RISIKO OPERASI

Institusi kewangan kekal berdaya tahan dari segi operasi meskipun menghadapi cabaran

Institusi kewangan kekal berdaya tahan dari segi operasi tanpa sebarang gangguan yang besar di seluruh sistem pada separuh kedua tahun 2022. Kerugian risiko operasi kekal kecil berbanding dengan modal dan keuntungan sektor perbankan (masing-masing 0.04% dan 0.4%). Walau bagaimanapun, peningkatan bilangan insiden penipuan berkaitan pembayaran di luar dan di dalam negeri menggariskan tentang jenayah siber yang semakin membimbangkan. Hal ini berikutan serangan siber yang semakin kerap dan mengakibatkan kos yang semakin tinggi untuk pihak yang terjejas serta ekonomi secara meluas. Di Malaysia, sebanyak 19,165 kes penipuan perbankan dalam talian melibatkan RM94.6 juta dilaporkan oleh pelanggan institusi kewangan pada separuh kedua tahun 2022. Nilai ini merupakan peningkatan daripada 9,735 kes berjumlah RM39.9 juta yang dilaporkan pada separuh pertama tahun 2022.

Usaha memerangi jenayah siber memerlukan pendekatan yang komprehensif dan terselaras antara pengawal selia, agensi penguatkuasaan undang-undang, dan sektor swasta. Pada peringkat antarabangsa, Financial Action Task Force (FATF)[37] memperakui keperluan ini dan telah memulakan inisiatif baharu yang memberikan tumpuan pada isu penipuan dan perisian tebusan yang digerakkan oleh siber. Inisiatif ini termasuk penerbitan laporan mengenai trend dan kaedah terkini serta saranan untuk mengekang aktiviti perisian tebusan secara berkesan. Selain itu, beberapa pengawal selia kewangan telah mengeluarkan panduan penyeliaan kepada institusi kewangan untuk memperkukuh kawalan bagi menghadapi penipuan perbankan dalam talian. Pada masa yang sama, beberapa kerajaan telah menerajui kempen antipenipuan peringkat kebangsaan untuk mempertingkatkan kesedaran pengguna.[38] Di Malaysia dan beberapa negara lain, pusat antipenipuan kebangsaan telah ditubuhkan dalam usaha memusatkan tindak balas yang pantas dan berkesan terhadap penipuan dalam talian.

Bank Negara Malaysia dan industri kewangan terus menggiatkan usaha yang sedang dijalankan untuk mendidik orang ramai mengenai langkah-langkah keselamatan siber (*cyber hygiene*) yang memainkan peranan penting untuk mencegah penipuan. Selain itu, Bank menghendaki semua institusi perbankan untuk memperketat langkah-langkah tambahan terhadap penipuan kewangan yang semakin canggih dan sentiasa berubah-ubah yang mengambil kesempatan ke atas tingkah laku sosial yang meningkatkan kelemahan kepada penipuan.[39] Langkah-langkah ini termasuk keperluan bagi bank-bank mempercepat peralihan daripada penggunaan kata laluan sekali sahaja (*one-time password*, OTP) yang berasaskan khidmat pesanan ringkas (*short messaging service*, SMS) kepada kaedah pengesahan yang lebih selamat untuk aktiviti atau transaksi dalam talian menjelang bulan Jun 2023. Bank-bank juga dikehendaki untuk melaksanakan langkah-langkah perlindungan yang lain termasuk:

- mengeluarkan semua pautan boleh diklik dalam komunikasi SMS dan e-mel;
- mengehadkan peranti yang digunakan oleh pelanggan untuk pengesahan transaksi perbankan dalam talian kepada satu peranti mudah alih;
- memperkukuh proses untuk mendaftarkan peranti mudah alih baharu dan menukar "peranti selamat";
- memperketat peraturan pengesanan dan pencetus penipuan untuk menyekat transaksi yang mencurigakan; dan
- mempertingkatkan keselamatan siber (*cyber hygiene*) bagi peranti pelanggan yang digunakan untuk perkhidmatan perbankan atau pembayaran dalam talian.

Setakat bulan Disember 2022, semua institusi perbankan utama telah menawarkan kaedah pengesahan alternatif dan memindahkan semua pelanggan mereka secara berperingkat kepada kaedah yang lebih selamat. Bank-bank juga terus memperhalus dan menambah baik langkah-langkah

[37] FATF ialah badan pemerhati global aktiviti pengubahan wang haram dan pembiayaan keganasan. Badan antara kerajaan ini merumuskan piawaian antarabangsa yang bermatlamat untuk mencegah aktiviti haram dan mudarat yang diakibatkan oleh aktiviti ini kepada masyarakat. Sebagai badan perumus dasar, FATF berusaha mewujudkan hasrat politik (*political will*) yang diperlukan untuk menghasilkan pembaharuan perundangan negara dan pengawalseliaan dalam bidang ini.

[38] Contohnya, kempen "Take Five to Stop Fraud" di United Kingdom dan "Stay Smart Online" oleh kerajaan Australia.

