United Nations ECE/TRADE/C/CEFACT/2024/INF.5

Economic and Social Council

Distr.: General
10 July 2024

English only

Economic Commission for Europe

Executive Committee

Centre for Trade Facilitation and Electronic Business

Thirtieth session
Geneva, 11 and 12 July 2024
Item 6 (a) of the provisional agenda
Review of the Bureau and Regional Rapporteurs' activities since the twenty-ninth Plenary
White papers for information

White Paper on Cross-Border Management of Trade

Submitted by the Bureau

Summary

Document ECE/TRADE/C/CEFACT/2024/INF.5 is submitted to the thirtieth session of the UN/CEFACT Plenary for information.

Table of Contents

Note....1
Acknowledgements .... **Error! Bookmark not defined.**
1. Introduction....3
2. Background....4
3. What is a digital corridor....4
   3.1. Buy-Ship-Pay Reference Data Model....5
4. Need for cross-border multimodal digital corridors....6
   4.1. Buy-Ship-Pay Reference Data Model processes and transactions....6
5. How to go about implementing a digital corridor....7
6. Benefits of a digital corridor....11
7. Challenges....12
   7.1. Stakeholder digitalization challenges, concerns and costs....12
8. Constraints and strategies to mitigate constraints....13
9. Industry and government initiatives....14
10. Legal framework – recommendations....14
11. Conclusions and recommendations....16

1. Introduction

This white paper has been created under the purview of the UN/CEFACT cross-border management domain and focuses on improving the cross-border flow of all types of freight consignments by applying digital solutions. A **digital corridor** is an electronic platform that connects multiple trade ecosystems (e.g. air/ocean/land community systems or single window systems) to share the status of business activities and relevant cargo information.

Movement of cargo through international (air/ocean/land) borders is often delayed due to lengthy and complex regulatory clearances. Several research projects have shown that a large amount of reusable data exists between origin and destination, for example in customs declarations, carrier manifests etc. If reusability of data is established and information on cargo status is exchanged between origin and destination, then it removes non-tariff barriers to trade between countries and their respective land, sea and airports.

In several countries, these types of ports are exploring the possibility of establishing such data and logistics corridors but cannot find any standard guidance material on the topic. The purpose of this effort is to create guidance material on corridor set-ups, create linkages, and establish appropriate standards for the exchange of information between ports and airports of two or more countries.

The project builds on the existing data pipeline model and buy-ship-pay reference data model to create a white paper and guidance material for the exchange of data through digital corridors.

The following activities were completed to prepare for the creation of this white paper:

- ✓ Studied the need of digital corridors for air/sea/land modes of transport with focus on regulatory authorities
- ✓ Studied the reusability of information between origin and destination stakeholders

- ✓ Studied the existing similar initiatives
- ✓ Studied the potential of integrating with single windows
- ✓ Determined other factors that delay cargo processing at air/sea/land borders that could be addressed through the corridors
- ✓ Identified the common data elements
- ✓ Identified key steps in setting up the air/sea/land corridors
- ✓ Identified the possible challenges in setting up digital corridors
- ✓ Identified technologies that can facilitate the creation of digital corridors

2. Background

Existing UN/CEFACT research shows that the freight transport ecosystem extends far beyond the cross-border movement of consignments. In addition to the complexity of the supply chains, as suppliers change and markets evolve, the fundamental expectations of the sellers, buyers, consignors and consignees are changing. A significant cause of this change is the application of e-commerce norms to all cargo consignments. The common foundation of these expectations is consistency. Consignors, and especially consignees, want the functions that move the consignments to be consistent so that they can better plan inventory levels, cash positions and revenue streams.

In a study performed for a major airline, the findings of which are applicable to all modes of freight transport, the following expectations were universally mentioned, in rank order of importance:

- **Speed:** Usually, 48 to 72 hours' time in transit, end-to-end, is expected when air cargo is the chosen mode. A consistent repeatable speed of transit is expected.
- **Transparency**: Throughout the entire transportation cycle, there must be real-time visibility of information on the status, condition and location of the consignment.
- **Quality:** No claims or damage to any consignment should be made; the cargo should be delivered as promised.
- **Compliance:** Service providers have environmental and economic commitments. This is increasingly a key decision-making element.

Only when the above criteria are met does price factor into the decision-making process:

- **Price:** The price should be competitive with other service providers or gateways offering similar services or products. The transport company management must be aware of these new pricing dynamics.

These expectations challenge the capabilities and capacity of legacy, non-digital processes.

