RISIKO OPERASI

Sektor kewangan terus berwaspada untuk melindungi daya tahan operasi terhadap ancaman yang berlarutan

Usaha berterusan oleh institusi kewangan untuk memastikan amalan pengurusan risiko operasi yang kukuh dan kawalan penipuan kekal mustahak bagi menyokong daya tahan operasi sistem kewangan dalam menghadapi cabaran semasa daripada pendigitalan perkhidmatan kewangan dan pergantungan yang semakin meningkat pada penyedia perkhidmatan pihak ketiga (*third-party service provider*, TPSP). Insiden operasi terus menguji keupayaan pengesanan, pemantauan dan pemulihan institusi kewangan. Meskipun kerugian kewangan daripada risiko operasi yang dilaporkan oleh institusi kewangan kekal rendah (ST1 2024: RM183.9 juta; ST1 2023: RM188.6 juta), beberapa insiden gangguan yang sederhana kepada perkhidmatan perbankan dalam talian telah berlaku dalam tempoh tersebut. Hal ini memerlukan beberapa institusi mengambil langkah-langkah yang lebih kukuh bagi memastikan pelan tindak balas insiden lebih mantap dan pemantauan risiko berkaitan pihak ketiga yang lebih teliti. Institusi kewangan yang gagal mematuhi piawaian pengawalseliaan yang ditetapkan untuk memastikan tahap ketersediaan perkhidmatan yang tinggi[30] akan tertakluk pada tindakan penyeliaan atau penguatkuasaan yang berat, termasuk arahan untuk memperkukuh kawalan, mempertingkatkan keperluan modal untuk risiko operasi dan penalti monetari pentadbiran (*administrative monetary penalties*, AMP).

Risiko berkaitan teknologi dan siber akan terus menjadi cabaran dalam pengurusan dan penyeliaan risiko operasi dalam sistem kewangan. Peningkatan kecanggihan alat dan teknik yang digunakan oleh pelaku ancaman (*threat actors*), serta TPSP yang dijadikan sasaran untuk mendapatkan akses kepada sistem atau data institusi kewangan, telah meningkatkan lagi tuntutan yang perlu dipenuhi oleh institusi kewangan dalam usaha berterusan untuk melindungi persekitaran mereka. Institusi kewangan terus melaburkan sumber yang besar untuk mengukuhkan proses pengesanan dan mitigasi keselamatan siber mereka. Perbelanjaan tahunan teknologi maklumat (*information technology*, IT) oleh institusi-institusi kewangan untuk keselamatan siber sahaja telah meningkat paling tinggi pada tahun 2024 lantas melanjutkan peningkatan peruntukan keselamatan siber sebanyak dua angka bagi tempoh tahunan yang berturut-turut.

Piawaian pengurusan risiko operasi lebih tinggi yang terpakai pada penyedia perkhidmatan pembayaran juga telah meningkatkan tahap kawalan risiko keselamatan siber yang dipatuhi oleh pengeluar wang elektronik (*e-money issuers*, EMI) dan pemeroleh peniaga, dengan penambahbaikan berterusan diperhatikan pada tahap kematangan keselamatan siber para penyedia perkhidmatan pembayaran ini. Perkongsian maklumat secara proaktif antara BNM dengan industri tentang risikan ancaman siber melalui Platform Risikan Ancaman Siber Sektor Kewangan (Financial Sector Cyber Threat Intelligence Platform, FinTIP) terus menyokong keupayaan pengesanan ancaman dan tindak balas insiden oleh institusi kewangan. Bilangan laporan risikan ancaman siber yang dikongsikan dalam FinTIP meningkat sebanyak 40% pada separuh pertama tahun 2024 berbanding dengan tempoh yang sama pada tahun lepas. Selain itu, usaha mendidik dan menguatkuasakan amalan keselamatan siber yang kukuh dalam kalangan kakitangan dan pelanggan kekal penting untuk membina serta mengekalkan asas pertahanan keselamatan siber yang kukuh.

