Position Paper

Trading with Trust in the new Digitalised World: How Digital Trust can enable Regional Trade

eden strategy institute

With business increasingly digital, Trust has never been more important.

PURPOSE

Over the past two years, our world has completely transformed due to a digital revolution accelerated by the Covid-19 pandemic. In the New Normal, citizens have come to expect digital interaction in all areas of life including how we work, learn, connect, and shop. Businesses globally have had to speed up the adoption of digital technology to accommodate a strong growing preference for digital, contactless consumption. Spending on digital and technology initiatives as well as numbers of full-time equivalents in digital and technology roles increased during the pandemic despite budget cuts elsewhere in the business.[1]

However, the rapid digital growth raises questions on trust in the new digital environment, tools, and the companies that provide the digital experience.[2] This joint paper between the Asian-Oceanian Computing Industry Organization (ASOCIO) and SGTech aims to show how the Asia Pacific region (APAC) can continue to drive economic growth in digital trade by leveraging on the pillars of digital trust—identity, security, privacy, and data protection—to create an inclusive, innovative, globally connective, and integrated economy.

ASOCIO is an ICT federation whose members include ICT associations representing 24 economies throughout APAC. Its influence covers more than 10,000 ICT companies and represents approximately USD 800 billion of ICT revenue in the region. ASOCIO's objective is to promote, encourage, and foster relationships and trade among its members and to develop the computing industry in the region.

SGTech is the leading trade association for Singapore's tech industry. Representing over 1,000 member companies ranging from top multinational corporations, large local enterprises, vibrant small and medium-sized enterprises, and innovative startups, it is the largest community in Singapore where companies converge to advocate for change and drive what enables tech innovation and accelerates tech adoption to spur greater sustainability in the sector. SGTech's mission is to catalyse a thriving ecosystem that powers Singapore as a global tech powerhouse.

[1] McKinsey (2021)
[2] Chakravorti, Bhalla, Chaturvedi (2021)

Chairman's Statement

As ASOCIO, our objective is to develop the ICT industry across the Asia Oceania region by promoting trade as well as fostering relationships between its member economies. This has been our mission and objective since our founding in 1984.

With the global economy becoming increasingly digital, the world has also seen the rapid rise in misinformation, consumer scams, cybersecurity attacks and data breeches. Under such circumstances, Trust has never been more important as the key ingredient to ensure continued cross-border business transactions and sustaining global trade.

As such, we stand behind the recommendations outlined in this paper. We believe in the importance of sustaining regional trade as the digital economy grows, and encourage our member economies to nurture greater Digital Trust across the region by:

1. Exploring interoperable, regional Digital Identity systems;
2. Working towards mutual recognition of Trust Marks;
3. Harmonising standards for cybersecurity, privacy, data protection, and intellectual property to enable cross-border data flows;
4. Adopting standard data governance contractual clauses;
5. Establishing dispute resolution channels for regional consumer and business protection.

This is our pledge as a federation of ICT associations representing 24 economies throughout in the Asia-Pacific region, a region accounting for USD 800 billion of ICT revenue. We will strive to promote the best practices and recommendation outlined in the paper, in hopes to bring about a more prosperous future for the digital economy in the region.

David Wong Nan Fay
Chairman
ASOCIO

METHODOLOGY

ASOCIO and SGTech commissioned Eden Strategy Institute in 2022 to conduct an analysis of the trends and challenges in physical and digital trade based on secondary research to identify trade opportunities in the region where digital trust can serve as a driver for inclusive, cohesive, and innovative economic growth in APAC.

As part of the research, Eden interviewed experts in IT across the APAC region including policymakers, consultants, private sector practitioners, and academia to develop a holistic perspective of the unique digital trust challenges from a national and regional perspective. Eden also leveraged its insights from a 2022 Digital Trust Global Landscape Study, commissioned by SGTech.

THE APAC DIGITAL TRADE OPPORTUNITY

The pace of the digital change in the vast and culturally diverse APAC region has been rapid; 60 million people in Southeast Asia became online consumers during the pandemic.[3] Major drivers of this growth are the increase in internet connectivity and smart phone penetration—consumption of mobile data in South and Southeast Asia will triple between 2022 and 2025—that democratizes access to online consumption and new digital skills.

Some of the most prominent sectors to benefit from the digital revolution are eGovernment services, mobile financial services including payments, and eCommerce. The use of in-person government services halved across APAC nations in the last two years with 77 percent of citizens now primarily using digital platforms to access government services.[4] APAC eCommerce is expected to reach USD 2 trillion by 2025. [5] The growth in online sales has spurred adoption of digital payments such as mobile wallets; new fintech models such as Buy Now Pay Later (BNPL) are replacing credit cards in some markets.[6]

The region's digital transformation is opening new economic opportunities for citizens—especially the younger generation as digital natives—and businesses in the digital economy. For example, Philippines and Malaysia are the top two countries in global eCommerce retail growth, increasing by 25 percent and 23 percent per year respectively.[7] Countries such as India, Bangladesh, Pakistan, and Philippines 'export' online labour to the West.[8] Social media has dissolved boundaries for businesses to reach consumers across borders with new forms of engagement such as livestreams, with consumers accessing digital content and marketplaces globally. The increase in digital activity has spurred an explosion in data, which has become a valuable asset for businesses looking to generate more trade with insights derived from analytics.

[3] World Economic Forum (2022) A
[4] Deloitte (2022)
[5] World Economic Forum (2022) A
[6] Techwire Asia (2022)
[7] World Economic Forum (2022) A
[8] Ibid.