[39] Langkah-langkah tambahan yang diambil untuk membanteras peningkatan penipuan berkaitan perbankan dalam talian disenaraikan dalam Tinjauan Kestabilan Kewangan Separuh Pertama 2022 Bank Negara Malaysia.

keselamatan yang lain. Langkah-langkah ini termasuk mempertingkatkan proses pengesahan untuk pendaftaran peranti mudah alih, melaksanakan pengesahan panggilan, menambah baik peraturan pengesanan penipuan secara berterusan untuk menyekat transaksi yang mencurigakan, serta menjalankan pemantauan secara berterusan untuk mengesan dan menurunkan laman sesawang palsu dengan kerjasama Suruhanjaya Komunikasi dan Multimedia Malaysia (SKMM). Selain itu, bank-bank yang mempunyai jumlah kes penipuan yang tinggi telah masing-masing melantik Pengarah Kanan Bebas untuk mengawasi pengendalian insiden penipuan dan pencerobohan data serta mengadakan kerjasama dengan Pusat Respons Scam Kebangsaan (National Scam Response Centre, NSRC) untuk mengesan dan memintas dana yang dicuri. Pada bulan November 2022, industri kewangan turut menubuhkan pasukan petugas untuk merangka strategi dan menyelaraskan pelaksanaan tindakan di seluruh industri yang tepat pada masanya untuk membanteras penipuan kewangan. Perkara ini juga termasuk usaha yang berterusan untuk meningkatkan kesedaran orang ramai mengenai taktik penipuan serta membiasakan pengguna perbankan dalam talian dengan ciri-ciri keselamatan dan kawalan yang telah dilaksanakan.

Walaupun kerugian operasi daripada penipuan kewangan pada masa ini tidak menimbulkan risiko kepada kestabilan kewangan secara keseluruhan, keyakinan orang ramai terhadap bank-bank dan infrastruktur pembayaran boleh terjejas dengan lebih ketara dan tidak menentu jika trend yang semakin meningkat ini dibiarkan. Hal ini memerlukan tindak balas seluruh negara yang terselaras untuk mendidik orang ramai, mengekalkan langkah-langkah pencegahan yang kukuh serta membawa penjenayah ke muka pengadilan.

Institusi kewangan terus mencapai kemajuan yang besar dalam memperkukuh keupayaan pengurusan risiko teknologi secara keseluruhan. Pada tahun 2022, lebih 90% daripada institusi kewangan mencapai tahap pematuhan yang tinggi terhadap piawaian Pengurusan Risiko dalam Teknologi (Risk Management in Technology, RMiT) yang dikeluarkan oleh Bank, iaitu peningkatan daripada 35% pada tahun 2020. Berikutan pendigitalan perkhidmatan kewangan yang berterusan, institusi kewangan terus memberikan keutamaan pada pengurusan risiko teknologi dan membuat pelaburan besar untuk menaik taraf infrastruktur teknologi maklumat (*information technology*, IT). Semua penambahbaikan ini bertujuan untuk mempertingkatkan prestasi sistem dan ketersediaan perkhidmatan, meningkatkan daya tahan terhadap gangguan operasi serta mengurangkan risiko teknologi yang tidak lagi menerima sokongan atau kemas kini penyelenggaraan (*technology obsolescence*). Penilaian penyeliaan juga menunjukkan terdapat pengawasan yang lebih khusus oleh lembaga pengarah dan pasukan pengurusan kanan untuk memastikan kelangsungan sistem IT mereka, serta sumber untuk menyelenggarakannya, dapat menampung keperluan pada masa ini dan jangkaan pada masa hadapan. Libat urus penyeliaan ini juga akan digunakan untuk mempercepat penutupan sebarang jurang yang berkaitan dengan pengurusan risiko teknologi dan amalan keselamatan siber yang baik.

Bank sedang memberikan keutamaan yang berterusan bagi pengurusan risiko yang berkaitan dengan penyedia perkhidmatan pihak ketiga (*third-party service providers*, TPSP). Walaupun beberapa kemajuan telah dicapai dalam mengurangkan gangguan operasi disebabkan oleh gangguan sistem dan kebocoran data pihak ketiga, masih terdapat

Menyiasat Insiden Penipuan

Proses mengesan, memintas dan usaha mendapatkan semula wang yang dicuri adalah kompleks. Hal ini lazimnya melibatkan masa dan sumber yang banyak, serta memerlukan penyelarasan antara pelbagai agensi, institusi kewangan dan syarikat telekomunikasi. Paling mustahak, mangsa perlu membuat makluman segera kepada institusi kewangan mereka atau NSRC sebaik sahaja mengesan transaksi tanpa kebenaran atau menyedari yang mereka telah ditipu. Institusi kewangan akan menggunakan maklumat ini untuk menyekat akaun yang terjejas buat sementara dan mula mengesan pergerakan wang. Agensi penguatkuasaan undang-undang seterusnya akan memulakan penyiasatan, mengeluarkan arahan penguatkuasaan yang sewajarnya, dan memburu penjenayah di sebalik sindiket. Meskipun langkah-langkah ini kelihatan mudah, penyiasatan menghadapi cabaran yang besar disebabkan oleh pergerakan wang yang pantas ke dalam pelbagai akaun di bank-bank berbeza disusuli dengan pengeluaran wang tunai secara serta-merta. Jumlah transaksi yang begitu besar juga menyulitkan usaha membezakan antara transaksi yang melibatkan penipuan dengan transaksi yang tulen disebabkan oleh percampuran wang.

