Strategic Thrust 3
Advance digitalisation of the financial sector

Digitalisation continues to have widespread implications for financial services. Customers are expecting faster, more frictionless, and more customised services, with growing awareness about the importance of data privacy and security. Digital business models are also becoming more ecosystem-driven, whether through a platform or a network of partnerships. Alongside this, the risk landscape is also being reshaped. Boundaries are blurring, with new and more complex interlinkages within and beyond the financial sector. The key will be for Malaysia's financial industry to take advantage of the upsides of digitalisation, while managing the associated risks – especially those that may threaten system-wide stability, consumer outcomes, and confidence in the financial sector.

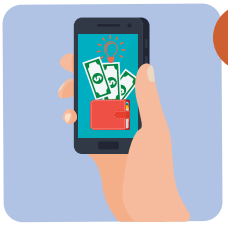
To this end, we will advance four key strategies (Diagram 1).

Diagram 1:
Advance digitalisation of the financial sector

A

Futureproof key digital infrastructures

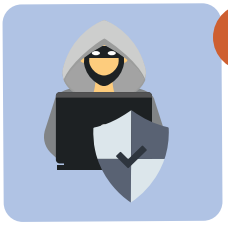
- Leverage key financial infrastructures for Malaysia's broader digital ecosystem
- Advance development of an open data ecosystem that is fair and fit for the future



B

Support a more vibrant digital financial services landscape

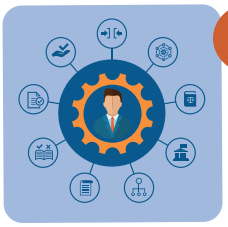
- Enhance pathways for digital innovations to test, scale and exit
- Support industry-led strategies for digital payments adoption
- Preserve effective oversight of digital business models



C

Strengthen cyber security readiness and responsiveness

- Strengthen system-wide cyber security oversight and capabilities
- Strengthen domestic and global collaborative efforts on cyber security



D

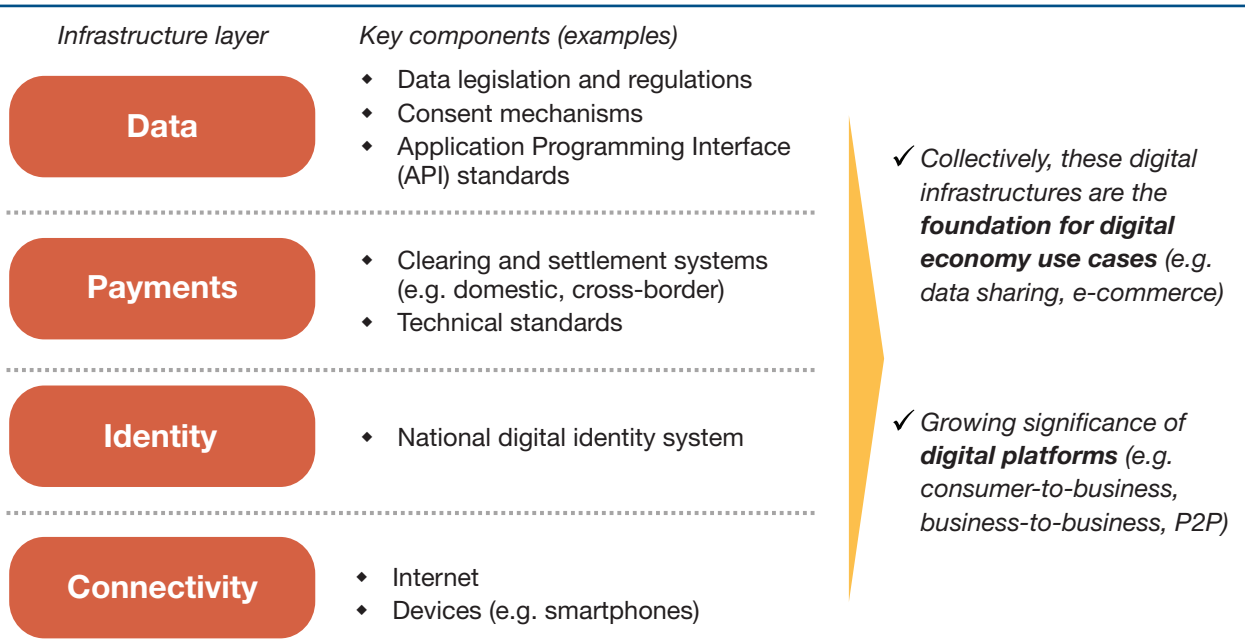
Support greater use of technology for regulation and supervision

- Leverage technology to further strengthen the Bank's regulation and supervision of the financial industry
- Futureproof the Bank's data strategy

Strategy 3A
Futureproof key digital infrastructures

A digital economy is built upon a combination of technological infrastructures (Diagram 2). Financial infrastructures are a vital part of that. Payment and settlement systems, for example, enable day-to-day economic activities of households and businesses. As more transactions move to the digital sphere, so does data – and the vast potential and risks that come with it.

