal Perubahan Peraturan Nomor II-A tentang Perdagangan Efek Bersifat Ekuitas. SK Nomor Kep-00025/BEI/03-2020.". Jakarta:PT Bursa Efek Indonesia

meningkatkan kapasitas order dan transaksi perdagangan di pasar modal. Saat ini JATS mampu memproses 15 juta order dan 7,5 juta transaksi per hari dengan kecepatan transaksi perdagangan 12.500 order per detik.³⁰

Berikutnya ialah *Central Depository and Book Entry Settlement (C-BEST)*. C-BEST yang dikembangkan PT Kustodian Sentral Efek Indonesia (KSEI) yang bertujuan sebagai sarana penitipan kolektif tertinggi di Bursa Efek Indonesia yang anggotanya adalah Bank Kustodian dan perusahaan efek. Sejak diberlakukannya perdagangan Efek tanpa warkat (*scriptless trading*), maka seluruh Efek yang tersimpan di C-BEST ditransaksikan di Bursa Efek. C-BEST berhasil mendorong peningkatan jumlah investor dan peningkatan jumlah penyelesaian transaksi. Sampai dengan 10 Juli 2020, rata-rata nilai transaksi harian sampai saat ini sebesar Rp7,65 triliun.

Lalu dikenal juga sistem *Electronic Clearing and Guarantee System (e-Clear)*. Sistem ini dimiliki oleh PT Kliring Penjaminan Efek Indonesia (KPEI). e-Clear digunakan dalam menjalankan fungsi kliring dan penjaminan transaksi sesuai dengan namanya. Oleh karena itu yang menjadi bukti kepemilikan atas saham bagi pemilik efek adalah rekening efek yang berbentuk seperti buku tabungan pada Bank Umum dan proses peralihan hak atas saham dilakukan dengan cara pemindahbukuan secara online.

Selain perbankan dan pasar modal, di sektor keuangan juga dikenal Lembaga Jasa Keuangan Nonbank (LJKNB) yaitu lembaga yang melaksanakan kegiatan di sektor perasuransian, dana pensiun, lembaga pembiayaan, dan lembaga jasa keuangan lainnya. Berbagai perusahaan LJKNB telah menyediakan layanan digital sebagaimana tercantum dalam tabel 2.

Perusahaan	Layanan Digital
Asuransi	Insurance <i>Technology</i> (InsurTech)

³⁰ Anastasia Arvirianty. 2018. "Sistem Perdagangan Bursa Bisa Lakukan 7,5 Juta Transaksi." <https://www.cnbcindonesia.com/market/20180507164404-17-13982/sistem-perdagangan-bursa-bisa-lakukan-75-juta-transaksi>. Diakses 25 Juli 2020, pukul 14:00

Dana Pensiun	Layanan Klaim Otomatis, Taspen SmartCard
Perusahaan Pembiayaan	Mobile Appication, Website, Pembayaran melalui ATM atau Debit Otomatis
Pegadaian	Pegadaian Digital

Tabel 2. Layanan Digital di LJK NON BANK

Selain lembaga jasa keuangan tersebut, terdapat pula satu jenis jasa keuangan berbasis teknologi informasi yang cukup populer saat ini yaitu model Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi / *Fintech peer-to-peer* (P2P) *Lending*. *Fintech P2P Lending* adalah penyelenggaraan layanan jasa keuangan untuk mempertemukan pemberi pinjaman (*lender*) dengan penerima pinjaman (*borrower*) dalam rangka melakukan perjanjian pinjam meminjam dalam mata uang rupiah secara langsung melalui sistem elektronik dengan menggunakan jaringan internet. *Fintech P2P Lending* diharapkan dapat memenuhi kebutuhan dana tunai secara cepat, mudah, dan efisien, serta meningkatkan daya saing serta dapat menjadi salah satu solusi untuk membantu pelaku usaha skala UMKM dalam memperoleh akses pendanaan.

Pada bulan Juni 2020, terdapat 158 perusahaan *fintech P2P* yang terdaftar atau mendapat ijin dari OJK. Akumulasi penyaluran pinjaman mencapai Rp 113,46 Triliun. Akumulasi rekening peminjam (*borrower*) sebesar 25.768.329 entitas. Akumulasi rekening pemberi pinjaman (*lender*) mencapai 659.186 entitas dan nilai *outstanding* pinjaman sebesar Rp 11,77 Triliun. Data tersebut menggambarkan berkembangnya *fintech P2P* dan semakin banyaknya masyarakat yang menggunakan *fintech P2P*.

Berikutnya terdapat juga layanan digital lainnya yang sudah banyak dikenal dan digunakan masyarakat. Yang pertama adalah *e-commerce*. *E-Commerce* di dunia dan di Indonesia tumbuh dengan cepat karena beberapa alasan yaitu peningkatan penetrasi telepon pintar, berkembangnya masyarakat kelas menengah dengan pendapatan yang lebih besar, meningkatnya investasi dalam platform *e-commerce* dan

meningkatnya infrastruktur pembayaran yang memungkinkan konsumen tanpa rekening bank untuk melakukan pembelian daring. Di Indonesia sendiri dikenal beberapa platform *e-commerce* yakni Tokopedia, Bukalapak, Shopee, dll. Tokopedia dan Bukalapak bahkan telah menjadi *unicorn* di Indonesia yang memiliki nilai valuasi lebih dari \$1 miliar.

Jumlah nilai transaksi di 14 *e-commerce* terbesar Indonesia diestimasi mencapai Rp 265,07 triliun di sepanjang tahun 2019. Jumlah nilai transaksi ini meningkat pesat dari nilai transaksi di keseluruhan tahun 2017 yang sebesar Rp 80,82 triliun dan keseluruhan nilai transaksi di sepanjang tahun 2018 yang mencapai Rp 145,95 triliun.³¹

Berdasarkan uraian di atas, terlihat bahwa Teknologi Informasi memiliki peran yang sangat penting terhadap sektor keuangan di Indonesia. Teknologi Informasi menjadi tulang punggung bagi perusahaan di sektor keuangan untuk dapat menyediakan berbagai layanan baik di bidang perbankan, pasar modal, industri keuangan non bank maupun *e-commerce*. Masyarakat juga sangat bergantung pada kemudahan, kehandalan dan keamanan teknologi informasi dalam mengakses layanan jasa keuangan. Ancaman pada teknologi informasi akan menimbulkan dampak besar pada kestabilan dan pertumbuhan ekonomi nasional dan kesejahteraan masyarakat. Untuk itu teknologi informasi perlu disiapkan dalam menghadapi bencana agar terjamin layanannya kepada masyarakat.

15. Ancaman Gangguan Bencana Terhadap Teknologi Informasi di Sektor Keuangan

Ketergantungan sektor keuangan sebagaimana tergambar pada uraian sebelumnya, pada sisi lain menimbulkan pula dampak negatif yaitu kerawanan atas kejadian bencana. Apabila ancaman ini tidak diantisipasi, maka dampaknya akan sangat besar, baik bagi masyarakat maupun bagi pertumbuhan ekonomi nasional.

³¹ Pink, Bidara & Laoli, Noverius. 11 Februari 2020. "BI Sebut Nilai Transaksi *e-commerce* Sepanjang 2019 Meningkat Drastis". <https://nasional.kontan.co.id/news/bi-sebut-nilai-transaksi-e-commerce-sepanjang-2019-meningkat-drastis?page=all>. Diakses 25 Juli 2020, pukul 21:00

Bencana adalah peristiwa atau rangkaian peristiwa yang mengancam dan mengganggu kehidupan dan penghidupan masyarakat yang disebabkan, baik oleh faktor alam dan/atau faktor non-alam maupun faktor manusia sehingga mengakibatkan timbulnya korban jiwa manusia, kerusakan lingkungan, kerugian harta benda, dan dampak psikologis.

a. Jenis Bencana dan Dampak Bencana

Jenis bencana terdiri dari bencana alam, bencana non-alam dan bencana sosial. Bencana alam adalah bencana yang diakibatkan oleh peristiwa atau serangkaian peristiwa yang disebabkan oleh alam antara lain berupa gempa bumi, tsunami, gunung meletus, banjir, kekeringan, angin topan, dan tanah longsor. Bencana non-alam adalah bencana yang diakibatkan oleh peristiwa atau rangkaian peristiwa non-alam yang antara lain berupa kegagalan teknologi, gagal modernisasi, epidemi, dan wabah penyakit. Bencana sosial adalah bencana yang diakibatkan oleh peristiwa atau serangkaian peristiwa yang diakibatkan oleh manusia yang meliputi konflik sosial antar kelompok atau antarkomunitas masyarakat, dan teror.

Bencana non-alam yang semakin sering terjadi adalah bencana kegagalan teknologi. Tak heran dengan semakin tingginya ketergantungan kita terhadap penggunaan teknologi, maka semakin tinggi pula ancaman bencana akibat kegagalan teknologi. Kegagalan teknologi ini dapat terjadi pada berbagai bidang seperti transportasi dan industri. Di bidang transportasi misalnya kegagalan teknologi dapat mengakibatkan jatuhnya pesawat terbang, tenggelamnya kapal, terputusnya jaringan listrik, kebocoran gas atau ledakan kimiawi di kawasan industri, dan bencana atau serangan di dunia maya (*cyber attack*).

Bencana dapat mengakibatkan dampak terhadap berbagai aspek seperti fisik, lingkungan, sosial dan ekonomi. Di aspek fisik, bencana dapat menyebabkan kerusakan atau kehancuran rumah, gedung, jalan, jembatan, dan infrastruktur lainnya. Di aspek lingkungan, bencana dapat menyebabkan pencemaran atau kerusakan lingkungan seperti persawahan, danau, hutan, udara, pertanian dan hewan. Secara

sosial, bencana dapat menimbulkan kematian, sakit, kehilangan pekerjaan, keamanan dan perdamaian. Secara ekonomi, bencana dapat menyebabkan kerusakan/kehilangan harta benda, simpanan, pendapatan, perdagangan, produksi, asuransi dll.

Khusus terkait dengan aspek ekonomi, bencana dapat menyebabkan ditutupnya kantor bank, tidak berfungsinya ATM, ditutupnya pasar dan pertokoan dan tutupnya lembaga finansial lainnya seperti asuransi, pegadaian dan penjaminan. Akibatnya masyarakat tidak dapat melakukan satu atau lebih hal-hal seperti berikut :

- Tidak dapat menarik uang dari Bank dan atau ATM untuk membeli kebutuhan sehari-hari, melakukan pembayaran untuk berbagai kebutuhan (membayar uang sekolah, angsuran/cicilan, transfer kepada anggota keluarga lain, tagihan dan biaya sewa rumah dsb);
- Tidak dapat membeli barang kebutuhan sehari-hari atau kebutuhan lainnya secara fisik;
- Tidak dapat mendapatkan pinjaman untuk keperluan usaha maupun keperluan lainnya;
- Tidak dapat menerima bantuan keuangan melalui bank;
- Tidak dapat membuka rekening baru di bank karena memerlukan tatap muka fisik; dan
- Tidak dapat menggunakan layanan jasa keuangan karena infrastruktur listrik dan internet terganggu;

Bencana pandemi Covid-19 yang saat ini sedang melanda dunia merupakan bencana non-alam yang menimbulkan dampak tidak hanya lokal maupun regional, namun berdampak ke seluruh dunia. Dampak bencana tersebut bukan hanya di bidang kesehatan tapi juga berdampak di bidang sosial dan ekonomi. Saat ini banyak negara telah mengalami resesi ekonomi. Selain itu banyak tenaga kerja yang terkena dampak dari pandemi ini baik diputus kontraknya secara sepihak atau dirumahkan. Hal ini akan berdampak langsung pada peningkatan angka pengangguran. Pada masa pandemi ini, peran Teknologi Informasi semakin diperlukan, seperti :

- akses terhadap layanan keuangan banyak dilakukan secara on-line dengan menggunakan aplikasi digital yang disediakan oleh industri jasa keuangan baik perbankan, pasar modal dan non-bank sebagaimana diuraikan sebelumnya
- kegiatan rapat, pertemuan, pendidikan, pembukaan rekening baru dsb dilakukan dengan menggunakan teknologi konferensi video seperti Zoom, Microsoft Teams, CISCO Webex dan Google Meet.
- peran *e-commerce* menjadi lebih diperlukan sebagai sarana usaha kecil untuk mempertahankan/meningkatkan usaha dan pendapatannya melalui penjualan secara *on-line*.
- penggunaan uang digital / e-wallet seperti GoPay, OVO, DANA dan LinkAja untuk transaksi secara *on-line*.

