RISIKO OPERASI

Operasi institusi kewangan kekal berdaya tahan dengan kewaspadaan berterusan terhadap risiko baharu

Operasi institusi kewangan kekal berdaya tahan sepanjang separuh kedua tahun 2025. Kerugian kewangan yang berkaitan meningkat namun kekal rendah iaitu hanya 0.11% daripada jumlah modal sistem perbankan (ST1 2025: 0.04%; ST2 2024: 0.03%). Kerugian ini berpunca terutamanya daripada beberapa kes terpencil melibatkan penipuan luaran dan gangguan sistem, yang telah ditangani menerusi langkah-langkah pembetulan serta pemulihan yang dilaksanakan tepat pada masanya. Pada masa yang sama, institusi kewangan terus memperkukuh sistem dan proses pengurusan risiko operasi mereka melalui pelaburan secara bersasar bagi menangani punca utama serta mempertingkatkan kawalan dalaman.

Pengukuhan daya tahan siber kekal menjadi keutamaan seiring dengan pendigitalan dan penggunaan teknologi dalam sektor kewangan yang semakin pesat. Institusi kewangan terus mengekalkan standard keselamatan siber yang tinggi serta kekal waspada terhadap risiko teknologi dan ancaman siber yang berubah-ubah. Walaupun insiden melibatkan penyedia perkhidmatan pihak ketiga (*third-party service provider*, TPSP) meningkat sedikit berikutan insiden kebocoran data dan gangguan rantaian bekalan pada peringkat global, tiada insiden yang serius atau pencerobohan data secara langsung yang menjejaskan institusi kewangan tempatan dilaporkan.[23] Risiko sistemik akibat kegagalan pihak ketiga kekal rendah berikutan kawalan pengurusan risiko yang lebih ketat oleh institusi kewangan terhadap perkhidmatan pihak ketiga serta penambahbaikan berterusan terhadap pelan tindak balas, pemulihan dan kontingensi bagi risiko berkaitan TPSP.

Institusi kewangan turut memperkukuh tahap kewaspadaan terhadap taktik penipuan yang berubah-ubah. Hasilnya, jumlah penipuan transaksi yang berjaya dibanteras pada tahun 2025 meningkat dengan ketara.[24] Walau bagaimanapun, kes-kes penipuan yang dilaporkan terus meningkat, didorong terutamanya oleh perisian hasad (*malware*) yang semakin canggih yang mampu menjejaskan peranti pelanggan dan membolehkan pemindahan dana tanpa kebenaran. Sebagai tindak balas, BNM dan industri telah mempertingkatkan keupayaan perlindungan untuk peranti mudah alih bagi melindungi platform perbankan mudah alih dan peranti pelanggan daripada perisian hasad serta akses tanpa kebenaran.[25] Bagi melengkapi usaha ini, BNM dan industri kewangan turut memulakan satu pelan perpindahan (*migration*) berstruktur untuk memastikan perkhidmatan perbankan dalam talian beroperasi melalui pelayar laman sesawang dan sistem pengendalian mudah alih yang disokong sahaja. Langkah ini mengurangkan kelemahan keselamatan pada peranti yang tidak lagi menerima kemas kini keselamatan kritikal dan pada masa yang sama mengekalkan keterangkuman kewangan melalui langkah perlindungan tambahan yang wajar.[26]

Berikutan penerbitan dokumen dasar Pengurusan Risiko dalam Teknologi (Risk Management in Technology, RMiT) yang telah disemak semula pada bulan November 2025, institusi kewangan telah melaksanakan keperluan terkini bagi mengukuhkan lagi daya tahan perkhidmatan dan keselamatan siber.[27] Sepanjang tempoh peralihan ini, pihak industri memberikan tumpuan terhadap usaha mengurangkan serta menangani gangguan perkhidmatan dan memperkukuh komunikasi dengan pelanggan semasa berlakunya insiden gangguan perkhidmatan.

