

Building trusted digital ecosystems in ASEAN





The GSMA is a global organisation unifying the mobile ecosystem to discover, develop and deliver innovation foundational to positive business environments and societal change. Our vision is to unlock the full power of connectivity so that people, industry, and society thrive.

Representing mobile operators and organisations across the mobile ecosystem and adjacent industries, the GSMA delivers for its members across three broad pillars: Connectivity for Good, Industry Services and Solutions, and Outreach. This activity includes advancing policy, tackling today's biggest societal challenges, underpinning the technology and interoperability that make mobile work, and providing the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events.

We invite you to find out more at www.gsma.com

GSMA Intelligence

GSMA Intelligence is the definitive source of global mobile operator data, analysis and forecasts, and publisher of authoritative industry reports and research. Our data covers every operator group, network and MVNO in every country worldwide – from Afghanistan to Zimbabwe. It is the most accurate and complete set of industry metrics available, comprising tens of millions of individual data points, updated daily.

GSMA Intelligence is relied on by leading operators, vendors, regulators, financial institutions and third-party industry players, to support strategic decision-making and long-term investment planning. The data is used as an industry reference point and is frequently cited by the media and by the industry itself.

Our team of analysts and experts produce regular thought-leading research reports across a range of industry topics.

www.gsmainelligence.com

info@gsmainelligence.com

Authors

Kenechi Okeleke, Senior Director, GSMA Intelligence

Celine Yuan, Senior Analyst, China and APAC, GSMA Intelligence

Contributors

Jeanette Whyte, Head of Policy & External Affairs, GSMA Asia Pacific

Ming Sheng Bensen Koh, Director, GSMA Asia Pacific

Published September 2026

Contents

Executive summary	04
--------------------------	-----------

01	Advancing digital nation goals	07
1.1	Shared regional vision and national priorities	08
1.2	Digital trust as an enabler of digital nation priorities	11

02	Measuring progress: the Digital Nations Index	13
-----------	--	-----------

03	Guardians of digital trust	23
3.1	Trust in the age of sovereignty	24
3.2	Mobile operators as guardians of digital trust	26

04	Strengthening the foundations of digital trust	35
4.1	Priorities for governments and regulators	36
4.2	Priorities for mobile operators	38
4.3	Priorities for ASEAN	40

Executive summary



Trust as an enabler of digital nation ambitions

In January 2026, member states of the Association of Southeast Asian Nations (ASEAN) adopted the ASEAN Digital Masterplan 2030, a five-year policy blueprint to guide regional digital cooperation and national technology strategies through to 2030. This was followed in May 2026 by the adoption of the Digital Economy Framework Agreement, a comprehensive regional digital economy agreement expected to help expand ASEAN's digital economy from \$1 trillion to \$2 trillion by 2030. Several ASEAN countries, including Indonesia, Malaysia, Singapore and Vietnam, have also introduced new digitalisation plans or strengthened existing ones, underscoring their commitment to building digital nations.

As ASEAN countries move from connectivity expansion towards integration, interoperability and intelligent digital transformation, a key factor to achieving regional and digital national ambitions is digital trust. This is the confidence that digital systems, services and the organisations behind them will operate securely, reliably, transparently and accountably while protecting users' rights and interests. Digital trust has therefore become a strategic delivery mechanism for building digital nations. Countries that build confidence in digital infrastructure, services and institutions will be better placed to convert digitalisation into adoption, innovation, investment and socioeconomic impact.

Trust is deeply connected to the five core components of the GSMA Intelligence Digital Nations Index, enabling them to function effectively and amplifying their economic and social impact. The index therefore serves both as a measure of digital progress and as a lens for assessing the conditions that support trusted, sustainable digital growth.

The key question has extended from whether people can access digital services to whether they can rely on them to be secure, reliable, transparent and accountable. This challenge is becoming increasingly visible from the growth of scams and fraud across ASEAN countries. As AI enables more convincing phishing attacks, deepfakes, voice cloning and digital impersonation, trust increasingly depends on the ability to verify identities, authenticate communications and prevent fraud before harm occurs. As such, building trusted digital nations will require stronger cooperation between governments, telecoms operators, financial institutions and digital platforms to strengthen confidence in digital interactions and protect citizens from increasingly sophisticated forms of deception.

Mobile operators as guardians of digital trust

To explain how digital trust can be strengthened, this report introduces four interconnected foundations of digital trust:



Identity

The ability to verify people and organisations in digital environments



Communications

The security and integrity of digital interactions and transactions



Resilient networks

The infrastructure and cybersecurity capabilities that keep digital services available and secure



Collective intelligence

The creation, sharing and use of trusted information to strengthen the security, resilience and integrity of digital systems

Traditionally viewed as connectivity providers, mobile operators are increasingly contributing to all four trust foundations, making them key enablers of digital trust. They support trusted identity through authentication and verification services, protect communications against fraud and cyberthreats, operate resilient digital infrastructure, and use data and AI to improve security and service delivery. Across ASEAN, operators are helping governments, businesses and citizens participate more safely and confidently in digital ecosystems.

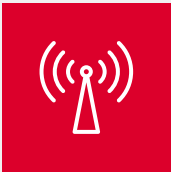
Key priorities for stakeholders

Strengthening the foundations of digital trust requires coordinated action from three stakeholder groups: governments and regulators, which set resilience policies; mobile operators, which act as enablers of digital trust and partners with the broader digital ecosystem; and regional institutions, which support interoperability, coordination and common frameworks for trusted cross-border interaction. The table below outlines how each group can contribute.

Table i

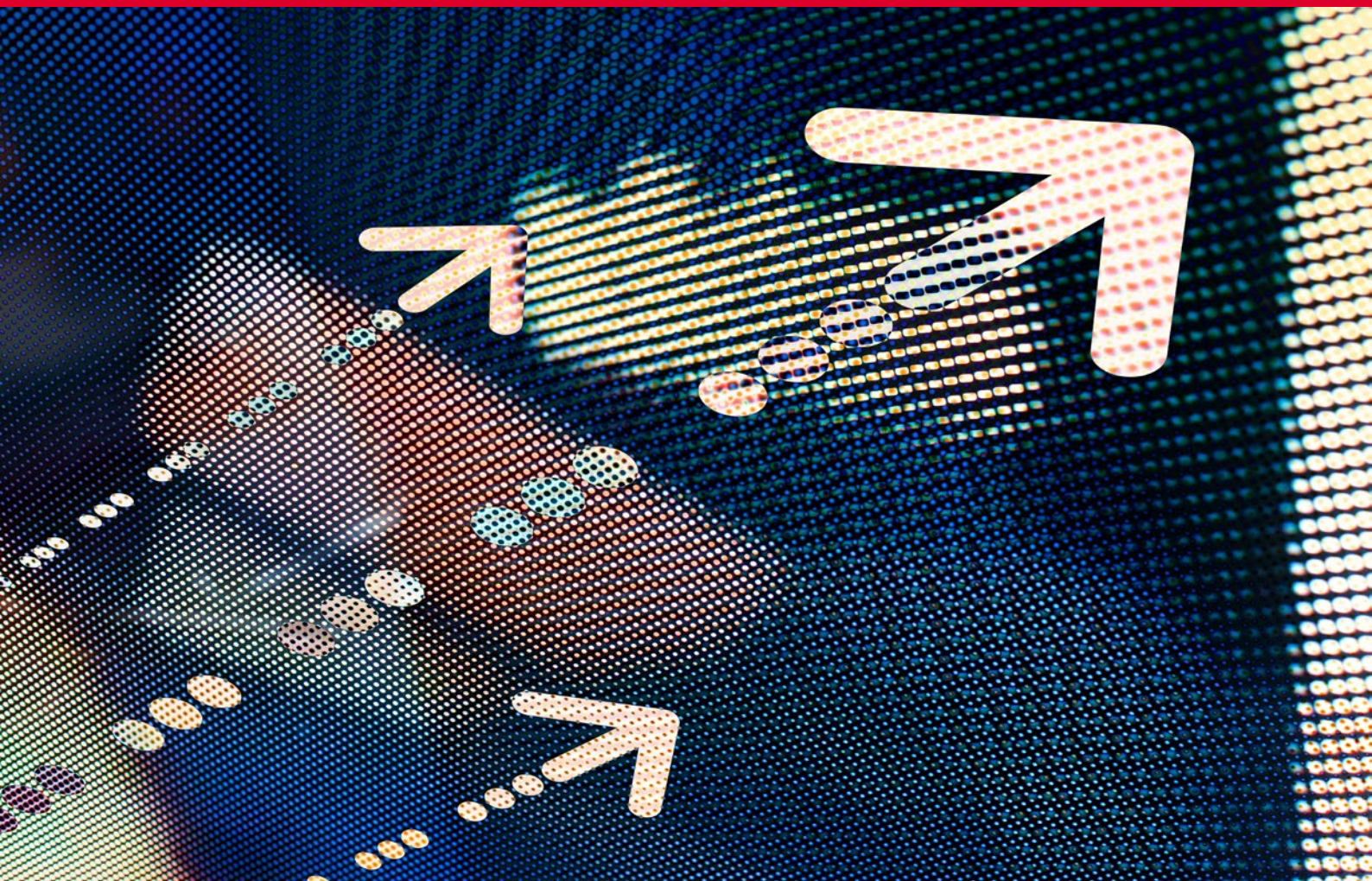
Key stakeholder priorities to strengthen the foundations of digital trust in ASEAN

Source: GSMA Intelligence

Stakeholder	Priorities
 Government and regulators	— Enabling trusted identity ecosystems — Strengthening secure communications — Enhancing cybersecurity and resilience — Supporting trusted AI and data governance — Deepening regional cooperation
 Mobile operators	— Building towards a digital trust layer — Collaborating with the broader digital ecosystem to combat scams and fraud — Investing in resilient infrastructure — Developing trusted intelligence capabilities
 ASEAN	— Advancing trust interoperability — Supporting trusted cross-border services — Embedding trust in DEFA implementation — Promoting a shared vision of trusted sovereignty

01

Advancing digital nation goals



Shared regional vision and national priorities

2026 marks the first full year since Timor-Leste became a full member of the Association of Southeast Asian Nations (ASEAN), expanding the bloc to 11 member states.¹ It also marks the beginning of the implementation of the ASEAN Economic Community Strategic Plan 2026–2030 and the ASEAN Connectivity Strategic Plan 2026–2035, the first major delivery mechanisms for the ASEAN Community Vision 2045. These plans signal ASEAN's ambition to deepen regional integration, build resilience, accelerate innovation and strengthen competitiveness in a fast-changing global economy. The Digital Nations ASEAN 2025 report² underscored the importance of the ASEAN Community Vision 2045 and its delivery mechanisms as foundations for the region's next phase of socioeconomic development.

