GSMA

Digital Nations 2026

# Building trusted digital ecosystems in Asia Pacific



GSMA

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.gsmaintelligence.com

info@gsmaintelligence.com

**Authors**

Kenechi Okeleke, Senior Director
Sayali Borole, Senior Analyst
Celine Yuan, Senior Analyst

**Contributors**

Jeanette Whyte, Head of Policy & External Affairs, GSMA Asia Pacific
Ming Sheng Bensen Koh, Director, GSMA Asia Pacific

Published October 2026

© 2026 – GSMA.

# Contents


**Executive summary** 04

**01** The trust imperative 07

1.1 From digital adoption to trusted digital systems 08

1.2 Digital trust as a foundation of digital nations 10

**02** Measuring progress: the Digital Nations Index 11

2.1 What the index measures 12

2.2 The Digital Nations Index in the context of trust 13

2.3 The 2026 picture: leadership, catch-up and uneven maturity 14

**03** Guardians of digital trust 25

3.1 Trust in the age of sovereignty 26

3.2 Mobile operators as guardians of digital trust 28

**04** Strengthening the foundations of digital trust 35

4.1 Priorities for governments and regulators 36

4.2 Priorities for mobile operators 39

4.3 Priorities for international cooperation 40

# Executive summary



## Trust as an enabler of digital nation ambitions

Asia Pacific is entering a new phase of digital development. Over the past decade, governments, businesses and citizens have benefited from significant investment in connectivity, digital services and innovation. The challenge now is to ensure that increasingly interconnected systems can be trusted. As digital platforms become integral to economic activity, public services, finance, communications and emerging technologies such as AI, trust becomes a critical enabler of digital transformation.

Across the region, policymakers are paying greater attention to the security, resilience and governance of digital systems. This reflects growing recognition that connectivity alone does not guarantee adoption, productivity or inclusion. Citizens must be confident that digital interactions are secure. Businesses must be able to operate within predictable regulatory frameworks. Governments must ensure critical infrastructure remains resilient in the face of cyberthreats, fraud and disruption. In this context, digital trust is emerging as a strategic asset, shaping competitiveness, innovation and long-term growth.

The Digital Nations Index highlights both progress and divergence across Asia Pacific. Many economies continue to improve across the digital nation components of infrastructure, innovation, data governance, security and people, though the nature of the challenge is changing in some countries. While emerging economies are still focused on expanding connectivity, digital skills and institutional capacity, more advanced digital nations are increasingly concerned with AI assurance, interoperability, cyber resilience and trusted data flows. Across all levels of development, trust is becoming the common factor that determines whether digital investments can be translated into meaningful economic and social outcomes.

## Mobile operators as guardians of digital trust

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



**Trusted identity**
Enables the verification of individuals and organisations in digital environments



**Trusted communications**
Ensures the authenticity, security and integrity of digital interactions



**Trusted resilient networks**
Provide the infrastructure and cybersecurity capabilities needed to keep services available and secure



**Trusted intelligence**
Enables organisations to create, share and use trusted information to strengthen security, resilience and decision-making

Digital trust is a shared responsibility spanning governments, regulators, technology providers, financial institutions, digital platforms and civil society. Mobile operators play a distinct role across all four foundations. Through their management of critical communications infrastructure, trusted customer relationships, authentication capabilities, cybersecurity functions and scam prevention tools, operators help strengthen identity, secure communications, improve network resilience and support collective intelligence.

As digital ecosystems become more interconnected and complex, operators are evolving beyond connectivity providers to become guardians of digital trust, helping governments, businesses and citizens participate in the digital economy with greater confidence and security.

## Key priorities for stakeholders

Building trusted digital nations will require coordinated action across governments, industry and regional institutions. Governments should focus on strengthening the policy, regulatory and institutional foundations of trust, while operators support efforts to preserve digital trust through identity, communications, resilience and intelligence capabilities.

At the regional level, cooperation mechanisms can help improve interoperability, strengthen cyber resilience and support trusted cross-border digital services.

Table 1

### Key stakeholder priorities to strengthen the foundations of digital trust in Asia Pacific

Source: GSMA Intelligence

| | Stakeholder | Priorities |
|---|---|---|
|  | **Government and regulators** | — Enabling trusted digital identity ecosystems<br>— Strengthening secure communications and anti-scam measures<br>— Enhancing cybersecurity and critical infrastructure resilience<br>— Supporting trusted AI and data governance<br>— Deepening cross-sector and international cooperation |
|  | **Mobile operators** | — Strengthening digital identity and authentication services<br>— Combatting scams, fraud and cyberthreats<br>— Investing in resilient and redundant infrastructure<br>— Developing trusted intelligence and threat-sharing capabilities |
|  | **Regional institutions and international cooperation mechanisms** | — Advancing trust interoperability across borders<br>— Supporting trusted data flows and digital services<br>— Strengthening cross-border cyber resilience<br>— Scaling up regional anti-scam cooperation<br>— Promoting a shared vision of trusted digital development |

# 01
# The trust imperative



# 1.1
# From digital adoption to trusted digital systems

Across Asia Pacific, the digital policy agenda is moving beyond deployment of individual assets to the integration of trusted national systems. Earlier phases of digital transformation focused largely on expanding connectivity, broadband coverage and digital service adoption. These remain priorities, but the wider availability of advanced networks, cloud services, digital identity, real-time payments, data platforms and AI has raised the complex question of whether people, businesses and institutions can trust the digital systems on which economic and social activity increasingly depends.

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. Digital trust is therefore a central enabler of digital nation building, rather than a secondary compliance issue. As digital services become embedded in finance, commerce, government, health and education, concerns around cybersecurity, privacy, fraud, misinformation, data governance and system resilience are moving to the forefront of policymaking.



The challenge varies across Asia Pacific. Advanced digital economies are strengthening governance frameworks for AI, data protection and cyber resilience. Rapidly digitising economies are focused on building trusted identity systems, consumer protection mechanisms and institutional capacity to support secure adoption at scale. Examples include the following:

- In July 2026, the Australian government established a new Office of AI and indicated a move towards mandatory national AI standards, with legislation expected in early 2027. The shift would place greater responsibility for AI safety on regulated, legally enforceable systems rather than end users.
- Japan's AI Act came fully into force in September 2025, establishing a principles-based framework for AI promotion and governance without penalty provisions. It was followed by its first AI Basic Plan in December 2025 and updated AI Guidelines for Business in March 2026. Parallel reforms to the Act on the Protection of Personal Information, promulgated in July 2026, introduced an administrative surcharge regime and clearer rules on the use of personal data for AI training.
- India's Aadhaar ecosystem has continued to expand through a new official app, offline verification options, enhanced face authentication and the rollout of Central KYC 2.0 from August 2026. The new Aadhaar app had exceeded 31 million downloads by June 2026, less than five months after launch.[1]
- In June 2026, Singapore's Cyber Security Agency published the final Securing Agentic AI guidance, which provides a structured taxonomy and workflow mapping to help manage security threats across autonomous AI systems.
- South Korea's AI Basic Act took effect in January 2026, introducing risk-management obligations for high-impact AI systems and establishing supporting institutions, including an AI Safety Institute and a strengthened National AI Strategy Committee. Administrative fines are subject to a one-year transition period.
- Thailand is advancing Phase 2 of its Digital ID Framework (2025–2027), with a focus on verifiable credentials, digital wallets and interoperability. Nearly 1,800 government e-services are already connected, while the Electronic Transactions Development Agency is licensing digital ID providers ahead of plans to expand private-sector and cross-border use from 2027.[2]
- Vietnam's AI Law, which came into force in March 2026, introduced requirements for labelling AI-generated content, including deepfakes, and maintaining human oversight. Since July 2026, banks have also been required to detect biometric spoofing attempts.

At the regional level, the ASEAN Digital Economy Framework Agreement (DEFA) – which substantially concluded in 2025 and is expected to be formally signed in 2026 – identifies trusted digital identity, e-signatures and practical data governance as priorities for cross-border interoperability. This highlights the growing expectation that national trust systems should operate within a wider regional architecture.

Meanwhile, the rapid democratisation of generative AI (genAI) has made authentic interactions harder to verify, as voices, images, documents and identities can now be replicated or manipulated at low cost and on a large scale. Sumsub's Identity Fraud Report 2025–2026 recorded a 142% year-on-year increase in synthetic personal data attacks in Asia Pacific, raising their share to 15.7% of all regional fraud attempts. Deepfake growth was particularly high in markets including Malaysia (+408%), Thailand (+199%), Sri Lanka (+194%), Singapore (+158%) and South Korea (+137%).[3] These increases are notable because they have occurred even where overall crude fraud rates have stabilised or declined, suggesting a shift towards more sophisticated, AI-enabled attacks.

This moves the trust question from whether a system is available to whether a person, message or transaction is genuine; whether data is used appropriately; whether automated decisions can be explained and challenged; and whether institutions respond effectively when harm occurs. The risks are economic as well as social. Fraud, privacy breaches, service outages and weak security can cause direct losses and discourage adoption. Manipulated content, online abuse and opaque automated decisions can erode confidence, wellbeing and institutional legitimacy. These impacts are greatest where digital literacy, consumer redress, cybersecurity capability and enforcement capacity remain uneven.