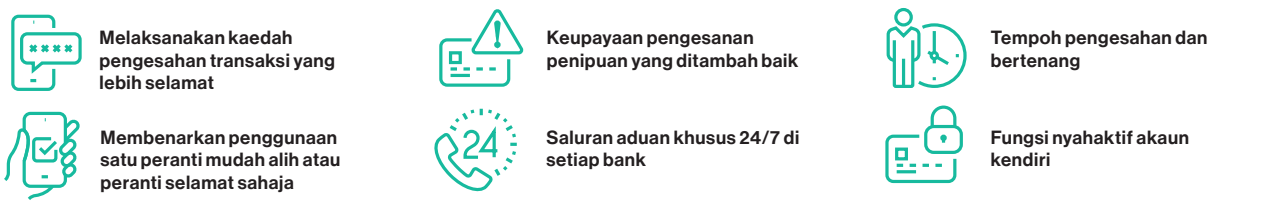
Bagi mengukuhkan lagi daya tahan operasi institusi kewangan, BNM akan memperkenalkan jangkaan yang dipertingkatkan dalam pengurusan risiko siber berkaitan TPSP. Perkara ini termasuk jangkaan terhadap institusi kewangan untuk:

- mendapatkan maklumat yang diperlukan untuk memahami dan mengenal pasti kemungkinan kelemahan yang berkaitan dengan tahap ketersediaan keselamatan siber dan rantaian bekalan TPSP mereka;
- menjalankan ujian bersama secara berkala terhadap pelan kesinambungan perniagaan (*business continuity plan*, BCP) dan pelan pemulihan bencana (*disaster recovery plan*, DRP) dengan TPSP yang penting; dan
- mengenal pasti dan menyediakan TPSP alternatif sebagai sandaran (*redundancy*) dan untuk mengekalkan perkhidmatan perlu (*essential services*) semasa gangguan.

Ujian tekanan IT berkala kekal sebagai langkah penting bagi meningkatkan keupayaan institusi kewangan untuk bertindak balas dan pulih daripada kejadian ekstrem atau kejutan luaran yang berpunca daripada gangguan IT dan serangan siber. Susulan satu tinjauan tematik yang dijalankan oleh BNM baru-baru ini terhadap program ujian tekanan IT bank-bank, BNM telah mengeluarkan panduan berhubung dengan senario tekanan yang lazim dan parameter kejutan minimum untuk ujian tekanan IT bagi menggalakkan ketekalan yang lebih tinggi pada tahap ketelitian ujian tekanan IT yang dijalankan oleh bank-bank. Tinjauan tematik ini juga membolehkan BNM mengenal pasti tindak balas dan tindakan pemulihan yang lazim dalam kalangan bank yang boleh menimbulkan risiko sistemik.

[30] Seperti yang termaktub dalam S10.32 dalam dokumen dasar Pengurusan Risiko dalam Teknologi (Risk Management in Technology, RMiT).

Gambar Rajah 1: Usaha Seluruh Industri untuk Memperkukuh Keselamatan Perbankan dalam Talian



Sumber: Bank Negara Malaysia

Institusi kewangan kekal berwaspada terhadap bentuk penipuan kewangan baharu dan terus memperhalus keupayaan pengesanan penipuan mereka. Penambahbaikan langkah-langkah pencegahan penipuan oleh bank-bank sebagai sebahagian daripada usaha yang lebih luas untuk memperkukuh keseluruhan pertahanan berbilang lapisan keselamatan perbankan dalam talian (Gambar Rajah 1) telah menghasilkan penurunan trend kes transaksi perbankan dalam talian tanpa kebenaran (2022 berbanding 2023: pengurangan 28%) yang telah dilaporkan kepada Pusat Respons Scam Kebangsaan (National Scam Response Center, NSRC). Pada tahun 2023, sebanyak RM383 juta nilai penipuan transaksi kewangan telah berjaya disekat oleh institusi kewangan. Langkah-langkah pencegahan penipuan juga telah diperluas kepada semua EMI yang layak bagi memastikan perlindungan seluruh sektor yang lebih berkesan.