keperluan untuk mempertingkatkan kejelasan tentang subkontraktor yang digunakan oleh TPSP, iaitu penyedia perkhidmatan pihak keempat (*fourth-party service providers*, 4PSP), khususnya dengan risiko penumpuan dan penularan yang disebabkan oleh beberapa 4PSP. Bidang risiko yang baharu adalah berkaitan dengan pergantungan dan penumpuan terhadap penyedia perkhidmatan awan (*cloud service provider*) yang semakin meningkat. Bagi memastikan institusi perbankan menilai dan menguruskan risiko sebegini secara teliti dalam strategi awan (*cloud strategy*) mereka, Bank akan mengeluarkan panduan tambahan kepada dokumen dasar RMiT pada separuh pertama tahun 2023 yang akan menggariskan kehendak utama bagi pengurusan risiko teknologi awan untuk institusi kewangan. Bank juga akan melaksanakan rundingan dengan industri pada separuh kedua tahun 2023 untuk menghasilkan senario lazim bagi pelan kesinambungan perniagaan bersama (*business continuity plan*, BCP) seluruh industri dengan TPSP IT yang sangat penting. Langkah selanjutnya sedang dilaksanakan untuk mengendalikan latihan simulasi krisis bersama (*crisis simulation exercises*, CSE) yang melibatkan Bank dan peserta industri terpilih. Latihan ini bertujuan untuk menguji dan terus memperkukuhkan pelan pemulihan dan tindak balas sedia ada oleh institusi kewangan untuk mengurangkan gangguan operasi yang meluas. Secara kolektif, usaha-usaha ini dijangka akan menunjukkan dengan lebih jelas kesalinghubungan penyedia perkhidmatan dan bertujuan untuk mengukuhkan keupayaan pengurusan risiko rantaian bekalan dalam sektor kewangan.

Meskipun gangguan operasi berkaitan dengan gangguan sistem dan kebocoran data akibat kegagalan pihak ketiga masih rendah setakat ini, terdapat trend pencerobohan siber yang semakin meningkat yang memerlukan tahap kewaspadaan berterusan. Ancaman utama yang dikenal pasti oleh institusi kewangan termasuk beberapa kes pencerobohan yang berlaku dalam persekitaran penyedia perkhidmatan serta kempen jenayah siber yang semakin canggih seperti perkhidmatan menggunakan perisian tebusan (*malware-as-a-service*) dan kempen pancingan data bersasar. Insiden-insiden ini terus menekankan keperluan untuk mempertingkatkan perkongsian mengenai risikan ancaman siber tepat pada masanya. Sehubungan dengan itu, tujuh institusi kewangan baharu telah menyertai Platform Risikan Ancaman Siber Sektor Kewangan (Financial Sector Cyber Threat Intelligence Platform, FinTIP)[40] pada separuh kedua tahun 2022, dengan bilangan entiti yang menyertai rangkaian kini mencapai 40 peserta. FinTIP terus menyokong usaha industri untuk terus mengukuhkan pertahanan siber melalui perkongsian risikan ancaman siber dalam kalangan institusi kewangan. Usaha sedang dijalankan oleh FinTIP untuk mempertingkatkan liputan perkongsian risikan ancaman setempat di luar industri kewangan. Usaha ini dicapai melalui kerjasama dengan agensi keselamatan siber tempatan untuk mengumpul risikan ancaman masa nyata dan dipertingkatkan untuk penilaian landskap ancaman yang lebih tepat pada masanya.

Institusi kewangan terus mengenal pasti risiko siber sebagai risiko utama yang dihadapi oleh industri pada tahun 2023 berikutan pendigitalan dan penggunaan teknologi dalam kewangan yang semakin berkembang serta pengaturan pekerjaan dari jarak jauh secara meluas yang meningkatkan kemungkinan berlakunya eksploitasi terhadap kelemahan. Hal ini dijangka mengekalkan tumpuan institusi kewangan pada usaha yang lebih utama untuk mengukuhkan daya tahan siber.[41] Risiko operasi utama lain yang dikenal pasti oleh institusi kewangan pada masa hadapan termasuk ketidakpatuhan pengawalseliaan, persaingan untuk mendapatkan tenaga kerja mahir penting serta risiko berkaitan dengan penyumberan luar (Gambar Rajah 1.1).

[40] FinTIP ialah platform teknologi bagi institusi kewangan tempatan untuk berkongsi risikan ancaman keselamatan siber dan amalan yang terbaik dengan pantas.
[41] Berdasarkan Emerging Operational Risk Survey 2022/2023 yang dijalankan oleh Bank Negara Malaysia.