Diagram 2:
Key infrastructure layers in the digital economy



Our strategies to futureproof key financial infrastructures will be anchored on several desired outcomes. First, these infrastructures should be resilient, particularly to enable a secure ecosystem and preserve the continuity of critical services in adverse situations. Second, these infrastructures should be inclusive – designed to promote openness and interoperability, reflecting the increasingly diverse profile of stakeholders in the financial landscape, without compromising the safety of the system. Third, these infrastructures should be adaptable to emerging developments, including new technologies and operating models.

Broader digital infrastructures, including non-financial ones, are also equally important for financial development objectives. Similar outcomes like resilience, inclusivity, and adaptability should also guide the development of these infrastructures. Connectivity and digital identity are some key examples that support greater innovation and adoption of digital financial services. It will also be important to leverage emerging digital platforms to unlock major upsides for the financial sector and broader economy.

For the data ecosystem, we will look to advance efforts that can better serve financial consumers. These include policies and safeguards that support responsible and ethical usage of data, as well as facilitate fair and reciprocal data sharing initiatives among participants in Malaysia's data ecosystem. These efforts will be reinforced by collaborative initiatives with the Government to accelerate the roll-out and enhancements of these broader infrastructures.

To this end, we will:

i. Leverage key financial infrastructures for Malaysia's broader digital ecosystem; and
ii. Advance the development of an open data ecosystem that is fit for the future.

i Leverage key financial infrastructures for Malaysia's broader digital ecosystem

- We will aim to **futureproof Malaysia's payment systems – particularly real-time payment infrastructures**, including real-time gross settlement systems and retail payment systems, focusing on three areas:

  - **A multi-year modernisation exercise for the Real-Time Electronic Transfer of Funds and Securities Settlement (RENTAS)**. As part of this exercise, we will review the RENTAS access model to cater for more diverse participation – including by non-bank payment service providers (PSPs), without compromising the operational and cyber resilience of RENTAS. Besides levelling the playing field between banks and non-bank PSPs, this would expand the range of transactions settled using central bank money – in turn, potentially lowering settlement risk in the ecosystem. The modernisation exercise will also include initiatives to strengthen the end-to-end risk management in RENTAS, promote interoperability and efficiency, facilitate competition and innovation, as well as to enhance user functionalities (see Diagram 3 for summary).

> We will review the RENTAS access model to cater for more diverse participation, including by non-bank payment service providers

  - Enabling **shared payment infrastructures** in Malaysia's payments ecosystem, including the RPP. These infrastructures allow industry players to pool resources and share costs, while competing at the product level to better serve end-users, such as consumers and merchants. A key priority will be to preserve and ensure effective implementation of open and risk-based access regimes for banks and non-bank PSPs – whether through direct or indirect participation regimes[1].

  Other areas of focus include facilitating the adoption of common technical standards (e.g. ISO 20022, DuitNow QR), and exploring opportunities to leverage on shared payment infrastructures for more use cases (e.g. welfare payments, tax refunds, fraud analytics, trade finance).

Diagram 3:
Key objectives of RENTAS modernisation exercise

Strengthen resilience
- Review system infrastructure holistically, including to reinforce protection against cyber threats and enable flexible infrastructure to accommodate future needs

Promote interoperability and efficiency
- Promote alignment with international standards (e.g. industry-wide adoption of International Organisation for Standardisation (ISO) 20022 by mid-2024, via a phased approach)

Enable competition and innovation
- Review RENTAS access model to cater for more diverse participation arrangements
- Explore potential central bank digital currencies (CBDC) and distributed ledger technology (DLT) applications for RENTAS

Enhance user functionality
- Facilitate enhanced real-time reporting and monitoring capabilities, and develop better tools for analytics under RENTAS iLINK*
- Explore use of API interface to replace existing access channels for RENTAS

* *RENTAS iLINK is a web-based system in RENTAS that provides real-time information to participants such as cash position, securities holdings and settlement status.*

[1] Indirect participation regimes are where a non-bank payment service provider relies on an intermediary (also known as a 'sponsor institution') to indirectly join the network of a shared payment infrastructure. Some PSPs may prefer the indirect participation regime due to specific commercial or operational needs.

- **Intensifying efforts to enhance cross-border payments efficiency**. We will work with industry players to address challenges associated with cross-border payments, such as high costs, low speed, limited access, and insufficient transparency. This includes linking up the RPP with other real-time payment systems in the Association of Southeast Asian Nations (ASEAN) region and beyond, focusing on countries with strong economic linkages with Malaysia. We will build on the recently established QR payment linkages with Thailand and Indonesia and the ongoing work with Singapore and the Philippines. The goal will be to expand the scope of use cases to P2P fund transfers as well as to establish similar linkages with other countries in the region and beyond. Beyond this region, we are also working on a proof-of-concept (POC) with the Bank for International Settlements (BIS) Innovation Hub and other partners in Project Nexus to develop a multilateral and scalable mode, which aims to connect all real-time payment systems globally to facilitate fast and seamless cross-border payments.

  In addition to real-time payment linkages, we will **explore emerging payment innovations for cross-border payments**, such as the use of multi-CBDC arrangements. Unlike existing correspondent banking arrangements, the use of CBDC could shorten the transaction chain and free up liquidity that is 'trapped' in correspondent banking accounts – thus resulting in faster and cheaper cross-border payments. We will be embarking on collaborative initiatives in this regard. This includes building on findings from our participation in Project Dunbar, where we have partnered with the BIS Innovation Hub and other central banks – namely, Reserve Bank of Australia, Monetary Authority of Singapore, and South African Reserve Bank – to test the use of multiple CBDC and DLT for cross-border settlements.

