DATA: ENSURING QUALITY, SECURITY & PRIVACY
Part VIII

Data: Ensuring Quality, Security & Privacy

This Part provides an executive overview of data sources, interchange of data, data quality, issues of privacy and commercial secrecy, and data protection in a Single Window environment.
Contents

1. INTRODUCTION .......................................................................................................................... 3
   1.1 ABOUT PART VII .................................................................................................................. 3
   1.2 RELATED TOPICS ................................................................................................................. 3

2. TRUSTING THE SOURCE OF DATA ......................................................................................... 4

3. ENSURING DATA QUALITY ..................................................................................................... 7
   3.1 USE OF INTERNATIONAL STANDARD CODES ...................................................................... 7
   3.2 ACCEPTABLE AND UNACCEPTABLE TERMS ......................................................................... 8
   3.3 REGISTRATION AND AUTHENTICATION OF USERS ............................................................. 9
   3.4 SETTING UP A DECLARANT GOVERNANCE FRAMEWORK .................................................... 10
   3.5 TRAINING AND COMPLIANCE IMPROVEMENT .................................................................. 10

4. ACCEPTING THE LODGED DATA .............................................................................................. 13
   4.1 DATA LODGED BY BUSINESSES ....................................................................................... 13
   4.2 DATA SHARED BETWEEN GOVERNMENT AGENCIES ......................................................... 13
   4.3 IDENTIFICATION, AUTHENTICATION AND AUTHORIZATION ........................................... 14
   4.4 GLOBALLY NETWORKED CUSTOMS ..................................................................................... 17
   4.5 DATA EXCHANGE – PUSH VS PULL ................................................................................... 18

5. THE LEGITIMATE USE AND SHARING OF DATA .................................................................... 18
   5.1 RECORD-KEEPING OBLIGATION ......................................................................................... 18
   5.2 TECHNOLOGICAL CHALLENGES: CLOUD COMPUTING ..................................................... 19
   5.3 DATA BACK-UP, DATA ARCHIVING AND DATA RETENTION ............................................. 20
   5.4 DESTRUCTION OF DATA ..................................................................................................... 21

6. DATA SECURITY AND PRESERVATION .................................................................................... 22
   6.1 DOCUMENTED SECURITY POLICY ..................................................................................... 22
   6.2 CLASSIFYING DATA ASSETS .............................................................................................. 22
   6.3 FOLLOWING A RISK MANAGEMENT APPROACH ................................................................ 22
   6.4 DATA SECURITY ASSURANCE PROCESS ............................................................................ 22
   6.5 INFORMED USER BASE ...................................................................................................... 23
   6.6 ENSURING BUSINESS CONTINUITY .................................................................................. 23
   6.7 PREVENTING CYBER ATTACK ............................................................................................ 23
   6.8 USING DIGITAL ASSETS IN FORMAL LEGAL PROCEEDINGS ............................................. 23
   6.9 COMMON VULNERABILITIES ............................................................................................... 24
1. Introduction

Data is the lifeblood of the international supply chain. The flow of trade and transport data occurs alongside the physical flow of goods and means of transport. Information is exchanged between the participants in the supply chain – namely, traders, transporters, intermediaries and regulatory agencies. In a digital and connected world, the data flow consists of information exchanged between the supply chain participants in the form of documents, fragments (or components) of documents, and real-time data streams.

Stakeholders in the supply chain seek to provide and receive the necessary information with a view to minimizing risk and uncertainty to the free flow of goods, thereby preserving value represented by those goods. This is accomplished by carrying out risk assessments as early as possible in the global supply chain, preferably at the time of the origination of the consignment. All of this is premised on the capability of the supply chain participants to: (i) trust the source of data; (ii) be assured of the quality of data provided and received; and (iii) have confidence that the data that is exchanged will be handled safely and protected from unauthorized access.

Entities participating in the Single Window environment share data extensively with each other. The manner in which data is handled is a critical aspect of the design and functioning of a Single Window environment.