Usaha berterusan dilaksanakan untuk memastikan daya tahan sistem pembayaran dan penyelesaian

Sistem Pemindahan Dana dan Sekuriti Elektronik Masa Nyata (Real-time Electronic Transfer of Funds and Securities System, RENTAS) dan sistem pembayaran runcit (*retail payment systems*, RPS) utama terus mengekalkan ketersediaan sistem yang tinggi sepanjang separuh pertama tahun 2024. Meskipun tiada insiden besar atau gangguan perkhidmatan berlaku pada RENTAS, terdapat gangguan perkhidmatan pada DuitNow di bawah Platform Pembayaran Runcit Masa Nyata (Real-time Retail Payment Platform, RPP) dan pada perkhidmatan cek dalam Sistem Penjelasan Maklumat Cek Elektronik Kebangsaan (National Electronic Cheque Information Clearing System, eSPICK) pada bulan Mei disebabkan oleh kegagalan perkakasan. Kedua-dua perkhidmatan tersebut telah dipulihkan dengan segera berikutan kejayaan pengaktifan pelan luar jangka (*contingency plan*) dan pelan pemulihan yang beroperasi seperti yang dijangka. Tiada insiden berulang yang berlaku.

Sejak 1 Julai 2024, semua peserta RENTAS telah berjaya memindahkan transaksi pembayaran RENTAS mereka kepada standard ISO 20022. Pemindahan ini menandakan selesainya projek yang bermula pada tahun 2019 dalam usaha menyokong pengukuhan infrastruktur pembayaran domestik utama bagi persediaan masa hadapan. Penerapan piawaian penghantaran mesej ISO 20022 membolehkan institusi kewangan mengakses data yang lebih terperinci dan lebih berstruktur, termasuk rujukan pembayaran, butiran invois dan maklumat pengawalseliaan. Dengan maklumat ini, peserta RENTAS boleh menambah baik saringan pematuhan, meningkatkan automasi proses dan menyediakan perkhidmatan pelanggan yang lebih baik. Peserta RENTAS kini memberikan tumpuan pada peralihan ke arah pembayaran rentas sempadan yang dijangka selesai pada bulan Jun 2025 untuk mesej

pembayaran utama, dan bulan November 2026 bagi mesej bukan utama untuk memenuhi garis masa yang ditetapkan oleh SWIFT.[31] Setakat bulan Julai 2024, sekitar 32% peserta telah menyelesaikan perpindahan untuk pembayaran rentas sempadan, dengan baki peserta dijangka menepati jadual untuk memenuhi garis masa yang ditetapkan.

Rangkaian pembayaran rentas sempadan masa nyata serantau antara Malaysia dengan Indonesia, Thailand dan Singapura telah menyumbang kepada peningkatan penggunaan pembayaran kod Respon Pantas (Quick Response, QR) rentas sempadan. Jumlah transaksi pembayaran QR pada enam bulan pertama tahun 2024 sahaja adalah dua kali bilangan transaksi yang dicatatkan bagi keseluruhan tahun 2023. Dengan jumlah transaksi pembayaran yang dijangka terus meningkat, usaha memastikan pengendali sistem pembayaran terus memenuhi spesifikasi teknikal yang ditetapkan secara berterusan akan menjadi sangat penting bagi meminimumkan gangguan perkhidmatan dan meningkatkan keselamatan. Perkara ini dikukuhkan lagi oleh usaha berterusan BNM untuk mempertingkatkan pengaturan pengawasan rentas sempadan secara bersama dengan badan pengawalseliaan di negara masing-masing.

[31] The Society for Worldwide Interbank Financial Telecommunication (SWIFT) merupakan pengendali rangkaian global yang memudahkan transaksi kewangan dan komunikasi yang terjamin antara institusi perbankan dengan institusi kewangan lain.