- We will **intensify research and experimentation on the use of central bank digital currencies** for Malaysia's monetary and financial infrastructures – with the initial focus on wholesale payments – as part of broader efforts to respond to digital currency developments (refer to the box article "Digital currencies: A new frontier").

- The effective delivery of digital financial services also hinges on the **availability of common, non-financial digital infrastructures that support all sectors of the economy**. To this end, there are three key areas that we will continue to pursue in cooperation with the Government and relevant agencies:

  - **The establishment of a national digital identity,** which requires a coordinated collaboration between different government agencies and the private sector. We will continue to advocate for speedy and effective implementation, to cater to both existing and future needs (particularly in relation to the choice of technology for authentication).

  - Legislative and regulatory reforms to facilitate end-to-end digitalisation of business processes, such as **the use of digital and electronic signatures** by the both private and public sectors.

  - Speed, quality, and affordability of **internet connectivity** across the country and segments of society. This in turn will facilitate greater accessibility and usage of digital financial services, especially among the underserved and unserved segments as well as those in the rural areas.

Common digital infrastructures at the national level are critical to facilitate end-to-end digitalisation of the value chain

ii Advance the development of an open data ecosystem that is fit for the future

- We will continue to **facilitate efforts to develop common standards for data sharing in the financial sector, particularly for high-impact use cases**. Therefore, we aim to focus efforts on use cases that:

  - Promote greater **financial inclusion**. These include facilitating new data sharing arrangements, such as on "thin file" consumers – namely, those with little or no credit history – to enable the development of alternative credit scoring models. This aims to make use of alternative forms of data such as payments or utilities data, which can help enrich the creditworthiness assessment.

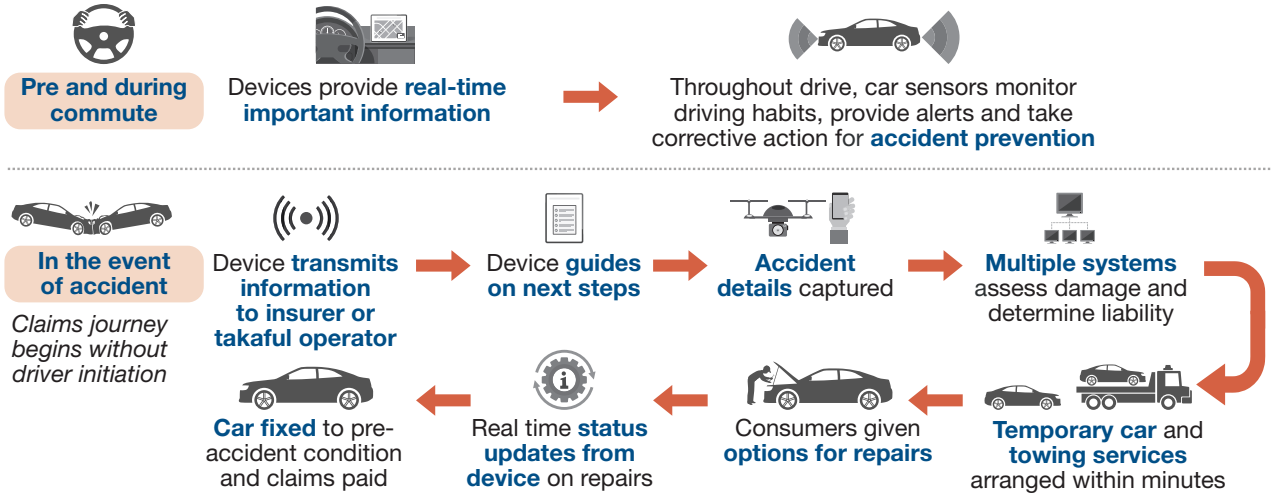
  - Support consumers to make **better informed financial decisions**, such as through financial planning. These include personal financial management solutions, providing better quality information to consumers, and nudging consumers towards better financial behaviour (such as encouraging habits in relation to savings and investments).

  Where specific use cases have been identified by the industry, we will work closely with the relevant stakeholders on the development of common data standards and suitable data sharing arrangements – with the view to provide guidance on policy and regulation, where appropriate. A market-led approach will generally be preferred to provide industry players with sufficient space to test and iterate, before converging on standards that are fit-for-purpose. However, we may consider establishing mandates to accelerate progress, where warranted, to serve the broader public interest in line with the Bank's regulatory objectives.

- We will **support efforts to establish shared data infrastructures for the financial sector and its broader value chain**. This would include emerging digital platforms that enable more seamless and efficient connections among various users. As with other key digital infrastructures, our priority will be to promote the adoption of open and interoperable design principles. Examples of these infrastructures include trade finance infrastructures (e.g. for detection of duplicate invoicing), a medical claims data exchange (e.g. for costs of common medical procedures) that is accessible by industry players, as well as modernised systems that enable an end-to-end digital experience for motor claims.

