APRIL 2022

STRATEGIC FRAMEWORK FOR DIGITAL ECONOMIC COOPERATION

A PATH FOR PROGRESS

Institute of International Finance

Summary

International rules for the digital economy continue to be elusive while national restrictions on the flow of data proliferate. This is an increasing problem for the broad-based economy including dynamic startups, small and medium sized enterprises (SME) and other high-growth sectors all of which have come to rely on global digital infrastructure to support their activities. The international finance firms that enable transactions across borders are watching the rising barriers to data flows and concerned that the unintended consequences of these restrictions could erode economic growth and limit widely valued digital services across the economy.

We are rapidly reaching an inflection point where data localization requirements and fragmented standards for data and privacy may begin to break the on-demand services and real-time systems that we have come to expect and rely on. Some leaders have called for a "Digital Bretton Woods" moment to hammer out these new rules for a digital economy. The Japanese G20 Presidency highlighted this challenge in 2019 with its "Data Free Flow with Trust" initiative, and data flows were at the heart of the 2021 G7 Trade Ministers' Digital Trade Principles. Unfortunately, progress was elusive and geopolitical headwinds are growing stronger against the likelihood of these efforts yielding broad international solutions.

The international financial services industry has much at stake if the current trajectory continues. Protectionist localization measures could hinder the efficiency of international finance and viability of some business models. Such measures could challenge firms' ability to serve customers across borders in real-time, efficiently connect customers to capital markets, or deliver secure low-cost payments. The financial services industry is also well-placed to play a strategic leadership role to solve these digital policy questions from its extensive experience dealing with complex cross-border regulatory issues.

The broad-based economy also has much at stake. In terms of GDP impact cross-border data flows surpassed the impact of the global goods trade back in 2014—$2.8 trillion digital impact vs $2.7 trillion in goods (Mckinsey Global Institute)—and sectors driven by digital technology have been growing at twice the rate of other sectors. While large institutions can manage expensive and duplicative new requirements, that is not always the case for individual entrepreneurs, SMEs, and others who may be cut off from cross-border services and connectivity through public cloud platforms.

This paper puts forward a framework for a modular approach to tackle this problem from several directions rather than waiting for apex solutions from global bodies. This framework is intended to inform debate; we suggest five areas of focus to drive progress:

1. **Leadership & Coordination:** Encourage adjusted focus and leadership by international bodies. While they continue working towards international standards, they could increase coordination between regional developments thereby helping combat fragmentation, duplication, and conflict to the greatest degree possible while encouraging mutual recognition and interoperability.
2. **Knowledge & Skills:** Support the development of new digital knowledge and skills in the public and private sectors to better understand the economics of data and smart approaches to privacy.
3. **Regulatory Architecture:** Advance consistent regulatory architectures for activities across different sectors and borders.
4. **Protocols & Standards:** Create interoperable protocols and standards for data flow, safety, and privacy.
5. **Digital Trade Enablement:** Encourage agreements between like-minded economies such as the Singapore-Australia Digital Economy Agreement (DEA) which has become part of a wider set of DEAs Singapore has concluded with Chile and New Zealand, United Kingdom, and Korea.

We also intend for this paper to inform future work with members and policymakers on: fragmentation of technology standards and implications for operations and risk; the impact of data frameworks on cross-border payments; case studies illustrating qualitative and quantitative impacts; and future engagement with relevant entities including the Financial Stability Board.

Table of Contents

I. Introduction

The world is experiencing tremendous change in how we work, live, and conduct economic activities. Not only are our lives becoming more digital, but money and the way we transact are also evolving. Data flows play an ever-increasing role in this environment, making cooperation on digital policy and digital trade important priorities across society. Benefits from this kind of cooperation include economic growth, improved healthcare, climate risk management, resilience of small businesses, and digital inclusion.

In contrast, data localization measures interfere with the principle that data's value is maximized when it can flow with trust and permission across companies, sectors, and national borders to be used. That trusted and permissioned flow, with economic and legal frameworks to ensure safety, security, and equal access opportunity, should be the goal of data policy. Policy measures that prevent the flow of data, or render that flow less efficient and/or more expensive, cause an impairment in value for the economy. These impacts also transmit across the broad economy through weakened systems, reduced connections to global value chains, and less opportunity to leverage global data and technology resources.

Gains from the digital economy (e.g. digital trade, content, e-commerce, platform services, and cross-border data flows) have been significant. Commerce has become even more global as e-commerce allows consumers to buy products online and ship/receive products anywhere in the world at the click of a button. Digital content, social platforms, and apps are accelerating these trends. To enable seamless transactions in this environment, payments data is sent around the world in seconds and goes through multiple security checks.

These advances have come with challenges, such as privacy breaches and cyber-attacks. Unfortunately, these challenges and other valid concerns from governments are driving an increase of protectionist measures in response. In our 1st report in this series, titled Strategic Framework for Digital Economic Cooperation – State of Play, we highlighted that we are fast approaching an inflection point where further hardening and fragmentation in the digital economic landscape will lead to a downward spiral for data-driven parts of the economy that have been an engine for growth.

Protectionist Policy and Data Localization

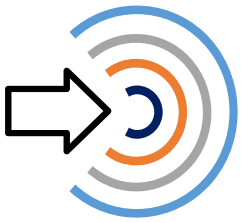
- Restricted data flows
- Duplicated infrastructure
- Closed loop systems
- Fragmented supervision
- Blocked digital trade

Digital Economic Cooperation

- Mutual recognition
- Trust mechanisms
- Interoperability
- Cross-border data flows
- Trade facilitation
- Cooperative supervision

Global and multilateral institutions have recognized the challenges but so far have failed to find consensus and meaningful solutions. The Japanese G20 Presidency in 2019 advanced the "Data Free Flow with Trust" initiative, and data flows were at the heart of the 2021 G7 Trade Ministers' Digital Trade Principles, but standards remain elusive and geopolitical headwinds are growing stronger against the likelihood of these efforts making progress. Now is an important moment for like-minded firms, industries, and states to focus on digital economic cooperation and find pathways to progress.

The financial industry has a leading role to play. It is inherently global with a long history of cross-border transactions, operating within a well-developed web of international regulatory bodies. It also uses data in ways that are tangible to consumers, businesses, and policymakers alike, providing nearly instantaneous payments around the globe for individuals and companies, and using AI to prevent small-scale fraud and sophisticated financial crime. Financial institutions lie at the heart of every industry's operations as they facilitate the transactions required to execute contracts and ensure global supply chains function efficiently. They are well-placed to explain how data can be used to promote economic opportunity, competition, and security, and to work with policymakers to shape smart regulations that foster data flows while guarding against potential harms. To support such an effort, we offer a strategic framework for consideration.



II. Strategic Framework for Digital Economic Cooperation

Objective and Principles

Digital economic cooperation should promote trust, security, privacy, and consistency so that data can be allowed to flow freely across sectors of the economy and across borders. This would support sustainable growth in the digital economy that benefits all participants. Mechanisms to advance these objectives, establish minimum standards, and resolve disputes could help ensure that these high-growth sectors of the economy can continue to drive economic opportunity while producing more stable and consistent conditions in markets around the globe.

Data localization and other protectionist barriers to digital economic activity will not deliver a secure high-growth environment. Instead of employing these blunt policy tools, developing guard rails would support more innovation and flexibility while maintaining some control and protection. In this approach, a set of principles for digital economic cooperation can help guide governments and industry in design.