Selain pandemi Covid-19, contoh bencana non-alam lainnya adalah bencana kegagalan teknologi. Bencana kegagalan teknologi, khususnya teknologi informasi sering dikenal dengan kejahatan di dunia maya (*cyber crime*). Bencana di dunia maya ini, semakin hari semakin meningkat baik frekuensi maupun dampaknya. Bencana di dunia maya ini dapat dikelompokkan menjadi 3 aspek yaitu dari aspek kerahasiaan (*Confidentiality*), keutuhan (*Integrity*) dan ketersediaan (*Availability*). Pengamanan atas ketiga aspek tersebut merupakan kewajiban dari Penyelenggara Sistem Elektronik yang sebagaimana diamanatkan oleh Pasal 4 huruf b PP No. 71 Tahun 2016 tentang Penyelenggaraan Sistem dan Transaksi Elektronik (PP PSTE). Dalam PP PSTE sendiri juga disebutkan bahwa untuk memastikan bahwa penyelenggara sistem elektronik diharuskan untuk menerapkan manajemen risiko terhadap kerusakan atau kerugian yang ditimbulkan.

Ancaman gangguan bencana terhadap teknologi informasi di sektor keuangan dapat dikelompokkan ke dalam 3 (tiga) ancaman, yaitu ancaman bencana kebocoran data (*confidentiality*), ancaman bencana perubahan data (*integrity*), dan ancaman bencana terhentinya layanan teknologi informasi (*availability*).

b. Ancaman Bencana Kebocoran Data (*Confidentiality*)

Pada era digital ini kerahasiaan data menjadi semakin vital karena mudahnya suatu rahasia diketahui oleh pihak yang tidak berkepentingan. Berbagai data pribadi saat ini berada di berbagai tempat dan berbagai layanan/aplikasi. Kemudahan untuk mengetahui data tersebut telah timbul pada saat penyimpanan suatu data digital beserta pengirimannya kepada pihak lain. Risiko yang inheren dengan data digital yang dikirimkan atau disimpan adalah diaksesnya data tersebut oleh pihak yang tidak berkepentingan. Akses tersebut dapat dilakukan dengan mengakses media penyimpanannya atau mengintersepsi transmisi data digital tersebut pada saat dikirimkan. Pada saat data rahasia tersebut diakses oleh pihak lain, maka data tersebut telah dinyatakan bocor.

Kebocoran data memiliki dampak yang luas. Kerugian dapat dirasakan pada tingkat individu hingga kelembagaan. Pada tingkat individu, bocornya data individu tersebut akan menghasilkan berbagai perasaan antara lain rasa malu, rasa tidak aman, was-was dan sejenisnya. Bocornya data pribadi ini sendiri membuat pemilik dari data tersebut sangat rentan dari serangan-serangan siber (*Cyber Attack*) seperti, diserang dengan *malware*, *phising*, *scamming*, dan lainnya.

Untuk entitas bisnis seperti perusahaan, setidaknya ada beberapa kerugian yang disebabkan dari bocornya data, yaitu dampak finansial (seperti jatuhnya harga saham perusahaan, kerugian karena terhentinya layanan dan tambahan biaya untuk menanggulangi kebocoran data), dampak reputasi atau nama baik dari merek yang dimiliki perusahaan akan jatuh, turunnya kepercayaan konsumen dan gugatan hukum.

Di aspek ekonomi, saat ini banyak peretas baik perorangan maupun negara yang mengincar data-data penting dari suatu negara untuk meningkatkan keunggulan ekonominya. Sebagai contoh data nasabah Indonesia yang dicuri dapat digunakan untuk melakukan penawaran atau mengajak nasabah tersebut untuk memindahkan dananya ke luar negeri.

Di aspek ketahanan dan keamanan, data penting yang berkaitan dengan pertahanan dan keamanan negara juga harus dilindungi.

Sebagai contoh data detail mengenai kekuatan militer negara termasuk jumlah personil militer, jumlah alutsista, lokasi militer, di mana kapal perang dan patroli berada dsb dapat dimanfaatkan. Wilayah lautan dan udara Indonesia yang sangat luas dapat disusupi dan dieksplorasi oleh negara lain. Informasi mengenai titik-titik lemah perbatasan Indonesia dapat dimanfaatkan untuk kejahatan lintas negara seperti transaksi narkoba dan pengiriman pengungsi.

Di Indonesia, kebocoran data telah menimpa berbagai perusahaan dan instansi. Sekitar 91 Juta data pribadi milik pengguna Tokopedia dijual di *Dark Web*, yang berupa user ID email, tanggal lahir, jenis kelamin, dan nomor telepon. Meskipun kata sandi dari pengguna tidak sampai bocor, data pribadi tersebut sudah cukup untuk disalahgunakan oleh pihak yang tidak bertanggung jawab. Atas kejadian ini, Tokopedia digugat oleh Komunitas Konsumen Indonesia sebesar Rp. 100 Miliar atas dasar kegagalan Tokopedia selaku penyelenggara sistem elektronik dalam menyimpan serta melindungi kerahasiaan data pribadi dan hak privasi dari pengguna situs tersebut. Sedangkan Untuk Bukalapak sendiri kebocoran data terjadi pada tahun 2019. Pembobolan tersebut mengakibatkan setidaknya 13 juta data pengguna Bukalapak dijual di *Dark Web*.³²

Kebocoran data tersebut dapat menimbulkan berbagai dampak bagi masyarakat/pengguna seperti :

- Penyalahgunaan data (nama, alamat, tanggal lahir, NIK dll) untuk tindakan kriminal (*fraud*) seperti pemalsuan KTP, kartu kredit, pembelian barang atas nama pengguna sehingga menimbulkan kerugian finansial.
- Pencemaran nama baik pengguna jika terjadi penyebaran informasi yang tidak baik, misalnya kebiasaan belanja barang mewah/tertentu, hubungan dengan pihak lain yang tidak untuk konsumsi publik (pengiriman barang kepada pihak tertentu)

³² CNN Indonesia. 2020. "13 Juta Data Bocor Bukalapak Dijual di Forum Hacker". <https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker>. Diakses 1 Agustus 2020 pukul 08:00

- Hilangnya kepercayaan (*trust*) kepada baik kepada perusahaan tertentu maupun kepada semua layanan yang menggunakan teknologi informasi sehingga akan berdampak kepada ekonomi nasional.

Beberapa kebocoran data yang pernah terjadi disajikan dalam tabel berikut ini:

No.	Jenis data yang bocor	Jumlah Data	Data yang terdampak	Waktu Kejadian
1.	Data Pemilih Tetap Pemilu 2014	2,3 juta data penduduk	Nama, Alamat,, Tempat Tanggal Lahir, Nomor KK, NIK	Mei 2020
2.	Data Tokopedia	91 juta pengguna, 7 juta merchant	Nama akun, alamat surel, nomor telepon	Mei 2020
3.	Data Bukalapak	13 juta pengguna	Nama akun, alamat surel, tanggal lahir	Juni 2019
4.	Lion Air	30 juta data penumpang Malindo Air dan Thai Lion Air (Lion Air Group)	Paspor, alamat rumah, nomor telepon	September 2019
5.	Penyadapan telepon Presiden Susilo Bambang Yudhoyono dan Petinggi negara lainnya oleh Australia	-	Pemantauan aktivitas keseharian Presiden SBY melalui telepon genggam.	Selama 15 hari pada bulan Agustus 2009
6.	Zoom	530 ribu akun pengguna	Email, kata sandi, <i>link meeting</i> , <i>host key</i> , dan nama <i>host</i>	April 2020

7.	KreditPlus	890 ribu data nasabah KreditPlus	Nama, email, kata sandi, alamat rumah, nomor telepon, data pekerjaan dan perusahaan, dan data kartu keluarga	Juli 2020
8.	Data Pasien Suspek Covid-19 Indonesia	230 ribu data pasien yang sedang tes Covid-19	Nama, alamat, nomor telepon, umur, kewarganegaraan.	Juni 2020

Tabel 3. Bencana Siber Dari Aspek Kebocoran Data

Sebagaimana yang dapat dilihat, bahwa terjadinya kebocoran data ini bukan merupakan suatu hal yang terjadi sekali atau dua kali saja. Dalam sejarahnya sudah banyak kasus mengenai kebocoran data yang bersifat rahasia. Salah satunya sendiri terdapat platform rapat daring, yaitu Zoom. Kasus ini sendiri menyebabkan kebocoran data yang berupa Email, kata sandi, *link meeting*, *host key*, dan nama *host*. 530.000 data pengguna Zoom ini dijual di *Dark Web* dengan harga US\$ 0,002 per akun

Selain itu contoh kasus kebocoran data yang dialami oleh Indonesia adalah disadapnya Ponsel milik Presiden Susilo Bambang Yudhoyono dan sejumlah petinggi negara lainnya. Penyadapan ini terjadi pada Agustus 2009 selama 15 hari, namun baru terungkap pada tahun 2013 berdasarkan dokumen yang dibocorkan ke publik oleh mantan kontraktor NSA, Edward Snowden. Penyadapan ini dilakukan oleh Australia untuk mendengarkan percakapan serta mengetahui pergerakan Presiden SBY dan beberapa menteri.³³

Selain pada sektor kenegaraan, kebocoran data di Indonesia juga terjadi pada sektor bisnis, seperti yang terjadi pada Lion Air Group dan yang baru-baru ini terjadi yaitu pada Perusahaan Fintech KreditPlus.

³³ Michael Perry. 18 November 2013. "Australian Spies Tried to Tap Indonesian President's Phone Calls. <https://www.reuters.com/article/us-usa-security-australia-indonesia/australian-spies-tried-to-tap-indonesian-presidents-phone-calls-media-reports-idUSBRE9AH03R20131118>. Diakses 2 Agustus 2020, pukul 10:00

Kasus kebocoran 7,8 juta data pengguna grup Lion Air sendiri melibatkan beberapa negara ASEAN seperti Malaysia, Indonesia, Singapura, Vietnam, Myanmar, dan Kamboja.³⁴ Dari jumlah tersebut setidaknya 158 ribu data pengguna yang berasal dari Indonesia terancam.³⁵ Sedangkan untuk kasus kebocoran data perusahaan *fintech* KreditPlus, data yang bocor tersebut dijual di *Dark Web*. Data pengguna yang berjumlah 890 ribu dijual di *Dark Web* yang mana data tersebut mencakup nama pengguna, alamat surel, kata sandi, alamat rumah, nomor telepon, data pekerjaan dan perusahaan, serta data kartu keluarga.³⁶ Adanya beberapa kasus kebocoran data baik di dunia maupun di Indonesia menunjukkan bahwa masih adanya beberapa kekurangan dalam persiapan dalam menghadapi serangan-serangan siber seperti ini. Menjaga kerahasiaan data menjadi salah satu aspek kunci dalam menghadapi bencana-bencana digital yang mungkin terjadi.

c. Ancaman Bencana Perubahan Data (*Integrity*)

Ancaman bencana perubahan data adalah risiko hilangnya keutuhan data yang disebabkan karena perubahan atau modifikasi pada suatu informasi untuk berbagai tujuan, salah satunya adalah kejahatan. Sebagai suatu rangkaian kejahatan, risiko integrasi data dapat menjadi suatu kelanjutan dari risiko kerahasiaan. Pelaku kejahatan melakukan penelusuran lebih lanjut data yang bocor dengan tujuan untuk memodifikasi data induk dari data yang bocor tersebut.