Research in 2022 shows that most enterprises in the region have received buy-in from stakeholders to increase IT investments in their budget, compared to only 15 percent of enterprises in 2021, with major spending categories including security, risk management, cloud computing, digital workspace, and IT automation.[9]

[9] Bajwa (2022)

AN END-STATE VISION FOR APAC TRADE

APAC economies strengthened intraregional trade linkages amid the pandemic rose to its highest level in three decades; it grew 29.6 percent in the first three quarters of 2021, compared with the global trade growth of 27.8 percent.[10] In addition to creating greater inclusivity and shared prosperity, fostering digital trade creates inter-dependencies across countries, helping the region become more cohesive and attractive to international investors. Digital services trade in the region has more than tripled from 2005, achieving over USD 1.5 trillion in 2020; digital services trade is showing rapid growth relative to total services.[11] The region has a tremendous opportunity to grow digital trade by developing a regional economy which is **Inclusive; Innovative; Globally-connected; Integrated and Cohesive.** [12]

Inclusive
Businesses of all sizes, including startups as well as micro, small and medium enterprises, will have equal opportunity to trade goods and services across borders. Currently, many SMEs are facing issues with complying with digital laws and regulations due to various resource constraints, and are encountering complex customs administrations which present delays and added costs.[13]

Innovative
The free flow of data across borders is a driver of innovation as it enables information, ideas, and knowledge-sharing, as well as collaboration and cross pollination among individuals and companies. In places with restrictions on digital collaboration, people are less likely to experiment and innovate.[14]

Globally-connected
APAC businesses gain access to new international markets by being integrated into global and regional value chains, expanding their growth potential, influence, and footprint.

Integrated and Cohesive
International trade is frictionless because of interoperable technological and governance systems. APAC businesses are able to work with each other seamlessly, encouraging new business relationships and collaboration across national borders.

[10] Asian Development Bank (2022) A
[11] Asian Development Bank (2022) B
[12] ASEAN (2015)
[13] World Economic Forum (2022) B
[14] Pepper, Garrity, La Salle (2016)

THE NEED FOR DIGITAL TRUST

However, digital trade in the Asia-Pacific region continues to be stifled by four key frictions to trade.

1. **Verification.** Companies are not always able to verify if an overseas counterparty they are trading with is in fact the entity it purports to be, and may prefer to only deal with parties they already know and trust. In the absence of trusted relationships, there is always the concern that the trade may not actually go through.

2. **Standards.** Even when one party has a local trust mark obtained from the government, it is not always easy for a trading partner overseas to understand the exact level of assurance this provides around its cyber-hygiene, or to navigate the local data protection frameworks and regulations.

3. **Contracting.** When entering into a contract, a company might be hesitant to accept the different contract terms and data policies from its counterparty in a different jurisdiction, which affects its accountability to its own clients and consumers.

4. **Recourse.** In the event of a disagreement, there are not many mediation options that can expertly handle cross-border digital disputes in a cost-effective way.

These issues all signal a lack of trust in digital transactions. Okta's State of Digital Trust Report 2021 found that 58 per cent of Asian respondents are unlikely to purchase a product from a digital brand they did not trust; an average of 38 per cent indicated that they would delete their account with the company, after losing trust in its brand due to a data breach or misuse of data.[15] They create considerable uncertainty, inability to forge cross-border agreement, and resulting duplication. These frictions, in turn, will stifle cross-border digital trade.

Instead, we envisage a future where Digital Identity allows new counterparties to directly and efficiently verify each other's identities. A set of harmonized standards, trust marks, regulations, and even contract terms will ease the overseas that many multinational headquarters need to incur when managing their operations across countries, while simplifying the amount of checking, reconciliation, and negotiation required to trade regionally. A well-functioning, expert regional mediation hub will supplement trust technologies such as Distributed Ledgers; Privacy Enhancing Technologies; as well as Governance, Risk, and Compliance systems, to ensure that digital contracts are fairly enforced in the event of disputes.

Digital Trust is a key enabler for this end-state vision. From getting users to trust digital products and services, to building seamless digital transactions for enterprises, digital trust is a critical part of driving and maximizing the full potential of the digital revolution. It is important to note that some member economies still face financial, technological, social, and political challenges in large-scale

[15] Okta (2021)

digitization. For these countries, the concept of digital trust may seem like a secondary concern in the face of trying to overcome digitization challenges.

Nonetheless, we argue that digital trust needs to evolve in parallel with societal developments, in order for countries to reach a vision of an inclusive, innovative, globally-connected, integrated and cohesive APAC region.

Cybersecurity is typically the first component of digital trust that comes to mind, and the pillar of digital trust that has been most widely written about recently. In 2021, Asia was the most targeted region for cyberattacks globally, with member economies of Japan, Australia, and India bearing the brunt of server access and ransomware attacks.[16] Across the region, experts place a strong emphasis on developing cybersecurity legislation, and putting in place cybersecure systems and processes. However, cybersecurity is but one component of digital trust. [17] In this white paper, we will explore and focus on the other pillars of digital trust such as digital identity, privacy, and data protection – additional pillars equally important in building this end state vision for the APAC region.[18]

[16] Yu (2022)
[17] Eden Research and Analysis (2022)
[18] Ibid.