Gambar Rajah 1.1: Risiko Operasi Utama dan Tindakan Mengurangkan Risiko



Ancaman siber

- Proses pengurusan TPSP yang mantap untuk pengenal-pastian, penilaian dan pengurusan risiko yang berterusan
- Pelaksanaan arkitektur tiga peringkat yang diperkukuh dengan peranti keselamatan seperti sistem pencegahan pencerobohan *(intrusion prevention systems,* IPS) dan sistem pengesan pencerobohan (*intrusion detection systems*, IDS)
- Ujian penembusan tahunan dan pemantauan keselamatan 24/7, perlindungan DDoS, kawalan akses, pengurusan tampalan dan insurans siber
- Pendidikan dan kesedaran keselamatan yang berterusan serta latihan keselamatan khusus dan pensijilan bagi kakitangan IT



Ketidakpatuhan kawal selia

- Analisis jurang secara berkala dan laporan tentang pengecualian kepada pihak pengurusan kanan dan lembaga pengarah
- Penilaian yang tepat pada masa tentang keperluan pengawalseliaan pematuhan baharu menggunakan pendekatan berasaskan risiko
- Mempertingkatkan prosedur dalaman untuk memperkenalkan pengasingan tugas, semakan bebas, kawalan akses sistem bersegmen dan proses pemberian kuasa berbilang peringkat
- Pelan tindakan untuk menyokong pengurusan risiko kelestarian seperti menilai semula portfolio pelaburan dan memperkenalkan dana tenaga hijau



Persaingan mendapatkan tenaga kerja mahir

- Kajian penandaarasan bagi meningkatkan pengambilan dan pengekalan tenaga mahir
- Mempertingkatkan pengurusan tenaga mahir dan pelan penggantian



Risiko berkaitan penyumberan luar

- Memperkukuh proses dalaman untuk penyumberan luar dan pengurusan risiko pihak ketiga
- Menubuhkan jawatankuasa kerja dengan penyedia perkhidmatan untuk memantau pematuhan terhadap perjanjian tahap perkhidmatan (*service level agreement*, SLA)
- Mesyuarat secara berkala dengan penyedia perkhidmatan untuk membincangkan isu-isu dan hasil kerja
- Pengawasan secara berkala oleh jawatankuasa risiko tentang pengaturan penyumberan luar dengan sumber khusus, tadbir urus yang sesuai serta daftar risiko yang dikemas kini secara berkala
- Memastikan penyedia perkhidmatan mengekalkan pelan kesinambungan perniagaan (*business continuity plans*, BCP) dan pelan pemulihan bencana (*disaster recovery plans*, DRP) yang mencukupi



Ralat manusia dalam melaksanakan tugas

- Memperkukuh kawalan dalaman dan mengautomasikan proses manual yang terdedah kepada ralat manusia
- Memantapkan pemahaman tentang punca utama bagi membangunkan proses dan kawalan yang lebih berkesan

Sumber: Bank Negara Malaysia

Sistem pembayaran dan penyelesaian terus berada pada tahap ketersediaan sistem yang tinggi

Sistem Pemindahan Dana dan Sekuriti Secara Elektronik Masa Nyata (Real-time Electronic Transfer of Funds and Securities System, RENTAS)[42] dan sistem pembayaran runcit (*retail payment system*, RPS) utama terus berada pada tahap ketersediaan sistem yang tinggi, tanpa sebarang insiden siber dikesan pada separuh kedua tahun 2022.

Bagi memastikan ketersediaan sistem yang tinggi, Bank dan Payments Network Malaysia Sdn. Bhd. (PayNet) sebagai pengendali sistem pembayaran, masing-masing untuk RENTAS dan RPS utama, terus mempertingkatkan langkah kawalan untuk mengekalkan tahap daya tahan yang kukuh terhadap ancaman siber, mengukuhkan pengurusan penyedia perkhidmatan yang sangat penting (*critical service providers*, CSP) dan terus menambah baik pengurusan kesinambungan perniagaan (*business continuity management*, BCM):

- Pelbagai inisiatif sedang dilaksanakan untuk terus mengukuhkan keupayaan pertahanan dan tindak balas siber oleh Bank dan PayNet.
- RENTAS dan Sistem Pembayaran Yang Ditetapkan (Designated Payment System, DPS) tertakluk kepada keperluan BCM yang dipertingkatkan berikutan penerbitan kehendak BCM yang lebih mantap oleh Bank pada bulan Disember 2022. Keperluan yang dipertingkatkan bersama-sama dengan ujian secara langsung dan senario BCP yang dijalankan dengan jayanya pada tahun 2022, akan terus mengukuhkan tindak balas sekiranya berlaku gangguan; dan
- Selaras dengan saranan Committee on Payments and Market Infrastructures (CPMI),[43] pengendali

[42] RENTAS ialah sistem penyelesaian kasar masa nyata untuk pemindahan dana antara bank, penyelesaian sekuriti hutang dan perkhidmatan penyimpanan untuk sekuriti hutang tanpa skrip.

[43] Lampiran F Principles for Financial Market Infrastructures yang diterbitkan oleh CPMI menggariskan lima kehendak pengawasan untuk penyedia perkhidmatan yang sangat penting, iaitu pengenalpastian dan pengurusan risiko, keselamatan maklumat, kebolehpercayaan dan daya tahan, perancangan teknologi dan komunikasi dengan pengguna.