No.	Peristiwa	Pihak terlibat	Akibat	Waktu kejadian
1)	Perubahan saldo nasabah Bank A	PT. Bank A Persero (Tbk) dan nasabah	Terjadi pendebetan/ pengkreditan dana nasabah secara massal tanpa sepengetahuan nasabah	20 Juli 2019

³⁴ Agus Tri Haryanto. 26 September 2019. Hasil :Investigasi: 7,8 Juta Data Penumpang Lion Air Group Bocor." <https://inet.detik.com/security/d-4723338/hasil-investigasi-78-juta-data-penumpang-lion-air-group-bocor>, Diakses 2 Agustus 2020, pukul 11:00.

³⁵ CNN Indonesia. 2019. "Kemenkominfo: 156 Ribu WNI Terimbas Kebocoran Data Lion Air." <https://www.cnnindonesia.com/teknologi/20190926200343-185-434426/kemenkominfo-156-ribu-wni-terimbas-kebocoran-data-lion-air>. Diakses 2 Agustus 2020, pukul 012:00.

³⁶ Oik Yusuf. 4 Agustus 2020. "Data Ratusan Ribuan Nasabah Kredit Plus Diduga Bocor dan Dijual di Internet." <https://tekno.kompas.com/read/2020/08/04/07150007/data-ratusan-ribu-nasabah-kredit-plus-diduga-bocor-dan-dijual-di-internet?page=all>. Diakses 2 Agustus, pukul 16:00.

2)	Penyalahgunaan sistem ATM Bank B	PT. B	Penarikan nasabah secara berulang-ulang namun tidak mengurangi saldo rekening nasabah sehingga Bank B rugi Rp51 miliar	Mei-Agustus 2019
----	----------------------------------	-------	--	------------------

Tabel 4. Bencana Siber Dari Aspek Keutuhan Data

Tabel di atas menggambarkan dua kejadian bencana dalam hal keutuhan. Kedua kasus berkaitan dengan saldo rekening nasabah dengan kerugian yang diderita oleh pihak berbeda, kasus pertama kerugian diderita nasabah sedangkan kasus kedua kerugian diderita oleh nasabah. Pada kasus Bank A, penyebab perubahan saldo nasabah adalah proses pemulihan data pada sistem cadangan yang terlewatkan. Akibatnya adalah, perubahan saldo pada nasabah karena tidak ada data pembanding sebagai koreksi mengenai data nasabah yang sebenarnya.³⁷

e. Ancaman Bencana Terhentinya Layanan (*Availability*)

Ancaman bencana terhentinya layanan Teknologi Informasi merupakan risiko akibat terganggu atau terhentinya ketersediaan layanan digital atau yang dikenal dengan istilah '*down*'. Dalam relevansinya terhadap bencana, ketersediaan data bagi sektor keuangan memiliki kerentanan tersendiri yang memiliki karakteristik berbeda dengan sektor keuangan yang bersifat konvensional. Semakin terintegrasinya sektor keuangan secara digital memang senantiasa memberikan kemudahan bagi bank dan nasabah dalam melakukan segala jenis transaksi keuangan. Di sisi lain, hal ini juga menimbulkan adanya risiko tersendiri ketika membicarakan masalah ketersediaan data atau layanan apabila dikaitkan dengan situasi kebencanaan.

Contoh bencana yang mempengaruhi teknologi informasi terkait ketersediaan data yang pernah terjadi adalah sebagai berikut:

No.	Bencana	Jenis bencana	Dampak bencana	Kejadian
-----	---------	---------------	----------------	----------

³⁷ Ariyani Yakti Widyastuti. 21 Juli 2019. "Sistem Bank Mandiri Sempat Error, Ahli IT Sayangkan Hal Ini". <https://bisnis.tempo.co/read/1226755/sistem-bank-mandiri-sempat-error-ahli-it-sayangkan-hal-ini/full>. Diakses 2 Agustus 2020, pukul 16:30

1	Gempa dan Tsunami di Palu	Alam	1.678 BTS yang tidak berfungsi dari total 4.193 BTS yang ada di Sulawesi Tengah atau setara 40,02 persen.	28 September 2018
2	Banjir di Jabotabek	Alam	2446 BTS tidak berfungsi dari 22,867 (10,7%)	Februari 2020
3	Serat Optik Putus di Palembang	Non-alam (Kegagalan Teknologi)	Jalur Internet Jawa-Sumatera-Kalimantan dan Luar Negeri terputus	29 Februari-1 Maret 2008
4	Tidak berfungsinya ATM Bank C	Non-alam (Kegagalan Teknologi)	5300 ATM dari 17.600 ATM tidak dapat diakses	4-5 Agustus 2019
5	Serangan DDoS Bank	Non-alam (Peretasan)	Serangan gagal, 273 virus dan 67.000 pesan spam membanjiri server Bank	20 Juni 2016

Tabel 5. Bencana Siber Dari Aspek Ketersediaan Data

Tabel di atas menggambarkan sebagian kecil bencana yang memiliki dampak pada ketersediaan data. Bencana-bencana tersebut dapat diakibatkan oleh faktor alam maupun non-alam, sehingga selalu terjadi pada saat kapan pun.

Dua bencana alam yang digambarkan di atas adalah tsunami dan gempa Palu 2018³⁸, dan banjir Jabodetabek 2018.³⁹ Kedua-duanya berdampak pada tidak berfungsinya BTS yang digunakan untuk memfasilitasi komunikasi nirkabel sehingga komunikasi nirkabel (termasuk internet) di wilayah tersebut terputus.

Bencana non-alam juga memiliki berpengaruh terhadap beroperasinya sistem informasi. Pada tabel di atas tiga bencana non-alam yang terjadi disebabkan dua oleh kegagalan teknologi dan peretasan. Kegagalan teknologi merupakan kegagalan yang diakibatkan sifat yang melekat pada suatu obyek, dalam kasus ini adalah mudahnya

³⁸ Agus Tri Haryanto. 29 September 2018. "Dampak Gempa Donggala Bikin 1.678 BTS Tak Berfungsi". <https://inet.detik.com/telecommunication/d-4234684/dampak-gempa-donggala-bikin-1678-bts-tak-berfungsi>. Diakses 2 Agustus 2020, pukul 19:30.

³⁹ Sulistia Endah. 8 Januari 2020. "99,8% BTS Sudah berfungsi Normal Usai Banjir Jabodetabek 2020". <https://telko.id/998-bts-sudah-berfungsi-normal-usai-banjir-jabodetabek-2020-267339>. Diakses 2 Agustus 2020, pukul 21:00.

kabel untuk terputus dalam transmisi kabel, dan terputusnya suplai listrik pada kasus ATM Bank C.⁴⁰

16. Kegiatan Peningkatan Kesiapan Teknologi Informasi di Sektor Keuangan Dalam Menghadapi Bencana

Pada pembahasan sebelumnya telah diuraikan mengapa teknologi informasi di sektor keuangan perlu disiapkan dalam menghadapi bencana dan bagaimana bencana dapat mengganggu teknologi informasi di sektor keuangan.

Selanjutnya akan dilakukan analisa mengenai kegiatan-kegiatan yang perlu dilakukan dalam meningkatkan kesiapan teknologi di sektor keuangan dalam menghadapi bencana.

a. Analisa SWOT Atas Kondisi Kesiapan Teknologi Informasi Serta Pokok-Pokok Masalah Yang Dihadapi

Upaya peningkatan kesiapan teknologi di sektor keuangan dalam menghadapi bencana dapat dirumuskan dengan terlebih dulu menjabarkan kondisi kesiapan teknologi informasi serta pokok-pokok masalah yang dihadapi. Analisa dilakukan dengan menggunakan kerangka SWOT (*Strengths, Weakness, Opportunities, Threats*). Analisa SWOT dilakukan dengan mengacu pada 3 aspek sebagaimana dikembangkan oleh Harold J. Leavitt, yaitu aspek Manusia (*People*), Proses (*Process*) dan Teknologi (*Technology*). Hasil analisa SWOT adalah sebagaimana tercantum dalam tabel 6.

⁴⁰ Maizal Walfajri. 6 Agustus 2019. "Aliran listrik PLN Padam, 5.300 ATM BCA Sempat Offline (H. K. Dewi, Ed.). <https://keuangan.kontan.co.id/news/aliran-listrik-pln-padam-5300-atm-bca-semat-offline>. Diakses 2 Agustus 2020, pukul 22:00.

Kekuatan (<i>Strengths</i>)		Kelemahan (<i>Weakness</i>)	
Aspek Manusia (<i>People</i>)			
S1.	Terdapat cukup banyak Perguruan Tinggi yang memiliki pendidikan bidang teknologi digital	W1.	Kurangnya kesadaran masyarakat akan risiko bencana dan untuk menggunakan teknologi digital dengan prinsip kehati-hatian
Aspek Proses (<i>Process</i>)			
S2	Telah terdapat lembaga yang menangani bencana (BNPB), infrastruktur teknologi (Kominfo), keamanan siber (BSSN) dan sektor keuangan (OJK)	W2	Belum banyak perusahaan dan instansi yang menerapkan manajemen kelangsungan usaha secara maksimal
Aspek Teknologi (<i>Technology</i>)			
S3	Indutri teknologi digital di Indonesia semakin berkembang	W3	Sistem keamanan teknologi, deteksi dini, kewaspadaan bencana, cadangan belum memadai
Kesempatan (<i>Opportunity</i>)		Ancaman (<i>Threats</i>)	
Aspek Manusia (<i>People</i>)			
O1	Berkembangnya bisnis digital yang menarik masyarakat untuk belajar dan bekerja di bidang digital	T1	Adanya gap kompetensi SDM Asing dengan SDM Dalam Negeri baik dalam penggunaan maupun pengelolaan
Aspek Proses (<i>Process</i>)			
O2	Terjalannya koordinasi dan kolaborasi antar pemangku kepentingan (pemerintah, pendidikan, bisnis)	T2	Pengenaan denda akibat Indonesia tidak comply dengan standar internasional
Aspek Teknologi (<i>Technology</i>)			
O3	Minat investasi DN dan LN di industri digital besar	T3	Semakin meningkatnya frekuensi dan <i>magnitude</i> bencana baik bencana alam maupun non-alam

Tabel 6. Analisa SWOT Terhadap Kesiapan Menghadapi Bencana

1) Kekuatan (*Strengths*) dalam Menghadapi Bencana

Adapun beberapa faktor yang menjadi kekuatan yang telah dimiliki Indonesia dalam menghadapi bencana terkait teknologi antara lain :

a) Terdapat cukup banyak Perguruan-perguruan Tinggi yang memiliki pendidikan bidang teknologi digital (S1, Strength Nomor 1).

Saat ini telah terdapat cukup banyak perguruan tinggi baik negeri maupun swasta yang memiliki jurusan dan lulusan perguruan tinggi dalam bidang keilmuan yang terkait dengan teknologi informasi. Berbagai universitas baik negeri maupun swasta memiliki fakultas, jurusan maupun bidang studi terkait teknologi digital dengan nama yang beragam seperti ilmu komputer, teknik komputer, teknik informatika, sistem informasi, sistem digital, dan sebagainya.

b) Telah terdapat lembaga yang menangani bencana (BNPB), infrastruktur teknologi (Kominfo), keamanan siber (BSSN) dan sektor keuangan (OJK) (S2).