Principles

1. Improve trust, safety, and privacy for all participants
2. Promote an open and competitive environment for all players in new sectors of the economy
3. Enable small and medium size business growth
4. Establish mechanisms for collaboration across borders to enable free and secure data sharing
5. Promote network, technical, and regulatory interoperability across territories
6. Establish mechanisms to resolve conflicts, eliminate duplication, and reduce systemic inefficiencies.

Strategic Framework

The dynamics at play are complex and there are no easy one-size-fits-all solutions. Failure to advance broad multilateral solutions in global forums such as the G20 underlines the challenges. Implementing principles for digital economic cooperation will require a multi-pronged approach involving a wide range of stakeholders in efforts to foster trust and transparency beginning with areas of common ground to build momentum.

A strategic framework helps organize attention on those areas where measured progress is possible, and we have categorized the themes that require attention into primary domains as illustrated below.

Leadership and Coordination

Overlapping networks organize our society including monetary systems, supply chains, and the internet. To function, these networks require coordination, standards for interoperability, protocols for conduct, and mechanisms for conflict resolution, none of which would be possible without some form of leadership and coordination of activities. To date, limited regulatory intervention in the development of the internet has fostered diversity, innovation, and growth. It has also been a good match for the attributes of data including the ability for a single data element to be used simultaneously in different locations.

As governments become more active in their regulation of data and its use, they are creating a variation and duplication of requirements that is unsustainable, increasing the cost of compliance without necessarily enhancing security and resilience. Greater collaboration will be required across a wide spectrum of stakeholders to reverse this trend.

During the 2021 IIF Annual Membership Meeting (AMM), Visa's Bob Hedges stressed the importance of digital economic cooperation, stating: "Given the speed and scale at which the world digitizes, it is critical that the international community have a clear vision on how to enable international digital

economic cooperation. The fundamental challenge today is not digital policy, but rather economic cooperation." In the same AMM, BBVA's Carlos Torres Vila underscored the need for coordination, commenting that "we do not have traffic rules for data, privacy, liability, and competition in the digital economy".

Government authorities, regulators, industry bodies, and business interests all have a very important role to play. In addition, it is vital that we leverage and update those existing governance structures rather than defaulting to creating yet another layer of governance that could bring about even more fragmentation.

There is a need for this coordination, perhaps via a coalition of willing entities if not a single entity, to shape global standards, regulations, and policies for data, privacy, virtual goods, and digital rights across the economy. Advice on best practices, as well as foresight regarding the impacts of regulatory and policy actions, is required to address vulnerabilities, monitor risks arising from new technologies, including their impact on society and the broader digital economy, and develop regulatory and policy interventions to address them. These efforts would also require careful design to avoid further fragmentation of the regulatory and supervision landscape, while overcoming the challenges to functioning with so many stakeholders.

The current geopolitical dynamic and revival of economic sovereignty would make even the establishment of a new multilateral function, and not a single coordinating entity, difficult in its own right and could similarly result in yet another layer of complexity and fragmentation if not carefully designed. Therefore, leveraging existing leadership structures transformed to fulfill this role might have a greater likelihood of near-term success.

The Financial Stability Board (FSB) is well-placed to explore this need, subject to further developing the required digital skills and capacity. The financial services industry, its regulators, and supervisors are highly informed and impacted by various data frameworks and have already begun exploring their effects on cross-border payments. The alternative, but less effective approach, would be to form a coalition of existing governance mechanisms to fulfill this role.

If pursued, multilateral digital cooperation mechanisms should interface with the broader political and policymaker community, international organizations, standard-setting bodies, and institutions such as the IMF, World Bank, OECD and the BIS to ensure that various initiatives underway are aligned with broader digital economic cooperation objectives.

Challenges to a global digital cooperation mechanism shift focus to a coalition of the willing, where likeminded countries with similar financial systems and similar values work together to prioritize regional nodal and bilateral initiatives that focus on near-term benefits while establishing building blocks for more international solutions in the longer term. We see these efforts underway and encourage greater coordination on key standards questions across these efforts.

There are several leadership and coordination actions that would yield benefits, the most important of which have been outlined in the table below.

Stakeholder grouping	Leadership actions that are required
Political leadership & Policymakers G7 G7 + Friends G20 FSB Coalition of the willing	• Explore a multilateral data governance mechanism • Modernize international standards to support data flows with trust • Open multi-stakeholder participation • Establish mechanisms to resolve conflicts and support enforcement • Assess vulnerabilities and risks in cooperation with governance mechanisms and the private sector
Global Governance Mechanisms BIS IMF World Bank OECD	• Coordinate development of global governance standards, regulations, principles, and policies for data frameworks • Establish and promote mechanisms for cross border equivalence recognition • Monitor implementation of principles, standards, and policies with an eye to harmonization
Industry Private sector Industry bodies	• Work with regulators and industry bodies to bring about coherence and harmonization in regulatory requirements • Support industry baseline standards across territories • Promote cross-industry mechanisms for risk identification and management • Contribute significantly to skills and knowledge development in the public sector
Trade World Trade Organization Bilateral and regional agreements	• Make a firm, improved commitment on electronic payments and harmonization of digital economic trade • Update frameworks to assess new technologies' implications for trade and trade-rule compliance
Nation states	• Participate in international initiatives • Develop skills and expertise in data, its attributes and economics, and new business models • Pursue trade initiatives that include digital cooperation and avoid protectionism

Knowledge and Skills

New technologies and business models continue to develop rapidly, making it a challenge to keep pace. Most business leaders, politicians, policymakers, and regulators require upskilling on topics that have become central to their domains in just a few short years such as digital assets, machine learning, and data governance.

As a result, knowledge and skills gaps require attention while communication gaps can be just as significant a challenge. Collaboration between the public and private sectors can be an important part of the solution to improve understanding in a few key areas:

- **Attributes and economics of data** - how value and revenue are generated from data and what conditions maximize benefits
- **Data security and protection techniques, including encryption keys** - what solutions best deliver desired conditions
- **Impacts of data localization measures** - the tradeoffs and opportunity costs across the economy

Regulatory bodies have limited policy and technology expertise in critical areas including machine learning, digital assets, quantum computing, cloud security, data management and data architecture. This deficit, and the intense competition for talent, makes it challenging for regulation and supervision to be well targeted while supporting innovation. Prioritizing a rebalancing of skills at all levels of the institutions is important. This could be supported by the private sector helping to inform upskilling training efforts.

Many involved in the public policy debate have a limited understanding of the benefits of cross-border data flows or the benefits of cross-border digital economic activity for small business. This leads to misconceptions of the perceived benefits of data localization measures.

Diplomats and negotiators could be better informed by technology experts on attributes of data and the impacts of various policies. The current knowledge gap is an additional challenge to resolving conflicts.

Politicians and technology leaders tend to focus on different domains due to the nature of their roles. There is a need for more informed dialogue so that stakeholders understand, both, what is politically feasible and what is technologically possible.

Few understand how new risks presented by new technology compare to existing risks we have grown accustomed to from old technology in operations or financial crime. For instance, cloud technology can be configured to improve security and resilience over that of many legacy systems.

Private sector firms could inform and support public sector knowledge and skills development, while continuing to invest and grow their own knowledge and skills base of policy considerations. Private sector firms could also expand digital expertise at board, senior management, and middle management levels, as skills and knowledge transformation are required for most firms.