Inclusive. Promote inclusive growth with digital identification and the mutual recognition of trust marks

INTEROPERABLE REGIONAL DIGITAL IDENTIFICATION

Issue
APAC is highly-diverse in terms of culture, language, governance, and economic development. Businesses incorporated in countries with geopolitical and economic instability may find it difficult to build trust with international customers; this applies particularly to SMEs as they are not able to rely on their brand and reputation to establish integrity and track record. [19]

Solution
Digital Identification ("Digital ID") can create a trustworthy system to enable easy end-user identity verification. For individuals, digital ID contains personal information such as legal name, gender, address, photograph, and biometrics. For businesses, it can contain company registration numbers, bank accounts or sector and industry memberships. In business and finance, customer identification and verification are critical first steps to avoid losses and fraud, and to better understand the counterparties to the transaction. Beyond identification, corporate digital ID can link to other information and attributes about the identity which facilitates know-your-customer (KYC) and other mandatory due diligence procedures.[20]

Implementation Considerations
Digital identities have the potential for abuse and misuse if they are not intentionally designed to protect privacy, as well as the individual or corporation's autonomy to control the use of the data. While Aadhaar has been held up as the poster child for centralized digital ID, it has come under criticism for privacy and security lapses, and for its compulsory use for accessing services which may systematically exclude certain marginalized societal segments such as refugees.[21]

Corporate digital ID is interlinked with individual digital identity as it requires external users to identify and authenticate individuals that claim to represent a company as their representatives, owners, and controllers.[22] The digital identity should also include the company's track record. Another consideration for the centralized digital identity system is that there is a new industry of third-party

[19] Ibid.
[20] Bank for International Settlements (2022)
[21] Access Now (2021)
[22] Bank for International Settlements (2022)

verification services that is needed, if certain countries don't trust another country's accrediting organization.

An alternative to the centralized database is decentralized identifiers (DID), with blockchain technology a critical enabler of DID. [23]A DID is where there is no central database and every stakeholder – whether government, ministry, or business – gets to choose its own system. The benefits of DID is enhanced privacy and protection, as no single entity has control over the ledger, making it less susceptible to misuse, and entities have control over who views the data. [24] For it to interlink globally, different platforms or sources of data need to be interoperable. To achieve this, international standards such as UN/CEFACT guidelines for digital identity could be the starting point when designing a national or regional digital identity system.[25] Additionally, there are also cultural factors to account for in establishing interoperable digital identities, such as the issue of non-romanised naming systems across the APAC region.[26]

With interoperable digital identity systems, businesses from different countries and of all sizes will be able to establish trust relationships enabled by technology.

Case study

Several countries in the region have successfully developed digital identities. India enrolled 99 percent of Indian adults, roughly 1.3 billion people, in Aadhaar, India's centralized digital ID programme. [27] Aadhaar collects residents' biometric data – iris scans, fingerprints, and photographs – and issues residents with a 12-digit identity number. As the world's largest biometric identification,[28] the government stores the data in a central database and third-party services can access the database to confirm identities when needed. Singapore's Personal Access Pass (Singpass) has evolved as a gateway to allow convenient and secure access to over 1,700 digital services offered by more government and private sector entities.[29] CorpPass is the authorization system for corporate entities to manage digital service access of employees who need to perform corporate transactions and access government services.[30]

[23] Eden Strategy Institute research and analysis; Monro (2021);
[24] Venture Beat
[25] Eden Strategy Institute research and analysis - Wanawit
[26] Ibid.
[27] Riddhima (2022)
[28] Nandi (2019)
[29] Singapore Government Developer Portal
[30] CorpPass

MUTUAL RECOGNITION OF TRUST MARKS

Issue

Trust marks are a mechanism that helps consumers recognized trusted providers and make informed decisions on whether to buy goods or services.[31] Trust marks have the potential to drive inclusiveness, enabling even small and microbusinesses to trade internationally. However, there are multiple, competing trust marks which leads to consumer and business confusion over their applicability and comparability. A European Commission survey on trust marks found that 53 percent of consumers do not trust a trust mark, because they did not know what the criteria was for getting a trust mark and how the trust mark was evaluated.[32] Some examples of existing trust marks include the ISO 27001, BSI Mark of Trust, Singapore's Data Protection Trustmark Certification (DPTM), Cyber Security Agency of Singapore (CSA) Cyber Trust Mark, and the EU Trust Mark.

Trust marks have also been criticized for acting as a barrier to entry for business who cannot afford to obtain the trust marks, instead of ensuring that data is secure and private.[33]

Solution

As more countries in the APAC region start obtaining or developing trust marks, it is important to achieve consensus in the comparability of trust marks so that companies can transact with other companies confidently, even if they obtained a different trust mark. For example, the requirements for the ISO 27000-1 certification can be mapped against those for a DPTM certification; this can also demonstrate how different trust marks best complement each other.

Engaging third party accreditation bodies who can provide professional mapping services for the different certifications can also enhance the credibility and congruency of different trust marks.

Implementation considerations

Creating consumer awareness on the scope of different trust marks is key in legitimizing trust marks in the eyes of consumers. When consumers are familiar with how trust marks are developed, the importance of these trust marks, and the functions of different trust marks, they are more likely to readily patronize businesses that have been awarded such trust marks.

[31] Next Generation Internet (2020)
[32] European Consumer Centres' Network (2013)
[33] Eden research and analysis – Wanawit Akhputra

Innovative. Enable cross-border information flows with multilateral frameworks which are critical for big data analytics. With more information and flow of ideas, companies can create innovative products and services.

ENABLING CROSS-BORDER DATA FLOWS

Issue

Free flow of data across borders enables the diffusion of advanced technologies, economic growth, and innovation.[34] Massive volumes of data travel across borders daily to support economic activity, research, and transactions along the value chain; this has become even more important due to the Covid-19 pandemic where transacting online has become the new normal.[35]

As member countries in APAC recognize the importance of digitalization and take action to support its growth, cross-border data flows become a priority to facilitate further digitalization. However, there is a concerning trend on the rise of restrictions on data flow, such as data localisation requirements in particular. Some governments have opted to create rules requiring that data, or certain types of data, remain onshore and are not transferred between countries. While these data localisation laws are seen to provide more safety and security for domestic data, they may not work as intended; for data security, investment in infrastructure and maintenance is more important than the physical location of data.[36]

Data localization laws cause friction in business transactions and increased expenses for compliance. For example, a company might not be able to transfer data seamlessly to its subsidiary or partner in another country. Both parties have limited data on which to run analytics which typically surface new information insights. Without these insights, the ability of the company to innovate for new products and services may be hindered, affecting the customer experience.