1.1 About Part VIII

This Part of the Compendium describes the various aspects of data handling in a Single Window environment. We look at the nature of laws and regulations governing the submission of harmonized data, and the legal and policy challenges in receiving, using, sharing, retaining and archiving of the data. The responsibilities and obligations on all participating entities in a Single Window environment in regard to security of data, as well as issues of privacy and data protection, are also explored in detail.

In an electronic environment, it is vital to ascertain who is sending data to whom. The Single Window operates on a foundation of certainty regarding the identity of the individuals and legal entities that governments and businesses can trust. This Part describes appropriate ‘Know Your Customer’ policies which are supported by technology-aided methods.

The Single Window operates against a backdrop of trust, whereby regulatory and commercial decisions are made based on electronic data lodged by businesses. The observance by all parties of data quality, including controls applied to improve data quality, is also covered. This Part deals with measures to achieve sustained improvements in data quality in a Single Window environment.

1.2 Related Topics

Part VII of Volume I of this Compendium, ‘Dealing with Legal Issues’, describes the various challenges faced by governments in establishing the entity that will operate the Single Window facilities. It also outlines the business processes which will be covered by the Single Window, and highlights the need for the relevant laws and regulations to be suitably adjusted to account for the shift that is brought about when a Single Window is implemented.
2. Trusting the Source of Data

Participants in the international supply chain share data with one another and with regulatory agencies. The integrity of the entire supply chain in relation to buy-sell processes, the chain of custody of goods, and the flow of information from one node to the next is based on a ‘positive identification’ of the node participant. A break in the positive identification of these entities introduces vulnerabilities into the security and integrity of the supply chain.

Data lodged by a supply chain participant whose identity remains uncertain could compromise all actions taken on the basis of that data. To prevent such an eventuality, regulatory agencies and businesses generally impose an obligation to ‘Know Your Customer’ (KYC) on the supply chain participants. KYC measures help prevent smuggling, impersonation (abuse of others’ identity), commercial fraud, trade-based money laundering, terrorist financing, terrorism, and above all, help link the supply chain data to its source.

Intermediaries and logistics providers (e.g. third parties and technology platforms) play a very important role in managing participants’ identity, as they are well placed to carry out the first level of scrutiny by following ‘KYC’ norms, before entities join the supply chain or join regulatory platforms such as the Single Window.

In a Single Window environment, some Customs administrations (especially those with national identification numbers for all citizens/residents and a well-developed address infrastructure) implement identity management of individuals: the individual’s details are validated by using national identification number and address databases, in close co-operation with the relevant government agencies/bodies. This has been found very useful in the risk management of low-value e-commerce shipments sold/bought by individuals.

A model for carrying out identity verification post-clearance exists in order to support a range of objectives. These include combating the use of express delivery and postal modes to trade in contraband or transfer valuable goods. By concealing their real identity, criminals can dispose of illegal imports or exports. Even those importers who do not wish to hide their identities can simply

---

**KNOW YOUR CUSTOMER – POLICIES & PRACTICES**

**WCO SAFE Framework of Standards:** This requires economic operators to verify upstream and downstream business partners by way of written processes and contractual agreements, among other methods. In an IT environment, it advocates for ‘rule-based’ access, which requires prior simplified registration and verification.

**Regulated Agent/Known Shipper (RA/KC):** In the air cargo environment, identification of every stakeholder and their credentials is key to aviation security regimes. Any cargo coming from a non-RA/KC has to be 100% screened before being loaded onto the aircraft.

**Supply Chain Finance:** Banks dealing with supply chain finance require KYC processes during the on-boarding of clients and beneficiaries, with subsequent checks to be undertaken periodically.

**Postal Supply Chain:** In 2012, the UPU launched the .post domain, with the primary goal of providing a secure and trusted space for postal services, especially for e-commerce purposes. Additionally, some postal operators are urged to come up with their trusted and ‘verified customer’ schemes. An example is the Australian postal service’s ‘MyPost’ loyalty programme, where customers can sign up with minimum information to enjoy benefits in terms of convenient delivery options and rebates.

**Express Industry:** As in the case of some postal services, express service providers insist that every customer coming to drop a parcel should provide his/her identification details. This is now a regulatory mandate in most jurisdictions.
misuse the ‘de minimis’ facility, splitting consignments in terms of value and re-assembling the components into goods of larger value. Confirmation of the trader’s identity can have a deterrent effect on misuse of the supply chain by fictitious entities or individuals who might be tempted to take advantage of the tax exemption system or simplified procedures for low-value goods.