Regulatory Architecture

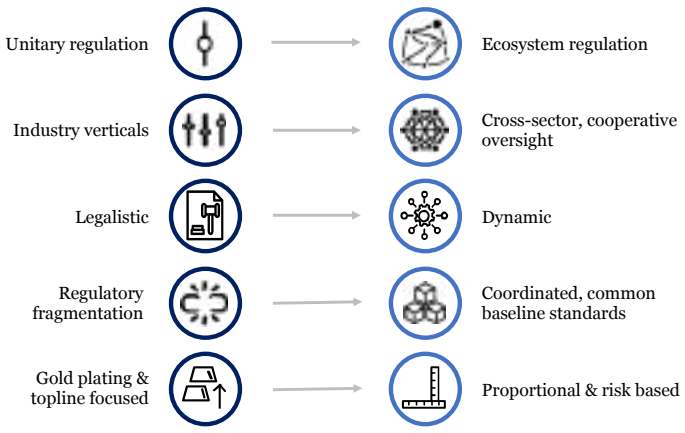
As digital transformation drives new players entering the market, new business activities being invented, new ecosystems forming, and new risks emerging, policymakers and regulators struggle to keep up with the change. Both the public and private sectors increasingly find that the existing regulatory architecture that was designed for an industrial era economy is difficult to apply to the digital economy. The velocity of change is exponential, adding to the urgency of addressing regulatory architecture shortcomings as they are identified.

In 2019, the International Monetary Fund (IMF) reported that, "Financial firms are spending significant resources juggling regulatory demands and implementing new rules. In some instances, regulations are overlapping, duplicative and conflicting." The situation has subsequently worsened, and most firms find that a significant number of resources are occupied trying to deal with the fragmentation in the regulatory landscape, instead of building stronger defenses and reducing risk.

In addition, new players and new activities are not always subject to the same level of regulatory scrutiny, creating regulatory asymmetry that distorts the ecosystem equilibrium and builds-up new risks. Recognizing the desire not to stifle innovation, the current "light-touch" approach to digital regulation presents an opportunity to keep pace with changes in the economic landscape, and deal with changes in the digital economy proactively, to manage the risks before they manifest.

A paradigm shift is required

The paradigm shift to a digital economy necessitates a paradigm shift in the regulatory architecture as illustrated below.



Change is required to remain relevant in today's environment. The five major areas outlined above are briefly discussed below.

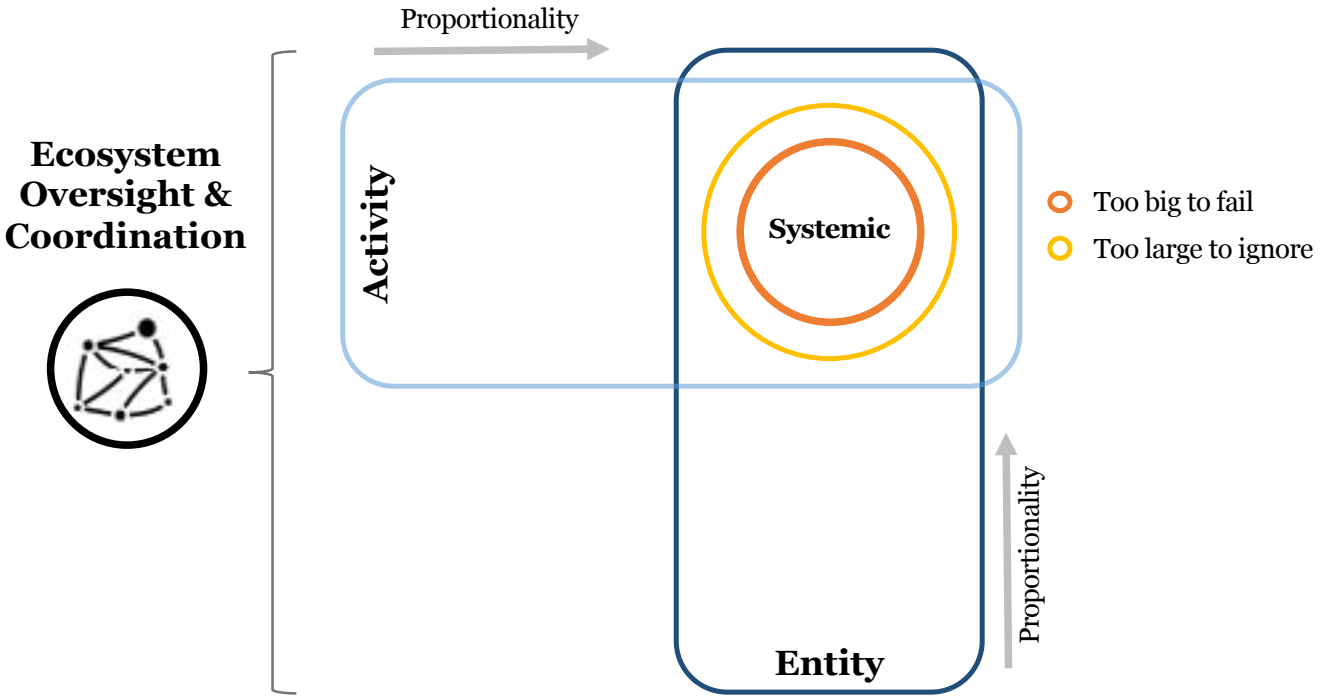
1. The current regulatory architecture has been built primarily for **unitary organizations**. However, financial services and the digital economy at large are becoming increasingly modular and distributed, with many parties involved, many of them new entrants. Data, assets, activities, and risks are now spread across multiple platforms, suggesting an **ecosystem approach** with close coordination would be more appropriate.
2. Regulators are predominantly focused on **industry verticals**. Meanwhile, in the digital economy, boundaries between industry verticals are dissolving, financial services are increasingly digital, and technology companies are moving into larger parts of the financial services value chains while approaching systemic importance. Boundaries between other industry verticals are also dissolving. Regulators must adjust to these changes and adopt a **cross-sectoral and cross-border approach**. Increased focus must be placed on **cooperation and coordination** at both local and international levels across all industry sectors. These cooperative arrangements could involve or augment existing arrangements and build on experience gained in running supervisory colleges for financial firm supervision. A key objective should be to establish adequate mutual recognition mechanisms to eliminate duplication and inefficiency in cross-border regulation.
3. Regulatory bodies are traditionally staffed with economists and lawyers. As a result, a strong bias exists to adopt a **legalistic approach** towards regulation and supervision with long gestation periods. The digital economy, however, is very dynamic and evolves and changes at a rapid pace. The regulatory process **must become dynamic,** flexible, and digitally smart to keep pace with the ever-changing landscape. The regulatory approach must adopt digital technologies such as: advanced data analytics, dynamic risk information, and more advanced platforms for structural sharing of information in secure ways. The adoption of these digital technologies must be integrated and embedded in business-as-usual regulatory activities to bring about a transformation in the regulatory architecture.
4. **Regulatory fragmentation** is a significant challenge, leaving consumers more at risk, creating barriers to entry, and stifling innovation. A change in direction is required towards an architecture that focuses on **coordinated and common baseline standards** to facilitate mutual recognition and greater **interoperability**.
5. At a national level, there is a strong focus on domestic priorities, creating a bias to adopt a **topline-focused approach**, resulting in **gold plating** of regulatory requirements. This dynamic, however, creates further fragmentation and interoperability problems across the global digital economic landscape. The regulatory approach should be changed to become **more proportional and risk-based** in its application, building on common objectives and **baseline standards**. Topline and entity-specific requirements should be dealt with on a case-by-case basis and applied to systemically important entities and activities, instead of a broad-brush approach of gold plating requirements for all participants.