Solutions

Creating a balanced regulatory environment that is attractive to business while protecting data security and privacy can be challenging, especially in countries that are just starting to prioritize digital growth. One solution could be for countries to join multilateral cross-border frameworks and certifications such as the Asia Pacific

[34] World Economic Forum (2021)
[35] Ibid.
[36] GSMA (2018)

Economic Cooperation (APEC) Cross Border Privacy Regulation (CBPR), which facilitates international data flows by harmonizing standards across areas of digital trust, enabling companies to feel safe transferring data. Currently, nine countries participate in the CBPR, including the United States, Mexico, Canada, Japan, South Korea, Singapore, Chinese Taipei, Australia, and the Philippines.

Developed by all 21 APEC economies, an APEC economy must demonstrate that it can enforce compliance with the CBPR System's requirements before joining.[37] CBPR sets up a network of reciprocally and mutually-agreed on regulations which preserve individual nations' privacy regulations. [38] The CBPR is separate from, and do not supersede, domestic legal requirements.[39] CBPR system requirements include enforcement, accountability, consumer empowerment, and consistent protections.[40] Certified companies and governments under the APEC CBPR System can transfer personal data across borders without meeting additional requirements.

Privacy Enhancing Technologies (PETs) are also another emerging privacy solution. PETs comprise of a broad range of software and hardware technologies, including Synthetic Data, Differential Privacy, Federated Learning, Homomorphic Encryption, Secure Multi-party Computing, Zero Knowledge Proof, and Trusted Execution Environments (TEEs).

PETs allow businesses to extract value from data without exposing the data itself, thereby protecting personal data and commercially-sensitive information. This increases the options for B2B data collaboration, enables cross-border data flows, and increases the availability of data for developing AI systems.[41]

Implementation Considerations

In assessing whether a country is ready to join the CBPR, or putting policies in place to do so, technology practitioners need to be involved in the policymaking stage to ensure that the policies are actually workable as some policymakers will not have in depth insights to the tech implications of the CBPR system requirements.[42]

Some state-of-the-art PETs require complex architectures and integrations to be built. Specialist engineering capabilities are often needed, such as data science backgrounds with grounding in cryptography and security. Some PET techniques such as Homomorphic Encryption and Multi-party Computing require high levels of computing power. This will improve with R&D, and will become less of an issue in the medium-term.[43]

Case study

Cross-border data flows are important to stimulate innovation and economic growth across different sectors. For example, in the energy sector, wind turbine manufacturers use data from turbines to maintain and optimize wind energy parks

[37] APEC
[38] Business Times (2019)
[39] Ibid
[40] APEC
[41] IMDA
[42] Eden Strategy Institute – Wanawit Akhputra
[43] Eden Research and Analysis (2022)

across different countries. These data flows are essential to identify areas where they can reduce operational costs as well as data analytics to optimize productive, subsequently increasing the competitiveness of their product.[44]

In the medtech sector, for example, hearing aid manufacturers rely on data flow to customize how devices can fit to customers' ears. Pre-sale, they scan customers' ear channels to create a precise 3D-model of the inner ear. Post-sale, they support remote technical calibration for better delivering of the hearing aid. This is the same for high-end dental procedures such as invisible braces. Such processes involve cross-border flows of personal and health data.

[44] OECD (2019)

Globally-connected. Promote global connectivity and access to regional and international markets by harmonising standards for cybersecurity, privacy, data protection, and intellectual property

HARMONISING STANDARDS TO IMPROVE GLOBAL CONNECTIVITY

Issue

Currently, cybersecurity, privacy, and data protection laws across the region are not harmonised, creating a complex landscape of requirements for companies in APAC to navigate through. Some APAC members have very high stringent levels of security, privacy, and data protection requirements. For example, South Korea has been granted an *adequacy decision* by the European Commission, which means that there can be transfers of personal data from the European Economic Area (EEA) to private and public entities in South Korea, with no requirement for additional transfers tools, conditions, or authorizations from data protection regulators in the EEA.[45]

In navigating this complex landscape, larger companies are usually able to accept additional expenses in compliance costs and hire external consultants to support them; however, smaller companies are usually unable to justify the additional expense and are left to navigate the requirements, often deterring them from accessing international markets.

Solution

There needs to be regional consensus on the standards of data protection, cybersecurity, data protection, and intellectual property. To do so, countries should strengthen their commitments to align their national laws to multilateral frameworks such as the ASEAN Data Management Framework which was developed by the ASEAN Working Group on Digital Data Governance and designed to provide voluntary and non-binding guidance based on best practices in data management for businesses.[46] The DMF also provides a step-by-step guide for businesses to set up a data management system, which includes data governance structures and safeguards.

[45] O'Donoghue and Ibranimova (2021)
[46] Allen and Gledhill (2021)

Additionally, countries should join the APEC Cross Border Privacy Regulation (CBPR) aims to facilitate global data flows, but requires countries to adhere to a minimum requirement under certain systems.[47] In doing so, companies from all member countries, and of all sizes, would be able to reduce compliance costs when transacting across borders since all member countries will meet minimum requirements on cybersecurity, privacy, data protection, and intellectual property.