In recognition of the central role of digital technologies in shaping the bloc's economic future, the 6th ASEAN Digital Ministers' Meeting in January 2026 adopted the ASEAN Digital Masterplan 2030 (ADM 2030), a five-year policy blueprint to guide regional digital cooperation and national technology strategies from 2026 to 2030. Building on the previous ADM 2025, the strategy is framed

around the theme of 'Adaptive ASEAN: From Connectivity to Connected Intelligence', signalling a shift from expanding digital infrastructure to harnessing advanced technologies, data and AI to support growth, innovation and social development. ADM 2030 is organised around eight desired outcomes, summarised in **Table 1**.

To operationalise ADM 2030, ASEAN member states concluded negotiations on the ASEAN Digital Economy Framework Agreement (DEFA) in May 2026, ahead of its expected formal signing in November. DEFA translates ADM 2030's strategic ambitions into a legally binding regional framework, supporting cross-border data flows, digital payments, digital trade, consumer protection, regulatory interoperability, AI and cybersecurity. By seeking to harmonise member states' digital regulations and promote interoperability, thereby reducing the regulatory friction that impedes cross-border digital trade, DEFA helps to bridge the gap between regional vision and implementation. Recognised as the world's first comprehensive regional digital economy agreement, DEFA is expected to play a key role in unlocking the full potential of ASEAN's digital economy, which could reach \$2 trillion by 2030.³

¹ Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, Timor-Leste and Vietnam

² Digital Nations 2025: Achieving the ASEAN Connectivity Strategic Plan, GSMA, 2025

³ "Statement of the Chairperson of the ASEAN Senior Economic Officials (SEOM) on the Conclusion of ASEAN DEFA Negotiations", ASEAN, June 2026

Table 1

Desired outcomes of ADM 2030

Source: ADM 2030, GSMA Intelligence

Desired outcome	Summary of rationale
Seamless and inclusive digital infrastructure across ASEAN	Reliable, affordable and inclusive digital infrastructure is essential to ASEAN's economic and social transformation. This outcome focuses on expanding high-speed broadband and 5G coverage, strengthening cloud, data-centre and digital ID ecosystems, and improving spectrum allocation and international cable connectivity. It also emphasises the need for resilient and interoperable infrastructure, including more diverse terrestrial, submarine and satellite links, to reduce disruption risks and support seamless cross-border digital services.
Sustainable and intelligent digital government	Sustainable and intelligent digital government is crucial to meeting citizen expectations, improving public service delivery and supporting regional collaboration. This outcome promotes citizen-centric, evidence-based and environmentally responsible government, underpinned by interoperable systems such as digital ID, data exchange and cross-border verification. It also encourages the use of AI, big data and foresight tools to design policies and services that are more anticipatory, coordinated and aligned across ASEAN.
Empowered, safe and inclusive ASEAN digital society	A resilient digital society depends on empowered individuals and trusted digital environments. As ASEAN's digital transformation deepens, citizens need the skills, confidence and protection to participate safely and meaningfully online, including safeguards against digital, online and telecoms scams. This outcome focuses on strengthening digital literacy, responsible digital behaviour, digital rights and lifelong learning, as well as closing access and skills gaps, so that all ASEAN countries – and all communities – can benefit from and contribute to the digital future.
Resilient, secured and trusted digital ecosystem	Digital trust and data integrity are needed for the adoption of digital services and trusted cross-border data flows. This outcome strengthens cybersecurity, privacy, anti-scam protection and secure interoperability through open standards, coordinated incident response, threat sharing and capacity building. It also supports harmonised approaches to data protection, cloud security, digital ID interoperability and cross-border data mechanisms, helping ASEAN build a trusted, resilient and inclusive digital ecosystem aligned with responsible digital growth and global norms.
Thriving ASEAN innovation and startup ecosystem	Future-proofing ASEAN's economy requires stronger innovation across sectors. This outcome focuses on accelerating the adoption and commercialisation of emerging technologies, supporting innovation for micro, small and medium-sized enterprises (MSMEs) and startup growth, and deepening collaboration between industry, academia and research institutions. Through regulatory sandboxes and public-private-academia partnerships, ASEAN can strengthen knowledge networks, foster entrepreneurship and build a more competitive, sustainable and globally connected innovation ecosystem.
Smart and digitally transformed ASEAN industries	A competitive industrial base depends on deeper digital integration across sectors. This outcome supports the digital transformation of strategic industries, including health, education, manufacturing and logistics, by enabling small and medium-sized enterprises (SMEs) and large firms to adopt Industry 4.0 technologies, participate in global digital value chains and develop smart urban solutions. In doing so, ASEAN can strengthen MSME productivity, advance regional industrial capabilities and reinforce its position as a trusted global manufacturing and logistics hub.
Sustainable, green and AI driven digital transformation	ASEAN's next phase of digital transformation must combine responsible AI adoption with sustainable digital development. This outcome focuses on managing AI-related risks through testing, assurance, common governance frameworks and internationally recognised standards while enabling ASEAN to contribute more actively to global AI governance debates. It also promotes energy-efficient infrastructure, circular ICT practices and the use of digital and AI solutions to strengthen climate resilience and resource optimisation.
Digital talent and future skills	ASEAN faces growing shortages in AI, cybersecurity, cloud, data science and other emerging technology skills, even as automation and AI reshape the skills needed across the workforce. This outcome focuses on building a future-ready workforce through advanced reskilling, industry-aligned training, regional talent mobility and foresight-led workforce planning. By strengthening cooperation on digital talent and future skills, ASEAN can improve competitiveness, support industrial digital transformation and prepare workers for opportunities in the digital and green economies.



Beyond the regional efforts, several ASEAN countries have introduced new digitalisation plans or strengthened existing ones, underscoring their commitment to building digital nations, including the following:

- **Malaysia:** In July 2026, Malaysia's Ministry of Digital and the newly rebranded AI Malaysia Berhad, the successor to the National AI Office, launched the National AI Action Plan 2026–2030 (AI Nation 2030). The plan sets out Malaysia's roadmap to become a top 10 country on recognised global AI indices and targets 1.2 percentage points of additional GDP growth and 300,000 new AI-related jobs by 2030.
- **Indonesia:** Indonesia's Digital Infrastructure Roadmap 2026–2030, launched in July 2026 by the Ministry of National Development Planning (Bappenas) and the Ministry of Communication and Digital Affairs (Komdigi), signals a shift from a connectivity-focused agenda towards a broader strategy centred on digital infrastructure, technological sovereignty and economic transformation. The roadmap brings together telecoms networks, cloud computing, local data centres and advanced computing capacity within a unified national digital architecture. Meanwhile, complementary draft regulations seek to accelerate AI adoption across national and local government institutions by the end of the decade.
- **Singapore:** The formalisation of Singapore's National AI Strategy (NAIS 2.0) in May 2026 marks a significant evolution in the country's digital transformation agenda, shifting from broad ecosystem development towards the targeted deployment of AI in strategic sectors. Led by the National AI Council, which is chaired by the prime minister, the updated strategy builds on the foundations laid in 2023 by introducing four national AI missions focused on advanced manufacturing, financial services, connectivity and healthcare.
- **Vietnam:** Vietnam has approved its National Digital Transformation Strategy for 2026–2030, setting a long-term ambition to become a data- and AI-driven digital nation by 2045. Under the strategy, the government aims to fully digitalise administrative records by 2030 and increase the digital economy's contribution to at least 30% of GDP, with data and AI positioned as key growth engines.⁴

4 "Vietnam approves national digital transformation strategy through 2030", Biometric Update, July 2026

Digital trust as an enabler of digital nation priorities

Digital trust is the confidence that digital systems, services and the organisations behind them will operate securely, reliably, transparently and accountably while protecting users' rights and interests. It is therefore more than a matter of cybersecurity or consumer protection. For digital nations, trust determines whether people use digital services, businesses invest in digital channels and governments can scale up digital transformation without creating new systemic risks. It underpins every part of regional and national digital transformation plans: infrastructure must be secure and resilient; digital government services need to be reliable and accountable; digital society must be safe and inclusive; innovation requires regulatory certainty; cross-border data flows depend on confidence in privacy and governance; and AI adoption needs transparency, assurance and safeguards.

Trust has become a more urgent concern in recent years. This reflects the deeper integration of digital technologies into daily life, as well as the way AI is reshaping digital trust itself. Traditionally, trust centred on protecting networks, devices and data from unauthorised access or malicious attacks. Today, generative AI (genAI) has made the authenticity of digital interactions harder to verify. Voice, video, images, documents and identities can now be convincingly created, altered or replicated at scale.⁵ As a result, individuals, businesses and governments must increasingly assess whether the information they receive, the people they engage with and the content they consume are genuine.

This shift has expanded trust concerns beyond financial loss, privacy breaches and cybersecurity incidents. There is growing recognition that digital environments can also affect mental and emotional wellbeing. AI-enabled information pollution, deepfake impersonation, synthetic identity fraud and hyper-personalised target profiling can create uncertainty, anxiety and confusion, making it harder for users to engage online with confidence. In recent years, for example, organised crime networks have progressed from simple static deepfakes to interactive video conferences and advanced AI voice cloning, enabling them to impersonate senior officials across the region, including leaders in Indonesia,⁶ Malaysia,⁷ the Philippines,⁸ Singapore⁹ and Thailand,¹⁰ In this environment, trust is not only a precondition for adoption – it is also essential to productive use, value creation and resilience. People must feel able to participate in digital life safely and confidently if digital technologies are to deliver their full social and economic benefits.

5 "Deep fake-Driven Identity Fraud in Southeast Asia", Oz Forensics, February 2026

6 "Indonesians swindled by scams using President Prabowo deepfakes", France 24, March 2025

7 "You Cannot Trust What You See Anymore: Malaysia's Deepfake Crisis and the Technology Fighting Back", Mimos, July 2026

8 "CICC warns vs. fake PBBM investment promotion video", Philippine News Agency, June 2025

9 "Footage From Zoom Video Conference Involving Impersonation Of Senior Government Officials", Singapore Police Force, May 2026

10 "AI-generated audio of Thai PM announcing border reopening misleads online", AFP Fact Check, May 2026



At the same time, citizens are more aware of privacy risks and more concerned about how their personal data is collected, shared and used. For instance, a Think with Google survey found that 70% of consumers in Asia Pacific would stop using a brand after a violation of their trust around data.¹¹ Businesses increasingly recognise that trust is not just a compliance obligation, but a source of competitive advantage, as consumers are more likely to engage with organisations that demonstrate transparency, security and accountability.¹² Regulators have responded by strengthening data-protection requirements, cybersecurity obligations and AI governance frameworks. In March 2026, Vietnam released a draft decree for public consultation on administrative sanctions for cybersecurity and personal data protection violations. The draft clarifies parts of the Personal Data Protection Law and sets out penalties for different types and levels of non-compliance.¹³ These shifts have elevated trust from an operational concern to a strategic priority.