1 "New Aadhaar app crosses 31 million downloads", Biometric Update, June 2026
2 "Thailand advances Digital ID 2.0 with expanded digital trust framework", Biometric Update, June 2026
3 "Annual Sumsub Report Reveals Synthetic Personal Data in APAC Soars 142% YoY Amidst Fraud Crackdowns", Sumsub, November 2025

# 1.2
# Digital trust as a foundation of digital nations

For digital nations, trust determines whether people use digital services, businesses invest in digital channels, and governments can scale digital transformation without creating new systemic risks. Infrastructure must be secure and resilient; digital government must 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 more urgent as digital technologies have become more deeply embedded in daily life and AI has reshaped the nature of digital risk. Traditionally, trust focused on protecting networks, devices and data from unauthorised access or malicious attacks. Recent incidents show how failures in both security and service continuity can quickly test that confidence. In South Korea, a major telecoms breach in 2025 exposed around 26.96 million USIM-related records.[4] In Australia, a nationwide telecoms outage in July 2026 disrupted mobile services, payments and rail operations, while failures affecting emergency calls triggered more than 300 welfare checks.[5] Such incidents illustrate that digital trust depends not just on keeping data secure but ensuring that critical digital services remain dependable when users need them most.

Citizens are more aware of privacy risks and more concerned about how their personal data is collected, shared and used. 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.[6] 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.

Regulators have responded by strengthening data protection requirements, cybersecurity obligations and AI governance frameworks. In New Zealand, Information Privacy Principle 3A took effect in May 2026, extending transparency obligations by requiring organisations that collect personal information indirectly to notify the individuals concerned, subject to specified exceptions.

Although national governments and institutions are central to building trust within their own digital ecosystems, national action alone is no longer sufficient. 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 strong national capabilities and deeper regional/international cooperation on cybersecurity, digital identity, data governance, fraud prevention and AI governance.

Digital trust is no longer a secondary compliance issue but a core design requirement for digital nation building. Without it, inclusion can 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 platforms. Regional integration may be constrained by concerns over data protection, cybersecurity, fraud 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 countries in Asia Pacific advance increasingly ambitious national digital strategies alongside deeper regional cooperation, the priority is not simply to adopt new technologies, but to ensure they operate securely, transparently and accountably at scale, within countries and across borders.

Asia Pacific's next phase of digital development will depend less on the availability of individual technologies and more on the confidence and capability with which they are integrated. In this context, digital trust is the enabling layer that turns connectivity into meaningful participation, data into responsible innovation, and investment into long-term national capability, providing the foundation for resilient and inclusive digital economies.

4 "Final investigation results on 2025 telecoms data breach", Ministry of Science and ICT (MSIT), July 2025
5 "Telstra outage in Australia disrupts trains and payments; no evidence of 'malicious' activity", Straits Times, July 2026
6 "Why meeting APAC consumers' expectations of data privacy is key to effective marketing", Think with Google, June 2023

# 02
# Measuring progress: the Digital Nations Index



# 2.1
# What the index measures

GSMA Intelligence developed the Digital Nations Index to assess countries' readiness to capture the economic and social benefits of digitalisation. The 2026 edition covers 22 Asia Pacific countries and combines five mutually reinforcing components: infrastructure, innovation, data governance, security and people.

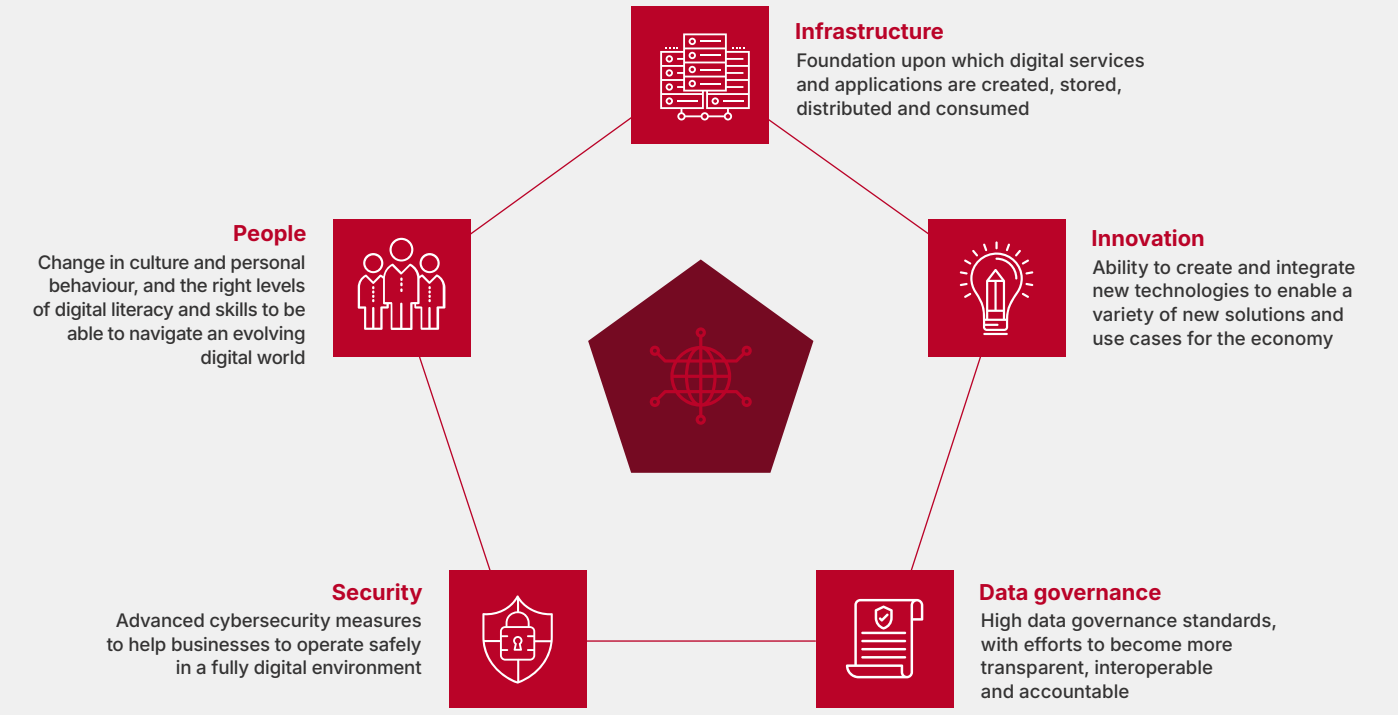
By bringing together indicators across these five areas, the framework provides a practical tool for benchmarking performance, tracking progress over time and identifying priorities for future policy and investment around the digital assets, institutions, safeguards and capabilities needed to translate digitalisation ambitions into broad-based outcomes.

The index should not be read as a league table. Aggregate scores provide a useful regional benchmark, but greater analytical value lies in the component profile behind each score. Two countries with similar totals may face very different constraints. One may have strong networks but weak skills; another may have capable people and firms but insufficient security or data governance foundations. The index is best used as a diagnostic tool to identify the weakest links in each country's digital system and to help policymakers sequence reform and investment.

Figure 1

## The five components of a digital nation

Source: GSMA Intelligence



# 2.2
# The Digital Nations Index in the context of trust

Digital trust cuts across all five components of the Digital Nations Index. It determines whether infrastructure is reliable, innovation is adopted, data is used responsibly, digital interactions are protected and people can participate with confidence. Trust is therefore the enabling condition that allows the five pillars to reinforce each other, shaping how digital capabilities are built but also whether they can translate into sustained economic and social value, as highlighted in Table 2.

Across all five areas, trust strengthens adoption, attracts investment and helps translate digital capabilities into sustained economic and social outcomes. The Digital Nations Index therefore serves as a measure of digital progress but also a lens for assessing the conditions that enable trusted, sustainable digital growth. The policy question has moved beyond whether people can access digital services to whether they can rely on those services to be secure, reliable, transparent and accountable. Digital trust should be treated as integral to the digital nations framework, rather than a separate pillar or standalone policy objective.

Table 2

## Trust as a cross-cutting factor

Source: GSMA Intelligence

| Component | Assessment focus | Trust question |
|---|---|---|
| **Infrastructure** | Connectivity, cloud and supporting digital infrastructure | Are essential digital systems available, resilient and recoverable? |
| **Innovation** | Ability to develop, adopt and scale technology | Can firms and institutions innovate with confidence and assurance? |
| **Data governance** | Rules and institutions for trusted data use and exchange | Can data be used and shared while safeguarding rights and legitimate interests? |
| **Security** | Cybersecurity, fraud prevention and online safety | Can users and organisations trust digital interactions to be safe and authentic? |
| **People** | Skills, inclusion and ability to use digital services | Can everyone participate with confidence and use digital services productively? |

# 2.3
# The 2026 picture: leadership, catch-up and uneven maturity

Singapore leads the 2026 Digital Nations Index with an aggregate score of 88, followed by Japan at 86. Their performances reflect broad-based capability rather than strength in a single component. Beyond these leaders, scores fall across a diverse regional cohort, with Myanmar, Papua New Guinea and Timor-Leste each scoring less than 30, underlining the variation in digital maturity across Asia Pacific.