RENTAS dan RPS juga mempertingkatkan dasar dan prosedur untuk pengurusan CSP yang lebih kukuh. Hal ini termasuk penambahbaikan dalam proses tadbir urus dan pemantauan, usaha wajar yang lebih baik dan penilaian terpilih di premis CSP.

Berkuat kuasa 10 Februari 2023, Platform Pembayaran Runcit Masa Nyata (Real-time Retail Payments Platform, RPP) telah ditetapkan sebagai sistem pembayaran yang di bawah Akta Perkhidmatan Kewangan 2013 dan Akta Perkhidmatan Kewangan Islam 2013. Penetapan ini memberikan Bank lebih banyak kuasa di bawah undang-undang untuk mengeluarkan arahan kepada peserta RPP dan mengambil alih operasi RPP dalam keadaan tertentu bagi melindungi kestabilan kewangan dan perkhidmatan pembayaran yang sangat penting.

Kecerdasan Buatan dalam Sistem Kewangan Malaysia: Peluang, Risiko, dan Langkah Seterusnya

Pengenalan

Kecerdasan buatan dan pembelajaran mesin (*artificial intelligence and machine learning*, AI/ML) telah semakin matang sejak beberapa tahun kebelakangan, dengan solusi nyata dan berkesan yang diaplikasikan dalam pelbagai industri.

Impak dan potensi transformatif AI/ML bagi perniagaan disumbangkan oleh beberapa faktor seperti penemuan baharu dalam algoritma dan teknik AI/ML, ketersediaan sumber data yang lebih meluas serta kemajuan dalam kuasa pengkomputeran. Pada masa yang sama, kumpulan tenaga mahir dan kepakaran dalam bidang teknologi yang semakin besar, infrastruktur awan yang mudah diskala, dan penyelesaian berkos rendah (contohnya, teknologi sumber terbuka) juga telah mengurangkan cabaran dalam penggunaan AI/ML, lantas mempercepatkan penerapannya.

AI/ML menjanjikan peluang baharu dalam kewangan...

Dalam bidang perkhidmatan kewangan, penggunaan teknik AI/ML yang lebih meluas menawarkan peluang baharu bagi menambah baik pengalaman pelanggan dan penawaran produk, terutamanya melalui pengkhususan produk pada skala besar serta penyediaan khidmat yang lebih cepat dan mudah. AI/ML turut membantu memberikan pemahaman baharu kepada penyedia perkhidmatan kewangan (*financial service providers,* FSP) untuk membuat keputusan yang lebih baik, di samping mengautomasikan proses mereka. Hasilnya, semua peluang ini berpotensi untuk membantu FSP menguruskan risiko dengan lebih baik, meningkatkan kecekapan operasi dan produktiviti serta mengurangkan kos.

Pada tahun 2021, Bank menjalankan kaji selidik awal mengenai penggunaan AI/ML oleh FSP dengan 25 responden yang terdiri daripada bank-bank, penanggung insurans dan pengendali pembayaran di Malaysia. Responden dipilih berdasarkan saiz dan rekod pencapaian inisiatif digital mereka serta keahlian dalam Kumpulan Pelaksanaan API Terbuka.[1] Gambar Rajah 1 mengambil kira kes penggunaan sebenar dan berpotensi bagi AI/ML yang dikenal pasti oleh responden, yang merentas pelbagai fungsi dan bidang perniagaan.

Kaji selidik mendapati bahawa banyak FSP di Malaysia sememangnya telah aktif menggunakan teknik AI/ML dan masih banyak inisiatif yang sedang dibangunkan. Pada masa ini, AI/ML paling lazim digunakan dalam bidang analisis data dan libat urus pelanggan, serta untuk proses kenali pelanggan anda secara elektronik (*electronic know your customer*, e-KYC) dan pendaftaran (*onboarding*) pelanggan secara digital. Beberapa institusi perbankan juga melengkapkan proses pengunderaitan kredit mereka dengan teknik AI/ML untuk produk pembiayaan terpilih. Kepekaan risiko yang lebih tinggi bagi model AI/ML ini menggalakkan dedahan berhemat terhadap peminjam berisiko lebih tinggi, dan penyediaan perkhidmatan yang lebih mudah diakses kepada pelanggan yang layak tetapi masih tidak menerima perkhidmatan perbankan. Kaji selidik juga menunjukkan minat yang tinggi dan sokongan yang padu daripada pengurusan kanan dan lembaga pengarah FSP. Kira-kira separuh daripada responden menganggap penggunaan AI/ML sebagai pengubah keadaan (*game changer*) yang berpotensi untuk mengubah cara mereka menjalankan perniagaan, dan sudah pun berusaha mencari peluang baharu di luar kes kegunaan termaklum dan projek AI/ML semasa. Gambar Rajah 2 memaparkan secara ringkas dapatan utama daripada kaji selidik tersebut.

[1] Ditubuhkan oleh Bank pada tahun 2018 untuk menggalakkan penyeragaman *Application Programming Interface* (API) Terbuka, yang akan meningkatkan akses pihak ketiga kepada data. Usaha ini turut disokong oleh rangka kerja keselamatan, undang-undang dan tadbir urus yang diperlukan untuk melindungi data pelanggan dan sistem teras institusi kewangan.