  For insurance and takaful services in particular, digitalisation is a key game changer that will bring the current level of services to new heights – especially to create a hassle-free experience for consumers making motor claims, and address prevailing pain points in the process. To this end, we will intensify efforts to pave the way for insurers and takaful operators to advance digital transformation efforts that will deliver more integrated, transparent, and seamless processes (see Diagram 4 for desired outcomes for the motor ecosystem). This includes establishing and improving existing infrastructure to support the adoption of digital technologies across the claims process. This is a necessary precondition for the full liberalisation of motor tariffs.

Diagram 4:
Digitalisation - A game changer for consumers' claims experience



- We will **continuously review the data governance framework for the financial sector**, in tandem with legal developments and technological applications to ensure the protection and fair treatment of financial consumers. This includes potential enhancements to customer consent mechanisms and requirements around the ethical and responsible usage of data – which are key elements in building a trusted data regime. We expect FSPs to collect, process, and share personal consumer data in a lawful and secure manner such that individuals know how their data will be used and give consent to such usage. Data must also be used in ways that do not result in the unfair treatment of consumers.

- Beyond the financial industry, we will continue to collaborate with industry players and other stakeholders to **enable broader arrangements for more open and secure data sharing, focused on three priorities**:

  - **Improving accessibility to public data** under the Government's open data initiatives. These initiatives, such as the Malaysian Administrative Modernisation and Management Planning Unit's (MAMPU) Open Data platform, provide the potential for various stakeholders – including the financial sector – to leverage datasets residing in other agencies to build data-driven innovations to better serve the public. To make data sharing more seamless, it will be important to synchronise key reforms discussed in flagship policy documents (e.g. RMK12, MyDigital) and develop a uniform approach to data governance. This in turn will provide the necessary foundations for the adoption of interoperable standards and formats across sectors.

  - **Supporting national efforts to develop a data protection legal framework**. Primarily, we will do this through our membership in national-level committees. We will also collaborate with government agencies in relation to key laws and policies, such as on the drafting of NDSP and amendments to the Personal Data Protection Act 2010 (PDPA). The implementation of both NDSP and amended PDPA will strengthen the confidence and trust of data users to facilitate greater data sharing in the digital economy as a whole.

  - **Supporting regional level data sharing initiatives**. To this end, we will continue to collaborate with government agencies and industry players to advance best practices with respect to cross-border data flows that are aligned with global standards and policies. Key focus areas include managing cross-border fraud and money laundering, support risk management practices of internationally active financial institutions, as well as promote trade activities, including within the ASEAN region.

Strategy 3B
Support a more vibrant digital financial services landscape

Technological changes have taken place at an unprecedented pace in recent years, enabling new applications in financial services. The pandemic has only accelerated this, as customers sought to access 'low-touch' or completely digital channels – in turn, shaping behavioural norms for financial services.

New technologies can redefine the landscape, pushing the boundaries of what is technically and operationally possible. Efforts need to be centred on keeping pace and responding effectively to technology.

Our strategies on this front will aim to foster an enabling environment for innovation, while preserving broader financial system stability. We will also prioritise strengthening institutional arrangements to facilitate greater collaboration – among industry players, regulators, and other agencies.

To this end, we will seek to advance the following:

i. Enhance pathways for digital innovations to test, scale, and exit;
ii. Support industry-led strategies for digital payments adoption; and
iii. Preserve effective oversight of evolving digital business models.

i Enhance pathways for digital innovations to test, scale and exit

- We will enhance testing mechanisms for financial innovation in two key ways.

  First, we will **refresh our Regulatory Sandbox**. The Sandbox has played an important role in advancing digital innovation so far, paving the way for critical use cases such as electronic Know-Your-Customer (e-KYC) and new business models such as digital insurers, P2P family takaful and digital remittance. The Sandbox will continue to support industry players in bringing financial innovations safely to the market, across different stages of the innovation cycle.

  Enhancements moving forward will aim to accelerate time-to-live testing under the Sandbox. For late-stage or more mature innovative solutions, this may include accelerated tracks for lower-risk activities or simplified testing parameters for players who can demonstrate robust governance and risk management practices. In particular, for financial institutions that we already regulate, we will simplify and reduce the Sandbox's gatekeeping processes to test new value propositions and address regulatory implications. This will aim to allow financial institutions to test their innovations more quickly and flexibly, supplemented with principles-based testing parameters.

  Drawing from our experience with a specialised e-KYC testing track, we will also consider similar accelerated tracks for other relevant use cases. This would cover activities where the risks are low or can be managed within standardised and pre-determined boundaries, or where development of relevant policies is already underway. Such activities include insurance and takaful aggregation activities.

  Second, we will look to **advance 'collaborative pilot' mechanisms** for areas where digital transformation is needed at the industry or national level. This is relevant for financial innovations that are multi-stakeholder in nature – whereby testing and iteration across the value chain is needed to pave the way towards viable business models and arrangements for the industry. These include efforts to establish shared utilities or platforms, promoting common standards, or piloting new industry use cases.