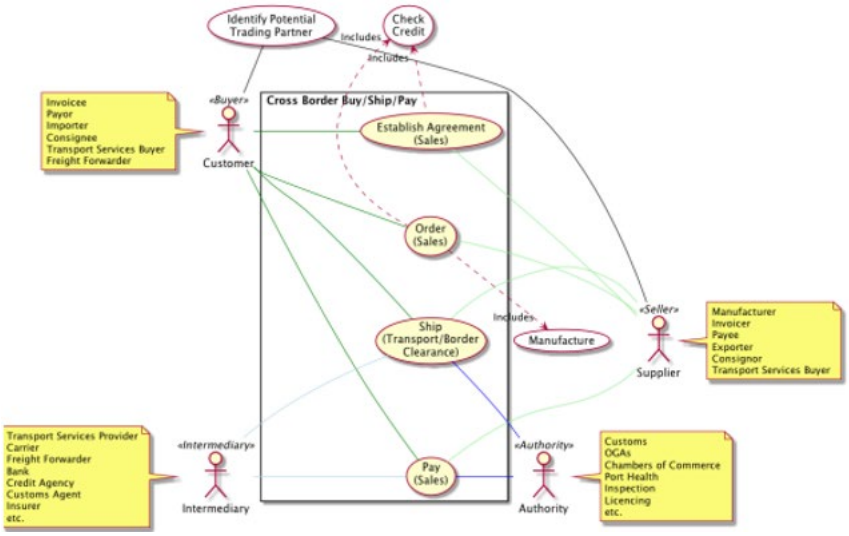
3. What is a digital corridor

A digital corridor is an electronic platform that connects multiple trade ecosystems (e.g. air/ocean/land community systems or single window systems) to share the status of business activities and relevant cargo information.

The International Monetary Fund (IMF) and the Organisation for Economic Co-operation and Development (OECD) define digital trade as 'all cross-border transactions that are either digitally

ordered (i.e. cross-border e-commerce), digitally facilitated (platforms), or digitally delivered".[1] Cargo community systems and digital corridors provide a framework within which the processes and parties engaged in transactions associated with the cross-border movements of consignments can function. As the following diagram illustrates, there are numerous information flows; many of which are composed of the same information. Cargo community systems, as explained below, reduce, if not eliminate, repetitive data entry, which reduces errors, speeds up the movement of the consignments and ensures that, from a regulatory perspective, the security of the borders is maintained and the applicable duties and taxes are collected in a transparent manner.

3.1. Buy-Ship-Pay Reference Data Model



Cargo community systems are encrypted platforms that facilitate direct interface between all the public and private stakeholders involved in creating, managing and handling the flow of goods. Wholesale changes to legacy systems are not required. Instead, through a series of application programming interfaces (APIs) and electronic data interchange (EDI) messages, information can be entered into the consignment ledgers through the digital platform.

The digital corridor is established when a community platform or a single window system at one location gets connected with a community platform or a single window system at another location to exchange relevant data. When community platforms are not available at a certain location, direct interface with individual stakeholders can be established and details can be made available to the partner at the cross-border destination.

A digital corridor enables the electronic exchange of information or e-documents between economic operators and/or government authorities, allowing them to fulfil business and/or regulatory requirements. It has the following characteristics:

- The platform has a single point of data entry for the exchange of information between regulatory agencies and trading participants.

[1] International Monetary Fund (IMF) and Organisation for Economic Co-operation and Development (OECD) (2018). "Towards a Handbook on Measuring Digital Trade: Status Update", discussion paper prepared for the Thirty-First Meeting of the IMF Committee on Balance of Payments Statistics in Washington D.C. (24-26 October).

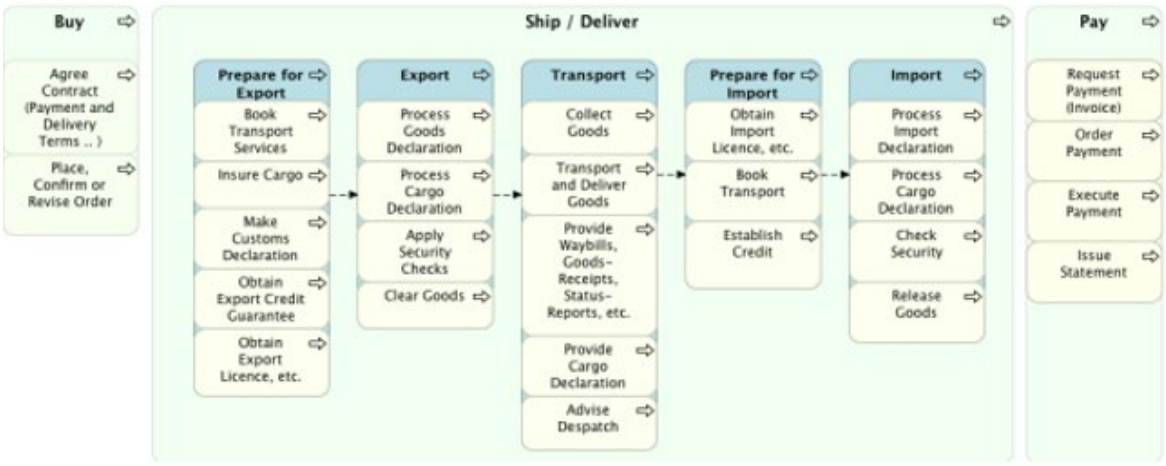
- Business activities are simpler, faster and more efficient with reduced risk of errors and data duplication.
- The seamless exchange of details allows for greater efficiency and transparency in processes.