A critical aspect of modern paperless processing systems is the ability to identify and trace back to a physical person. The same principle applies to businesses in a Single Window system, which will be accessed by individuals acting on their own behalf or as authorized representatives of businesses. Businesses will be registered as legal entities. When an online Single Window system is launched, individuals will access it on behalf of business entities. Like all online systems, Single Window systems should also take steps to guard against impersonation, as well as against fictitious individuals and business entities. Considerable progress has been made in the e-commerce and banking sphere in dealing with the risk posed by such entities. We can therefore work on the assumption that a modern e-Single Window system should be linked to a good KYC ecosystem.

**Australia: Evidence of Identity (EOI)**

“Importers are required to undergo an EOI check every time they undertake documentary transactions at a Department of Immigration and Border Protection Client Services counter. EOI is a verification process that individuals and businesses are required to undertake to prove who they are.”

Source: Australian Customs & Border Protection Service (ACBPS)

**Republic of Korea – Address Feedback**

In 2014, Korea Customs implemented a measure that obliges delivery service providers to report to Customs the actual destination of express cargo once delivery is complete. This has a deterrent effect on those intending to misuse the rapid clearance facilities and the ‘de minimis’ benefits for low-value goods delivered by express cargo service providers.

---

**Figure 1:** Example of Know Your Customer business processes used by financial and other institutions.
KYC processes are closely linked to entity identification, identity verification, identity management, authentication, authorization and customer support. While almost every logistics service provider in the supply chain has KYC obligations, no single organization should be forced to bear the entire burden of KYC. If the KYC responsibility lies with just one entity or system, it might become the weakest link. On the other hand, parallel KYC actions and KYC processes, which are partly technology-driven and partly involve human verification, can build up a healthy and sustainable KYC ecosystem. There are technology tools that automate and support some of the KYC tasks.

The Address Verification System (AVS) is a technology-enabled tool used by credit card companies to verify the address of a person claiming to own a credit card, by comparing the address with the registered address of the card holder in the company’s database.

Other technology tools are available to detect incomplete or fictitious addresses. Structured addresses containing names, streets, cities, country sub-divisions, country codes and post codes are superior to unstructured text-based addresses.

E-commerce companies use sophisticated address verification services and systems as they seek to avoid delivering ‘cash on delivery’ packages to fictitious addresses. These tools rely on checking the addresses provided against post codes and geo-codes, and help companies improve their screening of fraud-prone transactions.
3. Ensuring Data Quality

Many Customs administrations have introduced automated systems to support cross-border procedures. Traders enter relevant information into these systems for further processing by Customs. The data submitted is used further downstream for many functions, such as computation of Customs duties and other revenue collection, risk analysis, forecasting of trends, collation of statistics, analysis, compliance and enforcement checks, consignment targeting, and other regulatory controls. Ensuring the accuracy, integrity and/or completeness of this data is vital, as this expedites processing and clearance of legitimately traded goods. Data accuracy is a component of data quality and refers to the factual accuracy or correctness of data. To be correct/accurate, data values must be consistent and unambiguous. Data integrity refers to the continued reliability and consistency of data over the entire life-cycle, including generation, transmission and storage. Data integrity is lost due to its potentially unauthorized alteration.

If the data submitted is not true and accurate, its reuse can have damaging consequences – the revenue computed and collected will be incorrect, potentially high-risk consignments will not be flagged, and trade statistics will not be accurate. Errant traders can abuse the system to circumvent regulatory controls and evade taxes. The damaging effects are exponential when inaccurate data is reused internally or by other government agencies. This further erodes the integrity of the system, and reduces confidence in the system among its users.

Therefore, it is important when setting up a Single Window system to pay specific attention to ensuring data quality\(^1\). This can be achieved by introducing system (i.e. technical) measures, as well as non-system measures. Technical measures and mechanisms will ensure correctness and compliance with the format of the data field. Non-system measures help to achieve integrity and accuracy of the data submitted. Below are several suggestions on implementing technical measures to ensure data quality in automated Customs systems.