While national governments and institutions are central to building trust within their digital ecosystems, national action alone is no longer sufficient given that digital networks, platforms, services and threats increasingly cross borders, allowing vulnerabilities in one market to affect users and organisations elsewhere. As digital economies become more interconnected, safeguarding trust will require both strong national capabilities and deeper regional and international cooperation on cybersecurity, digital identity, data governance, scam prevention and AI governance.

For ASEAN, trust is central to the realisation of regional and national digital ambitions as the bloc moves from connectivity expansion towards integration, interoperability and intelligent digital transformation. Initiatives such as ADM 2030 and DEFA are therefore important not only for advancing digital integration, but also for establishing the shared rules, safeguards and frameworks needed to build confidence across borders.

As such, digital trust is now fundamental to building digital nations. Without it, inclusion may remain shallow, with people connected but reluctant to use online services meaningfully; digital governments may struggle to gain citizens' confidence; businesses may delay investment in digital solutions; and regional integration may be constrained by concerns over data protection, cybersecurity, scams and cross-border accountability. By contrast, countries that build confidence in digital infrastructure, services and institutions will be better placed to convert digitalisation into adoption, innovation, investment and socioeconomic impact. As ASEAN member states advance ADM 2030, DEFA and other regional and national digital strategies, trust will determine whether policy ambitions translate into inclusive, resilient and sustainable digital economies.

¹¹ "Why meeting APAC consumers' expectations of data privacy is key to effective marketing", Think with Google, June 2023

¹² "In Asia, Trust Isn't A Feature—It's Your Most Valuable Asset", Forbes, October 2025

¹³ "Businesses face tightened personal data protection requirements", Vietnam Law Magazine, May 2026

02

Measuring progress: the Digital Nations Index



The Digital Nations Index in the context of trust

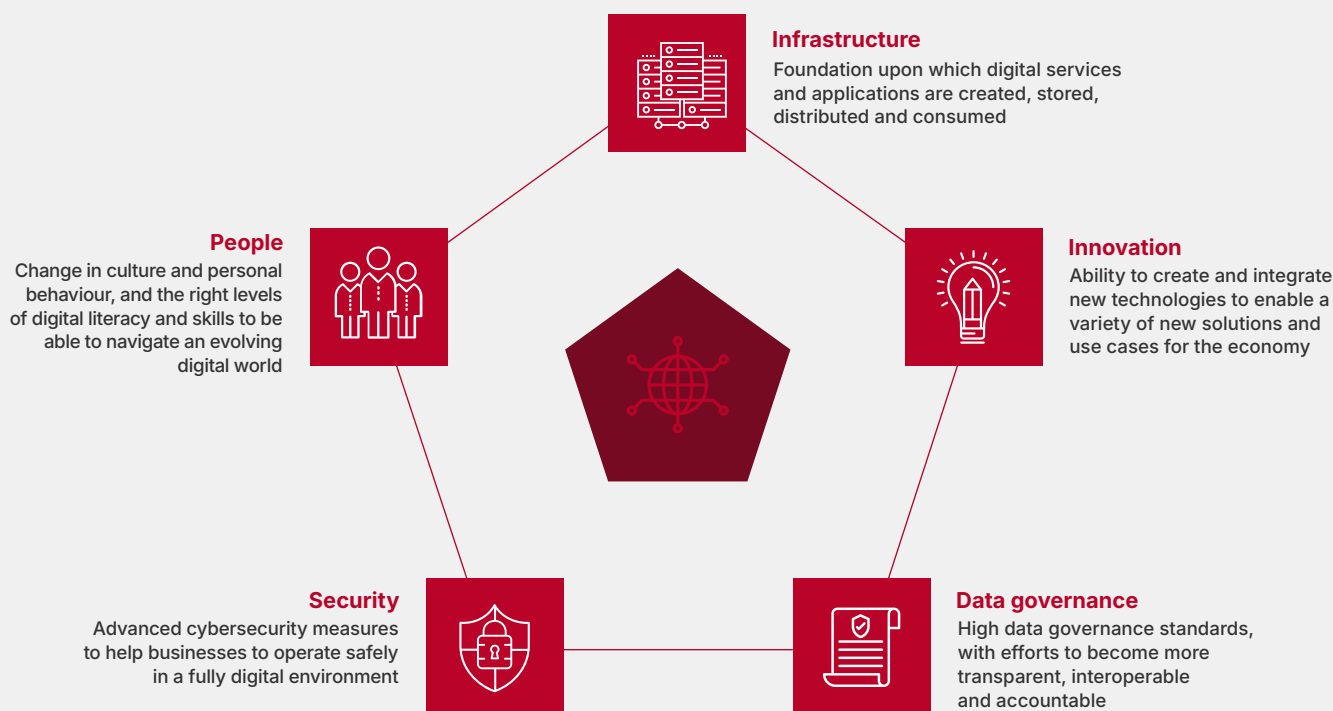
GSMA Intelligence developed the Digital Nations Index to assess countries' readiness to capture the economic and social benefits of digital transformation. The index measures progress across five interconnected dimensions of a digital nation: infrastructure, innovation, data governance, security and people. It offers a holistic view

of the foundations needed to participate effectively in an increasingly digital economy. By bringing together indicators across these five areas, the framework provides a practical tool for benchmarking performance, tracking progress over time and identifying priorities for future policy and investment.

Figure 1

The five components of a digital nation

Source: GSMA Intelligence



As ASEAN enters a new phase of digital development, shaped by the implementation of regional and national digitalisation priorities, trust has become central to whether these ambitions can be realised. Trust is deeply interconnected with the five core components of a digital nation, amplifying their impact on economic and social development:

- **Infrastructure:** Trust depends on the resilience and continuity of networks, cloud platforms, data centres and international connectivity.
- **Innovation:** Trust drives the adoption of AI and emerging technologies through governance, assurance and regulatory certainty.
- **Data governance:** Trust underpins responsible data sharing through privacy protections, digital identity and interoperable cross-border frameworks.
- **Security:** Trust is built on effective cybersecurity, fraud prevention, scam mitigation and online safety.
- **People:** Trust shapes the confidence needed for full participation in the digital economy.

Across all five areas, trust strengthens adoption, attracts investment and helps translate digital capabilities into sustained economic and social outcomes.

The index therefore functions both as a measure of digital progress and as a lens for assessing the conditions that support trusted, sustainable digital growth. The key question has extended from whether people can access digital services to whether they can rely on those services to be secure, reliable, transparent and accountable. As such, digital trust should be seen as integral to the Digital Nations Index framework, rather than as a separate pillar or standalone policy objective.

The 2026 Digital Nations Index ranks 22 Asia Pacific countries, including all 11 ASEAN member states, based on their aggregate scores. Singapore leads the index with an aggregate score of 88, followed by Malaysia with a score of 70 (see Figure 2). Timor-Leste appears in the index for the first time this year, recording an aggregate score of 17, which highlights the scale of the opportunity to strengthen its digital nation foundations. The greatest value of the index lies in helping countries assess performance across its five components, rather than focusing solely on comparisons with regional peers. This component-level view allows governments and partners to identify where intervention is most needed, focus policy and investment more effectively, and improve both overall scores and digital outcomes for citizens and businesses (See Figure 3).