A digital freight corridor between the two countries is very important in any trade. It enhances consignment visibility and optimizes the flow of cargo data from the point of origin to the destination and vice versa. Collaboratively established digital corridors facilitate the flow of information within the stakeholder chain and optimize cargo visibility across the stakeholder network. These digital data corridors can evolve from connecting stakeholders within one cargo network, like an airport/port community in one country, to connecting with the airport/port community in another country.

4. Need for cross-border multimodal digital corridors

A buyer of a product in Europe can order an item from a seller in Africa and have comfort that the right product will be delivered in the expected condition, at the right time, to the right address. The work of UN/CEFACT in developing the refence data models (RDM) illustrates the complexity of the transactions integral to cross-border trade. The following diagram of the buy-ship-pay model displays the many processes and transactions associated with cross-border trade.

4.1. Buy-Ship-Pay Reference Data Model[2] processes and transactions



Thus, the management of cross-border exchange of goods is challenging. To comply with import, export and transit-related regulatory requirements, companies involved in international trade must regularly prepare and submit large volumes of information and documents to government authorities. The information and documentation often must be submitted to several different agencies and various regulatory authorities, each with their own specific (manual or automated) systems and paper forms. The extensive requirements, together with their associated compliance costs, can constitute a serious burden to both governments and the business community. It is also

[2] UN/CEFACT, "Buy-Ship-Pay Reference Data Model", 13 August 2019, Figure 2, Page 8

a serious barrier to the development of international trade. There is a desire to address the following issues:

- Reduce and preferably eliminate extensive, usually duplicative paperwork which governs the export and clearance of consignments, and which can delay consignment processing. By reducing duplicative data and information entries, errors will be reduced, decreasing the workload of border agencies and clearing agents and reducing delays in the flow of the consignments.
- Strengthen the visibility (transparency) of consignments at all stages of the supply chain. Improved visibility can serve two needs: (1) to reduce the entry of illegal products, which is a threat to the safety and security of the entire chain; (2) to provide more timely information, which allows for better planning of staff and other resources, which in turn reduces costs, speeds up processing and attracts even more business to the locations that provide this level of service.
- Increase the ability of government agencies to collect the correct duties and taxes. Border agencies need to be able to easily identify when the declared value of the consignment is less than the actual value of the product.
- Improve compliance with export and import processes for customs agencies and traders to reduce unexpected delays at national borders.
- Eliminate consignment processing related to determining the real country of origin due to a lack of a verified certificate of origin.

The implementation of digital corridors aims to address all these issues.

5. How to go about implementing a digital corridor

Now that the need for a digital corridor is established, we need to deliberate upon how to set up a digital corridor. While clear guidelines for setting up a digital corridor will be the subject of another white paper, in this section we will examine how cross-border digital corridors might be set up.

As defined earlier in the paper, the digital corridors are electronic medium to share data securely and seamlessly between two or multiple entities. The following are the types of digital corridors:

- **Airport to airport**: a digital corridor established to exchange air cargo information through community platforms deployed at two different airports.
- **Port to port**: a digital corridor to exchange sea freight information through community platforms deployed at two seaports.
- **Regulatory corridor**: a digital corridor established to exchange and verify details such as customs declarations submitted at the origin airport; export/import licences of the shipper/ consignee; or licences for specific products between the two customs systems or single window systems.