Dalam hal kelembagaan, Indonesia sendiri sudah memiliki beberapa lembaga yang mana mampu untuk melakukan proses mitigasi bencana, baik itu bencana alam maupun non alam yang berupa bencana digital. Masing-masing lembaga memiliki fungsi tersendiri, seperti BNPB yang berfungsi untuk merumuskan kebijakan yang berfokus pada penanganan bencana dan melakukan penanganan bencana secara efisien.⁴¹ Kemenkominfo sendiri berfungsi untuk membentuk suatu kerangka hukum nasional mengenai mitigasi bencana digital secara luas. BSSN bertugas melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber.⁴² Sedangkan untuk OJK sendiri berfungsi untuk mengawasi dan memastikan bahwa sektor keuangan digital ini memiliki sarana dan prasarana yang cukup untuk memitigasi risiko seperti bencana IT yang mungkin terjadi pada sektor keuangan digital.

c) Industri teknologi digital di Indonesia semakin berkembang (S3)

Perkembangan teknologi digital yang disertai dengan tersedianya perangkat untuk mengaksesnya menjadikan industri teknologi digital di dunia semakin berkembang. Arah perkembangan industri teknologi digital akan menyesuaikan pada kebutuhan masyarakat, berdasarkan *World Economic Forum (Future of Jobs Survey 2018)*, empat tren teknologi yang akan mendominasi industri pada tahun 2018-2020

⁴¹ Ariansyah, A. 2017. "Tugas dan Fungsi BNPB." Diunduh 30 August 2020 dari <https://bnpb.go.id/tugas-dan-fungsi-bnpb>

⁴² Indonesia, Peraturan Presiden tentang Badan Siber dan Sandi Negara, Perpres No. 53 Tahun 2017, Ps. 2

adalah *high-speed internet mobile internet, artificial intelligence, big data analytics,, Internet of Things, machine learning* dan *cloud technology* serta *cloud computing*. Industri-industri lainnya pun akan dipengaruhi oleh perkembangan teknologi digital tersebut sehingga merubah perkembangan bisnis masing-masing industri. Secara global, penggunaan *big data analytics* sendiri meningkat penggunaannya sebesar 92% pada perusahaan global.⁴³

Perkembangan global tersebut sangat berarti pula pada perkembangan Indonesia. Survei dari 4.537 usaha di sektor industri pengolahan, perdagangan, penyediaan akomodasi, penyediaan makan dan minum, dan informasi di Indonesia menyatakan bahwa 24,64% perusahaan tersebut telah melaksanakan transformasi digital. Teknologi yang digunakan dalam transformasi digital tersebut adalah *cloud computing* dan *big data analytics* dengan porsi penggunaan masing-masing sebesar 7,91% dan 9,01% dari total industri tersebut.⁴⁴

2) Kelemahan (Weakness) dalam Menghadapi Bencana

Adapun beberapa faktor yang menjadi kelemahan yang dimiliki Indonesia dalam menghadapi bencana terkait teknologi antara lain :

- a) **Kurangnya kesadaran masyarakat akan risiko bencana dan untuk menggunakan teknologi digital dengan prinsip kehati-hatian (W1, Weakness nomor 1)**

Masih banyak masyarakat yang belum peduli terhadap risiko bencana. Maraknya penggunaan layanan digital belum diimbangi dengan sikap kehati-hatian. Hal ini dapat dilihat dari

⁴³ Kementerian Komunikasi dan Informatika. 2019. "Perkembangan Ekonomi Digital Indonesia" (hlm. 9). Jakarta: Pusat Penelitian dan Pengembangan Aplikasi Informatika dan Informasi dan Komunikasi Publik Badan Penelitian dan Pengembangan SDM Kementerian Komunikasi dan Informatika.

⁴⁴ Badan Pusat Statistik. 2018. "Penggunaan dan Pemanfaatan Teknologi Informasi dan Komunikasi (P2TIK) Sektor Bisnis 2018". hlm. 75. Jakarta: Badan Pusat Statistik.

banyaknya kejadian bencana yang diakibatkan oleh kurangnya kesadaran tersebut, seperti tidak menjaga data pribadi dan tidak menggunakan password yang kuat. Hal ini dapat dilihat berdasarkan data yang dimiliki oleh CISSReC, bahwa tingkat kesadaran pentingnya privasi itu sendiri sudah cukup tinggi namun tidak seimbang dengan tingkat kesadaran untuk menjaga privasi di layanan online. Dalam kasus, seperti pada tahun 2017 terdapat kasus Ransomware Wannacry, bahwa hanya sekitar 33% dari responden yang mengikuti anjuran Kemenkominfo untuk mengatur PC dan Laptop untuk mencegah serangan Ransomware Wannacry ini.⁴⁵ Hal ini menunjukkan masyarakat kita dalam hal tingkat kesadaran masih belum cukup untuk melindungi data yang dimiliki dan meminimalisir risiko bencana seperti apa yang terjadi pada kasus Ransomware Wannacry.

b) Belum banyak perusahaan dan instansi yang menerapkan manajemen kelangsungan usaha secara maksimal (W2).

Meskipun telah terdapat standar dan regulasi terkait manajemen kelangsungan usaha, saat ini masih belum banyak perusahaan dan instansi yang menerapkannya secara maksimal. Hal ini disebabkan antara karena kurangnya monitoring, penerapan sanksi yang tidak tegas, kurangnya SDM yang kompeten dan keterbatasan dana. Ketika dalam situasi yang tidak terduga seperti Pandemi Covid-19 ini, perusahaan harus mampu untuk melakukan manajemen kelangsungan usaha yang mampu beradaptasi dengan kondisi pandemi ini. Salah satu contohnya adalah telah memiliki standardisasi ISO: 22301, yang dimana standardisasi ISO ini bertujuan untuk memastikan pelaku usaha untuk mengatur perusahaannya dalam rangka melindungi, bersiap

⁴⁵ Communication and Information System Security Research Center. 2017. "Tingkat Kesadaran Masyarakat Tentang Keamanan Informasi". Jakarta: CISSReC.

siaga, menangani, dan memulihkan diri dari kondisi pandemi ini.⁴⁶

c) Sistem keamanan teknologi, deteksi dini, kewaspadaan bencana, cadangan belum memadai (W3)

Sistem keamanan teknologi di Indonesia belum memadai pada sektor pemerintah dan swasta. Berdasarkan pemeringkatan Indeks KAMI 3.1, yang salah satu penilaiannya adalah keamanan pada aspek ketersediaan, integritas dan kerahasiaan data, yang dilakukan pada tahun 2017 menunjukkan bahwa hasil rata-rata pada pemeringkatan yang dilakukan pada 9 Kementerian/Lembaga Pusat, 29 Pemerintah Daerah dan 9 BUMN/Instansi berada pada kisaran angka 60 dari 645.⁴⁷ Hal ini menunjukkan bahwa kesiapan keamanan teknologi di Indonesia berada pada keadaan yang tidak layak sehingga menunjukkan kerentanan Indonesia pada serangan dan bencana Teknologi Informasi.

Sistem deteksi dini bencana di Indonesia memiliki kuantitas yang bervariasi sesuai dengan jenis bencana yang dihadapi sehingga mitigasi berbagai bencana menjadi berbeda-beda. Walaupun berbeda-beda secara kuantitas, berdasarkan kualitas setiap sistem deteksi bencana tersebut memiliki suatu kesamaan kelemahan yaitu belum diterapkannya standarisasi dari sistem deteksi dini bencana tersebut. Proses standarisasi ini baru dilaksanakan pada tahun 2020.⁴⁸

⁴⁶ Badan Standardisasi Nasional. 2020. "Standar Sistem Manajemen Kelangsungan Usaha dalam Menghadapi Covid-19". Diunduh 30 Agustus 2020 dari <https://www.bsn.go.id/main/berita/detail/11102/standar-sistem-manajemen-kelangsungan-usaha-dalam-menghadapi-covid-19>

⁴⁷ Kementerian Komunikasi dan Informatika RI. 2018. "Pemeringkatan Indeks KAMI". Diunduh 29 Agustus 2020 dari <https://aptika.kominfo.go.id/2018/09/indeks-kami/>

⁴⁸ "Standardisasi Peringatan Dini, Tekan Dampak di Zona Bencana". <https://indonesia.go.id/narasi/indonesia-dalam-angka/ekonomi/standardisasi-peringatan-dini-tekan-dampak-di-zona-bencana>. Diakses 21 Agustus 2020, pukul 08:00

3) Peluang (Opportunity) dalam Menghadapi Bencana

Adapun beberapa faktor yang menjadi peluang untuk meningkatkan kesiapan Indonesia dalam menghadapi bencana terkait teknologi antara lain :

a) Berkembangnya bisnis digital yang menarik masyarakat untuk belajar dan bekerja di bidang digital ((O1, Opportunity nomor 1).

Perkembangan bisnis digital di Indonesia sendiri terhitung cukup pesat. Berdasarkan data yang dimiliki oleh Ernst and Young, bahwa setidaknya bisnis digital di Indonesia mengalami pertumbuhan sekitar 40% setiap tahunnya.⁴⁹ Hal ini juga didukung dengan tingkat pengguna internet Indonesia yang cukup tinggi. Pesatnya perkembangan kedua hal ini sangat mendukung untuk menarik masyarakat untuk belajar dan bekerja di bidang digital.

b) Terjalinnnya koordinasi dan kolaborasi antar pemangku kepentingan yaitu pemerintah, pendidikan dan bisnis (O2).

Adanya koordinasi serta kolaborasi antar pemangku kepentingan ini, menjadikan sebuah kesempatan dalam melakukan mitigasi bencana IT. Masing-masing pemangku kepentingan memiliki perannya masing-masing. Untuk memaksimalkan peran tersebut, maka perlu adanya kerjasama antar pemangku kepentingan untuk menciptakan suatu upaya mitigasi dan penanggulangan bencana IT yang mungkin terjadi.

c) Minat investasi DN dan LN di industri digital besar (O3).

Tren peringkat *Ease of Doing Business* Indonesia mengalami peningkatan peringkat hingga pada peringkat 73

⁴⁹ "Indonesia Akan Jadi Pemain Ekonomi Digital Terbesar di Asia Tenggara." https://kominform.go.id/index.php/content/detail/6441/Indonesia+Akan+Jadi+Pemain+Ekonomi+Digital+Terbesar+di+Asia+Tenggara/0/berita_satker. Diakses 21 Agustus 2020, pukul 08:30

di tahun 2019.⁵⁰ Hal ini berujung pada masuknya nilai investasi sebesar 949,8 juta dolar AS di Semester I 2019. Investasi tersebut digolongkan pada investasi di kelompok transportasi, pergudangan dan telekomunikasi.⁵¹ Peluang ini dapat digunakan untuk menjalin kerjasama antara perusahaan PMA dengan perusahaan PMDN sehingga industri teknologi informasi dalam negeri dapat berkembang.

4) Ancaman (Threats) dalam Menghadapi Bencana

Adapun beberapa faktor yang menjadi ancaman dalam menghadapi bencana terkait teknologi antara lain :

a) Adanya gap kompetensi SDM Asing dengan SDM Dalam Negeri baik dalam penggunaan maupun pengelolaan (T1, Threat nomor 1)

Adanya gap kompetensi SDM ini merupakan bentuk dari kalah bersaingnya SDM Indonesia dengan SDM lainnya. hal ini dapat dilihat dari peringkat Human Capital Index Indonesia yang berada pada peringkat 87 dari 157 negara, yang berada pada angka 0,53. Angka ini berbeda jauh dengan negara Thailand, Malaysia, Singapura, dan Vietnam yang secara berturut-turut berada pada angka 0,60; 0,67; 0,88, dan; 0,67.⁵² Adanya ketimpangan ini menunjukkan bahwa pembangunan SDM Indonesia sendiri masih belum optimal, sehingga menciptakan suatu keadaan gap kompetensi SDM Indonesia dengan SDM luar negeri.

b) Pengenaan sanksi akibat Indonesia tidak comply dengan standar internasional (T2).