Figure 2
Digital Nations Index: ASEAN ranking, 2026
Aggregate scores

Source: GSMA Intelligence

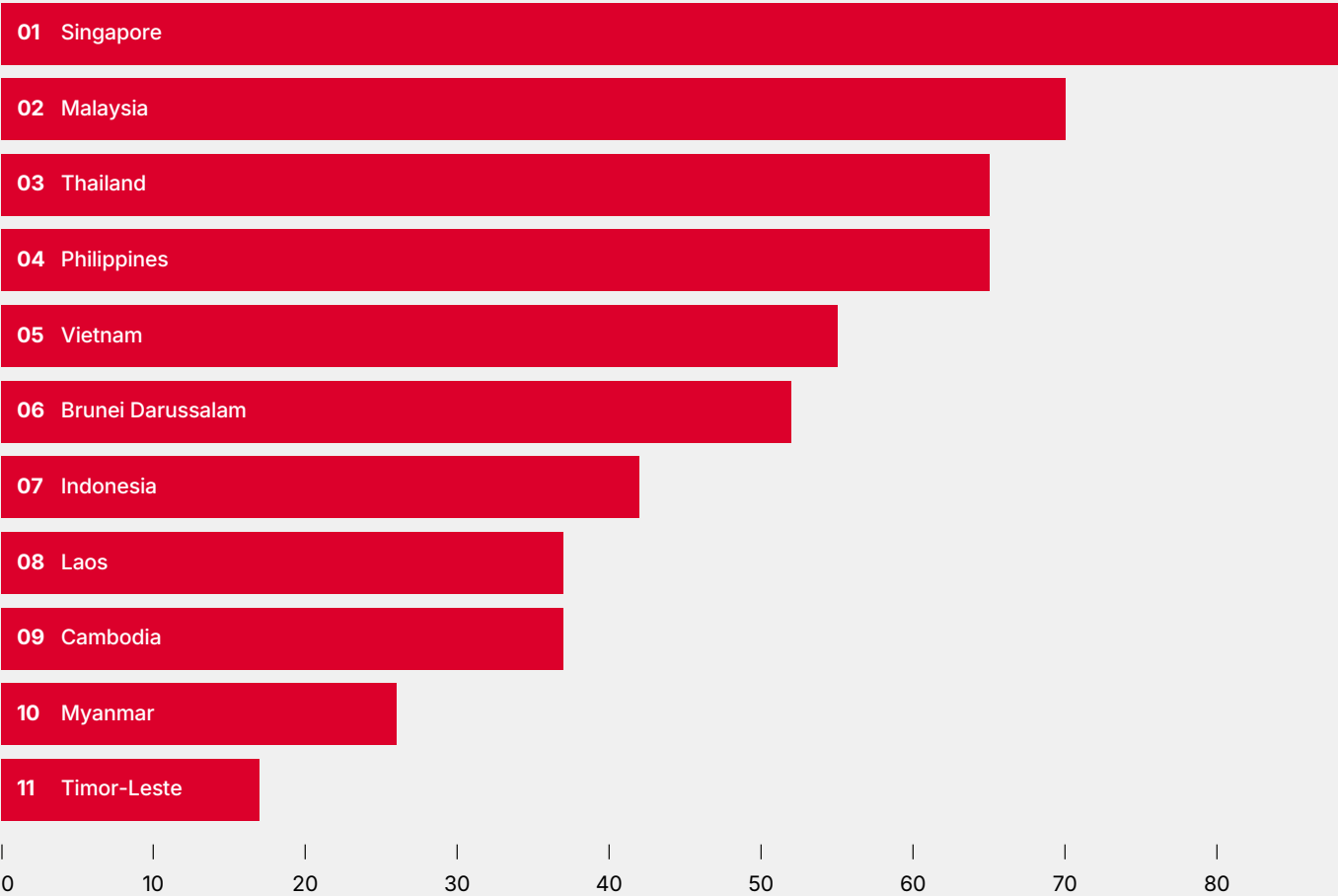


Figure 3

Digital Nations Index: component scores, 2026

Source: GSMA Intelligence

2026 score band

■ 0–24 ■ 25–49 ■ 50–75 ■ 76–100

Change from 2025

▲ Increase ▼ Decrease — No change

	 Infrastructure	 Innovation	 Data governance	 Security	 People
Singapore	■ —	■ —	■ —	■ —	■ —
Malaysia	■ ▲	■ —	■ ▲	■ —	■ ▲
Philippines	■ ▲	■ —	■ ▲	■ —	■ ▲
Thailand	■ ▲	■ ▼	■ ▲	■ —	■ —
Vietnam	■ ▲	■ —	■ ▲	■ —	■ ▲
Brunei Darussalam	■ —	■ —	■ —	■ —	■ ▼
Indonesia	■ —	■ —	■ ▲	■ —	■ ▲
Cambodia	■ —	■ —	■ ▲	■ —	■ ▲
Laos	■ —	■ —	■ —	■ —	■ —
Myanmar	■ —	■ —	■ —	■ —	■ ▲
Timor-Leste	■ —	■ —	■ —	■ —	■ —





Trust and infrastructure

Infrastructure is a fast-improving component of the Digital Nations Index, reflecting sustained investment in 5G, international connectivity, cloud and other digital infrastructure. Commercial 5G is now available across most ASEAN countries, though deployment pace, scale and models vary significantly by market. Singapore continues to lead among the ASEAN states in the reach of 5G standalone and in quality of experience. Meanwhile, Cambodia's launch of commercial 5G mobile services in January 2026 further expanded the region's footprint of live 5G. In July 2026, Timor-Leste launched commercial operations for its first international subsea cable, the Timor-Leste South Submarine Cable, which marks a major infrastructure milestone, reducing the country's reliance on costly, low-bandwidth satellite connectivity.

ASEAN's data-centre market is also expanding rapidly. The bloc already hosts more than 2,000 data centres across key markets, including Indonesia, Malaysia, Singapore, Thailand, Vietnam and the Philippines, and this is becoming one of Asia Pacific's main growth engines for digital infrastructure investment. Major investment commitments are reinforcing this momentum. Overall investment in Southeast Asia's data-centre sector could approach \$30 billion by 2030, with demand expected to grow strongly through to 2028.¹⁴ This expansion reflects a broader infrastructure race shaped by AI, sovereign-data requirements, hyperscale capacity constraints, access to land and power, and growing geopolitical pressures on technology ecosystems.

Digital trust increasingly depends on the resilience and availability of critical digital infrastructure. As economies digitalise, disruption can have consequences that extend well beyond connectivity. Mobile networks and digital platforms now underpin payments, healthcare, emergency communications, transport, public services and business operations. A major outage can therefore disrupt economic activity, delay emergency responses, interrupt access to essential services and weaken confidence in digital systems. Resilience and availability have consequently become core dimensions of digital infrastructure.

Recent incidents underscore the systemic importance of resilient digital infrastructure across ASEAN. In Singapore, a widespread mobile network disruption in March 2026 affected services intermittently over three consecutive days, with an initial eight-hour outage leaving around 600,000 users without signal and disrupting digital transactions, ride-hailing and food delivery services.¹⁵ In Malaysia, a service disruption during a planned payments system upgrade in April 2026 paralysed parts of the cashless payments infrastructure, including QR code transactions.¹⁶ More broadly, the global CrowdStrike outage in 2024 affected airlines, banks, healthcare providers and public services across Southeast Asia, showing how failures in interconnected digital systems can cascade across sectors and borders.

As digital technologies become embedded across economies and societies, infrastructure has become more than simply an enabler of digital activity; it is the foundation for economic growth, public services, financial systems and social interaction. This makes trust inseparable from infrastructure. Citizens, businesses and governments need confidence that the networks, cloud platforms, data centres and connectivity systems behind digital services are secure, resilient and available when required. Without that confidence, even advanced technologies may struggle to achieve broad adoption and deliver value at scale. ASEAN's next infrastructure challenge is therefore not only to expand connectivity, but to ensure that the systems underpinning digital nations remain secure, resilient and reliable as operating conditions become more complex.

Digital trust increasingly depends on the resilience and availability of critical digital infrastructure

¹⁴ "ASEAN races to attract data-centre investment as spending nears US\$30bn", The Nation, June 2026

¹⁵ "IMDA reviewing resilience regulations in wake of Singtel disruptions", The Business Times, April 2026

¹⁶ "Netizens frustrated over widespread CelcomDigi service disruption", Free Malaysia Today, May 2026



Trust and innovation

The innovation component of the Digital Nations Index measures an economy's capacity to create, adopt and commercialise new technologies. Progress across ASEAN has been uneven: seven of the 11 member states improved their innovation scores over the past year (led by the Philippines, which increased by three points). However, these gains were offset by persistent weaknesses in research commercialisation, venture capital development, intellectual-property creation and technology scaling. As a result, ASEAN's average score for innovation remains the lowest among the five components, highlighting both the structural constraints facing regional innovation ecosystems and the untapped potential.

Trust can help close these gaps by reducing uncertainty throughout the innovation cycle. Clear regulation supports long-term investment, governance frameworks reduce adoption risks and assurance mechanisms build confidence in AI and other emerging technologies. Citizens and businesses are more likely to adopt, fund and scale up new solutions when they trust how those technologies are governed and used.

However, building trusted digital ecosystems requires more than regulation and technical standards; it also depends on practical mechanisms that allow stakeholders to test, collaborate and learn in controlled environments. Regulatory sandboxes, pilots, testbeds and jointly funded innovation initiatives can help governments, industry and academia assess emerging technologies, identify risks and refine solutions before deployment. These approaches can accelerate innovation while keeping trust, security and user protection at the centre. Singapore's Punggol Digital District illustrates this model by bringing together businesses, researchers, government agencies and technology providers in a shared innovation ecosystem and enabling digital solutions to be tested in real-world settings.

As AI, automation and advanced analytics spread across fintech, e-commerce, digital health, cloud computing and industrial automation, ASEAN economies are moving from importing and adopting advanced solutions towards integrating them across sectors and, over time, developing proprietary models, datasets, algorithms and exportable applications. This transition will shape the region's innovation trajectory and its ability to capture a larger share of global digital value. By embedding trust into emerging technologies, ASEAN can accelerate innovation, reduce risk and maintain public confidence as digital transformation becomes more intelligent and data-driven.

Singapore and Malaysia demonstrate how trust can strengthen more mature innovation ecosystems. Both markets benefit from strong institutions, advanced research capabilities and internationally connected technology sectors, but continued progress depends on trusted pathways from research to commercialisation. Brunei, Cambodia, Laos and Timor-Leste are at an earlier stage and each have entry points into frontier technologies. Brunei combines institutional stability with a credible research base; Laos is formalising its technology agenda; and Cambodia and Timor-Leste continue to attract relatively strong foreign direct investment. Timor-Leste's ASEAN accession in late 2025 should also broaden access to regional expertise, standards and commercial networks. For these markets, the near-term priority is trusted adoption in nationally relevant areas such as agriculture, logistics, public services and disaster response, followed by gradual development of local datasets, integration capabilities and specialised applications.

By embedding trust into emerging technologies, ASEAN can accelerate innovation, reduce risk and maintain public confidence as digital transformation becomes more intelligent and data-driven

Malaysia's emerging framework for trusted AI innovation

Regulatory certainty: building confidence for long-term innovation

Trust begins with predictability. Malaysia's National AI Action Plan 2026–2030 strengthens innovation trust by providing developers, investors and enterprises with greater clarity on the government's long-term priorities for AI development and adoption. The plan identifies strategic deployment sectors – including manufacturing, healthcare, agriculture, energy, telecoms and public services – and couples these with planned investments in talent, research commercialisation, data and computing infrastructure. This reduces policy uncertainty and provides a credible foundation for long-term investment. The explicit ambition to develop globally competitive 'Made by Malaysia' AI products and services further signals commitment and direction, helping firms invest with greater confidence in the future growth of the domestic AI ecosystem. As AI adoption accelerates, maintaining a balanced regulatory framework and avoiding unnecessary regulatory or financial burdens that could discourage experimentation, investment and the deployment of AI solutions will be critical to sustaining this momentum.

Trust and commercialisation: creating pathways from innovation to adoption

Trust is also important in moving innovation from the laboratory to the marketplace. In February 2026, Malaysia's Ministry of Digital launched the Government Innovation Initiative through the MyInovasi portal, creating structured opportunities for locally developed AI solutions to address real public-sector challenges. By connecting innovators with clearly defined operational problems, testing environments and potential first customers, the initiative helps reduce the uncertainty often associated with early-stage technology adoption. This builds commercialisation trust by providing proof points, validating solutions in real-world settings and giving enterprises greater confidence that innovative technologies can deliver measurable outcomes at scale.

Assurance and validation: strengthening confidence in AI systems

As AI becomes more embedded across economies and societies, trust increasingly depends on assurance, transparency and validation. Malaysia's National AI Action Plan and emerging AI standards framework support this objective by establishing clearer expectations for the responsible development and deployment of AI while signalling a shift towards greater focus on domestic applications, talent development, R&D and intellectual property creation. As these frameworks evolve, strengthening methods to measure, test and verify AI performance will be increasingly important to building confidence in AI systems.





Trust and data governance

Data governance has become one of the most important determinants of trust in the digital economy. As digital services become more interconnected, data increasingly flows across organisations, industries and national borders, supporting everything from digital identity and payments to AI systems and digital government services. Effective data governance therefore requires more than protecting information from misuse, as it must also create the confidence needed for individuals, businesses and governments to share, access and use data responsibly. Trust is what allows data to move safely across digital ecosystems and generate value at scale.

This is not an ASEAN-only challenge. At the global level, governments have been developing common mechanisms to facilitate trusted cross-border data flows, a notable example being APEC's Cross-Border Privacy Rules system. These broader efforts provide an important foundation for interoperable data governance while also highlighting the distinctive value of regional approaches that can respond to the specific regulatory, economic and institutional diversity of ASEAN.