3.1 Use of International Standard Codes

There are many international standard codes published and maintained by international bodies, such as the UN, ISO, WTO and WCO. The WCO Data Model, in particular, provides the semantic and content reference to international code lists, so that users can benefit from greater levels of uniformity and consistency in the exchange of trade information between trading partners. International code lists ensure that standardized values can be used to refer to specified things, such as place names, products, entity types and transaction types. Validation can be applied to ensure that the values entered conform to the format defined, thereby providing an additional level of assurance to mitigate incorrect data entry.

---

\(^1\)This Section was prepared using the paper submitted by Mr. Desmond Chia of Singapore Customs, and Document PC0386.

\(^2\)The ISO 8000 series is the most widely used framework for dealing with data quality and master data management. More information can be found at https://en.wikipedia.org/wiki/ISO_8000.
3.2 Acceptable and Unacceptable Terms

Code lists and identifiers will not eliminate all data quality problems, though they are one of the most obvious measures to reduce errors. Code lists offer greater assurance than purely free-text fields. At the same time, efforts must be devoted to improving free-text data elements, which are prone to data entry errors or deliberate falsification. Some of the most important data fields are ‘General Description of Cargo’ (in cargo reports) and ‘Description of Goods’ (in goods declarations). Here, the declarant is free to enter the text within the space provided. These data fields are meant to be ‘human-readable’, and could include important information that may affect a Customs officer’s decision or assessment.

The crux of the matter here is user education. Administrations must be prepared to provide instruction manuals and guidelines that state clearly what is expected of private sector users when using the system. Administrations may even consider conducting training classes to ensure that private sector users understand how to use the system, and fill in forms properly.

Awareness raising and procedural governance can also be enhanced through transparent communication of what Customs considers to be ‘acceptable’ or ‘unacceptable’ text entries, including those used in the descriptions of goods. The WCO has created a list of descriptions provided in pre-arrival and pre-departure declarations. It is aimed at providing examples of unacceptable and acceptable wording for the description field. The list is not exhaustive but could be used as a guide which helps Customs communicate its requirements to members of the public who need to submit information to Customs.
3.3 Registration and Authentication of Users

All automated system users need to pre-register with the system owner, and each user should be authenticated when they are submitting information through the automated system. The registration process should require an applicant to submit his personal details, working details and contact information.

The applicant must be made aware of, and agree to, the terms and conditions for using the automated system, and accept that all information submitted by him must be true and accurate. The consequences and penalties for false or incorrect submission, or any other breach of regulatory requirements and conditions, must also be transparently laid out. Upon verification of the registration information, the applicant is given a user ID and password to access the system. Standard IT security procedures in line with industry standards and practices should be applied concerning the safeguarding of registration information, user ID and passwords. Sharing of login credentials, use of weak passwords and other unsafe practices must be prevented.

To further improve security, the system owner may consider having a secondary authentication process, or two-factor authentication. Common methods already deployed in government and e-banking systems include the issuance of security tokens that generate a one-time PIN (OTP), or the sending of an OTP to a registered mobile phone number via the short message service (SMS).

The registration and authentication process ensures that authorized users are the ones submitting the data through the automated system. This prevents unauthorized users from using stolen user IDs or passwords, or from trying to submit falsified or inaccurate information. In this way, the integrity of the system and the accuracy of the data are enhanced.

The effectiveness and performance of an automated system depend upon the data declared by users of the system. Though technical measures may be put in place to ensure data accuracy and correctness, they will not prevent fraudulent declarations by users, or compromised data quality through human error. Hence, in addition to technical measures, there should be a governance and

---

**Going paperless with e-KYC – the India experience**

In India, government agencies and businesses – indeed, virtually anyone – can perform the entire Know Your Customer (KYC) process entirely online. Financial institutions, government agencies involved in citizen benefits distribution, and telecom companies are some of the users of this facility.