Ecosystem regulation

The digital economy is currently driven by platforms, network services, data collection, analytics, digital intellectual property, new payment mechanisms, the advent of digital assets, and other innovations. These technologies and services have complex interactions and often use distributed architectures with multiple customers and service providers across terrestrial borders. These ecosystems, including the internet, operate on the premises that everything is interconnected with data flowing freely in real-time.

The current regulatory architecture has been designed to work best for unitary structures, silos, borders, and linear risks. Authorities face the challenge of modernizing the regulatory architecture to be fit for purpose for managing risks across the digital

economic ecosystem. To do so, one must consider both an entity-based and an activity-based approach, while simultaneously considering the application of proportionality and systemic importance as illustrated below.



During the 2021 IIF Annual Membership Meeting, several participants commented that activity plus entity-based regulation is necessary, and a comprehensive matrix approach is required that addresses prudential concerns as well as asymmetrical competition from non-bank players who pursue a data-monetization business model. Whilst bank regulators will always focus on their primary concern, the risk of bank failure, it is important to incorporate activity-based regulation into the regulatory architecture.

Mr. Fernando Restoy, Chairman, Financial Stability Institute, Bank for International Settlements, in a speech to the fintech working group at the European Parliament, noted that the slogan "same activity-same regulation" is often heard as the possible basis for regulatory reform, and that the phrase suggests moving from a framework for entities with a specific license to a system of rules for specific activities, which would be applied uniformly to all types of entities involved. Whilst acknowledging the need for a level playing field, he noted that the risks generated by different entities performing a similar activity are not necessarily the same. As a result, different entities may be subject to different rules in order to properly address the specific risks that they generate.

BBVA's Lucia Pacheco provided an insightful analysis of the complexities of entity and activity-based supervision in a paper dealing with entity vs. activity-based frameworks, in which she outlines the different dynamics in the digital economy and how certain technological activities at scale pose greater risks for financial stability. The paper proposes a combination of entity and activity-based approaches.

Principles of risk-based and proportional regulation are well embedded in existing regulatory frameworks

Whilst regulatory asymmetries will always exist, often for valid reasons, there has perhaps been too much focus on which approach will be most appropriate. Instead, we should realize that both approaches are important and the debate should be focused on how both approaches are applied effectively. Given that limited resources are available, focus should be placed on areas of systemic importance to the digital economic ecosystem, whilst also allowing a framework that is sufficiently flexible to enable innovation and new start-up formation.

Recommendations could include the following: i) A

matrix for both entity and activity-based approaches; ii) A risk-based approach to apply proportionality-based regulation and supervision, thereby allowing resources to be focused on systemic risk to the digital economic ecosystem, whilst enabling innovation and startup formation; iii) Supervision that not only focuses on entities and activities, but also the interconnectedness of the modular components of an ecosystem and how these connections could pose a risk to integrity and stability.

Protocols and Standards

Existing protocols and standards are developed with a common objective amongst industry and regulators: to ensure the resiliency, integrity, and stability of the financial sector and the broader economy. These protocols and standards provide the guard rails to identify and manage risks.

Fragmentation in frameworks, protocols, and standards

Over time, different motivations have led to a proliferation of different frameworks, protocols, and standards across most territories, leading to significant fragmentation and great complexity for multinational organizations who must deal with costly and inefficient many-to-many relationships between regulations, entities, and standards.

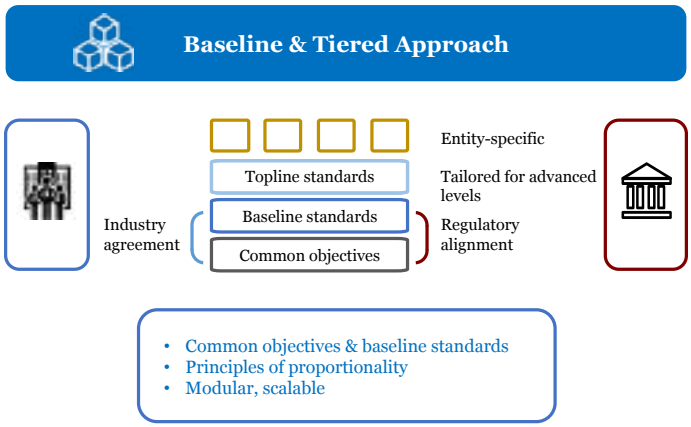
Rules are local, but threats to stability & integrity are global

Various regulators and supervisors will continue to take diverse approaches driven by different values, motivations, market conditions, and governance requirements; however, this increasing fragmentation is approaching a breaking point as finite resources are available to deal with fragmented, duplicated, and contradicting compliance requirements across territories. Established firms have all developed their own benchmark frameworks, standards, and controls, and have built capacity to deal with the fragmentation of requirements. However, the cost is spiraling out of control. For less mature, smaller firms and start-ups, navigating the complexity of requirements upon entering the market becomes an impossible task, especially with limited resources and skills.

Furthermore, cross-border threats evolve at a pace that policy development cannot match, and it is nearly impossible to adapt requirements quickly enough to stay ahead of the technological changes.

A baseline and tiered approach are required

The continuous change and innovation that technology is driving require that the frameworks, protocols, and standards architecture be simplified, rationalized, and focused on baseline requirements, as illustrated below. Protocols and standards must be scalable and allow for less mature companies, including earlier-stage fintechs, to connect with very mature organizations while maintaining a baseline level of requirements for all interoperability layers that are understood and accepted by all parties.



Focus is required on interoperability at all layers

Established mechanisms have been put in place over the past several decades, such as the WTO, to help the industrial economy operate internationally. Similar mechanisms are now required for the digital economy, as illustrated below. Different countries will have different values and motivations as they approach the task of regulating the digital economy. Therefore, interoperability in many layers — including laws, regulations, standards, networks, and technology — will be required for international operations to connect and function effectively.

When interoperability works well, it is invisible, enabling customers and service providers to connect seamlessly.

Low barriers to interoperability result in improved resilience, security, efficiency, and inclusivity. The global financial system as we know it functions on the back of interoperability that has been established at all layers, albeit through legacy systems that have in many cases been patched and adapted to accommodate disparate developments. Still, the digital economy has rapidly evolved, in particular, on the back of technical and network interoperability brought about with the development of the internet. Not all frameworks have kept pace with technological progress, but addressing these shortcomings would help improve stability, security, and prosperity.