ASEAN has made significant progress in strengthening data-governance frameworks. Thailand and Malaysia have now joined Singapore and the Philippines as ASEAN's most institutionally advanced data-protection regimes, while Indonesia has advanced the implementation of its Personal Data Protection Law with the design of a dedicated supervisory authority in 2025. For countries that are only starting to establish comprehensive data-governance frameworks, the late adoption creates an opportunity: rather than retrofitting privacy protections after successive waves of digitisation, these countries can develop personal rights, cybersecurity, cloud governance and responsible AI as part of a governance framework from the outset as digital government expands. Cambodia's 2025 draft Personal Data Protection Law achieves this by placing economy-wide privacy obligations alongside the country's expanding cloud, AI and digital-government architecture.

Data governance is central to ASEAN's ambitions for deeper regional integration. As ASEAN economies become more interconnected, the ability to securely share and exchange data across sectors and borders will become increasingly important to digital trade, cloud services, AI development and regional platforms. However, differences in national rules can fragment markets and raise compliance costs. The challenge is to create mechanisms that allow data to move securely across borders while respecting national priorities on privacy, sovereignty and security. ADM 2030 and DEFA provide an opportunity to strengthen this trust through greater interoperability, regulatory alignment and common safeguards.

ASEAN has made progress in aligning national data-governance regimes around shared principles, but the next phase must focus on making trusted compliance more portable across markets. Without stronger recognition of credible safeguards established in one jurisdiction, firms may still need to repeat transfer assessments, contractual protections, filings and sector-specific reviews for the same data architecture, even where standards are broadly comparable. The opportunity for ASEAN is not simply to replicate existing international mechanisms, but to make trust more portable across one of the world's most diverse regional digital markets. Its digital competitiveness will increasingly depend not only on the volume of data it generates, but on whether trust can move with that data across borders. This requires a shift from policy alignment to portable trust, where compliance, safeguards and assurance mechanisms recognised in one market can support trusted data flows across the region.



Trust and security

Security remains the strongest-performing component of the Digital Nations Index, with an average score of 64, reflecting sustained efforts by ASEAN governments, regulators and industry stakeholders to strengthen cybersecurity, combat scams and fraud and improve online safety. Malaysia, Thailand, the Philippines and Brunei already have mature secure-by-design processes.

However, the rapid emergence of AI-enabled threats is changing the security landscape. As attacks become more scalable, personalised and difficult to detect – including through deepfakes, voice cloning and AI-generated scams – the distinction between authentic and fraudulent interactions is blurring. As a result, trust cannot come from simply whether content appears genuine and instead depends on independent verification of identity, authority and transaction intent. This is pushing governments, financial institutions and telecoms operators to invest in stronger authentication, fraud-intelligence sharing and real-time risk detection capabilities.

Recent examples show how this shift is already taking shape. Singapore uses AI tools to review around 400,000 websites and disrupt roughly 1,000 suspected scam sites each day,¹⁷ while Bank Negara Malaysia reports that banks collectively blocked about MYR1.2 billion (\$293 million) in fraudulent transactions in 2025 through stronger fraud detection and intervention controls.¹⁸ In a similar vein, in the Philippines, the implementing rules of the 2025 Anti-Financial Account Scamming Act require institutions to detect, delay, verify and trace disputed transactions rather than relying on consumer vigilance alone. Thailand has also adopted a coordinated, system-level approach through its Committee for the Prevention and Suppression of Technology Crimes, which brings together the Ministry of Digital Economy and Society and other relevant agencies to coordinate and accelerate anti-scam efforts. Following these measures, Thai authorities reported that average daily scam losses fell from THB100 million (\$3 million) to THB25 million (\$754,000).

At the same time, the growing use of AI in defensive systems introduces new trust requirements. While automated tools can identify threats and respond to fraud at a scale that manual processes cannot match, confidence in these systems depends on transparency, accountability and human oversight. As agentic AI systems begin to make decisions and initiate actions autonomously, assurance frameworks will become increasingly important to ensure that powerful technologies remain explainable, auditable, contestable and aligned with human intentions.

For ASEAN, cybersecurity is becoming a strategic enabler for building digital nations. This extends beyond preventing cyberattacks and protecting systems from compromise to include the ability to detect threats quickly, respond effectively and restore services rapidly when disruptions occur. It also encompasses protection against online fraud, scams and digital deception. Trusted digital economies will therefore require resilient cyber defences, effective fraud prevention frameworks, regional threat-intelligence sharing and common approaches to AI assurance. Countries that build trust in emerging technologies will be better positioned to accelerate digital adoption, attract investment and support innovation, whereas persistent security concerns risk slowing progress across every other pillar of digital transformation.

Singapore illustrates how ASEAN can move from secure-by-design principles to evidence-based assurance. Its approach combines real-world testing, independent validation and international standardisation to build trust in AI systems before they are deployed at scale. For example, the AI Agents Sandbox, launched in 2025 by the Singapore government and Google, tests AI agents in live operating environments rather than evaluating models in isolation. By exposing agents to real workflows, data, tools and adversarial scenarios, the initiative identifies deployment risks that may not appear in theoretical assessments. This gives organisations greater confidence that AI systems can operate safely and reliably in practice while enabling governance controls to be refined based on observed behaviour.

Trusted digital economies will require resilient cyber defences, effective fraud prevention frameworks, regional threat-intelligence sharing and common approaches to AI assurance

¹⁷ "Singapore International Cyber Week 2025 – Speech by Mr Goh Pei Ming, Minister of State, Ministry of Home Affairs and Ministry of Social and Family Development", Ministry of Home Affairs, October 2025

¹⁸ Key developments in the second half 2025, Bank Negara Malaysia



Trust and people

People remain crucial to digital transformation. Infrastructure, innovation, data governance and security provide the foundations of digital nations, but their success ultimately depends on whether citizens feel confident, included and empowered to participate in increasingly digital societies. Trust is therefore a key factor in the people component of the Digital Nations Index, shaping not only digital adoption but also how individuals engage with emerging technologies and benefit from digital transformation. In the 2026 Digital Nations Index, ASEAN's average score for this component reached 62, reflecting significant progress in expanding digital inclusion through improved connectivity, affordability, digital literacy and online safety.

However, important inclusion gaps remain across ASEAN countries as they enter the AI era. Millions of people still face barriers related to device access, affordability, skills and confidence, even where network coverage is available. AI is also creating new divides between those able to use advanced digital tools productively and those without the skills or confidence to do so. Trust has become an essential bridge between access and meaningful participation, as people are more likely to adopt new technologies when they understand their value and can rely on trusted intermediaries to help manage risks and opportunities.

Schools, community organisations, public institutions and mobile operators all have a role in building digital confidence and resilience. Examples from the Philippines and Singapore show how trust can be built by linking digital access to practical outcomes. In 2026, the Philippines' Project ACTIVATE, under the Trabahong Digital initiative, combined ICT equipment with structured training for students and teachers, connecting access to learning, digital work and income opportunities. Meanwhile, Singapore incorporated genAI skills into its Digital Skills for Life framework in 2025, building on a network of Digital Ambassadors that has supported more than 370,000 older people.

Trust also has a workforce dimension. Across ASEAN, AI is expected to reshape jobs and business processes, making worker adaptation, skills development and workforce readiness increasingly important. People are more likely to embrace AI when they see opportunities for productivity, career progression and inclusion rather than displacement. Trusted digital nations are therefore built not only through technology investment, but by giving citizens the confidence, skills and agency to participate fully in the digital economy. Countries that strengthen digital trust among their populations will be better positioned to turn technological progress into inclusive economic and social development.

03

Guardians of digital trust



Trust in the age of sovereignty

As ASEAN moves into the next phase of digital transformation, trust is becoming as important as connectivity in shaping the region's digital economy. Citizens, businesses and governments rely on digital services for public access, transactions, communication and innovation – but adoption depends on confidence that these services are secure, reliable, resilient and accountable. Trust has become more than a technical or regulatory issue, becoming a strategic condition for digital growth, investment and regional integration.

Trust has grown in importance as digital technologies have become more embedded in economic and social life. Governments have expanded digital identity programmes, accelerated AI adoption, strengthened cybersecurity frameworks and stepped up efforts to combat online scams and fraud. In parallel, greater dependence on digital infrastructure, cloud services and data-driven systems has heightened concerns about resilience, security and accountability.

A key development has been the growing emphasis on digital sovereignty. Across ASEAN, governments are seeking greater assurance that critical digital assets – including data, digital identity systems, communications infrastructure, cybersecurity capabilities and AI systems – are governed in ways that support national priorities while remaining connected to global digital markets.

Trust and sovereignty are distinct. Trust is about confidence that digital systems, services and organisations will operate securely reliably, transparently and accountably; sovereignty focuses on the control and governance of critical digital assets. While sovereignty measures can support trust in some contexts, trust can also be reinforced through interoperability, international standards, effective regulation, public–private collaboration and cross-border cooperation. For ASEAN, the task is not simply to balance sovereignty with openness, but to build trusted digital ecosystems that enable innovation, investment, adoption and regional integration.

Digital trust can be understood through four questions that every person, business and government implicitly asks when engaging in the digital world, and these questions correspond to four interconnected foundations of digital trust:



Identity

Who am I interacting with?



Communications

What is the intent of the interaction and is it safe?



Resilient networks

Where is the interaction taking place?