The aviation and maritime corridors focus on the basic consignment information. The exchange of consignment information allows operational partners to better plan their operations, assign staff

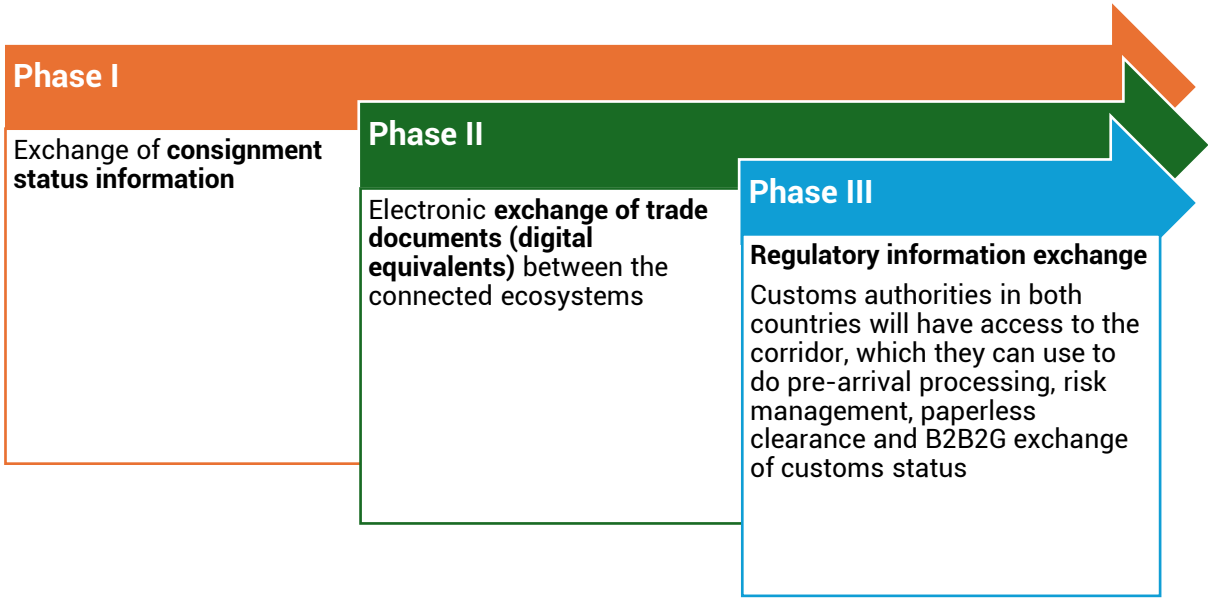
and physical assets appropriately, and reduce 'surprises', such as consignments which require special handling that might delay other consignments.

The regulatory corridor adds the border agencies to the exchange of information. The critical processes related to arrival alerts, selection of consignments for additional inspection, and the efficient processing of all consignments increases the speed of consignments moving through supply chains.

Phases in establishing a digital corridor

Digital corridors can be rolled out in different phases. The easiest place to start is with the exchange the consignment status information between two entities such as the origin and destination ports or airports. This can usually be achieved by exchanging EDI messages between these parties or through APIs developed between the community systems at these airports or ports. This phase doesn't necessitate any regulatory changes. However, it illuminates the entire cross-border supply chain, as the participants of the community systems at both ends now get extended cross-border visibility.

Digital corridor establishment process



The second phase focuses on consignment information being collected and shared among the operational parties. This phase ensures that critical and appropriate information is available to all the parties along the route of each consignment. By reducing data entry delays and errors, the speed of consignment movement is increased. Increased speed is important on many levels. Businesses can improve their financial position by reducing the order-to-cash cycle. This improves their resiliency and sustainability, especially in the face of internal and external disruptions. On a State level, increased transactions, especially international, are reflected in labour growth, wage improvements and critical revenues, which can support related programs. A State which supports and demonstrates high-speed consignment transactions at its border becomes a more attractive destination for foreign direct investment, which in turn leads to new or expanded business formation with all its attendant benefits.

The third phase involves the addition of border agencies to the mix of linked parties. By accessing applicable consignment status information and trade documents, border agencies can better police their borders, identify consignments that require additional inspection, and rapidly clear consignments that comply with all the applicable rules and regulations. This phase is more transformational in nature and might involve changes in laws if the data from the digital corridor is accepted for regulatory clearances.

Implementing digital corridors requires a collaborative and coordinated effort of all parties involved. As previously described, the benefits associated with implementing a cargo community system and digital corridor are maximized when all parties are participants and are exchanging all appropriate data and information.

As previously noted, the implementation process is best achieved through a combination of an active top-down mandate and a collaborative bottom-up set of tasks. Regardless of whether the implementation occurs within a public agency or a private enterprise, issues will arise which will require a collaborative effort to address, analyse and develop an acceptable solution for.

The proposed methodology of implementing a digital corridor is as follows:

1. Identify the scope of digital corridor (phase 1, phase 2 or phase 3),
2. Sign a memorandum of understanding between the anchor stakeholders like the ports or airports or customs agencies,
3. Educate the participating stakeholders on the concept of digital corridors,
4. Identify a technology partner to deliver the digital corridor,
5. Identify pilot members from a cross section of stakeholders (e.g. small, large and medium forwarders, airlines, shipping lines, trucking companies, chambers of commerce, etc.),
6. Train the stakeholders on the use of the technology (portal, mobile app etc.),
7. Execute pilot transactions,
8. Fine tune the technology solution based on pilot transactions,
9. Identify a target date for industry-wide (port/airport/country wide) roll out,
10. Provide online training tools for the stakeholders, and
11. Launch the digital corridor.