  Previously, we have adopted a collaborative approach in promoting common open API standards and developing Project Spyder[2] a DLT-based trade finance solution. In addition to continuing such efforts, we will also seek to advance efforts towards establishing shared digital infrastructures for insurance and takaful solutions, as set out in Strategy 3A(ii) of this chapter.

[2] Project Spyder is a proof-of-concept developed in 2019 between the Bank and an industry consortium of leading Malaysian banks to detect duplication of invoice financing and to enable interbank sharing of invoice information in a secure manner. The testing phase of Project Spyder concluded in November 2019, in which more than 1,700 duplicate invoices were detected from over 290,000 invoices submitted from participating banks.

- We will f**acilitate greater digitalisation of business models in financial services**, prioritising those that can advance greater financial inclusion by better meeting the needs of the unserved and underserved (refer to the chapter "Elevate the financial well-being of households and businesses").

  A key priority will be the **smooth implementation of the digital banking** framework. We are committed to ensure that the policy environment remains relevant, as digital banks and incumbents continue to evolve their business models (e.g. through greater partnerships with other FSPs or third parties) to create an ecosystem that will better address underserved and unserved segments, without jeopardising system-wide stability and consumer outcomes. A key consideration will be to foster an appropriate regulatory environment for all players engaged in banking services – be it through traditional or digital channels, consistent with the principles of parity, proportionality and neutrality (refer to Strategy 3B(iii) in this chapter).

  Additionally, we will **finalise a regulatory framework for digital insurers and digital takaful operators in 2022**, with the view to significantly elevate the dynamism of the sector. We aim to license new digital players in 2023 that can leverage technologies to deliver value propositions on three fronts. First, inclusion – to enhance the financial resilience of customers whose protection needs are not adequately served. Second, competition – to transform the existing market structure of insurance/takaful through innovative solutions. Third, efficiency – to deliver a more frictionless consumer experience and protection at lower costs.

- We will continue to **advocate and support the growth potential of Malaysia's broader fintech ecosystem**. In addition to broader digital infrastructures (refer to Strategy 3A in this chapter), we will also aim to seamlessly integrate our frameworks – such as the Sandbox – with other initiatives, both at industry and national level. This will aim to establish an extensive network of key stakeholders that can connect fintech start-ups to a comprehensive suite of support facilities, ranging from capacity-building resources to market access opportunities. This will build on various existing initiatives available, including those under the Malaysia Digital Economy Corporation (MDEC) and the newly formed Malaysian Research Accelerator for Technology and Innovation (MRANTI).

ii Support industry-led strategies for digital payments adoption

- Considering the trajectory of Malaysia's retail payment services landscape, we will **advance an industry-led approach to digital payments development**. Digital payments adoption has risen significantly in Malaysia, accelerated further by the recent pandemic. While regulatory efforts over the past decade have helped catalyse the progress so far, the retail payments industry is also maturing. In more recent years, we have observed the industry becoming highly competitive – especially with the entry of new players – resulting in cheaper and more innovative services to merchants, including SMEs. New consumer-facing technologies, such as biometrics and wearables, have also made digital payments more convenient. Against this backdrop, we expect industry efforts to sustain the momentum of digital payments adoption, as we play an enabling role.

  - As Malaysia's broader economy becomes more digitalised, the importance of payment system operators (PSOs), such as the Payments Network Sdn. Bhd. (PayNet), Visa and Mastercard, to system-wide stability will also intensify – along with growing commercial interest to be PSOs in Malaysia. Given this, we will **advance regulations for PSOs**, which will clarify and align expectations in areas such as governance, risk management, operational resilience, and transparency.

  - We will also **review existing regulatory policies on digital payments**, to ensure their continued relevance. These include the e-Payment Incentive Fund Framework (ePIF), Payment Card Reform Framework (PCRF), and the Interoperable Credit Transfer Framework (ICTF).

  - Efforts will also be made to **pave the way for greater industry leadership and market dynamism in relation to the shareholding of PayNet**. Consistent with PayNet's role as a shared payment infrastructure operator, its shareholding composition will be enhanced to be more reflective of the growing diversity in Malaysia's payments landscape – with the Bank progressively divesting its share in PayNet over time.

- We are **supportive of the broader national aspirations for digital payments under MyDigital.** We expect the commitment by federal and state agencies to adopt cashless payments to play a pivotal role in creating behavioural shifts towards greater digital payments adoption. We are committed to supporting these national aspirations and will intensify our awareness-building strategies to that end.

iii Preserve effective oversight of evolving digital business models

- We will **continuously refine and adapt financial sector policies on digital business models** to ensure that risks are managed effectively. Digital innovation is constantly evolving, shaped by technological change and commercial breakthroughs. In overseeing such a landscape, we will be guided by a set of key considerations to determine the way we regulate digital financial services (Diagram 5):

Diagram 5:
Our approach to regulating innovation

- We aim to **preserve parity, proportionality, and neutrality**. This means that same types of risks will be regulated the same way ('parity') – but with its rigour and intensity calibrated in a way that is commensurate with the level of risk ('proportionality').

  In implementing proportionate regulations, we will consider the nature of risks and public interests. For example, in the area of cyber security, especially where it concerns critical financial services, the same rigour of requirements may be warranted for all players to address 'weakest link' risks in the financial value chain – such as where activities are connected to one another across firms or infrastructures (refer to Strategy 3C in this chapter). Similarly, universal consumer redress mechanisms for financial services will continue to be preserved for all financial consumers, irrespective of the size or complexity of the FSP.