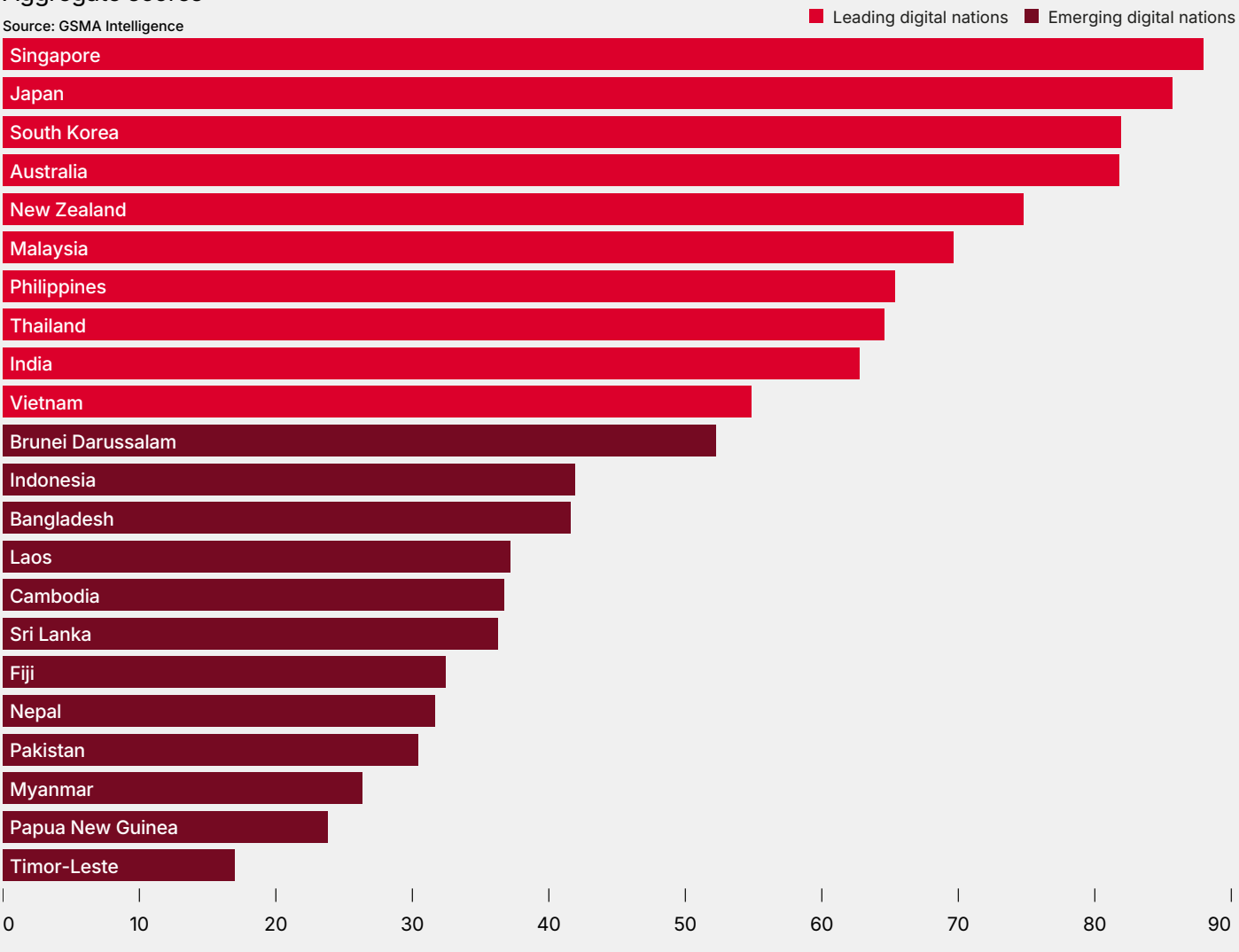
The headline ranking tells only part of the story. Progress across Asia Pacific is uneven – between economies and within them. Some lower-scoring markets are rapidly expanding infrastructure and putting in place the legal foundations for data governance, while more advanced economies face a different challenge of making complex, AI-enabled digital systems more resilient, accountable and widely usable. The region is not moving along a single pathway to digital maturity but navigating a series of distinct transition challenges.

Figure 2

Digital Nations Index: Asia Pacific, 2026

Aggregate scores

Source: GSMA Intelligence





Three findings should guide interpretation of the 2026 results:

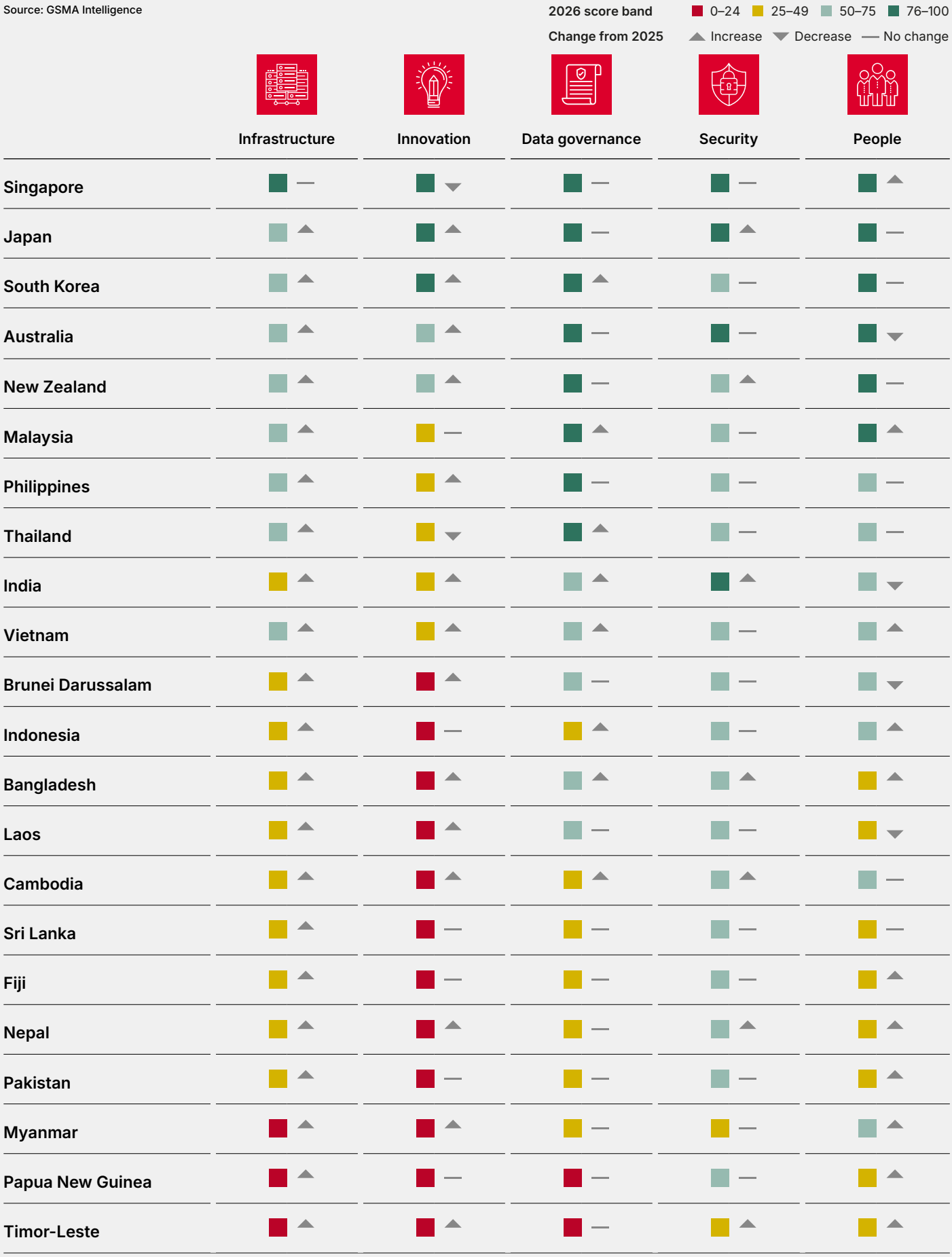
- **Catch-up is real, but it also creates new dependencies**. As emerging economies expand infrastructure, resilience, redundancy, energy supply and international connectivity become more important to sustaining digital progress. For example, Bangladesh has made significant progress expanding broadband coverage, increasing mobile internet adoption and developing digital public services, while also moving towards commercial 5G. However, recent reports of a worsening power and fuel crisis point to potential network disruptions that could affect internet access, mobile banking, emergency communications and other digital services.[7] As such, the policy challenge is shifting from merely building digital infrastructure to ensuring digital systems can operate reliably.
- **The binding constraint changes as economies mature.** Emerging economies often need foundational connectivity, institutions and digital skills, while more mature economies must focus increasingly on assurance, interoperability, diffusion and system-wide resilience. For example, Pakistan and Nepal continue to focus on strengthening digital identity systems, improving digital literacy and building the institutional capacity needed to support secure digital adoption at scale. Meanwhile, in Singapore and South Korea, policy attention is shifting to AI assurance, cybersecurity, governance and ensuring advanced technologies diffuse effectively across businesses, public services and regions.
- **Balanced capability matters more than isolated strength.** Weakness in one component can reduce the value of progress elsewhere. Networks without skills constrain adoption. Innovation without governance weakens confidence. Digital services without security expose users to harm. For example, the expansion of network coverage in Papua New Guinea is helping bring more people online, but affordability, digital literacy and limited awareness of digital services continue to constrain the economic and social benefits that connectivity can deliver. Similarly, economies including Bangladesh, Pakistan and Sri Lanka are experiencing rapid growth in digital financial services, e-commerce and online government services, which creates significant opportunities for inclusion and economic growth but also increases exposure to scams and fraud. Without effective cybersecurity measures, consumer protection frameworks and cross-sector collaboration, users may become reluctant to engage with digital services even when connectivity and platforms are readily available.

7 "Power, fuel crisis threatens telecom blackout in Bangladesh", Daily Sun, April 2026

Figure 3

# Digital Nations Index component scores: Asia Pacific, 2026

Source: GSMA Intelligence



# Trust and infrastructure: from connection to resilience

Infrastructure provides one of the clearest catch-up stories in the 2026 index. Nine markets have recorded double-digit growth, seven of which started from scores below 25 in 2025: Bangladesh, Brunei, Cambodia, Fiji, Laos, Nepal and Sri Lanka. Malaysia and Vietnam also advanced from higher starting points. Launches of commercial 5G in Bangladesh and Fiji in September 2025, Sri Lanka in December 2025 and Cambodia in January 2026 show next-generation connectivity extending beyond the region's established leaders.

This progress reframes the policy challenge. As people, firms and public services depend more heavily on digital infrastructure, availability alone is no longer enough. Networks, cloud platforms, data centres, international links and power systems need to function as a resilient stack, as failure in one layer can undermine the value of the others.