⁵⁰ Ease of Doing Business in Indonesia. Retrieved 29 August 2020, from <https://tradingeconomics.com/indonesia/ease-of-doing-business>. Diakses 21 Agustus 2020, pukul 09:00

⁵¹ Justiar, M. 2019. "Investor Asing Minati Investasi Ekonomi Digital" <https://kompas.id/baca/ekonomi/2019/10/17/investor-asing-minati-investasi-ekonomi-digital/?t=DtfUIJZugao1XY7w2SZ94Y4oVYZ6SbdElbHN2yEiM8iG9oi6BSEh5H3toRTT2>. Diakses 21 Agustus 2020, pukul 09:30

⁵² Victoria, A. 2019. "Bappenas: Kualitas SDM Indonesia Masih Ketinggalan Jauh dari Vietnam." <https://katadata.co.id/agustiyanti/finansial/5e9a50395709c/bappenas-kualitas-sdm-indonesia-masih-ketinggalan-jauh-dari-vietnam>. Diakses 21 Agustus 2020, pukul 10:00

Beberapa peraturan internasional mensyaratkan pengelolaan keamanan dunia maya yang ketat. Sebagai contoh *General Data Protection Regulation* (GDPR) yang ditetapkan masyarakat ekonomi Eropa mengharuskan pengelolaan data pribadi dengan aturan dan prosedur yang ketat. Perusahaan di seluruh dunia yang dinilai lalai dalam melindungi data pribadi konsumen yang berasal dari Eropa akan dikenakan denda yang cukup besar yaitu maksimal 20 juta Euro atau 4% penghasilan per tahunnya. Contoh pengenaan sanksi adalah denda kepada British Airways pada tahun 2018 sebesar 183 juta Euro karena kurangnya pengamanan dunia maya sehingga data pelanggannya bocor.

c) Semakin meningkatnya frekuensi bencana dan dengan skala bencana yang berbeda-beda baik bencana alam maupun non-alam (T3).

Tren bencana alam di Indonesia berfluktuatif pada rentang tahun 2011-2015, akan tetapi, tren tersebut selalu mengalami peningkatan pada 2016 hingga pada 2019 yang mencetak 9.382 kejadian bencana.⁵³ Data BNPB di tahun 2017-2019 menunjukkan bahwa pada tahun berturut-turut terdapat 3.182.136; 1.365.956 dan 5.366.489 jiwa terdampak bencana. Hal ini menunjukkan bahwa Indonesia mengalami frekuensi bencana yang semakin meningkat dengan jiwa terdampak bencana yang fluktuatif. Apabila mitigasi bencana tidak dilakukan dengan baik, maka tren jiwa terdampak bencana akan selalu meningkat pada tahun ke tahun.

Berdasarkan pembahasan di atas, dapat kita analisa kesiapan Teknologi Informasi dalam menghadapi bencana dengan memperhatikan hal-hal sebagai berikut :

⁵³ Badan Nasional Penanggulangan Bencana. 2020. "Data Informasi Bencana Indonesia (DIBI)". Jakarta:BNPB

- Frekuensi kejadian bencana, baik bencana alam, bencana non-alam termasuk kegagalan teknologi, masih tinggi dan semakin meningkat.
- Masih terdapat cukup banyak kelemahan (*weakness*) dan ancaman (*threats*) dalam kesiapan menghadapi bencana, baik di aspek manusia, proses maupun teknologi sebagaimana hasil analisa SWOT di atas.
- Laporan *Global Cybersecurity Index (GCI)* pada tahun 2018 menempatkan Indonesia di peringkat 41 dari 175 negara di dunia dan peringkat 9 di Asia Pasifik di bawah Singapura, Malaysia dan Thailand. Posisi ini meningkat dari tahun sebelumnya, namun masih menunjukkan kelemahan keamanan siber kita di beberapa aspek.
- Berdasarkan *World Risk Report 2018* yang dikeluarkan oleh ReliefWeb, Indonesia dinilai tidak mampu meminimalkan dampak negatif dari bencana.⁵⁴

Dengan demikian dapat diambil kesimpulan bahwa Teknologi Informasi belum memiliki kesiapan yang memadai dalam menghadapi bencana dengan pokok-pokok permasalahan sebagaimana diuraikan di atas,

b. Analisa TOWS Untuk Merumuskan Peningkatan Kesiapan Teknologi Informasi di Sektor Keuangan Dalam Menghadapi Bencana

Selanjutnya, perlu dilakukan analisa untuk menyusun berbagai kegiatan peningkatan kesiapan Teknologi Informasi di Sektor Keuangan dalam menghadapi bencana.

Dengan menggunakan hasil analisa SWOT yang dilakukan sebelumnya, selanjutnya dilakukan analisa TOWS (*Threats Opportunities Weakness Strength*) untuk menyusun kegiatan-kegiatan untuk meningkatkan kesiapan teknologi informasi di sektor keuangan

⁵⁴ Mucke, P., et. al. 2018. "World Risk Report 2018". Jerman: Naldo Gruden.

dalam menghadapi bencana. Hasil analisa tersebut adalah sebagaimana tercantum di dalam tabel 7.

TOWS MATRIX	Kekuatan (<i>Strength</i>)		Kelemahan (<i>Weakness</i>)	
Kesempatan (<i>Opportunities</i>)	<i>S-O STRATEGY</i>		<i>W-O STRATEGY</i>	
	SO 1..	(<i>People</i>) Membangun SDM kompeten teknologi melalui pendidikan yang <i>link-match</i> dengan bisnis	WO1.	(<i>People</i>) Meningkatkan kesadaran masyarakat terhadap bencana dan keamanan dunia digital
		S1: Terdapat cukup banyak Perguruan2 Tinggi yang memiliki pendidikan bidang teknologi digital		W1 Kurangnya kesadaran masyarakat akan risiko bencana dan untuk menggunakan teknologi digital dengan prinsip kehati-hatian
		O1: Berkembangnya bisnis digital yang menarik masyarakat untuk belajar dan bekerja di bidang digital		O2 : Berkembangnya bisnis digital yang menarik masyarakat untuk menggunakan, belajar dan bekerja di bidang digital
	SO 2.	(<i>Process</i>) Optimalisasi fungsi lembaga negara yang menangani bencana, teknologi informasi dan industri keuangan.	WO2.	(<i>Process</i>) Menerapkan standar dan <i>best practice</i> internasional seperti SMKI
		S2: Telah terdapat lembaga yang menangani bencana (BNPB), infrastruktur teknologi (Kominfo), keamanan siber (BSSN) dan sektor keuangan (OJK)		W2 Belum banyak perusahaan dan instansi yang menerapkan manajemen kelangsungan usaha secara maksimal
		O2: Terjalannya koordinasi dan kolaborasi antar pemangku kepentingan (pemerintah, pendidikan, bisnis)		O2 Terjalannya koordinasi dan kolaborasi antar pemangku kepentingan (pemerintah, pendidikan, bisnis)
	SO3 .	(<i>Technology</i>) Meningkatkan investasi di sektor TI baik dari dalam maupun luar negeri	WO3.	(<i>Technology</i>) Menggaet pihak swasta dalam negeri untuk bekerjasama dalam pengembangan sistem informasi deteksi dini (<i>early warning</i>), komunikasi dan pemetaan potensi bencana
		S3: Industri teknologi digital di Indonesia semakin berkembang		W3: Sistem keamanan teknologi, deteksi dini, kewaspadaan bencana, cadangan belum memadai
		O3: Minat investasi DN dan LN di industri digital besar		O3: Minat investasi DN dan LN di industri digital besar
Ancaman (<i>Threats</i>)	<i>S-T STRATEGY</i>		<i>W-T STRATEGY</i>	
	ST 1	(<i>People</i>) Pendidikan SDM agar dapat bersaing secara internasional	WT1	Meningkatkan kesadaran masyarakat agar dapat menggunakan teknologi digital dengan waspada
		S1: Terdapat cukup banyak Perguruan2 Tinggi yang memiliki pendidikan bidang teknologi digital		W1 Kurangnya kesadaran masyarakat akan risiko bencana dan untuk menggunakan teknologi digital dengan prinsip kehati-hatian
		T1. Adanya gap kompetensi SDM Asing dengan SDM Dalam Negeri baik dalam penggunaan maupun pengelolaan		T1. Adanya gap kompetensi SDM Asing dengan SDM Dalam Negeri baik dalam penggunaan maupun pengelolaan
	ST 2	Menyiapkan <i>strategy compliance</i> dengan ketentuan internasional.	WT2	Menerapkan standar <i>compliance</i> yang sesuai dengan ketentuan internasional
		S2: Telah terdapat lembaga yang menangani bencana (BNPB), infrastruktur teknologi (Kominfo), keamanan siber (BSSN) dan sektor keuangan (OJK)		W2 Belum banyak perusahaan dan instansi yang menerapkan manajemen kelangsungan usaha secara maksimal
		T2 Pengenaan sanksi akibat Indonesia tidak comply dengan standar internasional		T2 Pengenaan sanksi akibat Indonesia tidak comply dengan standar internasional
ST 3	Mengembangkan industri keamanan dunia maya (<i>cyber security</i>)	WT3	Mengembangkan aplikasi sistem yang canggih untuk menghadapi bencana	

	S3: Industri teknologi digital di Indonesia semakin berkembang	W3: Sistem keamanan teknologi, deteksi dini, kewaspadaan bencana, cadangan belum memadai
	T3. Semakin meningkatnya frekuensi dan <i>magnitude</i> bencana	T3. Semakin meningkatnya frekuensi dan <i>magnitude</i> bencana

Tabel 7. Analisa TOWS Untuk Merumuskan Kegiatan Peningkatan Kesiapan Teknologi Informasi Dalam Menghadapi Bencana

Berdasarkan analisa TOWS di atas, maka kegiatan peningkatan kesiapan teknologi informasi yang perlu dilakukan adalah sebagai berikut:

1) Kegiatan Peningkatan Kesiapan Teknologi Informasi di Aspek Manusia

a) Membangun SDM kompeten teknologi melalui pendidikan yang link-match dengan bisnis (SO1, *Strength-Opportunity* nomor 1).

Perguruan tinggi perlu didorong untuk lebih meningkatkan jumlah dan kualitas mahasiswa di bidang teknologi . Agar kurikulum dan kesiapan lulusannya sesuai dengan kebutuhan di pasar, maka program *link and match* dengan bisnis perlu didorong misalnya dengan program magang dan kerjasama terkait inovasi teknologi.

b) Meningkatkan kesadaran masyarakat terhadap bencana dan keamanan dunia maya (WO1, *Weakness-Opportunity* nomor 1).

Masyarakat pengguna digital perlu memiliki kesadaran terhadap risiko-risiko yang dihadapi dalam menggunakan teknologi digital. Mereka juga harus menerapkan langkah-langkah pengamanan seperti menjaga data rahasia, menggunakan *password* yang kuat, mengganti *password* secara berkala dan rutin, serta meng-*install* anti virus.

c) Pendidikan SDM agar dapat bersaing secara internasional (ST1, *Strength-Threats* nomor 1).

Pesatnya perkembangan teknologi diiringi pula meningkatnya risiko terjadinya bencana. Di era globalisasi ini,

tidak ada lagi batasan negara terkait teknologi digital. Serangan *hacker* yang menyebabkan bencana kegagalan teknologi dapat berasal dari hacker yang berada di negara manapun di seluruh dunia. Untuk itu SDM kita harus meningkatkan pengetahuannya di bidang teknologi digital agar tidak kalah dengan SDM di luar negeri.

d) Meningkatkan kesadaran masyarakat agar dapat menggunakan teknologi digital dengan waspada (WT1, *Weakness-Threat* nomor 1).

Banyaknya aplikasi maupun *hacker* dari luar negeri yang berusaha memanfaatkan dan menyerang masyarakat Indonesia. Untuk itu masyarakat perlu berhati-hati dalam menggunakan teknologi digital. Sebagai contoh seringnya kiriman e-mail yang berasal dari luar negeri berisi tautan (*link*) palsu dengan tujuan kriminal (*cyber crime*).

2) Kegiatan Peningkatan Kesiapan Teknologi Informasi di di Aspek Proses

a) Optimalisasi fungsi lembaga negara yang menangani bencana, teknologi informasi dan industri keuangan (SO2).