Implementation Considerations

It might be challenging to gain consensus in APAC on the minimum standards of all the components—cybersecurity, privacy, data protection, intellectual property—without too much dilution given the diversity of cultural, geopolitical, infrastructural, and technological factors. Policymakers will have to work together with industry and technology practitioners to understand the realities on the ground, and priorities for harmonization.[48]

[47] APEC

[48] Eden Strategy Institute – Aung Zwar Lwin

Integrated and Cohesive. Adopt standard contractual clauses and regional consumer protection recourse mechanisms to create an integrated and cohesive economy

STANDARD DATA GOVERNANCE CONTRACTUAL CLAUSES

Issue
Smaller companies may not have the financial capacity to hire legal and compliance expertise; hence, they might not have appropriate contractual documents required to transact with larger or more sophisticated companies. This disadvantage is exacerbated when transacting with international jurisdictions, as the level of contractual protections and legal expertise required are even more important given the differences in legal jurisdictional requirements. [49]

Clauses that are particularly prominent are data governance clauses and dispute resolution clauses: data governance clauses as data protection breaches carry large penalties in certain jurisdictions; dispute resolution clauses, as customers need recourse in case the transaction goes awry for a variety of reasons including product and service quality, shipment delay, and product safety. Hence, without sufficient contractual protections and legal expertise, smaller businesses are likely to be disadvantaged in winning business opportunities with larger companies nationally, regionally, and internationally.

Solution
Standard contractual clauses such as the ASEAN Model Contractual Clauses (MCCs)[50] may be included in binding legal agreements between parties transferring personal data to each other across borders. When businesses agree on widely-recognized standard contractual clauses, they can contract with regional and international parties easily as both parties have reassurance on each other's contractual obligations.

Implementation Considerations
Countries may face challenges in raising awareness about these standard contractual clauses and garnering widespread adoption. Businesses will need to be educated about the tangible benefits of adapting their operations to use new methods such as standard contractual clauses.

[49] Eden research and analysis (2022)
[50] PDPC

Case study

The European Commission's Standard Contractual Clauses (SCC) governs cross-border data transfers and data exchanges between data controllers and processors. SCCs are the mostly widely used mechanism among the business community in Europe. In a survey of 300 companies, 85 percent of companies use them; of the SMEs surveyed, 70 percent use them. Almost all industry sectors rely on SCCs for their transfers, with the ICT sector being the largest at 37 percent, and manufacturing coming in second at 22 percent.[51]

[51] Digital Europe (2020)

DISPUTE RESOLUTION FOR REGIONAL CONSUMER PROTECTION

Issue
Consumers and businesses are wary in transacting with suppliers which are not able to project legitimacy if they do not have a household brand name or have not attained a certain size or longevity of operations. This issue is more prominent in cross-border transactions as cross-border dispute resolution rights and mechanisms are complex and uncertain; customers may seek to only buy low value items from overseas suppliers because the quantum of losses is negligible even if the transaction goes awry. For example, a company in Malaysia had bought a product from a Chinese vendor which arrived faulty. However, the recourse mechanisms were complex and time consuming, so much so that they accepted the losses without making much effort to obtain a refund or exchange. However, this experience is likely to discourage them from making high-value cross-border purchases in the future. [52]

Solution
Harmonizing consumer protection laws and driving development of regional consumer recourse mechanisms to enforce these laws are possible solutions. Customers should be able to file a complaint to a central regional consumer body, or work through their national authority to obtain resolution from the seller's national authority[53]. In this way, customers will feel secure in transacting cross-border as there are similar protections and certain dispute resolution mechanisms in case issues arise with the transaction such as faulty goods, shipping delays, or safety flaws.

Implementation considerations
To achieve this, we need increased collaboration between consumer protection authorities across the region. Currently, the level of sophistication in consumer protection authorities across the region in terms of enforcement abilities and processes vary widely. Through collaboration, consumer protection authorities can share good practices and strengthen each other's institutional processes. [54]

Case study
The EU has a cooperation framework legislation called the *Consumer Protection Cooperation Regulation*, that allows national authorities from all countries in the European Economic Area to jointly address breaches of consumer rules when the trader and the consumer are established in different countries. Collectively, the national authorities form a European enforcement network: The "CPC Network".

National enforcement authorities have strong powers to address illegal practices and identify dishonest traders. They can request information from domain registrars and banks to detect the identity of the responsible trader, carry out mystery shopping, for example, to check geographical discrimination or after-sales conditions, and to order the immediate take-down of websites hosting scams.

[52] Eden research and analysis
[53] Modrall and Haverals (2021)
[54] Eden research and analysis

The European Commission coordinates the cooperation between these authorities to ensure that consumer rights legislation is applied and enforced in a consistent manner across the Single Market. It can alert the CPC network and coordinate EU-wide enforcement action to tackle practices which harm a large majority of EU consumers. Authorities can accept commitments from the businesses concerned that they will correct their practices, provide remedies and compensation to the consumers affected.[55]

[55] European Commission

Evaluating approaches for varying levels of Digital Maturity

Certain Digital Trust approaches might be more appropriate to a particular country or company's operating context, depending on its level of digital maturity. For example, countries early in their digital journeys might start by developing digital identity systems, so that counterparties may first identify each other before data will flow across borders. Similarly, data governance standards will have to be established before trust marks can be awarded.

To help assess the level of digital maturity in a company's or country's digital transformation journey, we can examine the use of Digital Maturity Models. We have identified four key categories of Digital Maturity Models, depending on the particular use case and business objectives. For example, countries or organizations can internally devise different indices, to measure different aspects of digital maturity. However, indices are typically not accredited and may differ across companies, and so may not be typically be used by companies to qualify new counterparties to trade digitally. Instead, while international standards such ISO 27000-1 may not offer comprehensive prescriptive detail, they are effective in helping organizations harmonize their digital practices.