  We are agnostic to different technologies, systems and approaches ('neutrality'). However, we expect industry players to demonstrate that risks associated with a particular technology or innovation are well-understood, and adequately managed.

  Collectively, we expect these to foster a level playing field, while ensuring that digital innovations are supported by sound risk management.

- We will **continue to adopt a combination of activity- and entity-based regulations**[3]. A purely activity-based approach can be suitable for circumstances where the risks are simpler and relatively insulated. That is, where frictions from adverse events – such as a business failure or temporary service interruption – will not have significant spill-over effects on the financial system or economy. We will adopt activity-based regulations with two key priorities. First, to ensure reasonable protection of sound consumer outcomes, such as through clear disclosures, dispute resolution and redress mechanisms. Second, to mitigate regulatory arbitrage, such that different businesses carrying out the same services are subject to the same rules.

  Entity-based regulations are appropriate where certain activities – when combined as part of a business model – can give rise to a more complex risk profile, as well as interdependencies that can amplify market-wide disruptions. This can arise in business models that combine a range of different activities that build an existing ecosystem or platform – sometimes described as 'embedded finance'. In these circumstances, entities may be subject to a comprehensive set of prudential expectations, including those on governance, risk management, financial capacity to absorb losses, and disclosures. Entities that pose systemic risks to the financial system may also be required to develop actionable recovery and resolution plans to protect critical financial services. Our licensing approach for digital banks reflects an entity-based approach, guided by our assessment of the underlying risks of the banking business.

  We will also **intensify our focus on business continuity and resolution frameworks**. A more competitive and innovative market can mean dealing with greater unknowns and more dynamic changes in the financial landscape – which may include a higher turnover of entities within the financial services industry. Our objective will be to ensure that financial services activities can be unwound in an orderly fashion without adversely affecting system-wide stability, while safeguarding consumer outcomes. At the same time, we will also focus on strengthening the credibility of financial institutions' business continuity plans to ensure that they adequately reflect changing operational configurations as well as increasing interdependencies on third parties and shared infrastructures.

- We will **continuously develop and refine our regulatory guidance on critical digital enablers** – such as the use of cloud, AI and ML. The focus will be to better align expectations among industry players to ensure the sound management of risks and fair treatment of consumers. We will also seek to address undue regulatory frictions or inefficiencies, if any – including in our supervisory processes – to support greater agility by financial institutions in adopting these technologies (refer to the box article "Medium-term priorities for the prudential framework and AML/CFT").

[3] Activity-based rules consist of requirements to be met by any institution offering a given service (e.g. lending, payment services). Entity-based rules consist of requirements imposed on institutions with a specific licence or charter, which in turn sets out the activities those entities are allowed to undertake.

- We will **enhance inter-agency cooperation to better oversee emerging non-bank business models**, focusing on two areas:
  - Economic sectors that are increasingly linked to financial services (such as telecommunications and e-commerce); and
  - Regulatory mandates that are closely intertwined with monetary and financial stability within the sphere of digital finance – particularly competition, data protection, and privacy.

  This approach reflects the growing prevalence of digital financial ecosystems (e.g. emergence of digital lenders, cross-selling of financial products by e-wallet operators, potential partnerships between banks or insurers with other technology-based service providers).

  In enhancing these arrangements, our priorities will be to support the timely identification, monitoring, and mitigation of risks in the overall financial value chain to financial stability and consumer outcomes. Given the potentially rapid pace at which digital models may scale, we will also work closely with the relevant authorities on timely information-sharing and intervention arrangements.

Strategy 3C

Strengthen cyber security readiness and responsiveness

Malaysia's financial sector is increasingly part of a broader network of digital relationships – with third party service providers (TPSPs), other financial institutions, and devices. As cross-border and global supply chain linkages deepen, so will new interdependencies and potential blind spots. In these networks, each of the nodes is a possible target. Unlike most operational risks, cyber security breaches in one node can quickly propagate to others in a short period. The cyber security strength of any single 'node' or institution is therefore only as strong as the weakest link in that network.

With the continued digitalisation of financial services in Malaysia, cyber security is arguably one of the biggest risks. The same digital ecosystems that accelerate innovation – and all its upsides to consumers and businesses – also bring risks and vulnerabilities for the financial sector. These include operational disruptions, data breaches, fraud, and financial losses. If not managed well, these can have severe consequences for financial and monetary stability, as well as the broader economy.

Importantly, the cyber security threat landscape is highly complex, shaped by a range of factors (see Diagram 6). The tools of cyber criminals are also constantly evolving, becoming easier and more inexpensive by the day. The threat is borderless, and increasingly more coordinated and sophisticated. Such factors compound the challenge of putting in place reliable safeguards.