While the scope of each digital corridor will be identified bilaterally or multilaterally, here are the documents and statuses that can potentially be exchanged through digital corridors:

From origin to destination:

- Invoice, packing list, shipper’s letter of instructions and air waybill;
- IE (importer/exporter) registration;

- Consignment announced for the airport by submitting advance consignment information (ASI);
- Shipper's declarations and dangerous goods declarations;
- Certificate of origin (CoO);
- Freight-on-hand status: The consignment is on hand on this date at this location, pending "ready for carriage" determination;
- Customs declaration and customs clearance (export permission);
- Receive-from-shipper status: This status is updated when consignment is physically received from the shipper or the shipper's agent. This indicates that the consignment is considered by the carrier as ready for carriage on the specified date at the specified location;
- Consignment manifestation status: The consignment has been manifested for a specified flight/voyage on a scheduled date for transport between the two locations; and
- Consignment departed status - This status is updated when consignment has physically departed from a location on the scheduled date on a flight/voyage, for transportation to the arrival location.

From the destination to origin

- Arrival status: This status is updated upon arrival of a consignment on a scheduled flight/voyage at this location;
- Consignment received from flight/voyage/ship status: The status indicates that the consignment has been physically received from a specific flight/voyage or surface transport;
- Consignment notified to consignee status: This status indicates the consignee or the consignee's agent has been notified about the arrival of consignment. The details such as date of arrival and the location of consignment is shared;
- Document delivered status– The status is updated when the arrival documentation is physically delivered to the consignee or the consignee's agent;
- Customs clearance status - The consignment indicates that the consignment has been cleared by the customs authorities;
- Consignment delivered status – The status is update when a consignment is delivered to the consignee or consignee's agent; and
- Proof of delivery.

Potential technologies involved in setting up digital corridors

Digital corridors involve connecting two airport or port communities or customs administrations. The basic level data exchange can happen with APIs or (UN/CEFACT, IATA, SMDG etc.) EDI

messages. Other technologies, like iSHARE[3], have also been used in implementing digital corridors. Attempts have been made to implement digital corridors using Microsoft's Corda blockchain infrastructure.

Essentially any technology that supports verifiable credentials, data encryptions, immutability (such as blockchain) are suitable for implementing digital corridors.

6. Benefits of a digital corridor

The following are the primary benefits associated with an electronic structure that leverages single windows and combines cargo community systems and digital corridors[4]:

For trade

- Reduction in the time and cost of complying with cross-border regulatory processes
- Simplification of regulatory procedures
- Reduction in (or elimination of) paperwork and the need to travel to the various PGAs
- Increased predictability and transparency
- Automation of regulatory processes in line with other business processes
- Electronic payment facilities
- Online, real-time monitoring of consignment status

For government

- Reduction in cost
- Enhanced efficiency of regulatory processes
- Elimination of duplicated processes between agencies
- Higher compliance levels with government regulations
- Enhanced traceability and statistics
- More accurate and often increased revenue yield for customs
- Improved government services (and the perception thereof)
- Greater economic competitiveness
- Increased transparency
- Improvement in world rankings for business competitiveness and efficiency (e.g. World Bank Trading Across Borders and Logistics Performance Index)
- Compliance with WTO TFA commitments

Achieving these benefits contributes to the expansion of cross-border trade, which in turn benefits the world's population.

[3] https://ishare.eu

[4] United Nations Conference on Trade and Development (UNCTAD), Roadmap for Building a Trade Single Window, *Trade and Transport Facilitation Series No. 21*, (19 December 2023), Pg. 4, available at https://unctad.org/system/files/official-document/dtlasycuda2023d2_en.pdf.

7. Challenges

Digitalization is not free. There are financial, operational and human resources costs. The scale of these costs will vary according to the scale of the conversion and the difficulty of changing from a non- or semi-digital operation. While the impetus of the digitalization project must come from senior management, the actual implementation is best achieved through a bottom-up process. The following table identifies stakeholder challenges and costs for public agencies and private enterprises.