Given that the maturity models differ in scope and use case, each type of model will be developed by different private or public sector stakeholders in varying ways. For example, in the case of trust marks and legislation, government agencies will be heavily involved, with support from the private sector. For instance, in Singapore, the Infocomm Media Development Authority (IMDA) appoints assessment bodies that will verify whether applicant organisations satisfy the requirements for the Data Protection Trustmark and the APEC Cross Border Privacy Rules (CBPR) System, before issuing these certifications. Such a top-down approach facilitates mutual recognition of such certification across borders.

Digital Maturity Model	Benefits	Disadvantages
Standards[56]: e.g. ISO 27000 -1 *ISO 27001 is the only auditable international standard that defines the requirements of an information security management system (ISMS)*	• Standards such as ISO 27000-1 are recognized globally as a benchmark of good practices, and adds credibility to the organization while also enhancing their competitiveness and reputation • ISO 2700-1 also supports compliance with laws such as GDPR, enabling organisations to avoid costly penalties due to non-compliance	• Getting accredited in these standards can be an additional business expense which may be costly (both in time and finances) in the short-term for SMEs in particular. For example, SMEs may need to pay consultancy fees, application fees, assessment fees, as well and maintenance fees.
Indices e.g. Digital Intelligence Index (DII) by the Fletcher School at Tufts University in partnership with Mastercard	• Enables comparisons between different countries or organisations along a clearly defined set of metrics • Different indices will target particular aspects of digital maturity that an organization may want to focus on. For example, the DII provides insight on how to enhance digital competitiveness, whilst Deloitte's Digital Maturity Model evaluates digital capabilities	• Since indices are often not company-specific, they may more relevant for internal planning purposes and may be less effective in enhancing a company's credibility with external parties
Trust Marks and Certifications e.g. Cyber Trust Mark, Digital Trust Label	• As these tend to be more localized, they are more attuned to local, regional, or industry-specific contextual	• Just as with Standards, becoming awarded with a Trust Mark can be an additional business expense which may be costly in the

[56] IT Governance Ltd

	requirements and nuances • Certifications such as CBPR, which target APAC, enhance cross-border collaboration among organisations through data flows	short-term, especially for SMEs.
Legislation e.g. GDPR	• Lowest mark of credibility for compliant companies • Where legislations cut across more than one jurisdiction, this enhances a company's geographical reach	• Smaller businesses may struggle to stay up to date with legal requirements and may be overwhelmed with legal terms and requirements • Non-compliance would be very costly for small businesses

Conclusions

As digitization and the need for digital trust becomes more prominent, the role of the IT professional needs to evolve in line with it. IT can no longer be viewed as a siloed department within the organization. IT feeds into all the organization's processes, and forms part of the organization's competitive advantage in a digital world.

IT professionals have a critical role to play in being involved in policymaking, to offer technological perspectives on creating and enforcing new digital trust initiatives such as data sharing protocols. To contribute effectively, IT professionals across APAC ought to upskill continuously and stay informed on the most material issues facing digital trust in the region. Multilateral frameworks and policies are a key driver for regional, large-scale change; IT professionals need to be involved the process of developing these frameworks and policies to ensure that they are realistic and technologically feasible in each country's context. Cross-border IT talent readiness will also ease discrepancies in capabilities across APAC.

The new IT professional needs to be strategic, business-minded, and future-oriented to offer views on not only the best IT systems the company can implement, but also how companies can build trust through these digital systems with their vendors and customers in order to gain a competitive advantage. We envisage that this will pave the way for more companies to appoint Chief Trust Officers, that steward an organization's numerous trust initiatives, and acts as a business partner to the C-suite to enable their respective functions with trust. Companies will be able to drive business growth with Chief Trust Officers that ably understand, communicate, and advocate for how digital trust initiatives drive growth. For example, companies will now appreciate that undertaking the CBPR is not only a certification programme that builds credentials, but ultimately enables innovation, facilitates cross-border data flows, and in so doing creates tangible business value.

References

Purpose

McKinsey & Company. (2021, December 16). *The New Digital Edge: Rethinking Strategy for the postpandemic era*. McKinsey & Company. Retrieved August 24, 2022, from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/the-new-digital-edge-rethinking-strategy-for-the-postpandemic-era

Chakravorti, B., Bhalla, A., & Chaturvedi, R. S. (2021, August 31). *How Digital Trust varies around the world*. Harvard Business Review. Retrieved August 24, 2022, from https://hbr.org/2021/02/how-digital-trust-varies-around-the-world

Bajwa, K. (2022, January 1). *Digital priorities in the new normal*. Business Times. Retrieved August 23, 2022, from https://www.businesstimes.com.sg/life-culture/digital-priorities-in-the-new-normal

The APAC digital trade opportunity

Deloitte. (July,2022) *Accelerating digital government for citizens in the Asia-Pacific: Deloitte Australia: Economics*. Deloitte. (2022, July). Retrieved August 24, 2022, from https://www2.deloitte.com/au/en/pages/economics/articles/accelerating-digital-government-citizens-asia-pacific.html

World Economic Forum (2022, February) B. *How digitalization is making South and Southeast Asia Engines of growth*. World Economic Forum. (2022, February 10). Retrieved August 23, 2022, from https://www.weforum.org/agenda/2022/02/digitalization-south-southeast-asia/

Devanesan, J. (2022, May 25). *Mobile wallets are beating traditional payments in Apac*. Tech Wire Asia. Retrieved August 24, 2022, from https://techwireasia.com/2022/05/its-endgame-for-traditional-payments-as-mobile-wallets-emerge-victorious/

An end-state vision for APAC trade

Asian Development Bank. (2022, February 15) A. *Trade integration deepens in Asia and the Pacific Amid Pandemic*. Asian Development Bank. Retrieved August 24, 2022, from https://www.adb.org/news/trade-integration-deepens-asia-and-pacific-amid-pandemic