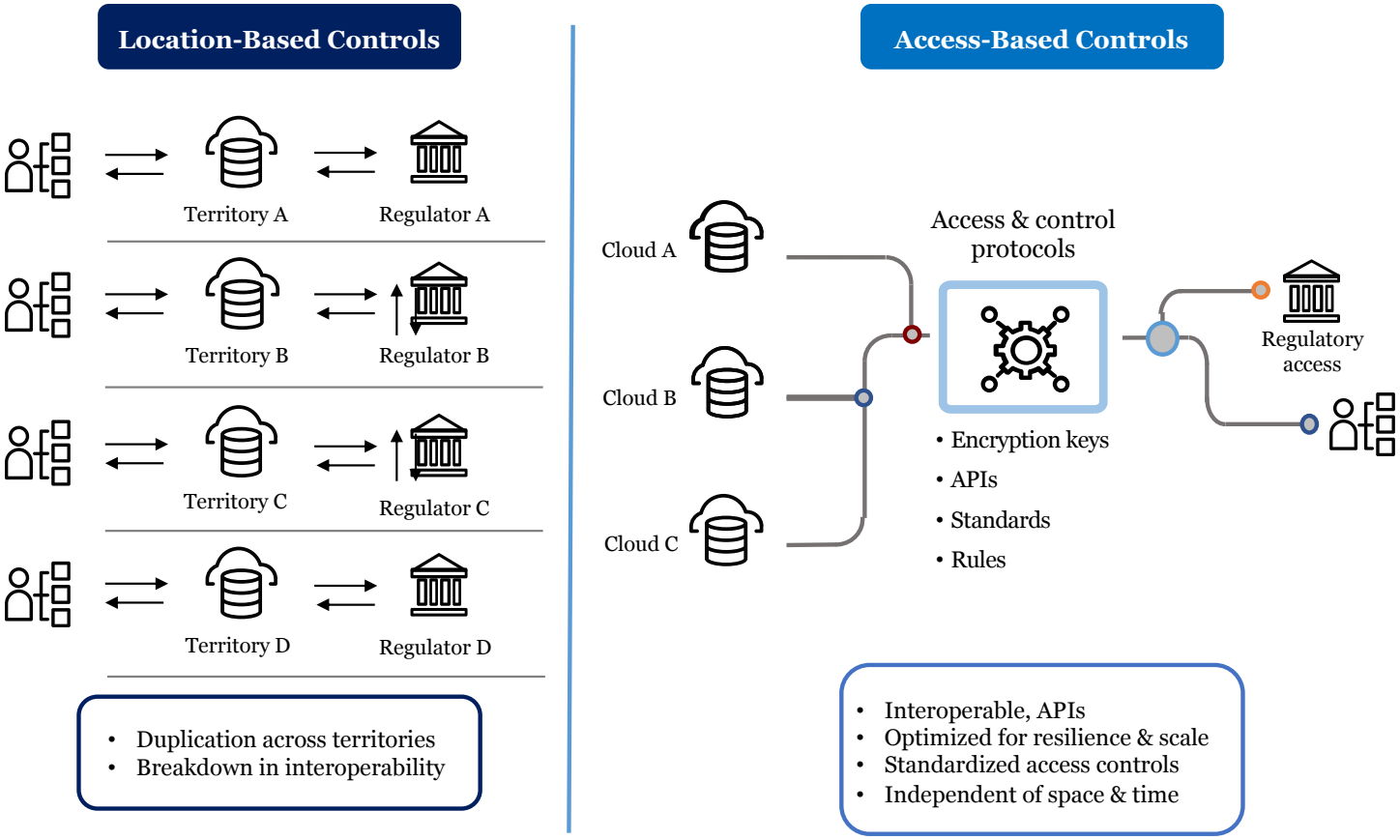
Interoperability does not mean uniformity and rigidity, which could stifle innovation. Rather, it would benefit from common taxonomies, definitions, baseline standards, and mutual recognition mechanisms that enable cross-border operations and open systems rather than barriers, walls, and closed-loop systems. In "Let's talk about how we talk about interoperability" the Visa Economic Empowerment Institute laid out technical, network, and regulatory areas of interoperability. Legal and standards aspects, beyond regulation, round out the list.

- **Technical** interoperability requires the ability to facilitate and process transactions and data exchange between different parties, applications, and infrastructure to enable real-time transactions and services independent of space and time, without manual intervention. The private sector, together with standard-setting bodies, should continue to focus on technical interoperability standards to ensure open access, particularly for the use of AI, digital identity, digital currency, and APIs.
- **Network** interoperability requires the ability for multiple parties to connect through a network, or intra-network, to facilitate transactions and exchange of data and services. Common rules are important for building trust, resilience, open access, and value-added services such as risk and fraud analytics. The private sector, together with standard-setting bodies, should continue to focus on network interoperability standards to ensure open access, particularly for the modernization of payments systems and digital currencies.
- **Regulatory** interoperability requires the ability to connect digital transaction and service platforms across different jurisdictions governed by differing regulatory requirements (often contradictory). The **financial services regulatory community** should take the lead to ensure cross-industry and cross-territory regulatory interoperability for areas such as law enforcement, data sharing, privacy, consumer protection, and dispute management.
- **Legal** interoperability requires certainty over legal liability in the different jurisdictions in which a firm operates. **Policymakers and political leaders** must ensure the establishment of treaties and international governance mechanisms that enable cooperation, mutual recognition, and legal conflict resolution.
- **Standards** interoperability enables closed-loop systems to become-open loop systems and removes barriers, enabling cross-border digital economic activities. The **FSB and BIS** models for standard-setting, proportionality, equivalence mechanisms and supervision should be leveraged to enable similar mechanisms and coverage across the digital economy.

Access and control protocols can support interoperability

Access to secure, trusted networks and services that operate across borders is essential for much of the modern economy. Technology solutions to deliver these conditions — with resilience, safety, security, and privacy — rely on global capabilities and real-time connectivity. Strengthening and updating these systems to meet society's expectations for privacy and security should be the objective, rather than resorting to localization and digital protectionist measures that foment duplications, costs, and constraints. While challenging, shifting the emphasis away from a location bias and towards investment in better access and control solutions could be much more

productive in the long-run. For instance, application programming interfaces (APIs) allow new gateways for structural sharing of data in secure ways, allowing benefits to arise from business-to-business, business-to-regulator, regulator-to-business, and regulator-to-regulator sharing of data. Further progress in this direction and the next generation of encryption and distributed architecture could produce solutions. The development of quantum computing and preparedness efforts are already driving a rethink of security and updates to encryption standards. Perhaps this is an opportunity to think more broadly about how technology can support better access-based controls.



The private sector has an increasing role to play developing shared standards and a framework for connecting those standards

Technology and data have taken a central role in society, and as a result, different societal views on privacy, human rights, and the role of the state vs. the individual are becoming manifest in the regulations, protocols, and standards for technology and data. This is likely to increase, and therefore industry should not leave it to policymakers and regulators alone to solve. Common global standards are unlikely in many areas given these dynamics; however, a global framework to drive awareness, coordination, and design, so that systems maintain as much connectivity and interoperability as possible, will prevent the worst impacts from the creeping fragmentation of data frameworks.

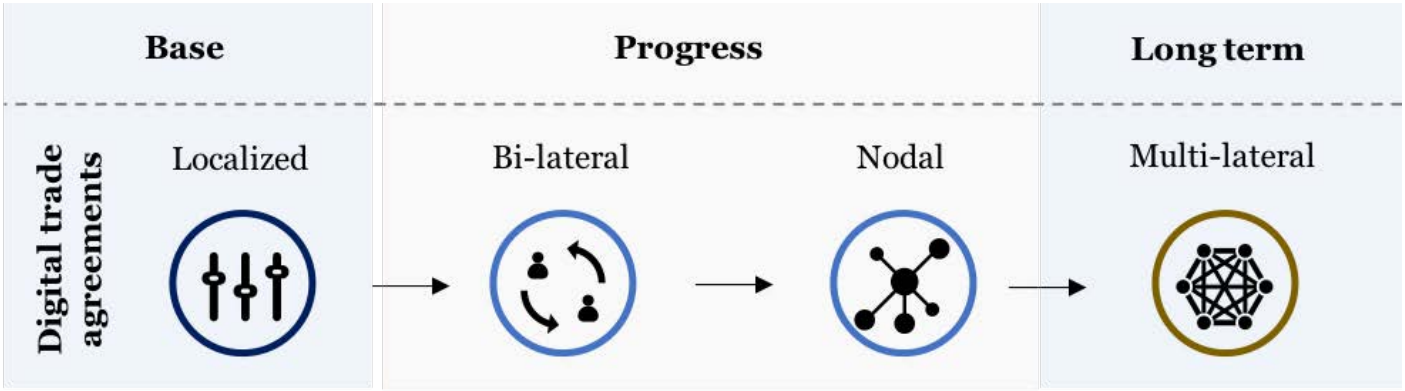
- Industry, via industry bodies, should take a leading role in articulating **common objectives** for digital economic frameworks, protocols, and standards. These objectives should consider cross-industry requirements as well as regulatory expectations.