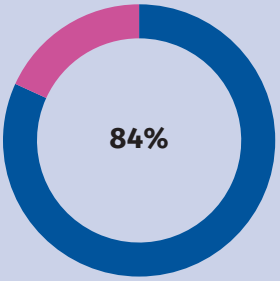
Gambar Rajah 1: Contoh Kes Penggunaan AI/ML dalam Perkhidmatan Kewangan



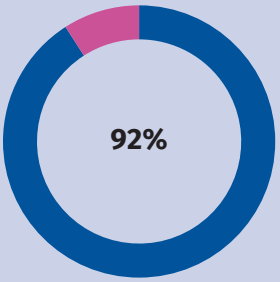
Sumber: Bank Negara Malaysia

Gambar Rajah 2: Ringkasan Dapatan Terpilih

Kebanyakan FSP sedang menggunakan atau membangunkan projek AI/ML secara aktif...



21 daripada **25** FSP mempunyai sekurang-kurangnya satu projek AI/ML yang digunakan secara aktif



23 daripada **25** FSP mempunyai sekurang-kurangnya satu projek AI/ML yang sedang dibangunkan

...terutamanya untuk analisis dan penglibatan pelanggan serta KYC

	Projek AI/ML Utama	Bil. FSP mengikut penggunaan AI/ML
Bank	AML dan pengesanan penipuan	13
Bank	KYC/Pendaftaran digital	12
Bank	Analisis dan penglibatan pelanggan	8
Bank	Pengunderaitan/ penilaian	8
ITO	Analisis dan penglibatan pengguna	2
ITO	Sumber Manusia	2
ITO	Pengurusan Risiko Teknologi	2
E-MI	KYC/Pendaftaran digital	3
E-MI	Analisis dan penglibatan pelanggan	2

Digerakkan oleh pihak Pengurusan dan Lembaga Pengarah FSP

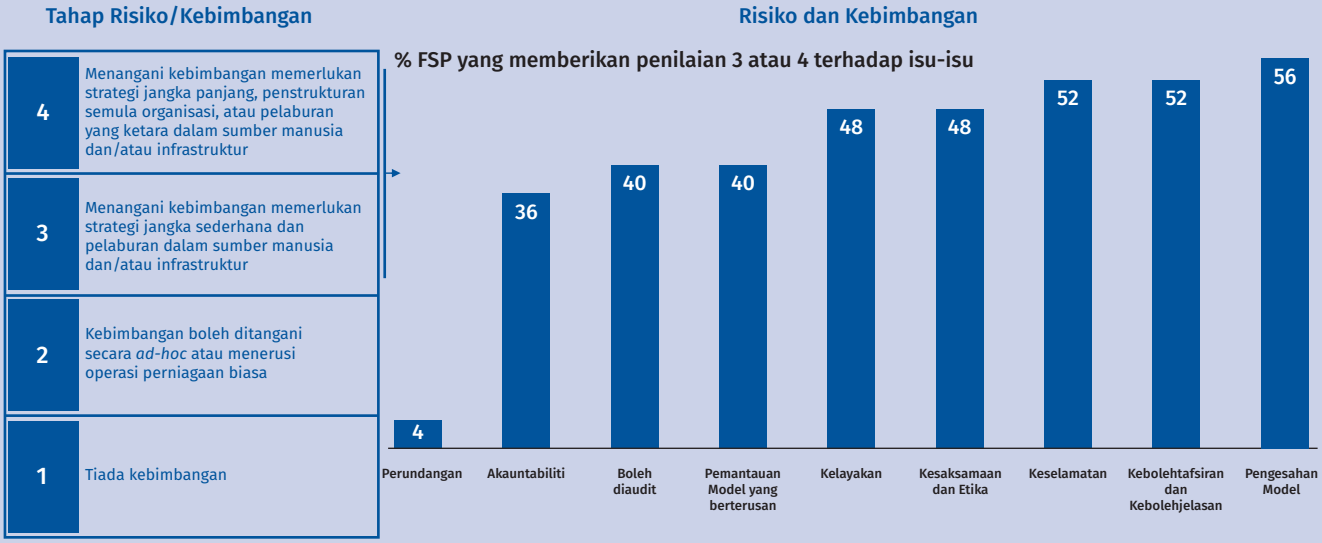


Sumber: Bank Negara Malaysia

...dan risiko yang perlu diuruskan dengan teliti

Walau bagaimanapun, pengenalan dan penggunaan AI/ML yang lebih meluas juga menimbulkan beberapa risiko yang perlu diuruskan oleh sektor kewangan. Kaji selidik menunjukkan beberapa risiko dan kebimbangan utama AI/ML yang telah dikenal pasti oleh FSP (lihat Gambar Rajah 3).