Collective intelligence

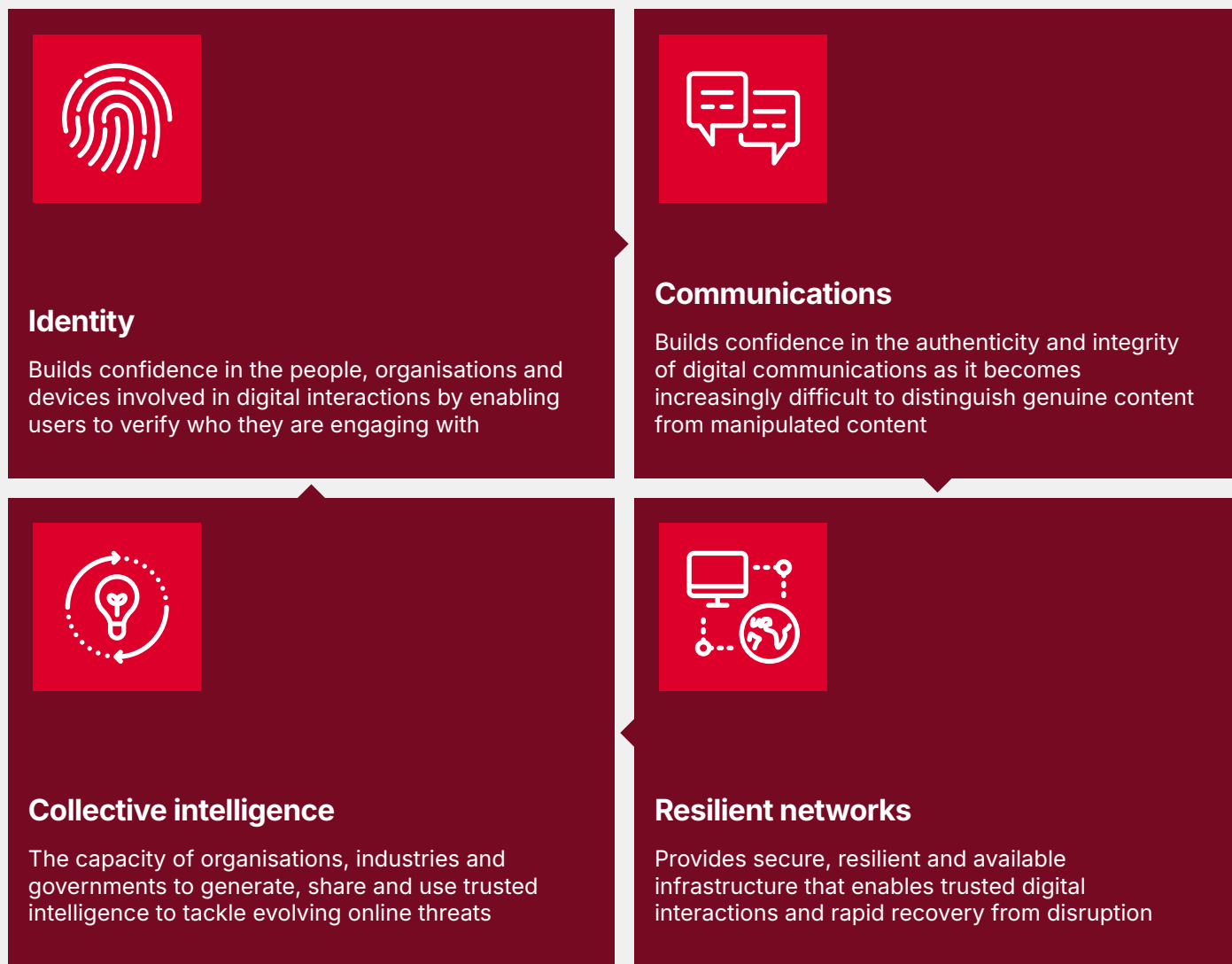
How are emerging risks being identified and managed, and how are our strategies evolving to outpace new malicious tactics?

As citizens, businesses and governments become more dependent on digital technologies, their confidence will increasingly rest on these foundations of digital trust (see Figure 4).

Figure 4

The four foundations of digital trust

Source: GSMA Intelligence



The interdependent nature of these foundations means that failure in one area can quickly weaken confidence across the wider digital ecosystem. For example, a cyberattack can disrupt communications; weak identity verification can enable fraud; and a lack of collaborative, cross-sector intelligence sharing can weaken efforts to stay ahead of cybercriminals, scammers and other malicious actors. When strengthened together, however, these foundations reinforce one another and create a virtuous cycle of trust that supports adoption, investment, innovation and growth.

Protecting these foundations requires active guardianship rather than passive compliance. Governments, regulators, technology providers, businesses, civil society organisations and mobile operators all contribute to strengthening the foundations of trust that digital economies depend on. However, few organisations work across all four trust foundations as extensively as mobile operators, giving them a distinctive role as guardians of trust in the digital age.

3.2

Mobile operators as guardians of digital trust

The growing importance of trust and digital sovereignty across ASEAN is reshaping the role of mobile operators. Traditionally viewed as providers of connectivity, mobile operators are increasingly becoming providers of trust. As digital economies become more dependent on secure identities, trusted communications, resilient infrastructure and trustworthy data and AI systems, operators are playing a central role in enabling each of these foundations.

Mobile operators occupy a unique position at the intersection of all four foundations of digital trust. They manage critical communications infrastructure, maintain trusted relationships with millions of customers, verify identities through SIM registration and authentication processes, secure networks against cyberthreats and generate insights from network data that support service delivery, security and innovation. This combination of assets, capabilities and reach makes them essential partners in the development of trusted digital ecosystems. Their roles in strengthening the core foundations of digital trust are outlined in the following sections.

Trusted digital identity: knowing who you can trust

Digital identity allows individuals and organisations to prove who they are online, providing a trusted basis for accessing services, completing transactions and interacting securely across digital platforms. Trusted digital identity systems support secure access to government services, banking, payments, document signing and business transactions while also helping to reduce fraud, strengthen cybersecurity and enable smoother cross-border digital interactions. Across ASEAN, digital identity is increasingly treated as a strategic asset and a key enabler of digital transformation.

For example, Singapore's Singpass provides secure access to a wide range of public and private services through a single trusted login, while Thailand's National Digital ID supports identity verification across financial institutions and government agencies. Malaysia's MyDigital ID and Indonesia's expanding digital identity infrastructure further reflect regional efforts to strengthen digital public infrastructure, improve service delivery and support financial inclusion. At the regional level, ADM 2030 encourages secure, interoperable digital identity frameworks to support trusted cross-border services and digital trade. As more social and economic activity moves online, these systems are becoming increasingly important enablers of trust, security and seamless digital interactions across ASEAN.



The role of mobile operators in enabling trusted identity

Mobile operators have long supported identity verification, with SIM registration making mobile numbers one of the most widely used digital identity anchors across ASEAN. Operators are now broadening this role through several complementary capabilities.

Authentication APIs

Operators are using APIs such as the Number Verify API to check that a phone number is associated with a particular device. This reduces reliance on SMS one-time passwords, which are increasingly exposed to interception and social-engineering scams. For example, in September 2025, Malaysian operators CelcomDigi, Maxis, U Mobile, Telekom Malaysia and YTL Communications unveiled plans to launch a new federated network service for online businesses to help them combat fraud and digital identity theft, through the GSMA Open Gateway initiative. This enables banks and online businesses to validate customer phone numbers against operator data during account registration and high-value transactions.

Network-based authentication APIs use secure connections to match live network signals, such as IP addresses and IMSI data, with carrier records to confirm device possession without requiring manual user input. For example, Singtel, AIS and Maxis formed an interoperable telco API alliance based on GSMA standards, allowing enterprise applications in Singapore, Thailand and Malaysia to use real-time network signals to detect threats such as bot attacks and unauthorised account changes. In Indonesia, Telkomsel partnered with IPification to deploy one-click mobile authentication in Indonesia, allowing its subscribers to access digital services through network-based verification without SMS codes or passwords.

Integration with digital identity ecosystems

Operators are also linking their verification systems with government-backed digital ID platforms, strengthening customer onboarding and know-your-customer (KYC) processes through trusted national identity infrastructure. For example, Malaysian operators have connected their verification systems to MyDigital ID, requiring new prepaid SIM purchases and account set-ups to be validated against the national ID platform to reduce identity theft and anonymous misuse. Similarly, Telkomsel and other Indonesian operators have worked with Komdigi to introduce biometric-based customer registration under the 'One Identity, One Nation' framework to link telecoms KYC records with biometric identity verification.



Trusted communications: protecting digital interactions

Communications covers the security, reliability and authenticity of interactions between people, businesses and governments. Increasingly, the challenge is less about securing communications alone and more about helping users assess whether the content and information they receive is authentic, reliable and not manipulated. As scams, impersonation and AI-enabled fraud grow, trust in communications has become a critical foundation for confidence in the wider digital economy.

Whether users are sending messages, making payments, using cloud-based applications, engaging in digital commerce or accessing public services, they need confidence that their communications are protected from fraud, interception and manipulation. As ASEAN's digital economy becomes more interconnected, trusted communications are critical to combating cybercrime, online scams, phishing and misinformation while enabling safer cross-border transactions and greater participation in digital services.

Across ASEAN, regulators and operators are also strengthening measures to tackle text-message scams, online fraud, cyber-enabled financial crime and identity-related abuse. The Philippines has intensified cooperation between telecoms operators, regulators and law-enforcement agencies, while Thailand and Malaysia have tightened SIM registration and fraud-prevention requirements. These measures show that secure communications is becoming central to digital trust, user protection and ASEAN's broader digital sovereignty agenda.

The role of mobile operators in enabling trusted communications

Across ASEAN, mobile operators are becoming a frontline defence against communication fraud, using network capabilities, real-time data and cross-sector coordination to detect, block and prevent scams before they reach users or compromise digital services.

Network-level spam filtering and malicious-message detection

Operators are moving from reactive blocking to real-time filtering at the network layer, suppressing scam URLs, smishing and phishing texts before they reach subscribers. In the Philippines, Globe Telecom and Smart Communications have deployed SMS blocking, with Globe blocking nearly 1 billion spam messages in 2025,¹⁹ and Smart blacklisting 615,788 mobile numbers linked to illicit activity and smishing in the first half of 2024.²⁰ In Thailand, operators block more than 1 million inbound scam SMS messages each day under the direction of the National Broadcasting and Telecommunications Commission.

SIM-swap detection and verification

SIM-swap fraud remains a major vulnerability across the region, particularly in Indonesia and the Philippines, where attackers could transfer a victim's number to a new SIM to intercept bank one-time passwords. Under the GSMA Open Gateway framework, Philippine operators Smart, Globe and Dito signed a memorandum of understanding in February 2025 to collaborate on the deployment of federated CAMARA APIs to combat fraud, enhance identity verification and foster a more secure and innovative digital ecosystem.

Anti-fraud APIs for banks and digital platforms

Operators are exposing network signals through standardised APIs, giving financial institutions real-time risk indicators to secure onboarding, payments and account changes. Singtel's SingVerify, for example, enables banks to assess device attributes such as network presence, location proximity and SIM-level connection security without relying on manual user confirmation or out-of-band communication.

Fraud-signal sharing

Because scams often cross borders and sectors, operators are also building shared mechanisms to exchange threat intelligence and coordinate responses. The GSMA-led Asia Pacific Cross-Sector Anti-Scam Taskforce (ACAST), launched in June 2025 under the Global United Against Scams initiative, brings together operators, digital platforms, technology specialists and public authorities to share evidence, align technical approaches and develop privacy-respecting data-sharing models. As the first structured cross-sector anti-scam mechanism in Asia Pacific, ACAST provides a foundation for more coordinated action by spearheading an industry response beyond competitive silos. By enabling information exchange and coordinated intervention, it strengthens Asia Pacific operators' ability to detect, block and disrupt scams through network-level controls, spam monitoring and other detection techniques. As of March 2026, ACAST had 39 members across 17 countries.²¹

¹⁹ "Globe blocks nearly 1 billion spam texts in 2025", The Philippine Star, February 2026

²⁰ "Globe, Smart block scam numbers amid unabated spam messages", Philippine News Agency, July 2024

²¹ "The scam economy thrives in silos. Coordination is our strongest defence", GSMA, March 2026



Trusted resilient networks: keeping digital systems running

Trusted networks are reliable, secure, resilient and able to recover quickly from cyberattacks, natural disasters, technical failures and other disruptions, ensuring that digital services remain available. As economies become more digital, communications networks, cloud platforms, data centres and cybersecurity systems are increasingly treated as critical national infrastructure. Disruptions to these systems can affect essential services, including banking, healthcare, transport, government operations and emergency communications.