Pada separuh kedua tahun 2025, BNM telah melaksanakan semakan bersasar terhadap pelan kesinambungan perniagaan (*business*

[23] Antara insiden besar global melibatkan TPSP pada tahun 2025 ialah pencerobohan data yang menjejaskan persekitaran awan legasi Oracle, iaitu sebuah penyedia perisian pengurusan pangkalan data global, yang menyebabkan kebocoran jutaan rekod berkaitan pengesahan. Satu lagi TPSP iaitu Salesloft juga mengalami kebocoran data yang menyebabkan gangguan rantaian bekalan. Dalam insiden ini, penyerang siber mengeksploitasi integrasi TPSP tersebut dengan aplikasi chatbot jualan yang lazim digunakan bagi memperoleh akses tanpa kebenaran ke beberapa persekitaran awan. Insiden ini menjejaskan beberapa TPSP lain, lantas menjejaskan institusi kewangan yang bergantung pada perkhidmatan mereka.

[24] Pada tahun 2025, bank-bank berjaya membanteras kira-kira RM1.2 bilion penipuan transaksi berbanding dengan RM399 juta pada tahun 2024.

[25] Langkah-langkah ini termasuk pengesanan perisian hasad secara lanjut, penyekatan aplikasi berisiko, penguatkuasaan penggunaan peranti dan sistem pengendalian yang disokong, kemas kini keselamatan secara berkala serta pemeriksaan integriti sesebuah peranti.

[26] Apabila peranti pelanggan tidak dapat menyokong sistem pengendalian yang diperlukan, institusi kewangan perlu meningkatkan pemantauan terhadap pengguna peranti berkenaan, memperkukuh langkah-langkah membanteras perisian hasad dan melaksanakan sekatan fungsi yang wajar bagi mengurangkan risiko keselamatan.

[27] Keperluan ini merangkumi penetapan sasaran ketersediaan perkhidmatan yang dipertingkatkan bagi memenuhi jangkaan pelanggan yang lebih tinggi, pengurusan proaktif terhadap isu prestasi yang bersifat sementara (*intermittent*), pengukuhan penyelarasan dengan TPSP untuk memastikan tindak balas insiden yang berkesan serta mewujudkan protokol komunikasi bagi memastikan pelanggan dimaklumkan dan disokong secara berterusan apabila menghadapi gangguan perkhidmatan.

continuity plan, BCP) institusi kewangan untuk perkhidmatan penting yang melibatkan interaksi dengan pelanggan. Semakan ini menilai kewajaran langkah-langkah penyelesaian sementara dalam menangani kesan gangguan operasi dan memastikan kesinambungan perkhidmatan kepada pelanggan. Walaupun penilaian terhadap pengaturan pelan tersebut secara keseluruhannya didapati memadai, beberapa aspek yang memerlukan penambahbaikan telah dikenal pasti, antaranya:

- membangunkan dan mengukuhkan keupayaan pemulihan, khususnya melalui proses memodenkan sistem perbankan teras untuk memenuhi jangkaan orang ramai yang semakin tinggi terhadap ketersediaan perkhidmatan;
- mempertingkatkan tadbir urus dalaman serta melaksanakan pengurusan tindakan akibat kegagalan bagi mengukuhkan akauntabiliti serta memupuk budaya daya tahan operasi yang mantap;
- mempergiat usaha untuk mengenal pasti titik kegagalan tunggal, khususnya dalam perbankan dalam talian, Mesin Juruwang Automatik (Automated Teller Machines, ATM) dan pusat panggilan, berikutan peningkatan kebergantungan yang semakin rumit serta potensi implikasi sistemik; dan
- melaksanakan ujian BCP yang lebih menyeluruh bersama TPSP penting bagi menjamin kesinambungan perkhidmatan kewangan utama apabila berlakunya gangguan.

Beberapa bank tempatan utama telah mengambil langkah-langkah proaktif untuk memperkukuh kesiapsiagaan krisis dengan membangunkan BCP yang khusus mengikut senario bagi menghadapi insiden seperti pencerobohan keselamatan siber, gangguan bekalan elektrik serta kegagalan infrastruktur teknologi maklumat (IT) penting. Usaha ini disokong oleh proses pelaporan dan tindakan yang berstruktur dengan tempoh masa yang ditetapkan secara jelas bagi mengurangkan kelewatan dalam penyelesaian insiden.