Keberadaan lembaga negara seperti BNPT, Kementerian Kominfo, BSSN dan OJK sangat penting untuk menyusun kebijakan dalam menghadapi bencana. Namun demikian sinergi antara lembaga-lembaga tersebut perlu ditingkatkan sehingga regulasi dan kebijakan nasional terkait kesiapan dalam menghadapi bencana lebih komprehensif dan integral. Berbagai ketentuan yang ada saat ini cenderung berdiri sendiri-sendiri seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) sebagaimana telah diubah terakhir dengan Undang-Undang Nomor 19 Tahun 2016, Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, Peraturan Otoritas Jasa Keuangan (POJK) Nomor

38/POJK.03/2016 tentang Penerapan Manajemen Risiko Penggunaan Teknologi Informasi Oleh Bank Umum dan Peraturan Otoritas Jasa Keuangan (POJK) Nomor 77/POJK.01/2016 tentang Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi.

b) Menerapkan standar dan best practice internasional Sistem Manajemen Kelangsungan Usaha (WO2).

Aspek kesiapan teknologi dan SDM perlu dilengkapi dengan prosedur pelaksanaan pengamanan dunia maya yang baik. Standar internasional Sistem Manajemen Kelangsungan Usaha (SMKU) sebagaimana tercantum dalam tinjauan pustaka perlu menjadi keharusan untuk diterapkan oleh semua penyelenggara layanan teknologi digital. Dengan penerapan ini, semua penyedia layanan digital akan menerapkan model PDCA (Plan - Do – Check - Act) yaitu merencanakan, mengimplementasikan, meninjau dan meningkatkan efektivitas dari kegiatan-kegiatan untuk menghadapi bencana.⁵⁵ Dengan demikian bencana dapat dimitigasi dan dihadapi dengan lebih siap oleh seluruh penyelenggara layanan digital di Indonesia.

c) Menyiapkan strategi *compliance* dengan ketentuan internasional (ST2).

Indonesia perlu menyusun strategi agar penyelenggara layanan digital dalam negeri dapat mematuhi ketentuan internasional terkait keamanan siber. Hal ini misalnya dapat dicapai dengan mendorong untuk dibuatnya peraturan yang relevan dalam masalah keamanan digital, khususnya pembuatan UU yang mengatur mengenai perlindungan data pribadi, di mana hal ini penting untuk memastikan bahwa keamanan data pada umumnya menjadi objek yang dilindungi dari berbagai ancaman terhadap keamanan dan integritas

⁵⁵ Leni Sagita Riantini Supriadi dan Low Sui Pheng. 2017. "Business Continuity Management in Construction, Management in the Built Environment". Singapura: Springer Ltd, hlm. 41

data misalnya karena kejadian bencana alam hingga kejadian peretasan sistem keamanan digital.

d) Menerapkan standar yang *compliance* dengan ketentuan internasional (WT2).

Saat ini belum banyak penyedia layanan digital di Indonesia yang menerapkan standar dan ketentuan internasional terkait bencana dan keamanan dunia maya. Untuk itu pemerintah perlu memastikan agar standar dan ketentuan tersebut diterapkan. Salah satu caranya adalah membentuk suatu peraturan perundang-undangan yang memaksa para penyedia layanan digital untuk menerapkan standar serta ketentuan internasional terkait bencana dan keamanan dunia maya. Selain itu, pemerintah juga harus memastikan bahwa segala rancangan mengenai standar keamanan yang telah *comply* dengan standar internasional tersebut benar-benar dijalankan, misalnya dengan memperkuat peranan yang lebih bagi institusi negara selaku *compliance regulator* dari peraturan tersebut.

3) Kegiatan Peningkatan Kesiapan Teknologi Informasi di Aspek Teknologi

a) Meningkatkan investasi di sektor TI baik dari dalam maupun luar negeri (SO3)

Semakin berkembangnya teknologi serta bisnis digital di dunia maupun di Indonesia, diiringi dengan besarnya minat investasi baik dari dalam maupun luar negeri merupakan kesempatan terbaik meningkatkan investasi di bidang TI baik secara kualitas dan kuantitas. Iklim investasi yang meningkat meningkatkan permintaan atas lingkungan sistem teknologi informasi yang kondusif agar kepercayaan investor meningkat.

Perkembangan teknologi menciptakan kondisi yang efisien untuk menciptakan perangkat-perangkat teknologi informasi dengan biaya serendah mungkin. Hal ini berujung

pada rendahnya biaya yang diperlukan untuk investasi di bidang keamanan TI sehingga tersedia teknologi di dalam negeri yang diperlukan untuk meningkatkan keamanan di dunia maya sehingga siap menghadapi bencana seperti sistem cadangan (*backup system*) dan layanan awan (*cloud*).

b) Menggaet pihak swasta dalam negeri untuk bekerjasama dalam pengembangan sistem informasi deteksi dini bencana (*early warning system*), komunikasi, pemetaan potensi bencana dan sistem cadangan (WO3).

Pengembangan industri dalam negeri memiliki dua keuntungan dalam penyiapan sistem mitigasi bencana. Keuntungan pertama adalah terciptanya kemandirian industri dalam negeri di bidang Teknologi Informasi. Keuntungan berikutnya adalah dengan terciptanya standardisasi atas peralatan mitigasi bencana. Standardisasi ini berujung pada kemudahan penggunaan oleh pengguna akhir sistem keamanan dan interkoneksi atas berbagai peranti yang digunakan sehingga terjalin suatu jaringan sistem mitigasi bencana yang dapat diandalkan. Pada sisi biaya, standardisasi sistem mitigasi bencana dapat mengefisiensikan perawatan dengan penggunaan komponen-komponen yang memiliki tingkat komonalitas (*commonality*) tinggi.

c) Mengembangkan industri keamanan dunia maya (*cyber security*) (ST3).

Semakin berkembangnya industri teknologi digital menjadi kekuatan yang perlu dioptimalkan untuk mengatasi tantangan berupa semakin meningkatnya frekuensi dan magnitudo bencana. Untuk itu industri teknologi yang mendukung keamanan dunia maya perlu didorong baik berupa teknologi perangkat keras (*firewall, intrusion prevention system*) maupun perangkat lunak (*software anti virus, anti malware*).

d) Mengembangkan sistem aplikasi yang canggih untuk menghadapi bencana (WT3).

Untuk meningkatkan sistem penanganan bencana, perlu dikembangkan aplikasi-aplikasi berbasis teknologi terkini seperti *big data*, *artificial technology* dan *internet of things*. Aplikasi tersebut diharapkan dapat membantu dalam mendeteksi potensi bencana serta meningkatkan pembelajaran berdasarkan pengalaman dalam menghadapi bencana-bencana sebelumnya.

Aplikasi yang dikembangkan tidak hanya memiliki teknologi yang canggih, melainkan juga bersifat modular. Artinya, dapat dilakukan modifikasi (*tweak*) terhadap aplikasi tersebut dengan mudah sehingga dapat menyesuaikan dengan perubahan ancaman bencana.

Kegiatan-kegiatan di atas berjumlah 12 kegiatan, terdiri dari 4 kegiatan di aspek manusia, 4 kegiatan di aspek proses dan 4 kegiatan di aspek teknologi. Dengan melaksanakan kegiatan di ke-3 aspek tersebut maka diharapkan dapat tercipta kondisi ideal di mana Teknologi Informasi di sektor keuangan memiliki kesiapan yang tinggi dalam menghadapi bencana. Kesiapan ini akan mendukung kestabilan ekonomi nasional sebagai bagian dari Ketahanan Ekonomi Indonesia



BAB IV

PENUTUP

17. Simpulan

Teknologi Informasi berkembang pesat mempengaruhi seluruh bidang kehidupan, termasuk di sektor keuangan. Ekonomi yang didukung oleh teknologi informasi menjadi tulang punggung bagi pertumbuhan ekonomi nasional.

Teknologi Informasi di sektor keuangan perlu disiapkan untuk menghadapi bencana. Hal ini disebabkan karena teknologi informasi memiliki peran yang sangat penting dan menjadi tumpuan untuk meningkatkan kesejahteraan masyarakat melalui peningkatan akses layanan keuangan. Dengan demikian bila terjadi gangguan pada teknologi informasi, maka akan berdampak besar pada kesejahteraan masyarakat dan perekonomian nasional. Peran Teknologi Informasi di sektor keuangan dapat dilihat dari beberapa data seperti besarnya nilai aset perbankan di Indonesia per akhir tahun 2019 sebesar Rp 9.237,158 triliun, total nilai aset di Industri Keuangan Non Bank sebesar Rp 2.557,78 triliun, total nilai kapitalisasi di pasar modal mencapai Rp7.299,283 triliun, akumulasi penyaluran pinjaman fintech peer-to-peer lending mencapai Rp 113,46 Triliun dan nilai transaksi e-commerce sebesar Rp 265,07 triliun.

Seiring dengan semakin tingginya ketergantungan pada teknologi informasi, maka semakin meningkat pula ancaman bencana berupa bencana kegagalan teknologi khususnya kejahatan di dunia maya (cyber crime). Contoh bencana dunia maya yang telah dialami di Indonesia antara lain kebocoran data pengguna e-commerce, penyadapan terhadap pemimpin negara, pembobolan kartu kredit/ kartu ATM/ rekening nasabah dan terhentinya layanan digital.

Untuk meningkatkan kesiapan teknologi informasi di sektor keuangan dalam menghadapi bencana maka perlu dilaksanakan kegiatan-kegiatan

peningkatan kesiapan teknologi informasi yang meliputi aspek manusia, proses dan teknologi.

Pada aspek manusia perlu dilakukan pembangunan SDM yang kompeten di bidang teknologi digital, peningkatan kesadaran masyarakat terhadap bencana dan keamanan dunia maya, peningkatan daya saing SDM di tingkat internasional serta peningkatan kesadaran masyarakat agar dapat menggunakan layanan digital dengan waspada.

Pada aspek proses diperlukan optimalisasi fungsi lembaga-lembaga negara yang menangani bencana teknologi informasi, penerapan best practice internasional Business Continuity Management, penyiapan strategi compliance dengan ketentuan internasional serta penenerapannya.

Pada aspek teknologi perlu dilakukan kegiatan peningkatan investasi di sektor teknologi informasi, pengembangan sistem informasi deteksi dini bencana (*early warning system*) dan sistem cadangan, pengembangan industri keamanan dunia maya (*cyber security*), serta pengembangan sistem aplikasi yang canggih untuk menghadapi bencana.

Dengan melaksanakan kegiatan-kegiatan di ketiga aspek tersebut maka diharapkan Teknologi Informasi di sektor keuangan memiliki kesiapan yang tinggi dalam menghadapi bencana. Kesiapan ini akan mendukung peningkatan kesejahteraan masyarakat dan kestabilan ekonomi sebagai bagian dari Ketahanan Ekonomi Nasional Indonesia.

18. Rekomendasi

Untuk menindaklanjuti usulan kegiatan sebagaimana dijabarkan di atas, maka sesuai konsep *Triple-Helix*, diperlukan koordinasi erat antara pihak pemerintah, akademisi dan dunia usaha.

- a. Pemerintah perlu melengkapi kebijakan terkait penggunaan teknologi informasi agar lebih komprehensif dan implementatif serta *comply* dengan ketentuan internasional, meningkatkan sosialisasi untuk meningkatkan kesadaran masyarakat dalam penggunaan teknologi, mendorong pengembangan industri digital dalam negeri dan menarik investasi dari luar negeri.

- b. Akademisi perlu meningkatkan kuantitas maupun kualitas lulusan pendidikan tinggi yang ahli di bidang teknologi seiring dengan perkembangan global. Hal ini dilakukan dengan mengevaluasi kurikulum pendidikan, menambah kapasitas mahasiswa dan bekerjasama dengan dunia usaha agar terjadi *link-and-match* dengan kebutuhan dunia usaha.
- c. Dunia usaha perlu mengimplementasikan standar internasional seperti sistem manajemen kelangsungan usaha untuk memastikan layanan digital yang diberikan aman dan handal. Kerjasama dengan dunia akademisi juga perlu ditingkatkan agar kekurangan SDM ahli teknologi dapat dipenuhi sesuai kebutuhan pasar.