- Industry should take the lead to develop and identify **common baseline standards** for digital economic activities where possible while working closely with international organizations. There are several existing developments that are in place and will need to be considered. Specific examples include:
    - **Cybersecurity** – ISO 27000 and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) are the most recognized and could be used as the cross-industry baseline standard.
    - **Privacy** – OECD privacy principles could provide a cross-industry baseline reference and Convention 108 has set the rules within the EU that others might adopt.
    - **Cloud Computing Standards** – Global standard-setters and several national financial regulators are exploring more direct supervision and standards.
    - **Digital Identity** – the Global Legal Entity Identifier Foundation (GLEIF) and the Global Assured Identity Network (GAIN) network are global standards and interoperability initiatives of note.
    - **Digital Currency** – Global Stablecoin (GS) proposals have driven an effort to establish global standards and CBDC experimentation has spurred G7 principles for CBDCs and work on bridges for interoperability.
- Additional areas will be much more difficult to find consensus given varying societal views but are important to maintain efforts:
    - **Consumer Consent**- the right for customers to determine what data they will share and its use.
    - **Law Enforcement Access to Data** – security rights to gain access across territorial borders for enforcement.
- The **FSB** and the **BIS** are good examples of global entities designed to drive global standards and coordination between regulators.

Regulators should explore where agreement exists on how topline standards and entity-specific requirements should be applied; this should be a risk-based framework using the principle of proportionality, specifically focusing on entities and activities of systemic risk. The FSB and BIS should take the lead in this regard.

- Establishing and promoting mutual recognition mechanisms should be a top priority.
- The EU's data protection adequacy decision process, which provides for a mutual recognition mechanism for data transfers to non-EU countries, requires a revamp of effort for broader coverage to more countries.

- Greater effort and resources should be invested by industry to drive the adoption and use case development of interoperability mechanisms, for example, Global Legal Entity Identifiers (GLEIF) for small and medium enterprises (SMEs).



Digital Trade Enablement

Many of the existing free trade agreements were designed for a different era. They predominantly focus on industrial economic activities such as agriculture, manufacturing, and some services, whilst there is little-to-no coverage of elements central to digital content and data-driven economic activity. Policymakers and regulators are encouraged to focus on new aspects of cross-border trade including the flow of data, digital identity, e-invoicing, and mutual recognition of data regulations and safeguards.

Achieving broad international coherence through either coordinated agreements, such as the historic Bretton Woods Agreement or leveraging forums such as the G20 or the World Trade Organization (WTO) to make progress, appear to be a long way from reality given the current geopolitical dynamic and revival of economic sovereignty. The objective of a digital economic multilateral agreement should remain a long-term goal. To support this, near-term bilateral and nodal group agreements should be accompanied by structured global efforts to build technical mapping, awareness, and coordination to maximize the potential for interoperability and connectivity between emerging blocks of nations with digital trade agreements.

Several trade agreements and initiatives have made good progress despite the challenges. For example:

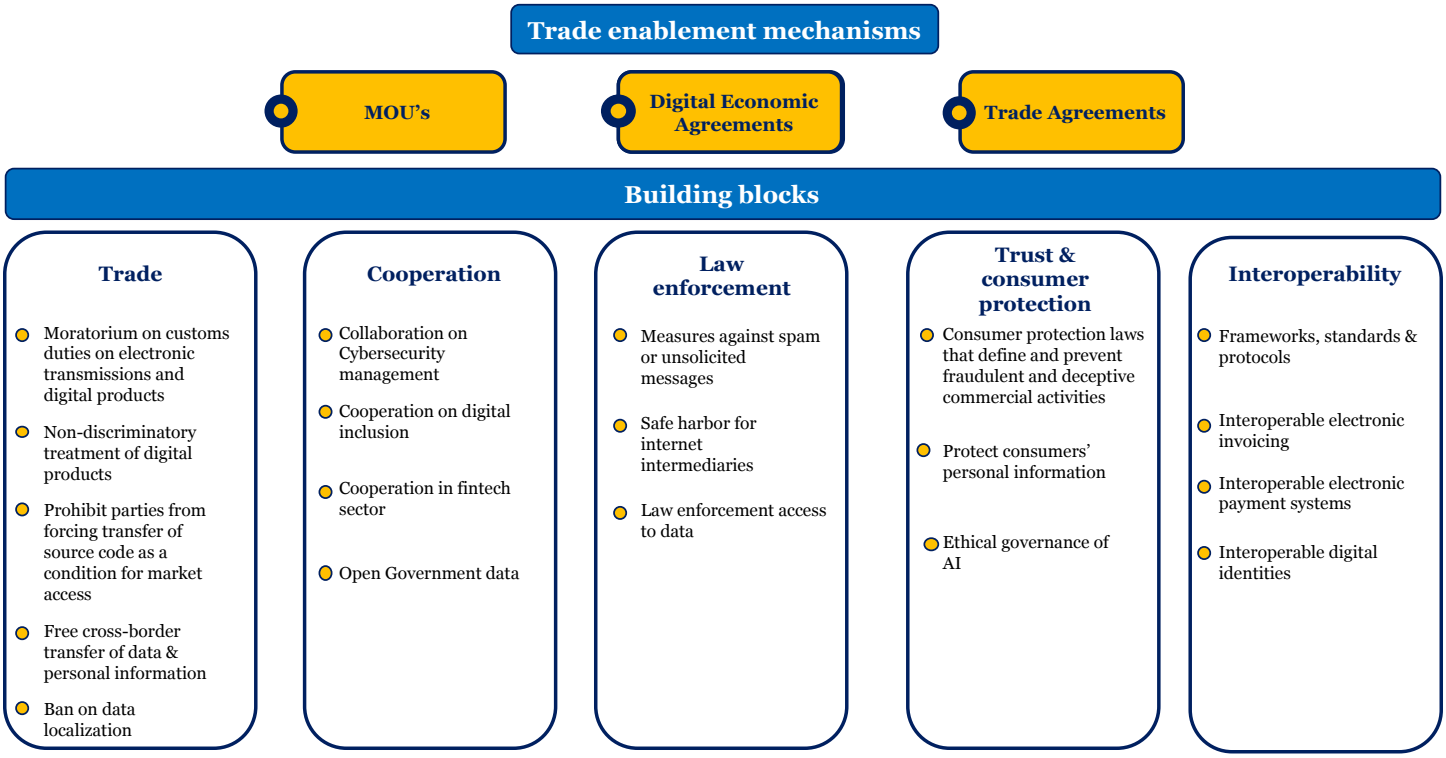
- The UK - Singapore Digital Economy Agreement (DEA)
- The United States - Mexico - Canada Agreement (USMCA) with chapters on digital trade
- The Singapore - Australia Digital Economic Agreement
- The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) with a comprehensive e-commerce chapter
- The Australia-Hong Kong Free Trade Agreement (A-HKFTA) with digital, financial services, and education sections
- The United States Department of the Treasury and the Monetary Authority of Singapore (MAS) MOU on Cybersecurity Cooperation
- The Monetary Authority of Singapore (MAS) and the Bangko Sentral ng Pilipinas (BSP) enhanced FinTech Cooperation Agreement (CA) to facilitate interoperable payments

The UK and Singapore DEA covers the digitized trade in services and goods across the whole economy for open and inclusive digital markets. Provisions support the free flow of data, duty-free digital content, cooperation on competition policy, standards and conformity assessment, protection for source code, mutual recognition of regulations, and digital trading systems including authentication, electronic contracts, and digital customs. This is also boosting hopes for the UK to join the 11-nation CPTPP agreement. This development provides further momentum towards a nodal approach for digital trade development, where bilateral agreements act as a springboard for broader extension to other territories. Singapore is currently playing a leading role in the nodal development of digital trade. We expect that other territories, such as the UK, will also increasingly play a key role in nodal digital trade development.