The online process called e-KYC uses a government-issued unique resident number called the ‘Aadhaar’. The Unique Identity Authority of India (UIDAI) issues this number after capturing the basic information of the resident, along with biometrics. UIDAI enables businesses and government agencies to instantly conclude KYC verification when the person whose identity needs to be verified provides his/her Aadhaar number, and has his/her fingerprint or iris scanned. The Aadhaar authentication service matches the Aadhaar number with the fingerprint and other details stored in the Aadhaar database. It returns a Yes/No confirmation, verifying the person’s identity, within seconds and without any documentation. At the same time, it completes the necessary ‘in-person verification’ (IPV).

The Aadhaar authentication service is available as an open application programmatic interface (API) and is capable of carrying out 100 million authentications per day, using everyday electronic devices. With over one billion records, Aadhaar is the world’s largest biometric database. End-to-end encryption ensures that personal data remains protected from the instant it is captured.
compliance framework to ensure the competency and professionalism of users in submitting quality data.

3.4 Setting up a Declarant Governance Framework

One of the main users of a Single Window system is the declarant or Customs broker (the ‘declarant’ hereinafter). The declarant is the entity that acts as the intermediary between the Customs authority, other government authorities and the trading community to facilitate the submission of trade declarations. It plays an important role in ensuring accuracy and completeness of the trade data submitted through the automated system. The governance framework seeks to raise the level of the declarant’s proficiency and professionalism by incentivizing agents with good internal control procedures and compliance records. The declarant is encouraged to improve internal work processes and maintain good Customs compliance in order to enjoy lower security requirements and shorter renewal processes. One example of an improved work process would be to screen customers or potential customers in order to ensure that they are not ‘shell’ companies looking to exploit the regulatory system.

3.5 Training and Compliance Improvement

The compliance level of declarants must also be monitored. Compliant declarants can be identified for greater levels of facilitation through specific schemes so that they benefit from reduced checks or simplified procedures; higher-risk declarants should be scrutinized and engaged until they improve. Penalties alone may not provide the necessary motivation to help companies to improve. Hence, engagement and partnership with the private sector should always be considered in tandem with penalties and other disincentives to shape the correct behaviours.

Declarants can be assessed for their overall compliance level and reliability based on a set of criteria, the results of which are used to place them into different categories or bandings. The lower bands will enjoy a lower degree of facilitation than the higher bands. For instance, companies in the lower band could be subject to annual assessment and renewal of their licences, while companies in higher bands could benefit from automatic renewal or longer validity periods. Other incentives that could be used to shape positive behaviours include the lodgment of security. Lower-band, less compliant declarants naturally pose a greater revenue risk and would be required to provide a higher level of security, such as a larger amount for a banker’s guarantee. Higher-band, more compliant declarants may not pose the same risks and the guarantee amount could be adjusted accordingly, to shape the necessary behaviours. In this way, declarants in the lower band could be encouraged to continue to improve and be promoted to the higher band to enjoy greater facilitation.

New Zealand Single Window

Clearance requests can only be submitted by registered Customs brokers, or by importers who are qualified to compile an import entry and have the necessary Customs declarant code to do so. For more information please see:


Source: New Zealand Customs
Training must also be provided on a periodic basis, including when there are new regulatory requirements or new system features, so that declarants can stay up to speed and perform their tasks in a compliant and risk-mitigated way.

**WCO RECOMMENDATION ON THE GUIDING PRINCIPLES FOR DATA QUALITY**

The WCO recommends the following principles to enhance data quality:

1. **Principle I** – Partnership between Customs administrations and trade is critical to establish understanding of each other’s data quality requirements, to identify new processes, and to improve existing processes and procedures for providing that data. Co-operation between these two parties in a constructive environment can ensure that the right data of the right quality is delivered at the right time.

2. **Principle II** – Analysis of data, systems and procedures should occur on a regular basis to identify any areas of concern related to data and its quality. Data quality is also dependent on systems being properly configured to obtain data in the most efficient way from the persons holding the data in the normal course of their business, whilst fully respecting applicable data privacy and data confidentiality laws and regulations, as well as an appreciation of the roles and functioning of different supply chain parties who provide that data.