7.1. Stakeholder digitalization challenges, concerns and costs

Challenge and cost	Public agencies	Private stakeholders
Protect intellectual property	Protection of user information and data is very important.	This is a significant consideration – loss of information control can adversely affect revenue and profits.
Protect consignment information	Access to consignment information should be restricted to border control purposes and collection of duties and taxes. Limit access to appropriate agencies.	Protect consignment information from competitors and other members of the supply chain who do not need access.
Protect consignment security	Minimize/eliminate alterations to original consignment.	Protect consignments from theft and/or introduction of illegal substances.
Data sharing	Protection of user information and data is very important.	Balance the protection of commercially sensitive information with improvements in consignment flow to accelerate collection of revenues and reduce costs.
Perceived benefits and incentives	Trade-off between higher costs and more accurate collections of duties and taxes.	Trade-off between higher costs and more reliable movement of cross-border consignments and levied duties and taxes.
Required investment	Costs to replace existing legacy systems with new computer systems versus creating digital apps to link the legacy system to a digital platform. Acquisition of new system and training. Cost-benefit analysis, budgeting process and negotiation of final amounts.	Costs to replace existing legacy systems with new computer systems versus creating apps to link legacy system to digital platform. Acquisition of new system and training. Identify revenue enhancement/cost reduction to justify funding.
Compatibility with existing systems	Decide whether to create a new system or to employ digital applications to link the legacy system to the new digital platform.	Decide whether to create new system or to employ digital apps to link the legacy system to a new digital platform.

	Level of support will be determined by new system vs. digital app decision.	Level of support will be determined by new system vs. digital app decision.
Compatibility with organizational structure	Ensure that all changes are compatible with existing legislation. Any changes to governing legislation, rules and procedures can delay implementation.	Form implementation team which brings together all key departments to ensure transition is comprehensive.

Identifying and quantifying each challenge and determining the appropriate actions to address each challenge should occur at the beginning of the project. The project team should be prepared to quickly alter their approach when new challenges and opportunities emerge. It is during a mid-course correction that senior leadership can ensure that the overall goals are still in focus.

8. Constraints and strategies to mitigate constraints

The following issues reflect concerns about data control, access and protection in a digital corridor:

- **Stakeholders may not be connected through a community network**: Digital corridors connect two community networks to share information. When the stakeholders at one of the locations are not connected through a community network, it may hinder the establishment of a digital corridor.
- **Data security concerns of stakeholders**: Storing data and important files on external service providers always poses risks. There are instances where a digital front end is backed up by a non-encrypted paper-based operation.
- **Downtime**: Cloud computing systems are internet based and service outages are always a possibility and can occur for any reason.
- **Vulnerability to attack**: Every component is online, which creates potential for cyber-attack vulnerabilities. Numerous government agencies have limited data security protocols and thus revert to the use of paper-based systems. This a security situation which should be permitted.
- **Limited control and flexibility**: Customers retain control of their applications, data and services, but may not have the same level of control over their back-end infrastructure.

When implementing a digital corridor, these concerns must be clearly addressed.

There are several strategies which can be employed to address each of these concerns. The process of addressing the concerns should be conducted through candid, collaborative dialogue with each stakeholder.

- **Enforcing the Global Data Protection Rule (GDPR)** controls the vulnerability of data hosted in the cloud. Data security is optimally ensured with an effective user-access management system in place.

- **Multi-region hosting** with automated handover to ensure business continuity can minimize the impact of downtime of cloud platforms. The exposure can be further reduced by considering a dedicated network connection with the cloud service provider. Understanding that tier 1 cloud providers generally guarantee 'uptimes' of over 99% can reduce concerns about the digital conversion of paper-based systems.
- **Making security a core value** of all IT operations can help reduce vulnerabilities to cyberattacks, in addition to regularly reviewing security policies and procedures, proactively classifying information, and applying strict access controls. Reviewing security compliance on a set schedule should be part of the system operation.
- **Understanding each parties' responsibilities**, including the cloud vendor in the shared responsibility model can reduce the chance of omission or error and increase functional flexibility.

An overarching strategy is to implement a dynamic risk management structure. The process of identifying, assessing, creating a plan (both proactive and reactive), and implementing the corrective plan has the maximum benefit when everyone in the organization is actively engaged. There are many models and templates for risk management programs. Selecting the appropriate one depends on the characteristics of the organization and form of activity.

9. Industry and government initiatives

The following initiatives have the same goals as those for cross-border digital corridors:

- ✓ Government corridors such as India-BeNeLux corridor;
- ✓ Industry associations such as the International Port Community Systems Association's (IPSCA) Network of Trusted Networks;
- ✓ Private initiatives such as the Mumbai Airport – Amsterdam Airport Schiphol Digital Air Corridor and the IATA initiative One Record.

10. Legal framework – recommendations

The unencumbered flow of digitized information is the key to implementing digital corridors. Addressing the issues surrounding these flows requires the careful adoption of policies and rules to protect the data and information.