This is particularly important for island, landlocked and smaller economies that rely on a limited number of international routes, gateways or suppliers. Fiji's use of satellite community Wi-Fi in rural and maritime locations shows how non-terrestrial connectivity can extend reach and provide fallback capacity. Bangladesh's planned SEA-ME-WE 6 submarine cable connection highlights the role of international route diversity. These examples should be viewed as implementation evidence rather than proof of outcomes until service continuity and adoption can be measured.

Economies making rapid infrastructure gains should assess resilience alongside coverage and capacity. Relevant indicators include route diversity, backup power, restoration times, cloud portability, disaster communications and continuity arrangements for critical public services.

## Examples of infrastructure resilience initiatives in Asia Pacific




In June 2026, **South Korea**'s Ministry of the Interior and Safety began implementing a new disaster-recovery strategy for critical digital government services. The programme will introduce geographically separated recovery arrangements for 13 priority systems, replacing traditional same-site backup models. Recovery planning is also being expanded to cover a wider group of high-priority government systems. The move reflects a broader shift to designing continuity and redundancy into digital infrastructure from the outset, rather than relying solely on post-disruption recovery measures.

In **Singapore**, the Economic Development Board and Infocomm Media Development Authority is allocating new data-centre capacity subject to strict energy-efficiency and sustainability requirements, including minimum power-usage effectiveness thresholds and green-energy commitments. By making access to scarce power resources conditional on efficiency and sustainability outcomes, Singapore seeks to expand compute capacity without undermining grid stability.

Governments are paying increasing attention to semiconductor capacity as a strategic component of digital resilience. In February 2026, Japan's Information Technology Promotion Agency and a consortium of private-sector investors completed a JPY267.6 billion ($1.7 billion) funding round for Rapidus, supporting plans to establish domestic 2-nanometre semiconductor production by 2027.[8] The initiative forms part of a wider effort to diversify sources of advanced compute and reduce dependence on overseas supply chains for critical technologies.

8 "Rapidus secures 267.6 billion Yen in funding from Japan government and private sector companies", Rapidus, February 2026



## Trust and innovation: from capability to diffusion

The innovation component measures an economy's ability to develop, adopt and commercialise new technologies. In 2026, 14 of the 22 economies covered improved their innovation score. This is encouraging, but innovation should not be assessed only through the research intensity, patents or frontier AI capabilities captured here. The greater economic return comes when new technologies diffuse into public services, established industries and smaller firms.

For economies with strong research capacity, capital and entrepreneurial depth, the challenge is shifting from generating innovation to scaling it predictably. This requires clear regulatory boundaries, credible compliance pathways, durable policy signals and stable rules on ownership, IP and investment. Assurance and validation can then turn compliance into portable evidence of reliability, lowering adoption costs across government and enterprise. South Korea has frontier strengths in communications, semiconductors, compute and manufacturing, but broad-based impact depends on adoption across regions and firms. Japan faces a similar challenge of moving beyond technology uptake to institutional and process redesign. India innovates at scale, using its large population and digital public infrastructure as a platform for the rapid development, testing and adoption of new technologies. Shared digital rails and expanding AI infrastructure can lower barriers to experimentation, but inclusion, accountability and access need to scale at the same pace.

Emerging economies with less mature innovation ecosystems face a different challenge – making emerging technologies investable, adoptable and commercially credible. Research and entrepreneurial activity may be expanding, but gaps in validation, local data, technology transfer and early market access still limit conversion into economic value. The near-term priority is to strengthen proof of readiness and trusted localisation through credible testing, locally relevant datasets and technical resources, and pilots or sector-specific applications that show where domestic innovators can create distinctive value. In these markets, trust is built less through rules for managing scale than through evidence that technologies are relevant, reliable and ready for adoption.

Table 3

## Building trust for innovation scale-up in Asia Pacific

Source: GSMA Intelligence

| Economy | Priority for scale | Recent efforts |
|---|---|---|
| **Australia** | **Regulatory certainty and adaptive assurance** Strengthening investment and deployment predictability while improving technical risk assessment | Australia's December 2025 National AI Plan confirmed that AI would continue to be governed largely through existing laws and sector regulators, giving firms greater policy continuity after earlier mandatory AI guardrails were set aside. It builds on the October 2025 Guidance for AI Adoption, which establishes six practical governance practices for responsible deployment, while the Australian AI Safety Institute tests emerging capabilities and provides regulators with technical evidence to adapt safeguards as risks evolve. |
| **South Korea** | **Predictable compliance** Clarifying AI regulatory scope and obligations to reduce deployment uncertainty | In January 2026, the Ministry of Science and ICT (MSIT) brought the AI Basic Act and Enforcement Decree into force, defining high-impact AI and setting transparency, safety and impact-assessment obligations. Transparency guidelines and a one-year transition period made the compliance pathway more practical, while July 2026 amendments expanded testing, certification, data access, public-sector adoption and startup support. |
| **New Zealand** | **Commercialisation certainty** Clarifying IP ownership and technology-transfer pathways to help research move into investable ventures | The Ministry of Business, Innovation and Employment's national IP Management Policy, effective July 2026, clarified ownership, assignment and benefit-sharing rules for publicly funded research, and gave researchers more scope to participate in commercialisation. The June 2026 Commercialisation Engagement Guidelines and an additional NZ$40.68 million ($24 million) in funding for the Commercialisation Partner Network further strengthened links between research institutions, investors and industry.[9] |
| **India** | **Shared innovation infrastructure** Broadening access to compute and data while embedding common governance and assurance mechanisms | In November 2025, the India AI Governance Guidelines from the Ministry of Electronics and Information Technology (MeitY) presented a proportionate, risk-based approach to give firms greater clarity to innovate within existing regulation. The IndiaAI Mission announced in February 2026 that it will scale its compute capacity beyond the existing 38,000 GPUs with the addition of 20,000 GPUs.[10] |

Innovation policy should be assessed by its ability to translate inputs into commercialisation and diffusion, not inputs alone. Relevant indicators include SME adoption, public-sector deployment, access to compute and test facilities, technology transfer, startup survival and measurable productivity gains.

9 "$40.7m boost backs university research from lab to market", Beehive, June 2026
10 "India to Add 20,000 GPUs Beyond Existing 38,000 to Strengthen National AI Infrastructure", MeitY, February 2026

# Trust and data governance: from legislation to usable trust

Data governance is now a core determinant of trust in the digital economy. As services become more interconnected, data flows across organisations, sectors and borders to support digital identity, payments, AI and digital government. Effective governance should therefore do more than prevent misuse; it should give individuals, businesses and governments confidence to share, access and use data responsibly. Trust is what allows data to move safely across digital ecosystems and generate value at scale.

The pillar performance in 2026 suggests that the institutional basis for trusted data use is broadening across Asia Pacific. Progress is no longer concentrated among established digital leaders. India and Bangladesh recorded the largest gains, while Cambodia, Indonesia, South Korea, Malaysia, Thailand and Vietnam also advanced. Data protection has been the principal driver, with six of the eight markets strengthening their frameworks. The shift is increasingly from establishing rules that signal trust to building the institutions, processes and accountability mechanisms that make that trust credible in practice. Examples include the following:

- **India** advanced implementation of its Digital Personal Data Protection framework in 2025, releasing draft rules and establishing the Data Protection Board to support oversight and enforcement.
- In April 2026, **Bangladesh** adopted the Personal Data Protection Act, establishing a comprehensive legal framework for the collection, use and protection of personal data across the economy.
- **Cambodia** advanced its first economy-wide personal data protection law to the validation stage in August 2026. This marked a significant step to establishing a comprehensive legal framework for personal data governance ahead of the formal legislative process.
- **Indonesia** moved to establish an independent Personal Data Protection Authority in July 2026, finalising a Presidential Regulation that would give the authority responsibility for compliance supervision, complaints handling, sanctions and cross-border enforcement under the 2022 Personal Data Protection Law.

More mature regimes are moving data protection upstream – from policing misuse after the fact to governing risk at the point where data is designed, processed and deployed. The policy direction is therefore shifting beyond additional protection laws to protection embedded in institutions, processes and system design. Malaysia's April 2026 guidance on Data Protection Impact Assessments, Data Protection by Design and automated decision-making illustrates this shift by requiring privacy risks to be assessed, mitigated and governed throughout the data lifecycle. South Korea's December 2025 policy agenda extends the same logic, moving from ex-post sanctions to preventive oversight through proactive sector examinations, a dedicated Technical Analysis Centre, stronger redress and expanded privacy-by-design mechanisms as AI and cloud reshape privacy risk.

Across Asia Pacific, the growing gap between stronger domestic data protection and more limited cross-border data portability reflects a structural challenge. Data protection laws can be enacted unilaterally, but trusted cross-border transfers depend on compatible legal frameworks, mutual recognition mechanisms and predictable safeguards across multiple jurisdictions. As a result, privacy reforms can initially increase friction in data flows as countries converge on the principle of protection but not on how that protection is recognised across borders. Indonesia and Vietnam demonstrate how stronger domestic protections can precede cross-border interoperability. Both have introduced more comprehensive frameworks governing international data transfers, but differences in transfer mechanisms, compliance processes and regulatory implementation increase the need for organisations to manage jurisdiction-specific requirements.

Meanwhile, concerns around data sovereignty are adding a more strategic dimension to the debate. As data and compute become increasingly important economic and infrastructure assets, governments are seeking greater control over how sensitive data is stored, accessed and transferred. This is particularly evident in sectors such as finance, healthcare, telecoms and government services, where additional restrictions on cross-border transfers are common. While the measures are often intended to support security and national interests, they can also contribute to fragmentation in regional data flows if not carefully designed and coordinated.