ASEAN member states are responding by strengthening network resilience, infrastructure security and cybersecurity governance. Notably, Malaysia's Cyber Security Act 2024 establishes a framework for protecting national critical information infrastructure and clarifies responsibilities for oversight and incident response, while Singapore's Cybersecurity Act and critical information infrastructure regime focus on safeguarding essential

services from cyberthreats. Indonesia is expanding domestic data centre and cloud capacity while strengthening cybersecurity through the National Cyber and Crypto Agency, whereas Vietnam has prioritised cyber resilience through its Law on Cybersecurity and related rules for protecting critical information systems.

At the regional level, the ASEAN Cybersecurity Cooperation Strategy 2026–2030 frames cybersecurity as economic infrastructure. Member states are also strengthening regional coordination through the ASEAN Regional CERT, which supports real-time cross-border threat-intelligence sharing. Complementary initiatives, such as the Malaysia-hosted ASEAN Cybersecurity Resilience and Information Sharing Platform, provide common channels for exchanging information on sophisticated cyberattacks and ransomware. Broader resilience efforts also include improving redundancy in intra-ASEAN submarine cables, reducing dependence on third-party hardware and aligning national cybersecurity frameworks with international standards such as the NIST Cybersecurity Framework and ISO 27001, particularly for critical energy and financial networks.

The role of mobile operators in trusted resilient networks

Across ASEAN, mobile network operators are evolving from connectivity providers into critical partners in national resilience. Their investments in hardened infrastructure, emergency communications, redundancy, supply-chain security and alternative connectivity help keep essential services operational during cyberattacks, natural disasters and other disruptions.

Hardening national communications infrastructure

Operators invest in resilient physical assets to protect core communication networks from extreme weather and other shocks. In the Philippines, for example, new cellular towers are engineered to withstand super typhoons with wind speeds of up to 300 kilometres per hour, helping transmission networks remain operational during severe storms.

Enabling emergency communications

During disasters, mobile networks can support targeted public safety alerts and coordination. In Cambodia, Smart Axiata works with the National Committee for Disaster Management and the Ministry of Post and Telecommunications on the 1294 Early Warning System, using geographic targeting to send high-priority flood alerts to subscribers near at-risk cell sites and giving communities more time to evacuate.

Building redundancy across network assets

Operators reduce single points of failure by using overlapping transmission paths and cloud-native network architectures. In Malaysia, CelcomDigi and Maxis combine terrestrial fibre, microwave links and cloud-based network cores so traffic can shift to alternative routes if flooding or other disruptions damage physical infrastructure.

Strengthening supply-chain security

As cyberthreats and supply-chain risks increase, operators are strengthening oversight of their technology supply chains through diversification, assurance processes and vendor risk management. In Singapore, telcos operate under the oversight of the Cyber Security Agency and IMDA, using multi-vendor strategies and ongoing firmware checks for critical 5G core components to reduce dependency and improve resilience.

Integrating satellite and non-terrestrial networks

Satellite-linked base stations and other non-terrestrial capabilities provide back-up connectivity when terrestrial networks are damaged or unavailable. In the Philippines, operators increasingly use satellite backhaul and portable connectivity solutions to restore communications following typhoons and other natural disasters, helping maintain essential services and emergency communications during recovery efforts.

Supporting disaster response

Operators provide rapidly deployable infrastructure for emergency services and humanitarian operations. In Indonesia, Telkomsel's compact mobile base stations are satellite-linked vehicles that can be sent into disaster zones to restore mobile coverage for rescue teams and aid distribution points and displaced communities.



Trusted collective intelligence: data sharing for online threat mitigation

As digital ecosystems become more interconnected, trust increasingly depends on the ability of organisations to anticipate, detect and respond to emerging risks together. Malicious actors routinely share tools, intelligence and tactics across borders, sectors and platforms, while defenders often remain fragmented. Strengthening digital trust therefore requires trusted mechanisms for collaboration and information sharing across the wider ecosystem.

Given this context, collective intelligence describes the creation, sharing and use of trusted information to strengthen the security, resilience and integrity of digital systems. It includes threat intelligence, fraud insights, operational data and risk indicators exchanged between governments, mobile operators, financial institutions, technology providers, cybersecurity agencies and law enforcement. By combining data, analytics and AI with human expertise and institutional cooperation, collective intelligence helps organisations identify threats earlier, coordinate responses more effectively and reduce the impact of cyberattacks, scams and fraud.

For ASEAN, strengthening collective intelligence will be essential to trusted digital economies. Regional cooperation, public-private partnerships and cross-sector information-sharing frameworks can improve situational awareness, accelerate incident response and support more effective scam and fraud prevention. As digital economies in ASEAN become more integrated, the ability to share and act on trusted intelligence will be a critical component of digital trust.

The role of mobile operators in enabling trusted collective intelligence

With visibility across networks, devices and communications, mobile operators can often detect emerging threats and fraud early. By sharing intelligence, enabling coordinated responses and working with governments and other digital ecosystem participants, they can strengthen collective resilience and act as important anchors of digital trust.

The GSMA Data Exchange Proof of Concept

Launched in 2025, the GSMA Data Exchange Proof of Concept (PoC) offers a practical example of collective intelligence in action. It explores how mobile operators can support ecosystem-wide scam prevention through trusted data sharing, recognising that no single organisation has full visibility of the scam lifecycle. Financial institutions can see fraudulent transactions, digital platforms can detect malicious accounts, law enforcement can investigate criminal networks, and mobile operators can provide network and communications signals that help identify suspicious activity earlier.

The PoC tests how privacy-preserving sharing of telecoms-derived scam signals can support earlier detection and intervention before scams are confirmed or victims suffer financial loss. By securely exchanging and analysing pseudonymised indicators, participating organisations can identify upstream scam risks, assess which telecoms signals deliver measurable prevention benefits and evaluate the technical and governance models needed for wider deployment.

The initiative shows that the value of collective intelligence lies not in sharing more data, but in combining diverse observations to build a fuller picture of emerging threats. Aggregate analysis of anonymised data enabled participating operators to identify overlaps in known scam activity, uncover new threat indicators and measure the additional insights created through collaboration. The pilot showed that scam risks often become clearer when signals from multiple organisations are viewed together, creating opportunities for earlier and more effective intervention.

More broadly, the PoC illustrates how mobile operators can contribute to collective intelligence. Their visibility across networks, devices and communications channels enables them to detect patterns that may be less visible to other stakeholders. When shared through trusted, privacy-preserving mechanisms with financial institutions, digital platforms, regulators and law enforcement agencies, these insights can strengthen ecosystem awareness, improve scam prevention and support more coordinated responses to emerging threats. In this way, the GSMA Data Exchange PoC demonstrates how cross-sector collaboration can strengthen digital trust.



The new trust challenge: scams, AI and the future of digital trust

For much of the digital era, trust was viewed mainly through a cybersecurity lens: protecting networks, securing systems and safeguarding data from unauthorised access. These priorities remain essential, but the trust challenge is changing. Increasingly, the issue is not only whether systems can be compromised, but whether people can distinguish legitimate digital interactions from fraudulent ones.

Across ASEAN, scams and fraud have become among the most visible threats to confidence in the digital economy because they affect people's everyday interactions. Consumers are increasingly expected to judge whether a message, call, payment request, website, social media post or digital identity is genuine. As fraud becomes more sophisticated, this becomes harder to verify, weakening confidence in digital services and reducing willingness to engage online.

AI is intensifying this challenge by allowing highly convincing phishing messages, fake websites, cloned voices, synthetic images and deepfake videos to be produced at scale and low cost. Fraudsters can also personalise attacks using publicly available information, making them more difficult to detect and potentially more damaging. Trust is therefore becoming an authenticity challenge: people need confidence not only that systems are secure, but that the individuals, communications and content they interact with are genuine.

This shift has important implications for digital policy. Consumer awareness and cybersecurity controls remain important, though they are no longer enough on their own. Building trust now requires stronger identity verification, authentication, fraud-intelligence sharing and cross-sector cooperation between telecoms operators, financial institutions, digital platforms and public authorities. Trust must be built into digital interactions, rather than relying on citizens to detect increasingly sophisticated fraud.

Mobile operators play an important role in this effort. Through network intelligence, authentication services, number verification and fraud-detection systems, they can help verify identities, detect suspicious activity and block fraudulent communications before they reach users. Initiatives such as the GSMA Open Gateway, anti-fraud APIs and industry cooperation mechanisms show how trusted communications infrastructure can support safer digital ecosystems. The GSMA-led Asia Pacific Cross-Sector Anti-Scam Taskforce (ACAST) also highlights the need for coordinated action against scams that operate across sectors and borders.

As ASEAN advances towards more sophisticated digital economies, digital transformation will depend on connectivity, innovation, access and, crucially, trust. In an era of AI-enabled deception, strengthening trust means strengthening authenticity, so people can participate with confidence that the identities, communications and services they rely on are legitimate, secure and accountable.

04

Strengthening the foundations of digital trust



As digital technologies become embedded across ASEAN economies, trust will shape the pace, scale and sustainability of digital adoption. Although governments, regulators, operators and regional institutions have made progress in building trusted digital ecosystems, emerging technologies, evolving cyberthreats, deeper digital interdependence and geopolitical uncertainty are increasing the need to strengthen trust foundations. This requires coordinated action from three stakeholder groups: governments and regulators that set resilience policies; mobile operators as guardians of digital trust; and regional institutions that support interoperability, coordination and common frameworks for trusted cross-border interaction.

4.1

Priorities for governments and regulators

Governments and regulators are central to creating the conditions for trusted digital economies. Their role is not only to manage risk but also to enable innovation, investment and inclusive digital participation.

Enabling trusted identity ecosystems

Digital identity is becoming a core component of digital economies. Governments have an important role in creating an enabling environment for secure, inclusive and interoperable digital identity ecosystems that allow citizens and businesses to access services safely and efficiently. Priorities include extending digital ID use across public and private services, improving interoperability between national and sector-specific systems, strengthening authentication, security and privacy safeguards.