Gambar Rajah 3: Risiko dan Kebimbingan yang Dikenal Pasti dalam Penerapan AI/ML

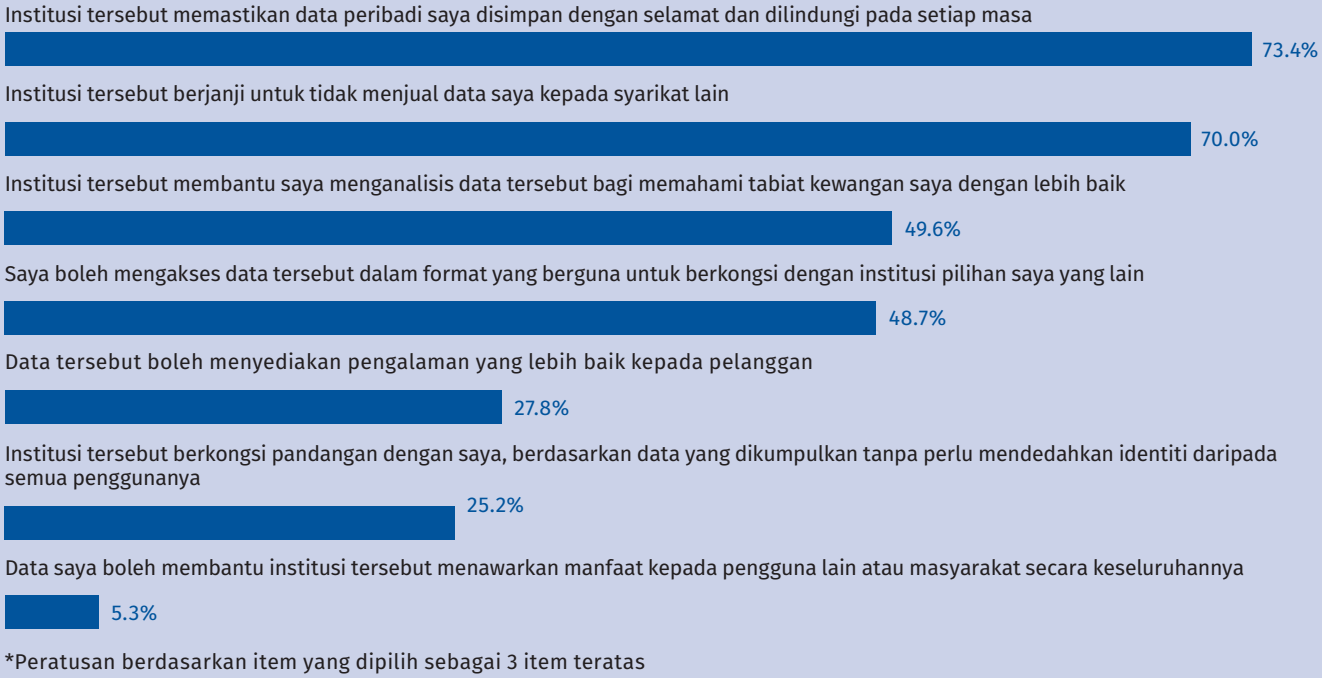


Sumber: Bank Negara Malaysia

Responden kaji selidik menyatakan bahawa pengesahan model merupakan kebimbangan utama bagi FSP. Risiko model ialah risiko kegagalan model untuk memberikan hasil yang tepat. Memandangkan kebanyakan model dan algoritma AI/ML jauh lebih kompleks berbanding dengan model linear tradisional, keputusan yang dijana mungkin sukar untuk dijelaskan dan disahkan. Kesukaran untuk memahami sistem dalaman AI/ML juga boleh melambatkan pengesanan sebarang kesilapan atau ketidaktepatan *(inaccuracies)*. Pengesahan model yang tepat pada masanya, yang menggabungkan algoritma yang dilatih menggunakan set data terkini, adalah penting untuk menguruskan risiko model dan mengekalkan keupayaan ramalan model. Tanpa proses pengesahan ini, prestasi model lazimnya menurun mengikut peredaran masa serta boleh menyebabkan ramalan yang tidak tepat atau kesilapan yang lebih besar daripada jangkaan, sekali gus menjadikan keputusan yang terhasil daripada model ini tidak boleh dipercayai. Hal ini boleh mengakibatkan hasil yang tidak diingini seperti kerugian kewangan atau keputusan yang berat sebelah atau tidak adil yang memberikan kesan negatif kepada pelanggan, dan seterusnya mendedahkan FSP kepada risiko reputasi dan undang-undang.

Satu lagi aspek utama dalam pengesahan model berkait dengan pengurusan data dan jaminan kualiti data. Sesetengah sistem AI/ML memerlukan jumlah data yang besar termasuk data transaksi berkepantasan tinggi daripada pelbagai sumber. Hal ini memerlukan tadbir urus data enterpris yang mantap bagi memastikan data yang diyakini dan berkualiti. Penggunaan rangkaian data yang lebih luas, termasuk data peribadi, juga menimbulkan kebimbangan mengenai keselamatan dan privasi data. Menurut kaji selidik awal mengenai kepercayaan pengguna yang dijalankan oleh Bank pada tahun 2021,[2] keselamatan dan privasi merupakan penentu paling penting berhubung dengan kesanggupan pengguna untuk berkongsi data peribadi dengan institusi kewangan (Lihat Gambar Rajah 4).