Asian Development Bank. (2022, February) B. *Asian Economic Integration Report 2022 - Advancing Digital Services Trade In Asia And The Pacific*. Retrieved August 24, 2022, from https://www.adb.org/sites/default/files/publication/770436/aeir-2022-highlights.pdf

World Economic Forum. (2022, August) B *The Digital Divide: Why SMEs Must Cross borders*. World Economic Forum. (2022, August 3). Retrieved August 24, 2022, from https://www.weforum.org/agenda/2022/08/smes-small-medium-business-cross-border-enterprise/

ASEAN. (2015, November). *ASEAN Economic Community Blueprint 2025* . Retrieved August 24, 2022, from https://asean.org/wp-content/uploads/2021/08/8.-March-2016-ASCC-Blueprint-2025.pdf

Pepper , R., Garrity, J., & La Salle, C. (2016). *Cross-border data flows, Digital Innovation, and Economic Growth*. The Global Information Technology Report 2016. Retrieved August 24, 2022, from https://www3.weforum.org/docs/GITR2016/WEF_GITR_Chapter1.2_2016.pdf

Okta. (2021, May). *The State of Digital Trust: A snapshot of trust in an increasingly digital Asian society*. Retrieved August 26, 2022, from https://www.okta.com/sites/default/files/2021-05/ASIA_DigitalTrustReport.pdf

The need for Digital Trust

Yu , E. (2022, February 24). *Asia most targeted region in 2021, taking on one in four cybersecurity attacks*. ZDNET. Retrieved August 25, 2022, from https://www.zdnet.com/article/asia-most-targeted-region-in-2021-taking-on-one-in-four-cybersecurity-attacks/

Hassan, N. (2019, October 12). *Getting digital IDs right in Southeast Asia*. The Diplomat. Retrieved August 26, 2022, from https://thediplomat.com/2019/10/getting-digital-ids-right-in-southeast-asia/

Leung, D., Nolens, B., Arner, D., & Frost, J. (2022, June 16). *Corporate Digital Identity: No silver bullet, but a silver lining*. The Bank for International Settlements. Retrieved August 26, 2022, from https://www.bis.org/publ/bppdf/bispap126.htm

Interoperable regional Digital Identification

Riddhima, D. (2022, April 25). *On biometric ids, India is a 'laboratory for the rest of the world'*. The Christian Science Monitor. Retrieved August 30, 2022, from https://www.csmonitor.com/World/Asia-South-Central/2022/0425/On-biometric-IDs-India-is-a-laboratory-for-the-rest-of-the-world

Nilekani, N. (n.d.). *India's Aadhaar System: Bringing E-government to life*. Chandler Institute of Governance. Retrieved August 30, 2022, from https://www.chandlerinstitute.org/governancematters/indias-aadhaar-system-bringing-e-government-to-life

Singpass – your improved digital ID. Singapore Government Developer Portal. (n.d.). Retrieved August 30, 2022, from

https://www.developer.tech.gov.sg/products/categories/digital-identity/singpass/overview

Nandi, S. (2019, December 12). *Aadhaar a game changer but concerns on security remain*. mint. Retrieved August 30, 2022, from https://www.livemint.com/news/india/aadhaar-a-game-changer-but-concerns-on-security-remain-11576090533817.html

Busting the dangerous myths of big ID programs. Access Now . (2021, October). Retrieved August 30, 2022, from https://www.accessnow.org/cms/assets/uploads/2021/10/BigID-Mythbuster.pdf

Corppass. (n.d.). Retrieved August 30, 2022, from https://www.corppass.gov.sg/cpauth/login/homepage?URL=%2Fcorppass%2Flogin%2Fsplogout&TAM_OP=login

Gupta, D. (2022, March 5). *Decentralized identity using blockchain*. VentureBeat. Retrieved August 30, 2022, from https://venturebeat.com/datadecisionmakers/decentralized-identity-using-blockchain/

Monro, S. (2021, October 6). *Decentralisation the way forward for Digital Identity Management in Asia*. Frontier Enterprise. Retrieved August 30, 2022, from https://www.frontier-enterprise.com/decentralisation-the-way-forward-for-digital-identity-management-in-asia/

Mutual recognition of Trust Marks

Report: Digital Trustmarks . Next Generation Internet . (2020). Retrieved August 30, 2022, from https://www.ngi.eu/wp-content/uploads/sites/48/2020/01/NGI-Forward-Digital-Trustmarks.pdf

Elliott, H., & Droemann, M. (2020, January 30). *A trustmark for the internet?* nesta. Retrieved August 30, 2022, from https://www.nesta.org.uk/blog/trustmark-internet/

Enabling cross-border data flows

Advancing data flow governance in the Indo-Pacific: Four country dialogues. World Economic Forum . (2021, April). Retrieved August 31, 2022, from https://www3.weforum.org/docs/WEF_Data_Flow_Governance_2021.pdf

What is the cross-border privacy rules system. APEC. (n.d.). Retrieved August 31, 2022, from https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system

Michalak, M. (2019, April 4). *How ASEAN Can Effectively Address the Data Privacy Conundrum*. Business Times. Retrieved August 31, 2022, from

https://www.businesstimes.com.sg/asean-business/how-asean-can-effectively-address-the-data-privacy-conundrum

Casalini, F., & Lopez Gonzalez, X. (2019, January 23). *Trade and Cross-border Data Flows*. OECD iLibrary . Retrieved August 31, 2022, from https://www.oecd-ilibrary.org/docserver/b2023a47-en.pdf?expires=1575651497&id=id&accname=guest&checksum=A9E4AF04E8F810E54C1A414ED35E32ED