The digital trade agreements have a common objective of making digital trade and connectivity more secure, more trusted, more efficient, and lower cost, whilst having a mutual understanding, comfort, and sometimes recognition of each other's protocols and regulations.

Trade enablement mechanisms usually take the form of a combination of either a Memo of Understanding (MOU) aimed at cooperation in various digital economic areas, specific Digital Economic Agreements (DEAs) such as the Singapore-Australia digital economic agreement which included digital financial services, or a comprehensive trade agreement with extensive coverage of digital trade, such as the CPTPP agreement.

These trade enablement mechanisms deal with specific trade, consumer protection, areas of cooperation, interoperability commitments, and law enforcement cooperation. These building blocks continue to evolve and will continue to mature and become more comprehensive in nature. The foundational requirements that have emerged from current agreements are detailed in the illustration below.



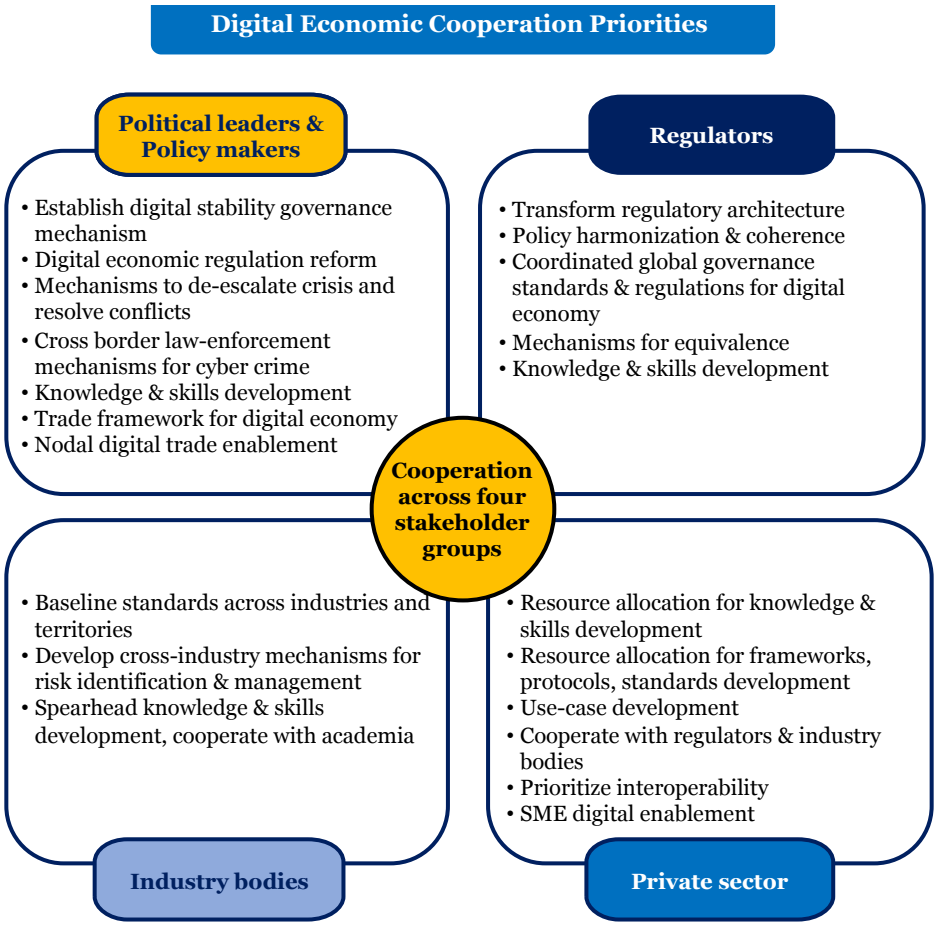
III. Way Forward

Priorities That Move the Needle

Political leaders and policymakers should align their trade enablement objectives with the foundational building blocks that have emerged from landmark agreements to-date, as illustrated above. Specific emphasis should be placed on law enforcement cooperation for cybercrime related activities. While a bilateral and nodal approach (coalition of the willing) are where progress is possible today, multilateral coordination, tracking, and planning should be added to minimize fragmentation and increase the opportunity for broad multilateral agreements in the long-term.

The technology and intellectual capabilities exist to solve the problems identified in this paper. What is required is leadership, mobilization, and coordination of resources to deliver progress. The stakes are high, and the current socio-economic dynamic requires that the enormous benefits that the digital economy has to offer become a reality. Several priority items require attention for progress. Collaboration between the private and public sector is required, and the

respective stakeholder groupings need to each play a leading role in advancing specific issues, as illustrated below.



What Should be Leveraged

Establishing new institutions and mechanisms could further complicate an already significantly fragmented landscape. It is therefore vital to align, leverage, and transform existing governance institutions and mechanisms to become future-fit for the digital economy.

Financial services governance mechanisms are uniquely positioned to take a leading role in dealing with the challenges at hand in light of their successfully established cross-border cooperation, standard-setting, interoperability mechanisms, and supervision protocols for the financial sector. The experience and principles developed over the recent decades should be leveraged to establish governance mechanisms for the digital economy. No other industry has the same reach and level of skills and experience in achieving interoperability for complex cross-border domains. Specific recommendations include:

- The **Financial Stability Board's** (FSB) structure of convening peer regulators to coordinate on policy issues should be leveraged to explore the impact of different data frameworks on long-term stability.
- The **Bank for International Settlements** (BIS) structured together with national central banks and regulators should be leveraged for the development and agreement of cross-border frameworks, standards, protocols, equivalence mechanisms, cross-industry supervisory colleges, cross-border supervision protocols, and principles for risk-based and proportional supervision. The innovation hubs and their work on digital currency and bridging mechanisms is an excellent example of existing international bodies extending into these new domains.

- Existing **law enforcement cooperation mechanisms** should be leveraged, and cyber capabilities and protocols established or enhanced where necessary to deal specifically with ever-increasing sophisticated cybercrime. Fraud, criminal conduct, and cybercrime are areas of common interest where there are significant benefits to be realized from cross-border cooperation. This should also be leveraged as a theme to set the foundation for broader cooperation in other domains.

Pitfalls to Avoid

These efforts should not digress towards establishing common rails or singular policy solutions as a shortcut for interoperability. Such designs would compromise resilience and innovation and result in the lowest common denominator effect where consumer experiences and capabilities are inhibited. Similarly, aiming for a gold standard whilst arguing whose approach is best will also create unnecessarily complex and costly infrastructure, inhibiting interoperability and creating barriers to entry for new participants and start-up formation. Multiple platforms, networks, and connections across borders are key features of the digital ecosystem and a rulebook should be designed for this complex, dynamic, and interconnected landscape.

Another important pitfall to avoid is the belief that trade agreements will automatically solve regulatory framework fragmentation challenges. Successful trade agreements can come unstuck at ground level where regulatory requirements are contradicting or implicit mechanisms are used to impose restrictions. Concerted effort is required at all layers for successful cooperation and implementation.

