Ensuring business continuity in the face of trade disruptions

Background

The COVID-19 pandemic has demonstrated the interconnection of modern economies and the importance of having customs certainty and efficiency and flexible business processes to global supply chains. Over the last three years, supply chains have been impacted by the pandemic, port congestion, demand-side shocks, and cyber-attacks.

These challenges highlight the need for businesses to proactively take steps to mitigate risks of possible disruptions. These steps could include creating contingencies to enable firms to, for example, serve their customers and remain competitive in the case of supply chain shocks. The need to respond to multiple cascading supply chain challenges supports the necessity of maintaining operational resiliency through continuous process improvements. By investing in a strong foundation of processes, systems, and people business can prepare to face future trade disruptions.

Following the PSCG paper on “Business Resumption: Lessons Learned During the COVID-19 Pandemic – Best Practices for Customs”, the group was asked to develop a follow-up paper that further elaborates on the measures that increase resilience and help ensure business continuity in light of trade disruptions – and how Customs authorities can contribute to increased resilience. These practices include:

1. Identifying Risks to Business Continuity

The COVID-19 pandemic exposed a general lack of preparedness by businesses to predict and react to supply chain risks. Given this lesson, there is an opportunity for businesses to identify and prepare for future risks.

What are some of those risks that could disrupt business continuity in the future?

Examples of external threats that could drastically limit a business’ and/or Customs’ operations include:

a) Cyber attacks
b) Natural disasters
c) New pandemics
d) Infrastructure challenges
e) Strikes (e.g., commercial and public transportation, oil refineries)
f) Conflict/war

While many customs authorities have begun to prepare for addressing these future threats, business must also plan and invest, particularly providers of vital goods and services (e.g., IT services, logistics), to operate during a crisis and to support post-crisis recovery.

For example, a company could be going through a cyber attack and their globally automated IT system is taken out of service. In such instances, what support can be provided by Customs authorities? It is not always possible to revert to manual processes. As a result, in this example, how could the goods pending customs clearance be handled or cleared in a way that does not further contribute to the disruption or increase cost and risk for the importing country or the trade stakeholders?

Today, supply chains are dependent on the timely flow of data and documentation, and in times of crisis, these flows could be disrupted. As a result, how could the movement of goods be facilitated in such instances?

2. Managing Risk Effectively

For business, it is critical that customs authorities provide as much consistency as possible during periods of service disruption. When many standard processes and systems within the supply chain are unable to operate during a disruption, there need to be emergency fallbacks procedures in place to maintain the flow of goods required during and after the crisis.

For many years, the PSCG has advocated for an effective implementation of existing tools and instruments to facilitate trade; however, effective implementation is particularly important when it comes to those instruments that include sections on crisis preparedness and management, such as:

- The SAFE Framework of Standards (SAFE FoS)
- The Framework of Standards for Cross-Border E-Commerce
- The Trade Recovery Guidelines
- The Coordinated Border Management Compendium
- The Risk Management Compendium
- Recommendations for Customs in fragile and conflict-affected situations

The impact of disruptions across the supply chain can be lessened through (further) streamlining of customs and security procedures. In addition, taking these actions can provide all stakeholders with better visibility and thus certainty about how processes will be handled– which is invaluable in times of crisis.

We believe that essential elements of private-public sector activity in the customs and larger trade environment include:

- Plan for disruption: think through the impact of the unexpected, while developing and capturing the best possible response mechanisms;
- Practice those responses: assess that essential elements are in place and test them to determine if they will accomplish the desired outcome; and
- Engage Partner Government Agencies: all agencies operating at the border must be involved in the planning and response testing to examine the outcomes and the ability to apply flexibility to their standard requirements.

Best practices for strengthening resilience could incorporate:

- Scenario planning to identify the extent of disruptions.
- Tabletop exercises held by government and private sector organizations to test and assess protocols.

Build on the WCO Guidelines on disaster management and supply chain continuity (June 2021) for capacity-building and explore the inclusion of disruptions to business in the Guidelines – as well as a thoughtful review and update mechanism.

One practical example for increasing crisis preparedness and for successful public and private sector cooperation is the development of a new set of standard operating procedures (SOPs) in Madagascar to fast-track foreign emergency relief as part of the WCO COVID-19 project, funded by the government in Japan, which was done in cooperation with the Global Alliance for Trade Facilitation and the National Center for Disaster Preparedness at Columbia University. In 2022, two workshops were organized in Antananarivo to assist the National Office for Disaster and Risk Management (BNGRC), Madagascar Customs and other stakeholders in testing these procedures and enhancing their preparedness in facing the COVID-19 pandemic and other emergency situations, such as the cyclone season (more details here).

3. Building a Crisis Management and Preparedness Framework – Example

A crisis management and preparedness framework could include:

Crisis Communication

- Internal
- External (Government, Customers, Suppliers, Third Party Providers, etc.)
- People – safety including known locations of employees, having a call to action in place, continuous system access, locations known, call to action, system access, training, equipment
- Government Agencies – AEO notification, IS Security, notifications, downtime procedures, flexibility
- Systems notifications
- Processes aligned with outside groups, such as NGOs

Business Continuity Plan (BCP) Operational Template

- Assess status (Reports, Prioritization)
- Record activities offline in a consistently planned format
- Data and document or documentation redundancy
- Validations
- Declarations or downtime procedures
- Delivery
- Resources needed
- Duty and Tax Management
- Finance
- Compliance considerations - Sanctions, Embargos, Screening, Restricted Commodities, Data Governance, Policies, Third Parties
- Resources – Crisis Management Teams, alternative tracking, SOPs, management, service providers, Country level instructions, milestone Systems – alternatives, back-ups, third-party systems, Electronic Data Interchange, email, etc. Best Practices – workshops, aligned plans
- Customer instructions and SOPs

- Authorizations
- Milestones
- Safeguard planning
- Visibility
- Documents
- Government Agencies
- Service Providers
- Third-party systems`
- Preparatory work

A Business Continuity Plan captures lessons learned and decisions made from the planning, practice, and preparation. A BCP will allow all parties to understand who is leading and engaged on which actions.

BCPs should be reviewed annually or after a significant disruption has occurred and a post-mortem is conducted. BCPs should include a change history as is typical of internal corporate compliance policies. A change history or summary should list out sections and scope of changes made, dates, and version history for awareness purposes.

We encourage governments to engage with and invite the private sector to participate in crisis preparedness planning and exercises, where the scope and frequency of involvement is to be determined.