DAFTAR PUSTAKA

BUKU REFERENSI

- Badan Nasional Penanggulangan Bencana. 2020. "Data Bencana di Indonesia". Jakarta: BNPB
- Lembaga Pertahanan Nasional. 2020. Bahan Ajar Bidang Studi Geostrategi Indonesia dan Ketahanan Nasional". Jakarta:Lemhannas.
- Otoritas Jasa Keuangan. 2019. "Laporan Triwulanan IV-2019". Jakarta:Otoritas Jasa Keuangan
- Otoritas Jasa Keuangan. 2020. "Perkembangan Fintech Landing April 2020". Jakarta:Otoritas Jasa Keuangan.
- Otoritas Jasa Keuangan. 2016. "Panduan Penyelenggaraan Digital Branch oleh Bank Umum". Jakarta:Otoritas Jasa Keuangan.
- Otoritas Jasa Keuangan.2017. "Pasar Modal: Seri Literasi Keuangan Perguruan Tinggi". Jakarta:Otoritas Jasa Keuangan, hlm 2.
- The International Organization for Standardization. 2019. "ISO 22301:2019, Security and resilience – Business continuity management systems – Requirements". Geneva: ISO

JURNAL

- Arner, Douglas W. and Barberis, Janos Nathan and Buckley, Ross P. 2015. "The Evolution of Fintech: A New Post-Crisis Paradigm?" University of Hong Kong Faculty of Law Research Paper No. 2015/047, UNSW Law Research Paper No. 2016-62, hlm 7-16
- Leavitt, H. J. .1965. "Applied change in Industry: Structural, Technological and Humanistic Approaches". Pennsylvania:Carnegie Institute of Technology

PERATURAN PERUNDANG-UNDANGAN

- Indonesia. Undang-Undang Penanggulangan Bencana. Undang-Undang Nomor 24 Tahun 2007. Lembaran Negara RI No. 66 Tahun 2007, Tambahan Lembaran Negara RI No. 4723.
- Indonesia. Undang-Undang Otoritas Jasa Keuangan. Undang Undang Nomor 21 Tahun 2011. Lembaran Negara RI No. 111 Tahun 2011, Tambahan Lembaran Negara RI No. 5253.
- Indonesia. Undang Undang Perubahan Atas Undang Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Undang Undang Nomor 19

Tahun 2016. Lembaran Negara RI No. 251 Tahun 2016, Tambahan Lembaran Negara RI No. 5952.

Indonesia, Peraturan Pemerintah tentang Perlindungan Sistem dan Transaksi Elektronik, PP No. 71 Tahun 2019.

Indonesia. Peraturan Pemerintah tentang Perdagangan Melalui Sistem Elektronik. PP Nomor 80 Tahun 2019.

Indonesia, Peraturan Presiden tentang Badan Siber dan Sandi Negara, Perpres No. 53 Tahun 2017, Ps. 2

PUBLIKASI RESMI

APJII. 2019. "Laporan Survei Penetrasi dan Profil Pengguna Internet Indonesia Tahun 2018". Jakarta: APJII

International Telecommunication Union. 2018."Global Cybersecurity Index 2018". Geneva:ITU

Kementerian Komunikasi dan Informatika. 2019. "Perkembangan Ekonomi Digital Indonesia" (hlm. 9). Jakarta: Pusat Penelitian dan Pengembangan Aplikasi Informatika dan Informasi dan Komunikasi Publik Badan Penelitian dan Pengembangan SDM Kementerian Komunikasi dan Informatika.

Badan Pusat Statistik. 2018. "Penggunaan dan Pemanfaatan Teknologi Informasi dan Komunikasi (P2TIK) Sektor Bisnis 2018". hlm. 75. Jakarta: Badan Pusat Statistik.

Badan Standardisasi Nasional. 2020. "Standar Sistem Manajemen Kelangsungan Usaha dalam Menghadapi Covid-19". Jakarta:BSN

Communication and Information System Security Research Center. 2017. "Tingkat Kesadaran Masyarakat Tentang Keamanan Informasi". Jakarta: CISSReC.

Kementerian Komunikasi dan Informatika RI. 2018. "Pemeringkatan Indeks KAMI". Diunduh 29 Agustus 2020 dari <https://aprika.kominfo.go.id/2018/09/indeks-kami/>

Mucke, P., et. al. 2018. "World Risk Report 2018". Jerman: Naldo Gruden.

Leni Sagita Riantini Supriadi dan Low Sui Pheng. 2017."Business Continuity Management in Construction, Management in the Built Environment". Singapura: Springer Ltd, hlm. 41

INTERNET

- Bidara Pink & Noverius Laoli. 11 February 2020. "BI Sebut Nilai Transaksi e-commerce Sepanjang 2019 Meningkat Drastis". <https://nasional.kontan.co.id/news/bi-sebut-nilai-transaksi-e-commerce-sepanjang-2019-meningkat-drastis?>. Diunduh 4 Juli 2020 pukul 10:00.
- Kaushik Das, *et al.* 2020. "The Digital Archipelago: How Online Commerce is Driving Indonesia's Economic Development". <https://www.mckinsey.com/featured-insights/asia-pacific/the-digital-archipelago-how-online-commerce-is-driving-indonesias-economic-development>. Diunduh 4 Juli 2020 pukul 11:00.
- Roy Franedy. 7 Mei 2020. "91 Juta Data Pengguna Bocor, Tokopedia Digugat Rp 100 M". <https://www.cnbcIndonesia.com/tech/20200507083340-37-156876/91-juta-data-pengguna-bocor-tokopedia-digugat-rp-100-m/>. Diakses 18 Juli 2020, pukul 09:00.
- CNBC Indonesia. 16 April 2020. "Kacau, 530.000 Data Akun Zoom Dijual Hacker di Dark Web". <https://www.cnbcindonesia.com/tech/20200416082700-37-152270/kacau-530000-data-akun-zoom-dijual-hacker-di-dark-web>. Diakses 18 Juli 2020, pukul 10:00
- CNN Indonesia. 20 Juni 2020. "230 Ribu Data Pasien Covid-19 di Indonesia Bocor dan Dijual". <https://www.cnnindonesia.com/teknologi/20200620083944-192-515418/230-ribu-data-pasien-covid-19-di-indonesia-bocor-dan-dijual>. Diakses 18 Juli 2020, pukul 10:30
- Müller, J. 2020. "Indonesia Smartphone Users". <https://www.statista.com/statistics/266729/smartphone-users-in-indonesia/>. Diakses 19 Juli 2020, pukul 08.00
- Otoritas Jasa Keuangan. (2017). "Kajian Perlindungan Konsumen Sektor Jasa Keuangan: Perlindungan Konsumen Pada Fintech." <https://konsumen.ojk.go.id/MinisiteDPLK/images/upload/201807131451262.%20Fintech.pdf>. Diakses 19 Juli 2020, pukul 12:00
- Boyke P. Siregar. 1 November 2019. "Telkom Serap 21,6% Belanja Modal Hingga Kuartal III ". <https://www.wartaekonomi.co.id/read254465/telkom-serap-216-belanja-modal-hingga-kuartal-iii>. Diakses 25 Juli 2020, pukul 12:30
- Anastasia Arvirianty. 2018. "Sistem Perdagangan Bursa Bisa Lakukan 7,5 Juta Transaksi." <https://www.cnbcindonesia.com/market/20180507164404-17-13982/sistem-perdagangan-bursa-bisa-lakukan-75-juta-transaksi>. Diakses 25 Juli 2020, pukul 14:00
- Pink, Bidara & Laoli, Noverius. 11 Februari 2020. "BI Sebut Nilai Transaksi e-commerce Sepanjang 2019 Meningkat Drastis". <https://nasional.kontan.co.id/news/bi-sebut-nilai-transaksi-e-commerce-sepanjang-2019-meningkat-drastis?page=all>. Diakses 25 Juli 2020, pukul 21:00

- CNN Indonesia. 2020. "13 Juta Data Bocor Bukalapak Dijual di Forum Hacker". <https://www.cnnindonesia.com/teknologi/20200506065657-185-500477/13-juta-data-bocor-bukalapak-dijual-di-forum-hacker>. Diakses 1 Agustus 2020 pukul 08:00
- Michael Perry. 18 November 2013. "Australian Spies Tried to Tap Indonesian President's Phone Calls". <https://www.reuters.com/article/us-usa-security-australia-indonesia/australian-spies-tried-to-tap-indonesian-presidents-phone-calls-media-reports-idUSBRE9AH03R20131118>. Diakses 2 Agustus 2020, pukul 10:00
- Agus Tri Haryanto. 26 September 2019. Hasil :Investigasi: 7,8 Juta Data Penumpang Lion Air Group Bocor." <https://inet.detik.com/security/d-4723338/hasil-investigasi-78-juta-data-penumpang-lion-air-group-bocor>, Diakses 2 Agustus 2020, pukul 11:00.
- CNN Indonesia. 2019. "Kemenkominfo: 156 Ribu WNI Terimbas Kebocoran Data Lion Air." <https://www.cnnindonesia.com/teknologi/20190926200343-185-434426/kemenkominfo-156-ribu-wni-terimbas-kebocoran-data-lion-air>. Diakses 2 Agustus 2020, pukul 12:00
- Oik Yusuf. 4 Agustus 2020. "Data Ratusan Ribu Nasabah Kredit Plus Diduga Bocor dan Dijual di Internet." <https://tekno.kompas.com/read/2020/08/04/07150007/data-ratusan-ribu-nasabah-kredit-plus-diduga-bocor-dan-dijual-di-internet?page=all>. Diakses 2 Agustus, pukul 16:00.
- Ariyani Yakti Widyastuti. 21 Juli 2019. "Sistem Bank Mandiri Sempat Error, Ahli IT Sayangkan Hal Ini". <https://bisnis.tempo.co/read/1226755/sistem-bank-mandiri-sempat-error-ahli-it-sayangkan-hal-ini/full>. Diakses 20 Agustus 2020, pukul 16:30
- Rohmat Haryadi. 29 November 2019. "Narik Duit Tapi Saldo Tetap, Bank DKI Kebobolan Rp51 Miliar". <https://www.gatra.com/detail/news/459462/ekonomi/narik-duit-tapi-saldo-tetap-bank-dki-kebobolan-rp51-miliar>, Diakses 2 Agustus 2020, pukul 19:00
- Agus Tri Haryanto. 29 September 2018. "Dampak Gempa Donggala Bikin 1.678 BTS Tak Berfungsi". <https://inet.detik.com/telecommunication/d-4234684/dampak-gempa-donggala-bikin-1678-bts-tak-berfungsi>. Diakses 2 Agustus 2020, pukul 19:30.
- Sulistia Endah. 8 Januari 2020. "99,8% BTS Sudah berfungsi Normal Usai Banjir Jabodetabek 2020". <https://telko.id/998-bts-sudah-berfungsi-normal-usai-banjir-jabodetabek-2020-267339>. Diakses 2 Agustus 2020, pukul 21:00.
- Maizal Walfajri. 6 Agustus 2019. "Aliran listrik PLN Padam, 5.300 ATM BCA Sempat Offline (H. K. Dewi, Ed.)". <https://keuangan.kontan.co.id/news/aliran-listrik-pln-padam-5300-atm-bca-sempat-offline>. Diakses 2 Agustus 2020, pukul 22:00.
- Ariansyah, A. 2017. "Tugas dan Fungsi BNPB." <https://bnpb.go.id/tugas-dan-fungsi-bnpb>. Diakses 20 Agustus 2020, pukul 15:00

“Standardisasi Peringatan Dini, Tekan Dampak di Zona Bencana”.