The next challenge for Asia Pacific is to make protection portable. Overly broad localisation requirements can increase costs, reduce resilience and limit access to global cloud infrastructure, while providing only limited additional protection. Instead, policymakers are increasingly exploring frameworks that allow trust to travel with data through recognised safeguards and interoperable governance mechanisms. Recent initiatives seek to build mutual recognition across jurisdictions, including Thailand's introduction of binding corporate rules certification, South Korea's expansion of trusted-transfer mechanisms, and regional efforts such as the Japan–ASEAN Data Free Flow with Trust work plan and ASEAN DEFA negotiations. Their shared objective is to enable trusted cross-border data flows without requiring protection to be recreated each time data crosses a border.

Assessment should look beyond the adoption of legal and regulatory reforms to examine their practical implementation. This includes regulatory capacity, organisational compliance, access to redress, digital identity interoperability and the effective use of trusted data-sharing mechanisms.



# Trust and security: from compliance to system-wide protection

The 2026 Digital Nations Index results suggest cyber maturity in Asia Pacific is increasingly being defined by resilience rather than the existence of cybersecurity laws alone. Seven economies improved their security scores, ranging from emerging markets such as Timor-Leste to more advanced economies including India and Japan. Across the region, the operating assumption is shifting from preventing every cyber incident to ensuring digital systems can continue functioning through attacks. As governments, businesses and citizens become more dependent on digital services, resilience, continuity and rapid recovery are becoming central to maintaining trust in the digital economy.

Several lower-scoring economies have made progress building foundational cyber capabilities, helping to raise the region's overall security floor. Cambodia strengthened its response through new legislation that targets technology-enabled scams and continued development of incident-response capabilities. Nepal expanded the operational role of its National Cybersecurity Centre with monitoring, vulnerability testing and emergency-response functions. Timor-Leste established new coordination bodies and a cybersecurity legislative framework. Such developments are particularly important as Asia Pacific becomes more interconnected through digital trade and cross-border payment systems. Weak cyber capacity in one jurisdiction can increasingly create risks for others, making investment in foundational capabilities an issue of regional – not just national – importance.

Meanwhile, more mature cybersecurity ecosystems are confronting an increasingly sophisticated threat landscape. India – which achieved the highest possible score in the security pillar – continues to strengthen both domestic capabilities and international cooperation through initiatives such as the Australia-India Partnership on Cyber, Critical Technologies and Supply Chains (PACTS) framework and expanded threat-intelligence sharing. Yet cyber incidents continue to grow across the region, with cybercrime accounting for a significant share of recorded crime in many Asia Pacific economies. According to Interpol's 2025/2026 Asia and South Pacific Cyberthreat Assessment Report, cybercrime is growing in both scale and sophistication, with more than half the economies surveyed reporting that it now accounts for around 30% of all recorded crime nationally.[11]

Greater maturity therefore does not necessarily reduce exposure. Instead, it improves the ability to detect, contain and recover from attacks. The challenge is increasingly one of operational speed – shortening response times faster than attackers can exploit vulnerabilities. As a result, governments are placing a greater emphasis on trusted coordination mechanisms that enable timely information sharing and collective action. Bangladesh established a National Cyber Security Council and conducted a large-scale cyber exercise involving financial institutions and critical infrastructure operators. Meanwhile, New Zealand's Cyber Security Strategy 2026–2030 seeks to streamline incident reporting through a single national reporting service. Such efforts reflect a broader regional shift towards building coordination into cyber infrastructure itself.

> Trust is becoming operational, requiring institutions to give customers confidence that they can report incidents, that their information will be shared securely, and that organisations will cooperate to prevent disruption from spreading across increasingly interconnected digital ecosystems.

11 "New Interpol report highlights escalating cyber threats across Asia and South Pacific", Interpol, June 2026



## Trust and people: converting access to confident use

People remain central to digital transformation. Infrastructure, innovation, data governance and security provide the foundations of digital nations, but their value ultimately depends on whether citizens feel confident, included and able to participate in increasingly digital societies. Trust therefore plays a critical role in the people pillar of the Digital Nations Index, shaping digital adoption and how individuals engage with emerging technologies and benefit from digital transformation. Progress is evident across Asia Pacific, with half of the 22 economies assessed now scoring above 60 on the people pillar. Improvements in connectivity, affordability, digital literacy and online safety have expanded opportunities for participation, but inclusion remains uneven.

The rise of AI risks deepening divides if digital inclusion does not evolve alongside technology. Across the OECD, more than a third of individuals used genAI in 2025, but adoption varied significantly by age, education and income group. Those already constrained by connectivity, digital literacy or confidence now face the additional challenges of understanding how to interact with AI-enabled systems, assess the reliability of outputs and make informed decisions. Inclusion is therefore being redefined. It is no longer sufficient to equip people with the skills required to get online. Individuals increasingly need the capabilities to participate effectively, consistently and safely in AI-mediated environments.

This implies a three-layer approach to digital capability. The first layer is broad-based AI literacy, ensuring all citizens have a basic understanding of how AI works and where it is being used. The second is productive application, enabling workers and organisations to use AI to improve outcomes and create value. The third is judgement – the ability to evaluate AI outputs critically, retain human oversight and understand when not to rely on automated systems.

Several economies are pursuing these objectives through different approaches. Examples include the following:

- **India** is focusing on foundational AI literacy at scale. Through the YUVA AI for ALL programme, the IndiaAI Mission is providing free, self-paced AI training designed to make basic AI knowledge accessible to a broad population rather than allowing AI capability to become another source of digital inequality.
- **Singapore** is focusing on productive AI adoption through its goal of developing 100,000 "AI bilingual" workers by 2029.[12] The initiative aims to equip professionals across sectors with the ability to combine domain expertise with practical AI skills, enabling them to redesign workflows and apply AI effectively in their occupations.
- **Japan** is placing a greater emphasis on human agency as AI adoption expands. Its revised 2026 AI Basic Plan promotes a human–AI collaborative society and highlights the importance of preserving human accountability, judgement and decision-making as AI is increasingly embedded in daily life.

AI is changing the conditions for trusted online participation. By making synthetic content, impersonation and deception cheaper to create and harder to detect, AI increases the scale and sophistication of fraud, scams and online harms. This places a greater burden on individuals to verify information and assess authenticity, potentially weakening confidence in digital interactions.

12 "Singapore to train 100,000 AI-savvy workers by 2029", The Strait Times, March 2026

Some governments, such as those in Australia and Malaysia, have responded with enhanced restrictions, including minimum age requirements for certain social media platforms and online safety measures requiring proactive risk assessments and age-verification controls. However, the approaches remain at an evolving stage, with important questions around effectiveness, implementation and proportionality. If poorly designed, they could also create new trust challenges if they increase privacy risks or impose disproportionate barriers to legitimate participation.

The emerging policy challenge is to balance protection with inclusion. Effective online safety frameworks should target interventions according to risk and minimise unnecessary data collection, while preserving user choice, redress and accountability. Singapore's approach increasingly reflects this balance. Its regulatory framework combines platform duties to address systemic risks with targeted age-assurance measures and stronger avenues for user reporting and redress. The broader lesson for Asia Pacific is that trusted participation depends not just on protecting users from harm, but also ensuring that digital safeguards enhance rather than undermine individual agency.

As digital transformation accelerates, trust will increasingly be determined by whether people feel capable of navigating digital and AI-enabled environments with confidence, control and meaningful opportunity.

# 03
# Guardians of digital trust



# 3.1
# Trust in the age of sovereignty

Asia Pacific's digital transformation is entering a phase in which trust matters as much as connectivity. Digital platforms now support a growing share of public services, financial transactions, communications and economic activity. Continued adoption will therefore depend not just on whether people and businesses can access these services, but on whether they trust the systems and organisations behind them to be secure, reliable, resilient and accountable.

The assets that enable digital transformation are also becoming more strategically important. Governments across Asia Pacific are paying closer attention to how digital identity, data, cloud infrastructure, communications networks, cybersecurity capabilities and AI are governed and protected. This reflects a wider focus on digital sovereignty, as countries seek greater assurance over critical technologies and data while businesses and consumers continue to expect digital services that are open, interoperable and easy to use.

Digital sovereignty and digital trust are closely linked, but they address different questions. Sovereignty concerns the authority to govern and control critical digital assets; trust concerns confidence in how those assets, systems and services operate. National rules and capabilities can strengthen trust, but trust also depends on effective regulation, common standards, responsible innovation, interoperability and cooperation across organisations and borders.

This distinction is especially important in Asia Pacific. The region includes economies at different stages of digital development, with varied approaches to data governance, identity, cybersecurity and AI. Yet the services, infrastructure and threats shaping their digital economies increasingly transcend national boundaries. Trusted digital ecosystems must combine strong national capabilities with the ability to interact securely across the wider regional and global economy.