Melangkah ke tahun 2026, risiko siber kekal sebagai keutamaan bagi institusi kewangan berikutan ancaman siber yang semakin canggih serta kesan terhadap aspek operasi, prestasi kewangan serta reputasi.[28] Industri turut mengenal pasti risiko strategik dan organisasi sebagai risiko operasi utama berikutan perubahan model perniagaan dalam memenuhi keperluan pelanggan, persaingan yang lebih tinggi untuk mendapatkan tenaga kerja penting serta inovasi teknologi yang semakin pesat. Di samping itu, pematuhan pengawalseliaan kekal sebagai tumpuan utama bagi menyokong daya tahan institusi. Risiko operasi penting lain yang dikenal pasti bagi tahun 2026 termasuk gangguan IT, potensi kegagalan pelaksanaan akibat kesilapan manusia serta risiko yang berkaitan dengan peningkatan kebergantungan terhadap penyedia perkhidmatan luar (Gambar Rajah 1.1).

Memandangkan pentingnya institusi kewangan untuk mampu menghadapi gangguan yang berpotensi berlaku serta memastikan kesinambungan perkhidmatan kewangan, BNM telah menerbitkan Discussion Paper on Operational Resilience pada bulan Disember 2025 yang menggariskan pertimbangan pengawalseliaan utama dalam menentukan ketersediaan dan amalan daya tahan operasi sesebuah institusi kewangan. Kertas perbincangan ini menekankan keperluan bagi institusi kewangan mengekalkan keupayaan pengurusan risiko operasi yang mantap, disokong oleh teknologi dan pertahanan siber yang berdaya tahan dalam menangani serta mengawal gangguan dengan berkesan. Kertas perbincangan ini turut menggariskan kepentingan tadbir urus dan mekanisme akauntabiliti yang kukuh, dengan lembaga pengarah institusi kewangan berperanan mendorong hasil daya tahan operasi yang nyata dan mampan.

Pelbagai inisiatif utama sedang dijalankan untuk memastikan sistem pembayaran dan penyelesaian terus berdaya tahan.

Sistem Pemindahan Dana dan Sekuriti Secara Elektronik Masa Nyata (Real-time Electronic Transfer of Funds and Securities System, RENTAS) dan sistem pembayaran runcit (*retail payment systems*, RPS) utama kekal berdaya tahan dan mengekalkan tahap ketersediaan sistem yang tinggi pada separuh kedua tahun 2025, dengan beberapa insiden terpencil segera ditangani. Di samping pemantauan berterusan terhadap infrastruktur pembayaran utama, BNM telah melaksanakan semakan penyeliaan bersasar terhadap penyedia perkhidmatan pembayaran terpilih untuk menilai kecukupan dan keteguhan kawalan insiden penipuan,[29] keberkesanan pengurusan risiko IT dan siber serta kekukuhan amalan tatakelakuan. Semakan menunjukkan bahawa penyedia

[28] Berdasarkan Emerging Operational Risk Survey 2025/2026 yang dilaksanakan oleh BNM.

[29] Kawalan ini termasuk pelaksanaan lima langkah pencegahan penipuan utama yang dikehendaki oleh BNM untuk pengeluar wang elektronik yang layak, berkuat kuasa bulan Januari 2025. Langkah-langkah ini merangkumi pengesahan berbilang faktor yang kukuh, tempoh bertenang (*cooling-off*), pengesahan melalui satu peranti selamat, suis pemati (*kill switch*), serta penubuhan saluran aduan yang beroperasi selama 24 jam.

Gambar Rajah 1.1: Risiko Operasi Utama dan Tindakan Mitigasi



Keselamatan maklumat & risiko siber

- Penggunaan kawalan keselamatan siber utama seperti Pengesahan Pelbagai Faktor (*multi-factor authentication,* MFA), Pengurusan Akses Istimewa (Privileged Access Management, PAM), Pengesanan & Tindak Balas Titik Akhir (Endpoint Detection & Response, EDR) dan platform risikan ancaman bersepadu untuk meningkatkan ketahanan siber.
- Program kesedaran siber secara berkala termasuk simulasi pancingan data (*phishing*) untuk mengukuhkan kesediaan kakitangan.
- Prosedur tindak balas insiden yang dipertingkatkan, termasuk protokol pemakluman, komunikasi dan penyelesaian.



Pematuhan kawal selia & risiko ketelusan

- Analisis jurang kawal selia dan penilaian impak secara berkala untuk mengenal pasti jurang kawalan dan dasar.
- Latihan pematuhan yang bersasar untuk kakitangan yang selaras dengan keperluan kawal selia.
- Memperkukuh tadbir urus melalui pasukan petugas pematuhan, pengakusaksian formal dan libat urus kawal selia yang berterusan.