Schrems II Impact Survey Report. DIGITALEUROPE. (2020, November 27). Retrieved September 2, 2022, from https://www.digitaleurope.org/resources/schrems-ii-impact-survey-report/

IMDA. (n.d.). *Privacy Enhancing Technologies (PET) Sandbox*. Retrieved September, 20, 2022, from: https://www.imda.gov.sg/programme-listing/Data-Innovation/Privacy-Enhancing-Technologies-Sandbox

Harmonising standards to improve global connectivity

Singapore-led initiatives on Data Management Framework, model contractual clauses for cross border data flows and information exchange mechanism approved at first ASEAN digital ministers' meeting. Allen & Gledhill. (2021, February 25). Retrieved September 1, 2022, from https://www.allenandgledhill.com/sg/publication/articles/17823/led-initiatives-on-data-management-framework-model-contractual-clauses-for-cross-border-data-flows-and-information-exchange-mechanism-approved-at-first-asean-digital-ministers-meeting

O'Donoghue, C., & Ibraimova , A. (2021, December 22). *South Korea granted adequacy decision*. Technology Law Dispatch. Retrieved August 31, 2022, from https://www.technologylawdispatch.com/2021/12/global-data-transfers/south-korea-granted-adequacy-decision/

Standard data governance contractual clauses

PDPC: ASEAN Data Management Framework and model contractual clauses on cross border data flows. Personal Data Protection Commission. (n.d.). Retrieved September 2, 2022, from https://www.pdpc.gov.sg/help-and-resources/2021/01/asean-data-management-framework-and-model-contractual-clauses-on-cross-border-data-flows

Dispute resolution for regional consumer protection

European Union. (n.d.). *Consumer protection and cooperation regulation*. Retrieved September 20, 2022, from https://ec.europa.eu/info/law/law-topic/consumer-protection-law/consumer-protection-cooperation-regulation_en

Modrall, J., & Haverals, J. (2021, December). *The CPC network – consumer protection, EU style*. Global law firm | Norton Rose Fulbright. Retrieved September 1, 2022, from

https://www.nortonrosefulbright.com/en/knowledge/publications/ac43bb19/the-cpc-network-consumer-protection-eu-style

Evaluating approaches for varying levels of Digital Maturity

IT Governance Ltd. (n.d.). *Benefits of ISO 27001 Certification.* Retrieved 19, September, 2022, from https://www.itgovernance.eu/nl-be/iso-27001-benefits-be

Contributors

We would especially like to express our gratitude to the following global experts for their kind contributions to this study.

Japan
- Mr. Ken Masuda, Chief Marketing Officer, Blockchain Hub, Inc; and CEO, Global Startup Hub, Inc.

Malaysia
- Mr. Ong Kian Yew, CEO, PIKOM (The National Tech Association of Malaysia)

Myanmar
- Ye Naing Moe, Director, Information Technology and Cyber Security Department, Ministry of Transport and Communications
- Aung Zayar Lwin, Executive Committee Member, Myanmar Computer Federation (MCF)

Singapore
- Ms. Jane Lim, Deputy Secretary, Ministry of Trade and Industry

Sri Lanka
- Dr. Gihan Dias, Professor, Department of Computer Science and Engineering (CSE), University of Moratuwa
- Mr. Nadarajah Nirmalan, President of FITIS (Federation of Information Technology Industry Sri Lanka) Professional Consultancy Chapter (PCC)
- Mr. Kushan Sharma, Chief Operating Officer, TechCERT (Cybersecurity Company)

Taiwan
- Dr. Ren Dar Yang, Executive Vice President, Institution for Information Industry

Thailand
- Mr. Wanawit Akhputra, Senior Advisor to Permanent Secretary, Ministry of Digital Economy and Society (MDES)

The Asian-Oceanian Computing Industry Organization (ASOCIO) is a grouping of ICT industry associations representing the Asian-Oceania region. Established in 1984 in Tokyo, Japan, ASOCIO's objective is to develop the computing society and industry across the Asia Oceania region domain by promoting trade as well as fostering relationships between its member economies. ASOCIO has created links between ICT companies and the industry's growth in member economies.

The explosive epidemic of COVID19 has led to the expansion of activities in the cyber world by both companies and individuals, including the expansion of work from home and developments in the European Commission. At the same time, the way of thinking about cybersecurity has been changing dramatically worldwide.

ASOCIO recognizes the necessity to review the foundation of cyber technology utilization and policy vision in response to these changes in the environment, and to this end has established the NNEWG (New Normal Expert Working Group).

NNEWG provides research, analysis, as well as recommendations by experts from both technical and business perspectives.

SGTech, celebrating its 40th anniversary in 2022, is the leading trade association for Singapore's tech industry. Representing over 1,000 member companies ranging from top multinational corporations, large local enterprises, vibrant small and medium-sized enterprises, and innovative startups, it is the largest community in Singapore where companies converge to advocate for change and drive what enables tech innovation and accelerates tech adoption to spur greater sustainability in the sector.

SGTech's mission is to catalyse a thriving ecosystem that powers Singapore as a global tech powerhouse.

Eden Strategy Institute is an award-winning strategy consulting firm that drives sustainable advantage through social innovation, shared value business models, sustainable transformation, inclusive finance, and impact assessment.

We help corporations, governments, and multilateral organisations plan and set up industry blueprints, facilitate co-creation, forecast and evaluate the outcomes of policy interventions in creating and sustaining economic and societal impact.

Our Practice Areas include Digital Trust, Smart Cities, Sustainability, Education Innovation, Value-based Healthcare, and Public Service Transformation. To learn more about our work, please visit edenstrategyinstitute.com.