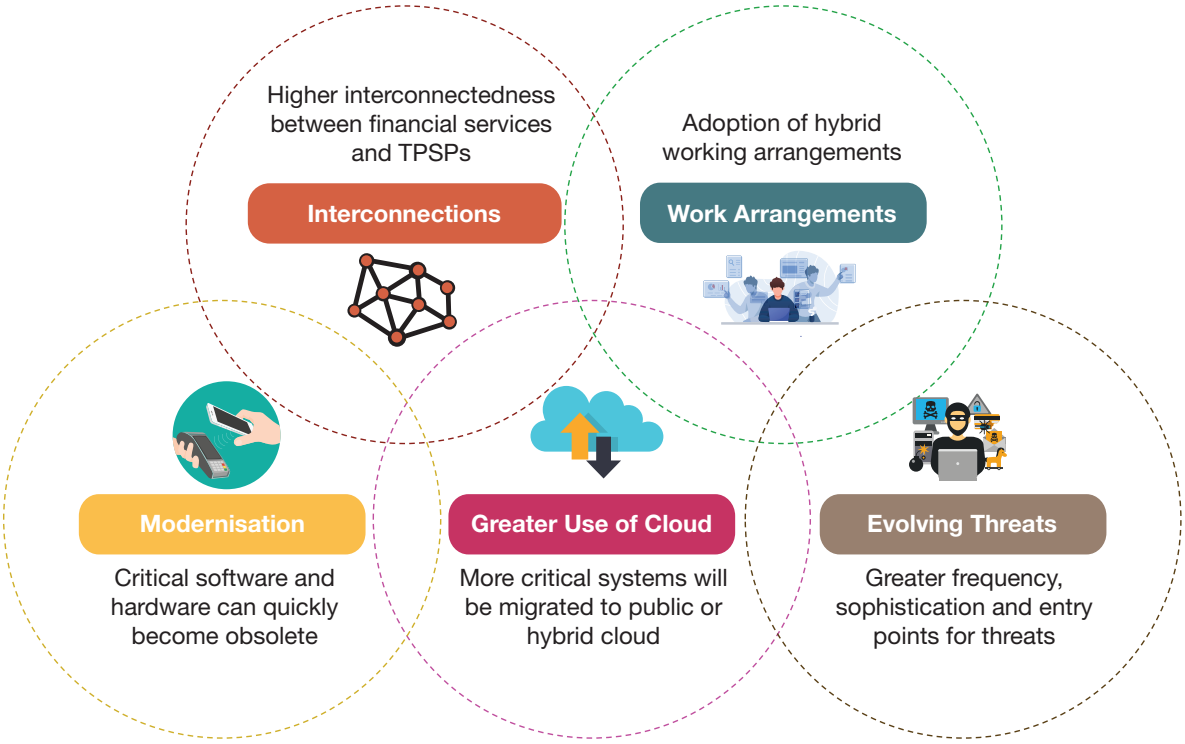
Against this backdrop, a financial system with strong cyber security fundamentals will continue to be a critical priority of the Bank, in turn providing a solid foundation for innovation to thrive.

Given the characteristics of cyber risk, our strategies are centred around readiness and responsiveness. While reducing the probability of cyber attacks remains an important objective, we will intensify efforts to mitigate the impact of such attacks. We will also strengthen collaborative arrangements – among authorities and industry players, domestically and internationally. These efforts will aim to develop holistic defences against cyber security risks to the financial sector, including those from telecommunications infrastructure and potentially critical TPSPs such as cloud operators.

We will seek to advance the following strategies:

i. Strengthen system-wide cyber security oversight and capabilities; and
ii. Strengthen domestic and global collaborative efforts on cyber security.

Diagram 6:
Key factors shaping the cyber security landscape



i Strengthen system-wide cyber security oversight and capabilities

- We will **continuously strengthen our oversight of cyber security risks, with an increased focus on the broader financial ecosystem**. This entails:

  - ☐ **Ensuring that the financial industry adheres to a strong set of minimum standards** on cyber risk governance and management.

  - ☐ **Intensifying our focus on cyber security issues arising from critical TPSPs**. This will entail assessing the adequacy of existing policies in managing TPSP risks and where necessary, developing additional frameworks to better protect the financial ecosystem throughout its entire value chain.

    Further, we will consider the need for strengthened oversight arrangements to take into account interactions between the financial sector and TPSPs that can give rise to systemic risks. These include expanding the regulatory perimeter given the increasing interdependence with TPSPs. We will consult with key industry players, including critical TPSPs to develop possible approaches for securing the financial system's technology linkages with third party providers.

    We will also consider integrating TPSPs as part of intelligence-sharing arrangements established in the financial sector (as set out below).

- We will **intensify sharing of actionable cyber security intelligence** by:

  - ☐ Further **developing our capacity to construct and maintain comprehensive cyber contagion maps of the financial industry**. The aim will be to identify, on a continuing basis, vulnerable points, potential concentration risks and interconnections in the financial sector arising from technological infrastructures and services that are being used by financial institutions. These contagion maps are expected to provide a more granular view of how the shock from a cyber incident could spread throughout the financial ecosystem, including its magnitude and impact.

  This will in turn guide our supervisory assessments of financial institutions, support better informed business decisions by the financial sector to manage potential risk concentration of TPSPs or related services, as well as focus our efforts at the national level to better safeguard critical infrastructures.