Gambar Rajah 4: Penentu Kepercayaan Pengguna dalam Berkongsi Data di Malaysia



*Peratusan berdasarkan item yang dipilih sebagai 3 item teratas

Sumber: Bank Negara Malaysia

Secara amnya, peningkatan penggunaan AI/ML oleh FSP berpotensi menimbulkan risiko baharu terhadap kestabilan kewangan, terutamanya jika model tidak ditentukur dengan baik atau digunakan secara tidak wajar. Contoh hasil yang tidak diingini termasuk meminggirkan kumpulan pengguna tertentu, mengurangkan daya tahan operasi, atau menggandakan kejutan kewangan daripada tingkah laku yang dipacu algoritma. Risiko

[2] Kaji selidik bertajuk "Tinjauan Keyakinan Pengguna" telah diterbitkan kepada orang ramai pada bulan Disember 2021. Kaji selidik itu mengumpulkan 413 maklum balas daripada individu daripada semua peringkat umur, kumpulan pendapatan dan tahap pendidikan.

sedemikian ketika ini kekal rendah berdasarkan sifat dan tahap penggunaan AI/ML oleh FSP. Kebanyakan FSP juga menggunakan pendekatan pelaksanaan AI/ML yang cermat dan berhati-hati. Sebagai contoh, pelaksanaan AI/ML untuk pengunderaitan kredit biasanya terhad kepada portfolio pembiayaan terpilih, dengan pemantauan rapi terhadap keputusan yang dijana, sebelum skopnya dikembangkan secara beransur-ansur. FSP juga mengambil langkah-langkah perlindungan bagi memastikan sistem AI/ML sentiasa dipantau, seperti pemantauan Kadar Penerimaan Palsu untuk pengesahan identiti yang menggunakan solusi e-KYC.

Peraturan untuk menggalakkan penggunaan AI/ML yang bertanggungjawab

Landskap pengawalseliaan global terhadap penggunaan AI/ML masih pada peringkat awal. Namun begitu, semakin banyak pengawal selia kewangan dalam ekonomi seperti di Singapura, Hong Kong dan UK telah menerbitkan prinsip-prinsip peringkat tinggi atau mengeluarkan panduan mengenai amalan terbaik penggunaan AI/ML yang bertanggungjawab bagi sektor kewangan. Sebahagian daripada dokumen ini dikeluarkan dengan kerjasama pakar industri atau akademik. Panduan yang dikeluarkan ini secara amnya bertujuan untuk memastikan sistem AI/ML adalah kukuh dan telus, menggalakkan pemberian akauntabiliti yang jelas dan memastikan FSP memberikan pertimbangan yang teliti terhadap isu kesaksamaan serta kebimbangan etika yang lain.

Gambar Rajah 5: Keperluan Kawal Selia dalam Menguruskan Risiko daripada Penerapan AI/ML

Layanan Adil kepada Pengguna Kewangan (2019) memerlukan FSP untuk memastikan bahawa pengguna tidak tertakluk kepada amalan diskriminasi yang tidak adil

Tadbir Urus Risiko (2013) menyatakan bahawa "... penggunaan model untuk mengenal pasti dan mengukur risiko harus disokong oleh proses yang mantap untuk menguruskan risiko model"

Pengurusan Maklumat Pelanggan dan Pendedahan yang Dibenarkan (2021) menetapkan keperluan yang berkaitan dengan amalan dan kawalan FSP dalam mengendalikan maklumat pelanggan

Garis Panduan Pengurusan Data dan Rangka Kerja MIS (2012) memerlukan institusi kewangan untuk mewujudkan dan mengekalkan rangka kerja bagi pengurusan data dan sistem maklumat pengurusan *(management information system, MIS)* yang kukuh

Pengurusan Risiko dalam Teknologi (2020) memerlukan rangka kerja pengurusan risiko teknologi institusi kewangan meliputi pengenalpastian risiko daripada penggunaan teknologi baharu atau teknologi sedang pesat berkembang, serta langkah kawalan dan pengurangan risiko tersebut

Sumber: Bank Negara Malaysia

Di Malaysia, FSP dikehendaki mematuhi keperluan pengawalseliaan sedia ada (lihat Gambar Rajah 5) dalam penggunaan aplikasi AI/ML mereka. Meskipun kumpulan piawaian sedia ada tertumpu kepada risiko dan pertimbangan utama dalam penggunaan AI/ML oleh FSP, penerapan yang lebih besar, iaitu dari segi tahap keluasan penggunaan serta kes penggunaan khusus yang mempunyai kesan yang lebih tinggi terhadap pemacu risiko yang sangat penting, akan mendorong penambahbaikan terhadap piawaian yang sedia ada. Khususnya, panduan selanjutnya mengenai kebolehtafsiran (*interpretability*) dan kebolehjelasan (*explainability*) model mungkin diperlukan apabila lebih banyak pemahaman diperoleh melalui evolusi amalan FSP. Bank Negara Malaysia akan terus memantau rapi perkembangan dan inovasi dalam industri untuk memaklumkan pendekatan pengawalan dan penyeliaannya, bagi memastikan risiko yang berkaitan dengan AI/ML dapat difahami dan diuruskan dengan baik.