IV. Conclusion

The last era, defined by an open global internet with free-flowing data across borders, has fueled innovation and high-growth sectors of the economy delivering digital content, virtual goods, and valued new services. Recent years, however, have revealed problems with privacy, security, monetization and taxation. Policy responses have been rapid, fragmented, and poorly coordinated at the international level. Data localization measures, a lack of coordination of data governance requirements, hastily drafted privacy laws, digital identity efforts without interoperability standards, far-reaching AI regulation, and an overall lack of coordination threaten to choke the future of the digital economy. These conditions are also challenging the ability for existing firms to deliver fast, low-cost, and consistent international services in finance, communications, and information. The neo-protectionist view that has informed many policy responses also runs contrary to economic theory about the benefits of free trade, the efficiency of scale, and the advantages of connectivity.

Global bodies should continue to highlight the issues and challenges while becoming active in tracking and coordinating more regional efforts to mitigate regulatory fragmentation. National regulators have a responsibility to consider the design of their policy, regulation, and supervision with more global awareness of the technology, industries, and activities they are impacting. This should be accompanied by a dramatically higher degree of coordination and effort toward interoperability or connectivity.

The financial services industry has a leading role to play in this effort. It is global, delivers cross-border transactions, and operates within a well-developed web of international regulatory bodies. It also uses data in ways that are tangible to consumers and policymakers alike, providing nearly instantaneous payments around the globe for individuals and companies, and using AI to prevent small-scale fraud and sophisticated financial crime. Financial institutions are well-placed to explain how data can be used to promote economic opportunity, competition, and security, and to work with policymakers to shape smart regulations that foster data flows while guarding against potential harms.

Working together, society can find pathways for progress on digital economic cooperation and create a framework for growth the same way the Bretton Woods Conference laid the foundations for an era of international prosperity and growth.

V. Appendix - Resource List

There are several very insightful publications, articles, videos and reports available that have been used as input to our research. The list below provides a reference of key resources used.

*Alliance for eTrade Development, Kati Suominen, "*Why data localization hurts implementing economies*"*

*Australian Government, Department of Foreign Affairs and Trade, "*Australia-Singapore Digital Economy Agreement: summary of key outcomes*"*

*Australian Government, Department of Foreign Affairs and Trade, "*Australia-Singapore Digital Economy Agreement*"*

*BBVA, "*Implementing the principle of 'same activity, same risk, same regulation and supervision'*"*

*Berkeley Technology Law Journal, Douglas Arner, Giuliana Castellano and Eriks Selga, "*The Transnational Data Governance Problem"

*BIS, "*CBDCs: an opportunity for the monetary system*"*

*BIS, "*Regulating big techs in finance*"*

*BIS, Burkhard Balz keynote address, "*Digital payments & European sovereignty*"*

*Carnegie Endowment for International Peace, "*Cyber security and the Financial System*"*

*CCDCOE, "*Tallinn Manual – Essential tool for policy and legal experts on how international law applies to cyber operations*"*

*Center for Strategic & International Studies, Kati Suominen, "*Two Years into CPTPP*"*

*Center for Strategic & International Studies, Kati Suominen, "*What Do CPTPP Member Country Businesses Think about the CPTPP?*"*

*Centre for International Governance Innovation (CIGI), Kieron O'Hara and Wendy Hall, "*Four Internets: The Geopolitics of Digital Governance*"*

*Centre for International Governance Innovation (CIGI), Robert Fay and Rohinton Medhora, "*A global governance Framework for Digital Technologies*"*

*Centre for the Study of Financial Innovation, "*Tech Wars - How Tech Disputes Are Becoming Trade Wars*"*

Council of Europe, Budapest Convention on Cybercrime

*Council of Europe, European Treaty Series - No. 108, "*Convention for the Protection of individuals with regard to Automatic Processing of Personal Data*"*

*Cyber Elders, Koverlin Naidoo, "*Analysing Cyberwarfare Within the Context of Transnational and International Governance Models*"*

European Commission, Adequacy decisions - How the EU determines if a non-EU country has an adequate level of data protection

*Federal Reserve Bank of Richmond, "*The relevance of Adam Smith – The Wealth of Nations*"*

*Financial Times, "*Mastercard, SoftBank and others call on G7 to create tech group*"*

Financial Times, John Thornhill, "Technology wars are becoming the new trade wars"

*G7, "*Public Policy Principles for Retail Central Bank Digital Currencies (CBDCs)*"*

G7, Carbis Bay G7 Summit communiqué, "Our Shared Agenda for Global Action to Build Back Better"

*GSMA, "*Cross-Border Data Flows: The impact of data localisation on IoT*"*

IIF Asia-Pacific Summit, International Digital Economic Co-Operation

*IMF, Daniel Garcia-Macia and Rishi Goyal, "*Decoupling in the digital era*"*

*Information Technology & Innovation Foundation (ITIF), Nigel Cory and Luke Dascoli, "*How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them*"*

*Institute of International Finance, FRT Podcast Episode 96, "*Connectivity and Customer Centricity: Highlights from IIF Asia Summit*"*

*Mastercard, "*Setting principles for the digital economy: Establishing a G7 Data and Technology Forum*"*

McKinsey Global Institute, Manyika, Lund, Bughin, Woetzel, Stamenov, and Dhingra, Digital globalization: The new era of global flows

*Milken Institute, Claude Lopez and Benjamin Smith, "*Share the data: Overcoming Trade-offs in Tech Regulation*"*

*Ministry of Trade and Industry Singapore, "*What are Digital Economy Agreements (DEAs)?"

*OECD, "*Digital Economic Outlook*"*

*OECD, "*Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use across Societies*"*

OECD, Privacy principles

*Office of the Privacy Commissioner for Personal Data (PCPD), Hong Kong, "*Guidance on the Ethical development and use of Artificial Intelligence*"*

*Office of the United States Trade Representative, Agreement between the United States of America, the United Mexican States, and Canada, "*Digital Trade*"*

Various reports and White papers on MSME ecommerce *(Incl Mexico, Africa MSME surveys)*

*Visa Economic Empowerment Institute, "*Cross-border payments for Central Bank Digital Currencies*"*

*Visa Economic Empowerment Institute, "*Small Business in the Digital Age: Recommendations for Recovery and Resilience*"*

*Visa Economic Empowerment Institute, Chad Harper, "*What's going on with remittances?*"*

*Visa Economic Empowerment Institute, Erin English and Jonathan Davis, "*Keeping the lights on for small businesses: Safeguarding the payments ecosystem during the pandemic*"*

*Visa Economic Empowerment Institute, Mike Gallaher, Chad Harper and Barbara Kotschwar, "*Let's talk about how we talk about interoperability*"*

*World Economic Forum, "*Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows*"*

*World Economic Forum, "*Rebuilding Trust and Governance: Towards Data Free Flow with Trust (DFFT)*"*

*World Economic Forum, "*Systems of Cyber Resilience: Secure and Trusted FinTech*"*

World Economic Forum, Data for Common Purpose Initiative

*Yale Law School, Amba Kak and Samm Sacks, "*Shifting Narratives and Emerging trends in Data governance Policy – Developments in China, India and the EU*"*

Authors

Conan French

Director, Digital Finance

cfrench@iif.com

Jaco Grobler

Founder, New Paradigm Finance

jaco@newparadigmfinance.com

Contributor

Jessica Renier

Managing Director, Digital Finance

jrenier@iif.com