Risiko strategi/organisasi

- Keupayaan tenaga kerja dan kepimpinan yang selaras dengan keutamaan strategik yang berubah-ubah melalui penandaarasan, pembelajaran berterusan dan pembangunan kepimpinan.
- Pemodenan teknologi dan model operasi untuk menyokong transformasi perniagaan dan keperluan pelanggan yang berubah-ubah.
- Tadbir urus yang kukuh dan pengawasan bersilang fungsi terhadap perubahan dan pengurusan risiko seluruh perusahaan.



Risiko gangguan IT

- Penambahbaikan infrastruktur termasuk pelaksanaan pelbagai pusat data yang beroperasi sepenuhnya untuk meningkatkan ketersediaan dan daya tahan sistem.
- Pengujian pelan kesinambungan perniagaan/pelan pemulihan bencana (*business continuity plan/disaster recovery plan,* BCP/DRP) secara berkala untuk mengesahkan kesediaan pemulihan.
- Penggunaan seni bina berasaskan awan terkini yang membolehkan peluasan secara automatik, kemas kini sistem yang terkawal dan keselamatan yang telah diterapkan untuk meningkatkan kestabilan sistem.



Risiko kegagalan pelaksanaan & proses

- Semakan prosedur operasi standard (*standard operating procedure*, SOP) dan latihan kakitangan yang besasar secara berkala untuk mengurangkan kesilapan manusia dan kegagalan proses dalam operasi harian.
- Jaminan kualiti yang dipertingkatkan dan penggunaan alat analitik untuk mengesan isu sistemik.



Risiko pihak ketiga & penyumberan luar

- Pemantauan vendor yang dipertingkat melalui penunjuk prestasi utama (*key performance indicator,* KPI) dan pengesanan isu.
- Perlindungan kontrak yang lebih kukuh meliputi tahap perkhidmatan, penamatan dan strategi keluar.
- BCP dan pelan kontingensi untuk mengurangkan gangguan daripada kegagalan vendor, dengan komunikasi krisis yang diperkukuh semasa gangguan perkhidmatan.
- Ujian BCP secara bersama dengan penyedia perkhidmatan pihak ketiga (*third-party service provider*, TPSP) yang penting.

Sumber: Bank Negara Malaysia

perkhidmatan pembayaran di bawah kawal selia mengambil langkah-langkah proaktif untuk memperkukuh usaha pencegahan penipuan dan mematuhi keperluan pematuhan. Meskipun langkah pengurusan risiko IT dan siber serta amalan tatakelakuan secara keseluruhan dinilai mencukupi, keberkesanan fungsi tadbir urus dan pengawasan ke atas aspek-aspek ini boleh terus dipertingkatkan. Tindakan pemulihan yang diambil berikutan semakan penyeliaan telah meningkatkan tahap pematuhan, mengurangkan risiko operasi serta memperkukuh kecekapan dan kebolehpercayaan terhadap perkhidmatan pembayaran.

Seiring dengan peningkatan penggunaan transaksi e-pembayaran, pengurusan risiko kredit dan penyelesaian yang berkaitan dengan pembayaran runcit masa nyata menjadi semakin penting.

Bagi menangani risiko penyelesaian antara bank yang wujud dalam model penyelesaian bersih tertangguh (*deferred net settlement*), BNM telah memperkenalkan penyelesaian secara hampir masa nyata (*near real-time settlement*) bagi transaksi Platform Pembayaran Runcit Masa Nyata (Real-time Retail Payments Platform, RPP) melalui pelancaran RENTAS+ pada hujung bulan September 2025. Dengan ini, transaksi RPP diselesaikan melalui penyelesaian kasar secara hampir masa nyata, lantas mengurangkan dengan ketara risiko kredit dan penyelesaian antara bank dan pada masa yang sama memperkukuh keyakinan terhadap sistem pembayaran. Maklumat lanjut mengenai RENTAS+ boleh didapati dalam bab ‘‘Menggalakkan Perkhidmatan Pembayaran dan Pengiriman Wang yang Selamat dan Cekap’’ dalam Laporan Tahunan BNM 2025.