Digital trust can be understood through four interconnected questions:



**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?



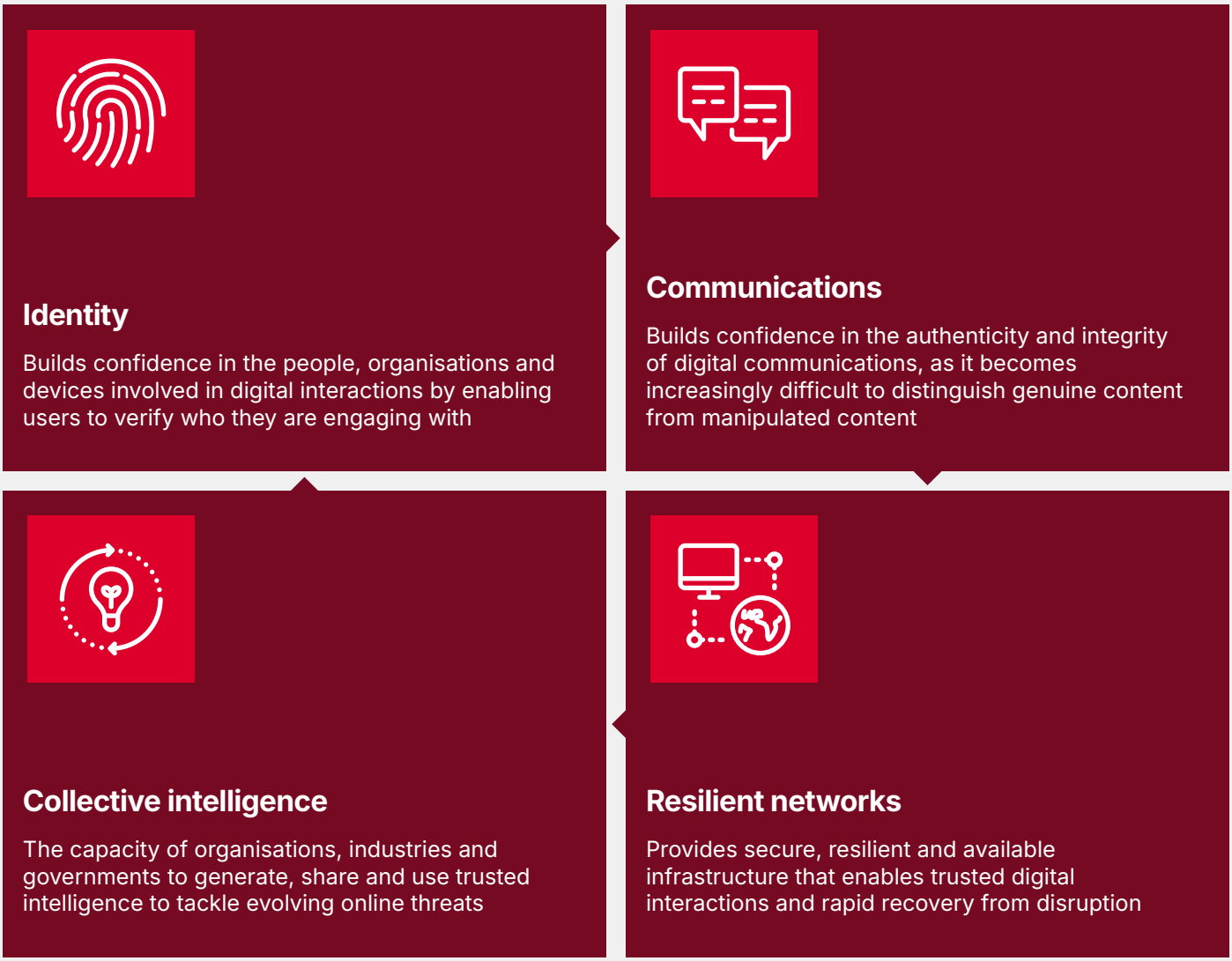
**Collective intelligence**
How are emerging risks being identified and managed, and how are our strategies evolving to outpace new malicious tactics?

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 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. However, when strengthened together, the foundations reinforce each other and create a virtuous cycle of trust that supports adoption, investment, innovation and growth.

# 3.2
# Mobile operators as guardians of digital trust

Building and sustaining digital trust is a shared responsibility across governments, regulators, technology providers, businesses, civil society and mobile operators. However, few organisations contribute across as many dimensions of trust as mobile operators do. Through their roles in digital identity, secure communications, critical infrastructure, fraud prevention, cybersecurity and threat intelligence, operators help citizens, businesses and governments participate safely and confidently in digital ecosystems. This positions mobile operators as guardians of digital trust, supporting the secure and reliable operation of increasingly digital societies.

As digital ecosystems become more sophisticated, the role of mobile operators is evolving beyond connectivity. While networks remain their core function, they also generate valuable signals that can help verify identities, detect suspicious activity, protect communications and strengthen resilience. Combined with trusted relationships with millions of customers and responsibility for critical infrastructure, this gives operators an increasingly important role supporting secure and trusted digital interactions.

This contribution is becoming more visible through the development of network APIs such as Number Verification, SIM Swap, Device Roaming Status and Know Your Customer Match. These capabilities allow banks, fintech firms and digital platforms to incorporate network-derived signals into their own security and authentication processes, adding a layer of assurance. This does not mean that operators are the sole source of trust. Rather, when combined with the capabilities of other ecosystem participants, their network intelligence and infrastructure can help create safer, more secure and more resilient digital services.



## Trusted digital identity: knowing who you can trust

Digital identity provides a trusted foundation for digital interactions, enabling individuals and organisations to verify who they are online when accessing services, completing transactions and sharing information. Beyond improving convenience, trusted digital identity systems can strengthen security, reduce fraud and support more seamless access to government services, banking, payments and other digital platforms. As digital economies mature, identity is increasingly becoming a core layer of trust infrastructure rather than simply a mechanism for accessing online accounts.

Across Asia Pacific, governments are investing in national digital identity systems tailored to their own needs and levels of digital maturity. Initiatives such as Singpass in Singapore, National Digital ID in Thailand, MyDigital ID in Malaysia and digital identity developments in Indonesia reflect this trend. Australia demonstrates how digital identity can evolve into widely used shared infrastructure. By late 2025, more than 15 million myID accounts had been created, supporting 80 million identity-verified transactions across 246 government services. As adoption grows, the policy challenge is increasingly shifting from deployment to ensuring the systems remain secure, interoperable, accessible and trusted by users.[13]

13 "Digital ID continues to grow and improve 12 months on", Australian Government Department of Finance, December 2025



## 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 Asia Pacific. As digital interactions become more complex, operators are extending this role through number verification, authentication APIs and integration with broader digital identity ecosystems. These help strengthen customer onboarding, reduce fraud and provide additional assurance when accessing digital services.

Several operators are now using network intelligence to support trusted digital identity at scale. In Singapore, Singtel, together with AIS in Thailand and Maxis in Malaysia, has developed interoperable network APIs that enable enterprises to use real-time network signals as an additional identity and authentication layer. Meanwhile, Smart in the Philippines offers roaming-status verification, providing organisations with an additional indicator when assessing the legitimacy of transactions and account activity.

Operators are also reducing reliance on passwords and SMS-based authentication. In Indonesia, Telkomsel has partnered with IPification to introduce one-click mobile authentication using network-based verification, while PLDT Enterprise launched SmartSafe SilentAccess in the Philippines to enable real-time authentication directly through the mobile network without one-time passwords. A further step is the integration of operator verification systems with government-backed identity infrastructure. From December 2025, Malaysia integrated MyDigital ID into telecoms apps to curb scam calls and identity fraud.

# Trusted communications: protecting digital interactions

Trusted communications are becoming a critical foundation of digital trust, as interactions between individuals, businesses and governments increasingly take place online. Users must have confidence that communication channels are secure and that the people, organisations and content behind digital interactions are authentic. This is becoming more important as scams, impersonation and AI-enabled fraud grow in scale and sophistication.

In July 2026, APEC described online scams as a systemic economic risk, highlighting the organised and cross-border nature of the scam economy.[14] This reinforces the need to move from fragmented, post-incident responses to coordinated prevention across communication networks, digital platforms and payment systems. In response, governments, operators and digital platforms are moving beyond fragmented, post-incident responses towards more coordinated approaches that combine sender authentication, message filtering, fraud reporting, SIM controls and cross-sector intelligence sharing.

For example, Singapore's SMS Sender ID Registry helps distinguish legitimate branded messages from impersonation attempts. Other markets are also strengthening protections against scam communications. Malaysia has tightened sender identification and SMS filtering rules; the Philippines continues to expand scam-message blocking and SIM-based accountability measures; Thailand has introduced stricter telecoms anti-fraud requirements and identity controls; and India has strengthened sender authentication and message verification through its Telecom Regulatory Authority of India Distributed Ledger Technology framework.

Attention has widened beyond SMS to address emerging threats such as deepfakes and voice impersonation. In 2026, Singapore announced measures to detect and remove scam-related deepfakes and introduce clearer identification mechanisms for government calls. These developments reflect a broader shift in trusted communications – from securing the communications channel itself to verifying the authenticity of both the sender and the content, helping users engage with digital services more confidently and securely.



## India demonstrates the role of mobile operators in enabling trusted communications

As digital banking, payments, e-commerce and government services become increasingly embedded into daily life, protecting communications from fraud and impersonation has become a growing priority.

In India, operators have responded by deploying a combination of network-level protections, AI-driven detection and industry-wide authentication mechanisms. Vodafone Idea's AI-powered Vi Protect service identifies suspected spam calls, fraudulent SMS and malicious links directly within the network. Meanwhile, Airtel has partnered with Google to combine operator network intelligence with spam filtering and secure RCS messaging capabilities.

India's commercial messaging ecosystem is increasingly protected by the Distributed Ledger Technology framework, which verifies sender identities, message templates and communications before delivery. Together with operator-led fraud detection initiatives and coordinated action with the Department of Telecommunications, these measures contributed to a significant reduction in spoofed scam calls between late 2024 and early 2025. Mobile operators have also introduced Calling Name Presentation, which displays a verified caller identity at the network level, and support government initiatives such as the Sanchar Saathi and Chakshu reporting platforms.

14 "Scams, Trust and the Cost of Digital Growth", APEC, July 2026

# Trusted resilient networks: keeping digital systems running

Trusted networks are a fundamental component of digital trust. As economies become more reliant on digital services, communication networks, cloud platforms, data centres and cybersecurity systems are increasingly being treated as critical national infrastructure. Their reliability depends on security but also resilience – the ability to withstand, respond to and recover from cyberattacks, natural disasters, technical failures and other disruptions. Failures in these systems can have far-reaching consequences, affecting essential services such as banking, healthcare, transport, government operations and emergency communications.