  - ☐ **Expanding the scope and coverage of ongoing resilience measures**. This includes the implementation of the cyber resilience maturity assessment (CRMA) framework, cyber drill exercises with other stakeholders and the Government, and the recently established Financial Sector Cyber Threat Intelligence Platform (FinTIP). Across these initiatives, we will aim to involve a greater range of stakeholders and industry players in the financial sector value chain. These initiatives are expected to enrich our collective understanding and improve the ecosystem-wide ability to proactively mitigate cyber risks.

ii Strengthen domestic and global collaborative efforts on cyber security

- We will continue to **support nationwide efforts in strengthening digital literacy and cyber hygiene practices** of financial consumers. With wider adoption of digital financial services, basic cyber hygiene practices will be crucial to protect consumers from threats such as online scams, financial fraud and identity theft. To this end, we will support and work with industry associations, law enforcement agencies and relevant government agencies to increase cyber security awareness among consumers so that they can effectively protect their data and digital devices.

- We will **advocate for greater standardisation in cyber security and cyber resilience terminology** at the national level. With a common language among all relevant stakeholders, ecosystem-wide efforts to safeguard and strengthen cyber security – whether to share information or to coordinate interventions – can be pursued more effectively. In our advocacy efforts, we will aim to leverage on widely accepted practices. This would consider global efforts such as those of the FSB's Cyber Lexicon, ISO, as well as domestic policies of various agencies such as National Cyber Security Agency Malaysia (NACSA), CyberSecurity Malaysia (CSM), Malaysian Communications and Multimedia Commission (MCMC), National Institute of Standards and Technology (NIST) and others.

- We will **facilitate initiatives to deliver specialised cyber security training and certification** that promote skills development and competencies in the financial industry. In doing so, we will work together with relevant government agencies and industry associations – such as MDEC, CSM, NACSA, and *Persatuan Penguji Keselamatan Siber* (PPKS) – to collect, compare, and assess data to design a clear roadmap to deepen Malaysia's cyber security talent pool.

Strategy 3D
Support greater use of technology for regulation and supervision

We are also committed to ensure that we leverage digital technologies to continuously improve our effectiveness and efficiency – particularly, as a financial regulator and supervisor. This will complement the financial industry's shift towards greater digitalisation.

A key consideration in our way forward would be to enhance how we create, collect, capture, synthesise and share data – aiming to improve the efficiency, integrity, and security of the ecosystem. This reflects the growing importance of data for a range of functions, from the surveillance of risks and vulnerabilities to facilitating efficient ways to comply with regulatory policies and requirements. As future enhancements will affect existing infrastructures, systems, and processes, we will ensure that the path forward is collaboratively mapped out, together with industry players and other regulatory authorities.

As part of this effort, we will seek to advance the following:

i. Leverage technology to further strengthen the Bank's regulation and supervision of the financial industry; and
ii. Futureproof the Bank's data strategy.

i Leverage technology to further strengthen the Bank's regulation and supervision of the financial industry

- We will aim to continuously strengthen our application of technologies – such as AI, ML, natural language processing, and automation – to deliver **process improvements** in our regulatory and supervisory functions. This will include:
  - Greater **integration of our risk analytics engines** to support more holistic surveillance across different datasets – and with it, explore further enhancements in the way we conduct our oversight activities. In particular, this is expected to enhance risk-based supervision, by providing richer insights in identifying and sizing up risks to financial institutions – and in turn, enabling more timely and targeted interventions.
  - **Streamlining and facilitating more efficient regulatory and compliance processes**. This includes providing a single, technology-supported applications and submissions interface, with monitoring capabilities, for all authorised financial institutions with the Bank.

ii Futureproof the Bank's data strategy

We aim to reform our data arrangements, including through the use of APIs and Open Data initiatives

- We will initiate a **comprehensive industry review on the financial data ecosystem**, which includes the submission, processing and usage of regulatory reporting and statistical submissions to the Bank. In the next five to ten years, we will focus on improving the timeliness, quality, granularity, and transparency of the data that we collect from the industry. This will be done through the implementation of a new data collection and sharing arrangement between the Bank, the financial industry and other partner institutions.
  - **Quality and timeliness.** We will work with the industry to gradually phase out manual or semi-automated data submissions and quality control processes, and explore the use of APIs to improve the overall data preparation and submission processes. This will reduce compliance costs for financial institutions and improve the Bank's regulatory and supervisory efficiency.
  - **Granularity.** We will increasingly leverage the use of geospatial and other technologies to continuously enhance the granularity of data – and in turn, drive better insights for our analysis and decision-making. This will build on efforts so far, such as pilot initiatives that we have pursued since the onset of the pandemic – where we collect more granular payments and financial inclusion data from selected financial institutions, on a near real-time basis. We will continue to expand the scope of such pilots to include other data sets, such as household and business data, climate-related exposures, and green financing data.
  - **Transparency.** We will continue to enhance public access and portability of the Bank's various financial and economic data sets that do not reveal any commercially sensitive information. This can play a role in catalysing the broader data community – such as through Open Data initiatives – to develop new insights and identify collaboration opportunities, including with the Bank. Where possible, we will also explore the development of dashboarding capabilities, leveraging on industry data reported to the Bank, for financial institutions to anonymously benchmark their risk profiles and practices relative to peers.