In many cases the exchange of consignment information is based on non-digital legacy systems[5]. A modern digital trade ecosystem fit for the 21st century requires national laws to recognize all trade documents in digital form, and legal systems to be aligned to enable digital transformation to move seamlessly across borders and between stakeholders – buyers, sellers, financiers, insurers, consignors, logistics and customs[6]. While some countries allow data to flow easily beyond their

[5] Nguyen, H., Trade digitization on a global scale: How far are we?, WCO News, 24 February 2022. Available at https://mag.wcoomd.org/magazine/wco-news-97-issue-1-2022/trade-digitization/.

[6] ICC, "G7 Creating a Modern Digital Trade Ecosystem: Cutting the Cost and Complexity of Trade: Reforming laws and harmonising legal frameworks" (2021). Available at https://www.iccgermany.de/wp-content/uploads/2021/10/Creating-a-Modern-Digital-Trade-Ecosystem-G7.pdf (accessed 11 June 2024).

borders with the appropriate legal protections, many more nations have enacted barriers to such data transfers. The barriers have made international data transfers more expensive, time-consuming and in some instances illegal.[7] This latter environment, known as "data localization", mandates local data-residency requirements that confine data within a country's borders.[8] Such policies are rapidly spreading globally. They are measurably reducing trade, slowing productivity and increasing prices for affected industries and consumers.

As part of encouraging regional and global trade, policymakers should put the concept of "digital interoperability" at the centre of their global digital economic strategy. At the most fundamental level, interoperability is the ability for firms to transfer and utilize data and other information across applications, systems, services and jurisdictions.[9] This goal acknowledges that countries have differing legal, political and social values and systems and there is no one law for any specific data-related issue.[10] Countries can then enact laws to address data privacy, cybersecurity and other issues which provides a similar level of protection or similarly addresses a shared objective, even if their specific legal and regulatory frameworks differ.[11]

The regulation of e-trade should be based on contract and financial laws pertaining to electronic documentation and signatures, e-payments, consumer protection, intellectual property, cybersecurity, personal privacy and data protection.[12] A proactive, supportive regulatory framework is necessary for vibrant digital markets, and the subsequent expansion of digital trade.[13]

The following are some recommendations regarding policy in areas such as data flows, global digital trade and data governance:

Global data governance: Policymakers should provide multiple mechanisms to transfer propriety data, encourage firms to improve consumer trust through greater transparency about how they manage data, support the development of global data-related standards, and provide more assistance to developing countries to help grow the digital economy policy.

Digital free trade: Policymakers should support rules that protect data flows, prohibit data localization, and only allow narrow exceptions to these provisions for e-commerce negotiations at the World Trade Organization (WTO). Policymakers should also create new tools to enact retaliatory measures against countries and businesses that enact or employ data localization and other digital protectionist rules. Trade negotiators should develop transparency and good regulatory

---

[7] Cory, N. and L. Dascoli, How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, and How to Address Them. Information Technology and Innovation Foundation (ITIF), 19 July 2021. Available at https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/ (accessed 11 June 2024).

[8] Cory, N, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Information Technology and Innovation Foundation (ITIF), 1 May 2017. Available at https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost/ (accessed 11 June 2024).

[9] Gasser, U., Interoperability in the digital ecosystem, *SSRN Electronic Journal*, 6 July 2015.

[10] Cory, N. and Dascoli, L. (2021).

[11] Ibid.

[12] Jaller, L. D., Gaillard, S., and Molinuevo, M., *The regulation of digital trade: Key policies and international trends*, Washington D.C.: World Bank Group (4 January 2020).

[13] Ibid.

practice provisions to ensure opaque regulatory rulemaking can't be used to enact barriers to data flows and digital trade.[14]

The following are some more specific recommendations for consideration by policymakers:

- Focus on the fundamental concept of interoperability between different regulatory systems.
- Pursue new cooperative digital economy agreements and mechanisms, such as those negotiated by Australia, Chile, New Zealand and Singapore.
- Employ the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR), a global model for data governance, by opening it up to non-APEC members.
- Support efforts by like-minded, value-sharing countries working together to develop a "Geneva Convention for Data" that establishes common principles, processes and safeguards to govern government access data.
- Develop a targeted strategy to support the adoption of financial oversight frameworks that focus on regulatory access to data rather than the location of data storage.
- Improve existing, and build new, mechanisms to improve cross-border requests for data related to law enforcement investigations, such as the CLOUD (Clarifying Lawful Overseas Use of Data) Act agreements and the updated mutual legal assistance treaties (MLATs) to provide timely assistance.[15]

11. Conclusions and recommendations

The need to digitize the cross-border processes that facilitate global trade reflects the volume and complexity of consignment flows. Sellers, buyers, consignors and consignees expect the continuous visibility of their consignments and the consistent and transparent application of border and commercial procedures. Whether the consignment moves by air, marine, rail or road haulage, these fundamental expectations are constant. As initially proposed in United Nations Recommendation No. 33, and confirmed in research by UN/CEFACT, digital solutions are recognized as essential to the efficient flow of global trade.