Strengthening secure communications

Trust in digital services depends on confidence that communications are authentic, secure and protected from fraud. Governments should work more closely with telecoms operators, digital platforms, financial institutions and technology providers to combat scams, phishing and cyber-enabled fraud. This includes stronger fraud reporting, cross-sector information sharing, consumer protection and enforcement against digital criminal networks. For example, the IMDA in Singapore enforces the mandatory SMS Sender ID Registry, requiring businesses that use alphanumeric sender names, such as bank names, to register in advance. Unverified messages are blocked at the operator level, helping prevent brand impersonation scams.

Enhancing cybersecurity and resilience

As digital infrastructure becomes critical to economic and social activity, resilience must be a core policy objective. Governments should strengthen cybersecurity capabilities, critical infrastructure protection and incident response. Priority actions include improving national computer emergency response team (CERT) and computer security incident response team (CSIRT) capacity, running regular cyber resilience exercises, strengthening incident reporting, promoting supply-chain risk management and encouraging business continuity planning across critical sectors. In Indonesia, following high-profile government data breaches, the National Cyber and Crypto Agency has established specialised CSIRTs across major regional municipalities with strict security audits for digital assets that handle national critical infrastructure data and clear protocols for reporting cyber extortion attempts.

Supporting trusted AI and data governance

AI and data are increasingly central to digital economies, but public confidence depends on governance that promotes transparency, accountability and responsible use. Governments should prioritise AI assurance, risk-based governance, transparency requirements for higher-risk applications and capacity building for regulators and policymakers. Data-governance frameworks should also support innovation while protecting privacy and maintaining public trust. In Thailand, the Ministry of Digital Economy and Society coordinates the National AI Strategy and Action Plan, which establishes ethical auditing standards for automated processing and prioritises locally relevant medical and agricultural AI tools that comply with the Personal Data Protection Act.

Facilitating cross-sector collaboration

Digital risks increasingly span communications networks, financial systems, healthcare services, government platforms and digital marketplaces. Yet responsibility for these areas is often split across regulators, agencies and ministries with separate mandates, creating coordination gaps that malicious actors can exploit. Building trusted digital ecosystems therefore requires a whole-of-government and whole-of-ecosystem approach, with public authorities able to share information, coordinate responses and align policy objectives. Similar collaboration is needed across the private sector, including mobile operators, financial institutions, digital platforms, cloud providers and cybersecurity firms. Trust now depends on these actors working together, rather than in isolation.

Strengthening anti-scam cooperation

Governments should promote closer collaboration between telecoms operators, financial institutions, digital platforms and law enforcement agencies to detect, disrupt and prevent scams. As fraud increasingly spans sectors and jurisdictions, trust will depend on coordinated approaches to authentication, intelligence sharing and consumer protection.

Ensuring the resilience of digital infrastructure

As digital systems become further embedded in critical economic and social functions, governments have an important role to play in fostering coordination across critical infrastructure sectors, including telecoms, energy, transport, cloud infrastructure and emergency services. This coordination will become increasingly important as new connectivity technologies are deployed. The growing role of low Earth orbit (LEO) satellite services, direct-to-device capabilities and hybrid terrestrial-satellite networks creates opportunities to strengthen resilience and extend connectivity, particularly in remote and disaster-prone areas.

Deepening regional cooperation

Many trust challenges, including cybercrime, online fraud and AI-related risks, extend beyond national borders. Governments should strengthen regional cooperation through joint cybersecurity initiatives, shared threat intelligence, cross-border fraud prevention and common trust-assurance frameworks. For example, the ASEAN-Japan Cybersecurity Capacity Building Centre in Bangkok trains regional cybersecurity professionals through live malware-containment simulations, helping strengthen technical defence capabilities across less-developed ASEAN economies.

4.2

Priorities for mobile operators

Mobile operators are well placed to provide a trusted layer of digital infrastructure that helps other parts of the digital ecosystem verify, secure and protect digital interactions.

Building towards a digital trust layer

Identity is one of the clearest opportunities for operators to create value while reinforcing trust. By combining trusted subscriber relationships with network intelligence, operators can make digital interactions more secure and easier to use. Priority areas include mobile identity solutions, number verification, authentication APIs, digital onboarding and integration with national digital ID systems. Initiatives such as the GSMA Open Gateway show how operators can help banks, digital platforms and governments verify users through network-based authentication, reducing reliance on vulnerable passwords and one-time passcodes. In Cambodia, Smart Axiata has deployed number verification and KYC-matching APIs to help protect fast-growing domestic e-wallets. Its backend systems silently verify requests from integrated financial institutions, confirming whether a mobile number matches the registered subscriber identity before a new digital account is authenticated.

Collaborating with the broader digital ecosystem to combat fraud

Scams remain one of the most visible threats to digital trust across ASEAN, and no sector can address them alone. Mobile operators are uniquely positioned to contribute network-level intelligence and capabilities, but effective scam prevention increasingly depends on collaboration across operators, financial institutions, digital platforms, governments and other ecosystem actors. Priority areas include sharing threat intelligence and scam indicators, coordinated detection and response, stronger fraud-risk controls, and joint consumer awareness campaigns. Such collaboration can help identify and disrupt scams earlier, close gaps between sectors and strengthen protection across the full digital journey.

The Philippines provides a strong example of cross-sector collaboration. In 2022, Globe entered into data-sharing agreements with the Bankers Association of the Philippines, representing 45 major banks, to establish an intelligence-sharing mechanism for combating scams. The arrangement enables banks to share information on suspicious numbers, phishing attempts and other fraud indicators with Globe, which can then investigate and block related messages, numbers and URLs. Globe reported an 85% decline in bank-related scam and spam SMS in the first three quarters of 2023, highlighting the potential impact of connecting intelligence across the telecoms and financial sectors.

Investing in resilient infrastructure

As critical infrastructure providers, operators must continue strengthening network and platform resilience. This includes investment in redundancy, cybersecurity, disaster recovery, emergency communications, security operations centres and threat intelligence. Given ASEAN's exposure to natural disasters and rising cyberthreats, resilience will remain a defining feature of trusted digital infrastructure. In Vietnam, Viettel has built redundancy into its 5G core, enabling the network to activate prioritised traffic-slicing layers for government and emergency-rescue communications during severe coastal typhoons, helping maintain service continuity when terrestrial links are damaged.

Developing trusted intelligence capabilities

Operators are increasingly using data, analytics and AI to improve customer experience, strengthen security and optimise network performance. The priority is to ensure these capabilities are deployed responsibly, transparently and securely. This requires AI governance frameworks, trusted analytics, privacy-enhancing technologies and responsible data management. By demonstrating leadership in trusted AI adoption, operators can improve operational performance while strengthening public confidence.



4.3

Priorities for ASEAN

ASEAN has a distinctive role in scaling up digital trust across borders. While governments set national frameworks and operators deploy trust capabilities, regional institutions can create the mechanisms for interoperability, coordination and collective action.

Advancing trust interoperability

Digital trust becomes more valuable when trusted systems can operate seamlessly across borders. ASEAN should continue supporting interoperability between national digital identity systems, authentication mechanisms and trust frameworks. Reducing fragmentation will improve user experience, lower compliance costs and support deeper regional digital integration. For example, the ASEAN Digital ID Interoperability Framework, driven by the ASEAN Digital Ministers' Meeting, is establishing common technical rules and assurance levels for national digital identity registries such as Singapore's Singpass, Malaysia's MyDigital ID and Thailand's ThaiID. By mapping how authentication tokens can be exchanged securely across borders, the framework could enable a business in Indonesia to verify a corporate client in Vietnam without relying on manual documentation, for example.

Supporting trusted cross-border services

Cross-border digital services are increasingly important to regional growth. Digital payments, e-commerce, cloud services and digital trade all require trust mechanisms that work consistently across jurisdictions. ASEAN can support this by facilitating regulatory dialogue, promoting common technical standards, encouraging mutual recognition and advancing regional fraud-prevention initiatives. For example, ASEAN's regional cross-border payment connectivity initiative, supported by the South East Asian Central Banks (SEACEN) and BIS Innovation Hub, links instant payment systems in Singapore, Thailand, Malaysia, Indonesia and the Philippines, including PayNow, PromptPay, DuitNow, QRIS and InstaPay. By embedding common anti-money-laundering and network-security standards into payment routing, the initiative enables safer, real-time cross-border QR payments for citizens and businesses.

Embedding trust in DEFA implementation

DEFA could become ASEAN's most important digital integration initiative, but its success will depend on trust. Guided by the ASEAN Economic Community Council, negotiators are embedding trust-by-design into DEFA's foundational text through harmonised frameworks for cybersecurity standards, cross-border data flows and consumer data protection. These provisions aim to give businesses operating across ASEAN clearer, more consistent compliance expectations.

Promoting a shared vision of trusted sovereignty

ASEAN can help shape a common regional understanding of trusted sovereignty. Although national approaches will differ, ASEAN can provide a framework that balances security, resilience and national control with openness, interoperability and innovation. By fostering dialogue and cooperation, regional institutions can help make trust a source of cohesion rather than fragmentation.

Scaling up regional anti-scam cooperation

ASEAN should support cross-border fraud-intelligence sharing, common authentication approaches and regional cooperation mechanisms to combat scams and AI-enabled deception.

A collective trust agenda for ASEAN

ASEAN's next phase of digital transformation will depend on its ability to strengthen and grow digital trust across the region. Trusted identity systems, secure communications, resilient networks and responsible intelligence are now essential foundations of digital economies. As AI systems advance, cyberthreats become more complex and digital services become more interconnected, trust will increasingly determine whether digitalisation supports resilience, inclusion and sustainable growth.

Trust can no longer be viewed solely through a national lens. Cross-border payments, digital identity systems, cloud services, e-commerce, data exchanges and AI applications all depend on trusted interactions between users, institutions and jurisdictions. A breach in one market, weak identity verification or inconsistent AI governance can create risks beyond national borders, while trusted and interoperable systems can accelerate regional integration and create new opportunities for businesses and consumers.

This interdependence reinforces the link between trust and digital sovereignty. ASEAN governments need confidence in the security, resilience and governance of critical digital assets while remaining open to trade, investment and innovation. The goal is therefore not to choose between sovereignty and openness, but to build trusted digital ecosystems that allow ASEAN countries to participate confidently in regional and global digital markets while maintaining confidence in the security, resilience and governance of critical digital assets.

Delivering this vision requires a collective trust agenda. Governments and regulators must create enabling frameworks and strengthen resilience; mobile operators must continue strengthening their role as providers of trusted digital infrastructure and services; and ASEAN member states must work together to support interoperability, coordination and trusted cross-border interaction. No single organisation can deliver digital trust alone; it emerges from coordinated action across the digital ecosystem.

GSMA
1 Angel Lane
London EC4R 3AB
United Kingdom
gsma.com