Across Asia Pacific, governments and operators are strengthening network resilience through investment in critical-infrastructure protection, cyber preparedness, supply-chain security and incident-response capabilities. Following a devastating battery fire at the National Information Resources Service data centre in Daejeon, South Korea has accelerated efforts to strengthen public-sector digital resilience. The incident exposed the risks of centralised single points of failure, destroying 858 terabytes of unbacked data and temporarily disrupting services across 709 government information systems, including tax portals, e-government systems and mobile ID verification.[15] In response, the government has invested heavily in geographically separated disaster-recovery arrangements and decentralised regional hubs.

While national strategies vary, there is growing recognition that resilience depends on both domestic capabilities and international cooperation. This was reflected in the fourth Australia–Japan Telecommunications Resilience Policy Dialogue in June 2026, where government and industry participants discussed topics including open RAN, submarine cables, data centres, cybersecurity and emergency communications.[16] The dialogue highlighted the increasingly interconnected nature of digital infrastructure and the importance of trusted partnerships in supporting continuity and preparedness.

These efforts take place against a backdrop of a rapidly evolving threat landscape where organised criminal networks are increasingly exploiting AI, ransomware-as-a-service and sophisticated social engineering techniques to scale operations. In this environment, trusted networks are no longer defined solely by their ability to prevent attacks, but by their capacity to maintain essential services, recover quickly from disruption and sustain confidence in increasingly interconnected digital ecosystems.

In Bangladesh, the newly established National Cyber Security Council and the 2026 National Cyber Drill brought together 68 teams from financial institutions and Critical Information Infrastructure (CII) organisations to enhance national incident-response readiness.[17]

## Japan demonstrates the role of mobile operators in trusted resilient networks

Japan is adopting a comprehensive approach to telecoms resilience that combines infrastructure hardening, network interoperability and coordinated emergency response. SoftBank has implemented measures to extend emergency operating capability from 48 to 72 hours during prolonged power outages,[18] while wider industry collaboration is strengthening access to backup power during disasters. In May 2026, NTT Group, KDDI, SoftBank and Rakuten Mobile announced a cooperative agreement with seven mobile battery manufacturers, including Anker Japan and EcoFlow, to provide mobile batteries, charging cables and other equipment to evacuation centres and other affected locations during large-scale disasters. The initiative became operational on 1 June 2026.[19] Resilience is also being enhanced through greater interoperability. A nationwide emergency roaming system launched in April 2026 allows smartphones to automatically connect to a competing operator's 4G network for voice and SMS if their primary network becomes unavailable.[20]

Complementing these initiatives, Japan's eight major telecoms providers agreed to coordinate disaster response responsibilities across different regions, ensuring evacuation shelters have access to communications, power and connectivity support while reducing duplication of effort.[21] Such measures demonstrate a shift from standalone operator resilience to a more integrated national approach that combines infrastructure hardening, operational coordination, emergency connectivity and public-private collaboration to maintain essential communications during crises.

15 "South Korea Data Center Fire: A Critical Wake-Up Call for Data Resilience", BDRShield, October 2025
16 "Results of Fourth Australia-Japan Policy Dialogue for Telecommunications Resilience", MoIC, June 2026
17 "Mutual Trust Bank PLC Wins National Cyber Drill 2026", Mutual Trust Bank, 2026
18 See www.softbank.jp/en/corp/sustainability/esg/social/disaster/restoration
19 "Japanese telcos and battery makers join forces on disaster power supply", Light Reading, May 2026
20 "Japan's Mobile Carriers Launch 'JAPAN Roaming,' a Nationwide Emergency Roaming Service", NTT Docomo, March 2026
21 "Japan's Telecommunications Carriers Enhance Collaborative Framework for Rapid Disaster Support by Implementing Evacuation Support Area Allocation", NTT, October 2025

# Trusted intelligence: ensuring data and AI can be trusted

As digital ecosystems become more interconnected, trust increasingly depends on the ability of organisations to anticipate, detect and respond to emerging risks collectively. Threat actors routinely share tools, techniques and intelligence across borders, sectors and platforms, while defensive efforts often remain fragmented. Strengthening digital trust therefore requires trusted mechanisms for collaboration and information sharing between governments, mobile operators, financial institutions, technology providers, cybersecurity agencies and law enforcement bodies. By combining threat intelligence, fraud insights, operational data and risk indicators with advanced analytics and AI, organisations can identify threats earlier, coordinate responses more effectively and reduce the impact of cyberattacks, scams and fraud.

The importance of collective intelligence is growing as digital economies become more integrated. Effective information-sharing frameworks can improve situational awareness, accelerate incident response and strengthen the prevention of cybercrime and fraud across increasingly interconnected systems. Across Asia Pacific, governments and industry are beginning to develop the structures needed to support this cooperation. By 2026, the GSMA-led Asia Pacific Cross-Sector Anti-Scam Taskforce had expanded to include operators, technology companies, digital platforms and public-sector organisations from across the region, creating a forum for sharing threat intelligence, coordinating evidence and exploring privacy-preserving approaches to data sharing.

This shift to collaborative defence is also being reflected in broader regional policy discussions. At the Digital Nation Summit Tokyo in 2026, government, telecoms and technology leaders highlighted active cyber defence, AI-enabled threat detection and cross-sector intelligence sharing as important elements of a more resilient digital ecosystem.[22] Similarly, the GSMA Asia Pacific Telecom Cybersecurity Forum emphasised the growing need for faster, more automated intelligence sharing in the AI era. Such initiatives reflect a growing recognition that digital trust increasingly depends on strong individual organisations but also the ability of institutions to share trusted intelligence and act collectively against common threats.

22 “GSMA APAC Cross-Sector Anti-Scam Taskforce (ACAST): Building Resilience Against Scams at Digital Nation Summit Tokyo 2026”, GSMA, May 2026

## 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 guardians of digital trust.

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 may see fraudulent transactions; digital platforms may detect malicious accounts; law enforcement may 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.

---

Ultimately, the four foundations of digital trust underpin trusted digital ecosystems, with mobile operators among the few actors with a role across all four. Their customer relationships, secure networks, authentication capabilities and growing involvement in intelligence sharing render them vital to the region's trust ecosystem, marking a broader evolution from connectivity providers to guardians of digital trust. As Asia Pacific balances openness with sovereignty and advances towards more secure, inclusive and integrated digital economies, operators can help governments, businesses and citizens participate with greater confidence and security, while remaining essential partners in building the trusted ecosystems on which the region's long-term competitiveness depends.



## 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 Asia Pacific, 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 that systems are secure but also that the individuals, communications and content they interact with are genuine. This shift has implications for digital policy. Consumer awareness and cybersecurity controls remain important, but 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 can play an important role. 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, while the GSMA-led Asia Pacific Cross-Sector Anti-Scam Taskforce (ACAST) highlights the need for coordinated action against scams that operate across sectors and borders. Policy and industry responses are beginning to reflect this shift. In August 2026, Singapore outlined measures to detect and remove deepfakes used in scams and identify legitimate government calls.

As Asia Pacific 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 Asia Pacific economies, trust will shape the pace, scale and sustainability of digital adoption. Although governments, regulators, operators and other digital ecosystem participants have made progress building trusted digital systems, emerging technologies, evolving cyberthreats, deeper digital interdependence and geopolitical uncertainty are increasing the need to strengthen the foundations of trust through coordinated action at three levels:

- Governments and regulators need to establish enabling policy and regulatory frameworks.
- Mobile operators play an important role as providers of trusted connectivity and digital services as part of the broader digital ecosystem.
- Regional and international cooperation is necessary to support interoperability, coordinated responses and 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 to manage risk but also to enable innovation, investment and inclusive digital participation.

## Enabling trusted identity ecosystems

Digital identity is becoming core infrastructure for digital economies, enabling citizens and businesses to access services safely and efficiently across both public and private sectors. Governments should therefore expand secure, inclusive and interoperable identity systems, strengthen authentication and assurance standards, improve interoperability between national and sector-specific systems, and protect privacy. They should work closely with private-sector stakeholders, including mobile operators, financial institutions and digital platforms, to enhance capabilities for authentication, verification and trust, while enabling new, innovative digital services. They should also ensure digital identity systems remain accessible to people with lower levels of digital literacy, limited documentation or restricted access to compatible devices, so that identity infrastructure supports inclusion as well as trust.

Australia illustrates how digital identity can evolve into widely used shared infrastructure across a growing range of services. In December 2025, the Australian government reported that 15 million myID accounts had been created and that 80 million identity-verified transactions had passed through the Australian government's Digital ID System during the previous year. The system was accepted by 246 government services.[23] By reducing the need to share and store identity documents repeatedly, digital identity can make access to services more convenient while limiting exposure of sensitive personal information.

23 "Digital ID continues to grow and improve 12 months on", Australian Government Department of Finance, December 2025

## 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, financial institutions and technology providers to combat scams, phishing and cyber-enabled fraud. This should include stronger fraud reporting, cross-sector information sharing, consumer protection and enforcement against digital criminal networks.

Thailand has pursued a collaborative approach through its anti-online scam framework, bringing together telecoms operators, financial institutions, regulators and law-enforcement agencies to share intelligence, identify fraudulent activity and disrupt scam networks. Recent measures include stronger SIM registration and identity verification requirements, blacklist screening, fraud-detection systems and closer coordination between telecoms providers and the Anti-Online Scam Operations Center. By combining industry cooperation with enforcement and consumer protection measures, Thailand aims to reduce scam activity while strengthening confidence in digital communications and financial services.

## 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.

Singapore's Cybersecurity Code of Practice for Critical Information Infrastructure establishes mandatory baseline security standards for essential digital systems. Issued by the Cyber Security Agency, the 2026 update places a greater emphasis on proactive resilience by extending regulatory oversight to interconnected enterprise networks and strengthening board-level accountability for cyber risk. Critical information infrastructure owners are required to deploy active threat-detection systems, conduct emergency-response exercises and attain Cyber Trust Mark Level 5 certification, supporting national security and operational continuity.