Industry initiatives including Cargo iQ, One Record and the IPCSA Trusted Network of Networks program are emblematic of the commitment to digitize elements. Projects such as the joint United States-Mexico clearance system, the Mumbai-Amsterdam Digital Air Corridor linking two airport cargo communities, and the commitment of Canada to digitize supply chains are examples of government commitments to the digitization of cross-border trade facilitation.

The technical implementation challenges and legal issues that must be addressed should not be considered insurmountable barriers. Acknowledging their existence, quantifying them and thoughtfully and purposefully addressing each issue will result in an environment where non-tariff

[14] Cory, N. and Dascoli, L. (2021).

[15] Office of the U.S. Attorney General, Notice of the United States Justice Department (A.G. Order No. 5453–2022) in the Federal Register, 6 July 2022, Clarifying Lawful Overseas Use of Data Act. Available at https://www.federalregister.gov/documents/2022/07/06/2022-14320/office-of-the-attorney-general-clarifying-lawful-overseas-use-of-data-act-attorney-general#:~:text=1213%E2%80%9325%20(2018)%2C,governing%20access%20by%20the%20foreign.

barriers are reduced, if not eliminated, and overall trade costs impacting global trade flows are reduced.

Based on this research, the project team proposes the following series of recommendations for regulators to consider and incorporate as they adopt digital systems and processes to facilitate cross-border trade flows. The critical value of the cargo community systems and digital corridors is to create an environment in which the consignment information is collected and made available as needed in a secure environment. By continuously collecting consignment information, the security of the system there is a significant reduction in the possibility of consignment tampering or theft. These recommendations focus on consignment status and data.

- **Cargo community systems**
  Cargo community systems are the key foundational element for implementing digital corridors. These systems bring together all the partners involved in cross-border trade. The ability to employ APIs and EDI messaging reduces the costs of joining. The assembly of consignment information in blockchain-based ledgers ensure unaltered entries. The encryption of digital platforms is a critical characteristic that protects valuable commercial and government information and data from external hackers. Mandating the implementation of these platforms should be a part of the trade policy of each nation.

- **Digital corridors**
  While a single isolated cargo community system provides a wide range of benefits to the members, linking cargo community systems via digital corridors magnifies those benefits. Sharing consignment information, entered at origin and employed at destination, is superior to re-entering the same information at subsequent steps. Realizing the full potential of a digital corridor will require close collaboration between the customs and other border agencies of the two countries and by implementing laws based on the Clarifying Lawful Overseas Use of Data Act structure.

- **Address risks**
  Addressing the many risks associated with cross-border trade facilitation requires a genuine commitment to collaboration among all stakeholders. Implementing well-established processes to identify, quantify, assess, develop and implement risk management actions is the optimal way to minimize risks across all supply chains. The beginning of this process is to acknowledge the challenges faced by public agencies and private enterprises. A thoughtful assessment of those challenges will provide the foundation for creating and implementing successful solutions.

- **Establish a data-focused legal framework**
  The free flow of information in digital format must be embraced in order achieve the full benefits of digitization of trade and the operation of digital corridors. Strategies such as the GDPR, multi-host structures, and very high levels of encryption exist and should be employed in drafting policies and formulating appropriate procedures. This legal framework must incorporate policies based on the Clarifying Lawful Overseas Use of Data Act structure.

- **Incorporate UN/CEFACT reference data models**
  This body of research provides the best foundation on which to devise and construct policies and procedures to facilitate cross-border trade. The RDMs clearly identify consignment information which is common and unchanged through a supply chain. These models also identify the parties and the types of transactions that are essential elements of supply chain operations. Reusing consignment information is the best way to reduce errors, improve efficiencies and ensure that illegal activities are quickly identified and stopped. By applying this information, the policies and procedures can be quickly and, more importantly, uniformly established across the world.

The evolution of global trade is challenging the capacity of legacy, non-digitized system to cope. Expanding upon Recommendation No. 33's emphasis on a single window system — aimed at streamlining the submission and processing of consignment information — digital corridors are being deployed. These corridors connect cargo community systems, establishing digital nodes and links that enable efficient gathering and dissemination of consignment data, as well as tracking the status of each shipment. The deployment of digital corridors is just beginning. There is much work ahead to broaden this effort.