<https://indonesia.go.id/narasi/indonesia-dalam-angka/ekonomi/standardisasi-peringatan-dini-tekan-dampak-di-zona-bencana>. Diakses 21 Agustus 2020, pukul 08:00

“Indonesia Akan Jadi Pemain Ekonomi Digital Terbesar di Asia Tenggara.”

https://kominfo.go.id/index.php/content/detail/6441/Indonesia+Akan+Jadi+Pemain+Ekonomi+Digital+Terbesar+di+Asia+Tenggara/0/berita_satker. Diakses 21 Agustus 2020, pukul 08:30

“Ease of Doing Business in Indonesia”.

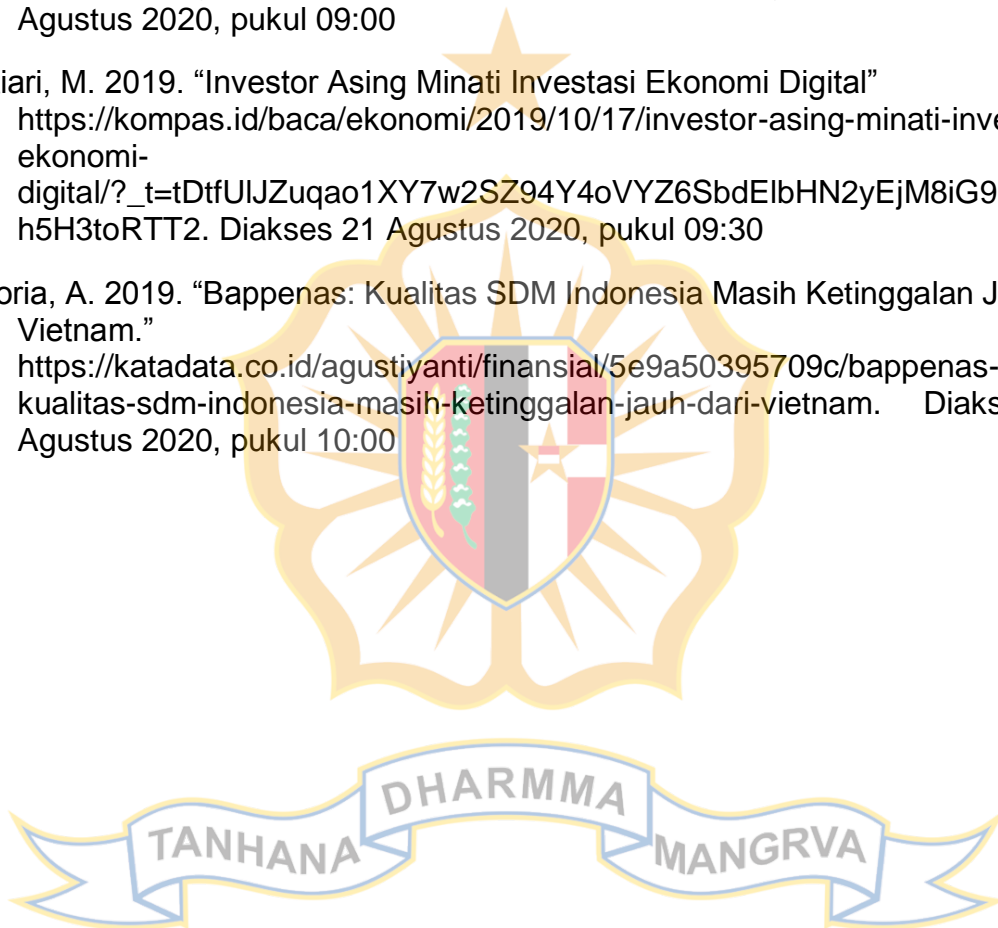
<https://tradingeconomics.com/indonesia/ease-of-doing-business>. Diakses 21 Agustus 2020, pukul 09:00

Justiari, M. 2019. “Investor Asing Minati Investasi Ekonomi Digital”

https://kompas.id/baca/ekonomi/2019/10/17/investor-asing-minati-investasi-ekonomi-digital/?_t=tDtfUIJZuqao1XY7w2SZ94Y4oVYZ6SbdElbHN2yEjM8iG9oi6BSEh5H3toRTT2. Diakses 21 Agustus 2020, pukul 09:30

Victoria, A. 2019. “Bappenas: Kualitas SDM Indonesia Masih Ketinggalan Jauh dari Vietnam.”

<https://katadata.co.id/agustiyanti/finansial/5e9a50395709c/bappenas-kualitas-sdm-indonesia-masih-ketinggalan-jauh-dari-vietnam>. Diakses 21 Agustus 2020, pukul 10:00



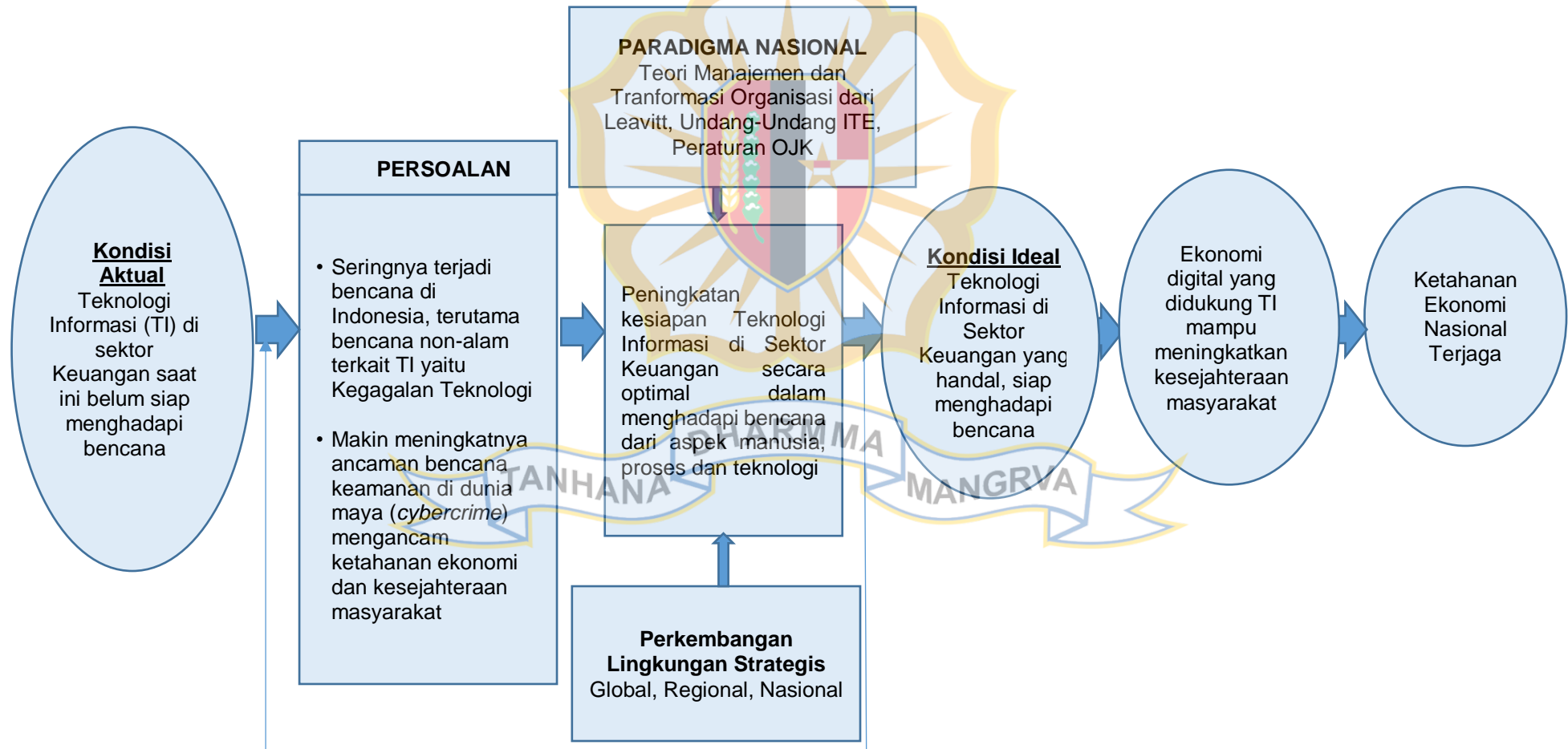
DAFTAR LAMPIRAN

1. ALUR PIKIR.....67
2. DAFTAR RIWAYAT HIDUP68



ALUR PIKIR

Peningkatan Kesiapan Teknologi Informasi di Sektor Keuangan Dalam Menghadapi Bencana Dalam Rangka Menjaga Ketahanan Ekonomi Nasional



RIWAYAT HIDUP

Nama : Ir. Dwi Kurniawan, MBA
 Lahir : Salatiga, 18 Juli 1967
 Jabatan : Kepala Grup Pengembangan Sistem Informasi
 Otoritas Jasa Keuangan
 Eselon : 1
 Alamat : Jl. Kristal G 11/A, Jakarta Selatan 12210

Pendidikan

S2 : Manajemen of Business Administration (MBA) di George Washington University, Washington DC, USA

S1 : Teknik Komputer ITS (Institut Teknologi Sepuluh November), Surabaya

Riwayat Kerja

Otoritas Jasa Keuangan :
 2020 – Sekarang : Kepala Grup Pengembangan Sistem Informasi
 2014 – 2019 : Direktur Strategi Sistem Informasi

Bank Indonesia :
 1994-2012 : Staf s.d. Deputi Direktur Sistem Informasi

PT Telekomunikasi Indonesia (PT Telkom) :
 1992-1993 : Staf di Departemen Sumber Daya Manusia

PT IBM Indonesia :
 1991-1992 : *System Engineer*

Sertifikasi, Pelatihan

1. *Certified Information System Auditor (CISA)* dari ISACA sejak 22 September 2005
2. *Certified Information Security Manager (CISM)* dari ISACA sejak 1 Mei 2008
3. *Cyber Capability Engagement Program* (Kerjasama Pemerintah Indonesia dengan Pemerintah Australia), 9 s.d. 21 September 2018 di Canberra, Australia
4. *IT Security Manager Academy*, London, Inggris, 22-29 September 2014
5. *Oceania CACS Conference*, Adelaide, Australia, 22-29 September 2013

6. *Project Management*, Manila (2008)
7. *IT Audit School*, Singapore (2004)

Penghargaan

1. Juara 1 - *The Best Helpdesk in Asia Pacific*, Contact Center World Award Tingkat Asia Pasifik, 15-19 Juli 2019, di Phuket, Thailand
2. Juara 2 - *The Best Contact Center Support IT Professional in the World*, Contact Center World Award Tingkat Dunia, 2-6 Desember 2020 di Barcelona, Spanyol

Pembicara / Dosen Tamu

1. Pembicara pada Seminar “Kepemimpinan Transformatif di Era Industri 4.0”, Program S2 PPM Manajemen, Jakarta 14 September 2019
2. Pembicara pada “Seminar Business & Economics National Conference – Blockchain dan Prospek Bisnis Masa Depan”, Universitas Atma Jaya, Jakarta, 27 Agustus 2019
3. Pembicara pada Kongres Teknologi Nasional, BPPT, Jakarta, 17-19 Juli 2017
4. Dosen Tamu di Program S2 Manajemen Teknologi Informasi Universitas Indonesia untuk mata kuliah IT Governance dan IT Risk Management, Jakarta Tahun 2015, 2016, 2019
5. Pembicara pada Forum Pertemuan Tahunan Direktur TI Bank Sentral se-Asia Pasifik (*Executives’ Meeting of East Asia-Pacific Central Banks*) di Malaysia, Hong Kong, China, Australia, dan Korea tahun 2005-2012

Lainnya :

1. Pengarang Buku “Implementasi IT Governance di Bank Indonesia”, bersama W. Hari Purnomo, November 2008
2. Tim Satuan Tugas Rekapitalisasi Perbankan, Bank Indonesia, Tahun 1999-2000
3. Tim Penyusun UU ITE - Informasi dan Transaksi Elektronik (Tahun 2006-2007)
4. Tim Penyusun SNI (Standar Nasional Indonesia) tentang Sistem Manajemen Keamanan Informasi / ISO 27001 (Tahun 2008-2009).