## 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 that can be translated into clear, measurable and implementable requirements. Governments should complement high-level, risk-based principles with practical guidance, technical standards, assessment methodologies and assurance mechanisms that organisations can apply consistently 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.

Singapore has emerged as a regional leader in AI governance through its Model AI Governance Framework, AI Verify testing and assurance toolkit, and ongoing work on genAI governance. Rather than relying solely on prescriptive regulation, Singapore has focused on practical tools that help organisations assess transparency, fairness, safety and accountability in AI systems. It has also strengthened data governance through the Personal Data Protection Act, demonstrating how governments can promote innovation while maintaining strong privacy protections and public trust.

## Ensuring the resilience of digital infrastructure

As digital systems become embedded in critical economic and social functions, resilience is increasingly a whole-of-system challenge. Effective governance therefore requires stronger coordination across telecoms, energy, transport, cloud infrastructure, financial services and emergency response sectors to ensure disruptions in one part of the ecosystem do not cascade across the wider digital economy.

Australia has adopted a whole-of-system approach through its critical infrastructure framework, which covers telecoms, energy, transport, data storage and processing, financial services and critical government functions. The framework supports information sharing, risk management and coordinated incident response across infrastructure operators, reflecting the growing interdependence between digital networks, cloud infrastructure, power systems and essential services. When disruptions occur, resilience depends on the continuity of telecoms networks as well as reliable access to electricity, transport links and secure digital infrastructure.

## Facilitating cross-sector collaboration and anti-scam cooperation

Digital risks increasingly span communications networks, financial systems, healthcare services, government platforms and digital marketplaces. Responsibility for managing these risks is often split across regulators, agencies and ministries with separate mandates. This creates 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, and with private-sector actors (including mobile operators, financial institutions, digital platforms, cloud providers and cybersecurity firms) working together rather than in isolation.

Anti-scam cooperation should be a priority use case as scams often move across platforms, messaging or telecoms services, and financial or digital asset channels before victims suffer losses. No single organisation sees the full sequence, so authentication, intelligence sharing, enforcement and consumer protection need to operate together. Governments should promote closer collaboration between telecoms operators, financial institutions, digital platforms and law enforcement agencies to detect, disrupt and prevent scams, recognising that trust will increasingly depend on coordinated approaches to authentication, fraud intelligence and consumer protection across sectors and jurisdictions.

## Deepening regional and international cooperation

Many trust challenges, including cybercrime, online fraud and AI-related risks, extend beyond national borders. Governments should therefore strengthen regional cooperation through joint cybersecurity initiatives, shared threat intelligence, cross-border fraud prevention and common trust-assurance frameworks. Cooperation should build on existing bilateral, sub-regional and international mechanisms, including the APEC forum, ASEAN, Asia-Pacific Telecommunity, bilateral partnerships, industry initiatives and international standards bodies. A key outcome of international cooperation should be to improve compatibility between national systems and make cooperation faster and more effective when risks cross borders.



# 4.2
# Priorities for mobile operators

Mobile operators are well placed to support all four foundations of digital trust. The next phase of evolution for operators will be to move beyond connectivity provision to support a wider range of trusted digital services in collaboration with other ecosystem stakeholders.

## Strengthening digital identity services

Identity is one of the clearest opportunities for operators to create value while reinforcing digital trust. By combining trusted subscriber relationships with network intelligence, operators can make digital interactions more secure and easier to use through mobile identity solutions, number verification, authentication APIs, digital onboarding and integration with national digital ID systems. Initiatives such as 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.

## Combatting scams and digital fraud

Scams remain one of the most visible threats to digital trust across Asia Pacific, requiring operators to design interventions around the full scam lifecycle rather than individual communications channels. By using network-level intelligence, operators can help identify and prevent fraudulent activity before it causes harm, with priority investments including advanced spam and scam detection, SIM-swap protection, fraud-risk scoring, shared fraud intelligence and public awareness campaigns. Mobile operators should look beyond their own networks and seek opportunities to share appropriate data and trusted signals with other sectors. These capabilities become more valuable when combined appropriately with observations from financial institutions, digital platforms and public authorities, helping to protect consumers and strengthen confidence in the wider digital ecosystem.

The GSMA-led Asia Pacific Cross-Sector Anti-Scam Taskforce (ACAST) demonstrates this direction of travel. By March 2026, ACAST had grown to 39 members across 17 countries, bringing together operators, digital platforms, technology specialists and public authorities to coordinate evidence, share threat intelligence and explore privacy-respecting, data-sharing models.

## Investing in resilient infrastructure

As critical infrastructure providers, operators should continue strengthening network and platform resilience through sustained investment in redundancy, cybersecurity, disaster recovery, emergency communications, security operations centres and threat intelligence. Resilience planning should increasingly account for dependencies across telecoms networks, energy systems, cloud platforms, data centres, submarine cables and technology suppliers, including the possibility that failures occur simultaneously or cascade across several parts of the infrastructure stack. Satellite and non-terrestrial capabilities can complement terrestrial networks during emergencies and in areas exposed to infrastructure disruption, but their integration into business continuity and emergency communications plans should be supported by appropriate standards for security, reliability and interoperability.

## 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 deploy these capabilities responsibly, transparently and securely, supported by AI governance frameworks, trusted analytics, privacy-enhancing technologies and responsible data management practices. By demonstrating leadership in trusted AI adoption, operators can improve operational performance while strengthening public confidence.

# 4.3
# Priorities for international cooperation

As Asia Pacific has no single institution with a region-wide mandate, cooperation should connect existing mechanisms.

These mechanisms include the Asia-Pacific Economic Cooperation (APEC) forum, United Nations Economic and Social Commission for Asia and the Pacific (ESCAP) and its Asia-Pacific Information Superhighway (APIS) initiative, the Association of Southeast Asian Nations (ASEAN) where relevant, Pacific regional bodies, bilateral and minilateral digital-economy partnerships, standards organisations and industry-led initiatives. The priority should be to solve practical cross-border problems rather than seek uniform governance.

## Advancing trust interoperability

Digital trust becomes more valuable when trusted systems can operate seamlessly across borders. Asia Pacific institutions should support interoperability between national digital identity systems, authentication mechanisms and trust frameworks – not by making national systems identical but by establishing common principles, technical standards and assurance levels that allow trusted systems to interact. Reducing fragmentation can improve user experience, lower integration and compliance costs, and support trusted cross-border services.

## Supporting trusted cross-border services

Cross-border digital services are increasingly important to regional growth, with digital payments, e-commerce, cloud services and digital trade all requiring trust mechanisms that work consistently across jurisdictions. Asia Pacific already contains several overlapping cross-border digital initiatives, particularly in payments and paperless trade. The next priority is to ensure expanding interoperability is accompanied by effective authentication, privacy, security, fraud prevention and accountability. This will require closer cooperation among telecoms regulators, data protection authorities, central banks, cybersecurity agencies, competition authorities and digital trade policymakers, as trusted cross-border services depend on these different frameworks working together rather than developing in parallel.

## Strengthening cross-border cyber resilience

Cyber incidents can affect infrastructure, organisations and users across several jurisdictions, making regional and international cooperation essential to stronger cross-border resilience. Priorities include closer cooperation between national CERTs and CSIRTs, joint cybersecurity exercises, common reporting and escalation arrangements, mutual assistance, shared assessments of infrastructure dependencies and mechanisms to restore cross-border services following disruption.

Cooperation should also address infrastructure that is inherently international, including submarine cables, satellite systems, cloud services, data centres and international telecoms networks. The Australia–Japan Telecommunications Resilience Dialogue illustrates how bilateral cooperation can combine government policy discussion with industry expertise across several of these areas.

## Promoting a shared vision of trusted sovereignty

Regional and international cooperation can help shape a shared understanding of trusted digital sovereignty. National approaches will differ, but sovereignty should not be treated solely as a question of localisation or control; it also depends on the security, resilience, governance and reliability of the systems on which countries rely. Cooperation should therefore help balance national control with openness, interoperability and innovation, as common standards, trusted international partnerships and compatible assurance mechanisms can strengthen national resilience by expanding access to secure infrastructure, expertise and alternative suppliers.

## Scaling up regional anti-scam cooperation

Asia Pacific institutions should support cross-border fraud-intelligence sharing, common authentication approaches and regional cooperation mechanisms to combat scams and AI-enabled deception. ACAST provides an industry-led mechanism spanning operators, platforms, technology specialists and public authorities, while the APEC forum offers a broader policy channel. Its 2026 Ministerial Statement encouraged cooperation with the private sector on trusted, secure and resilient infrastructure while recognising the different approaches of member economies.



## A collective trust agenda for Asia Pacific

Asia Pacific's digital trust agenda is entering a delivery phase. The priority now is to translate policy ambitions into practical outcomes through effective governance, stronger cross-sector coordination and greater interoperability. Governments, industry and regional institutions each have a role to play, while mobile operators will remain important partners in supporting secure, resilient and trusted digital ecosystems.

Progress should be assessed through outcomes. Safer participation, more resilient services, faster response to cyber threats and fraud, and broader adoption of trusted digital technologies provide the clearest indicators of success. In this context, the Digital Nations Index serves as a benchmark of performance and a practical framework for guiding the next phase of digital development across Asia Pacific.

For policymakers in the region, the goal is to build trusted digital ecosystems that allow Asia Pacific countries to participate confidently in regional and global digital markets. Delivering this vision requires a collective trust agenda. Governments and regulators should create enabling frameworks and strengthen resilience. Mobile operators should continue evolving into trusted digital service providers. Asia Pacific institutions should support interoperability, coordination and common frameworks for trusted cross-border interaction. No single organisation can deliver digital trust alone; it depends on coordinated action across the digital ecosystem.

**GSMA**
1 Angel Lane
London EC4R 3AB
United Kingdom

gsma.com