3. **Principle III** – Co-ordination within the global Customs community through the WCO to: implement and maintain systems that recognize and apply global messaging standards; reduce manual processes and procedures and promote electronic messaging; encourage implementation and updating of a non-exhaustive list of acceptable and unacceptable goods descriptions for pre-departure and pre-arrival declarations; identify originators of data in the global supply chain and facilitate their ability to provide data directly to Customs administrations; and encourage the use of coded information based on international standards, including the tools and instruments of the WCO, whenever possible.

4. **Principle IV** – Education of all relevant stakeholders in the international trade supply chain on data quality principles and improvements based on identified weaknesses in a systematic manner. Such education and awareness should not only take into account national and international Customs concerns, but should give due consideration to those raised by trade.

RECOMMENDATION OF THE CUSTOMS CO-OPERATION COUNCIL ON THE GUIDING PRINCIPLES FOR DATA QUALITY (June 2015)
Part V of Volume 2 deals extensively with the question of data harmonization. A harmonized data set contributes to implementation of a Single Window as it helps a trader lodge one set of harmonized data at a single entry point, and this will be shared by the different participating government agencies. This leads to time and cost savings for the traders since the same information need not be submitted again.

This Part highlights the issues/challenges associated with receiving data that is not harmonized. Each participating agency has its own data validation rules, which also need to be harmonized. For example, plant quarantine legislation requires the authorized officers to issue permits in a particular unit quantity code. While Customs also needs the same information for its purposes, e.g. quantity of goods imported under a consignment, the unit quantity code may be different. This forces the importer to supply two separate pieces of information, defeating the purpose of harmonization. Therefore, harmonization should also consider questions of data validation and data quality.

**EXAMPLES OF HARMONIZED DATA IMPLEMENTATION**

**Example 1: Canada Customs**
The new Integrated Import Declaration (IID) release service option further expands the ability for importers/brokers to submit and obtain electronic release for goods regulated by Participating Government Departments and Agencies (PGAs) [...].
*Source: Customs Notice 15-014*

**Example 2: Indian Customs**
Indian Customs has developed the ‘Integrated Declaration’, as part of which all information required for import clearance by the government agencies concerned has been incorporated into the electronic format of the Bill of Entry. The Customs Broker or Importer shall submit the ‘Integrated Declaration’ electronically to a single entry point, i.e. the Customs Gateway (ICEGATE). Separate application forms required by different PGAs like Drug Controller, AQCS, WCCB, PQIS and FSSAI would be dispensed with.
*Source: Indian Customs, Circular No. 10/2016-Customs*

**Example 3: New Zealand Customs**
The new electronic craft and cargo reporting and clearance messages in the New Zealand Trade Single Window are based on Version 3.2 of the WCO Data Model (WDM3), enabling information requirements to be harmonized across the border agencies as much as possible. For example, the new WDM3-based Import Declaration combines the Customs, biosecurity and prescribed food information required for clearance, in one message.
*Source: WCO news No. 72, October 2013*
4. Accepting the Lodged Data

4.1 Data Lodged by Businesses

The handling of data in a Single Window environment is always governed by a set of rules. These rules may be defined in primary legislation, or in secondary legislation and regulations. These provisions should cover the entire data life-cycle. Customs law in most countries covers the process of lodging declarations. The Australian Customs Act of 1901, described on this page, provides an example of lodgment provisions.

The manner in which a trader lodges data with each of the participating agencies is normally defined in the respective legislation or regulations. If these provide for data generally to be received by electronic means, there will be little need for change. Each participating agency in the Single Window will also have to align its rules in relation to the data its needs to collect in order to perform its respective regulatory functions.

4.2 Data Shared Between Government Agencies

When data is shared between participating agencies, a set of rules that describe the responsibilities and obligations between the agencies is required. These relationships can be defined through inter-agency Memoranda of Understanding (MoUs), or shared work manuals and operating procedures. There are legal issues involved in negotiating interchange agreements between the participating agencies. The respective laws of the government agency’s administration might prohibit the sharing or transmission of information collected as part of the agency’s work to register entities or issue authorizations. In the first instance, the legal impediments to sharing will have to be understood and addressed, so that the Single Window environment can make full use of system functions to collect, safeguard and redistribute information, and take into consideration the specific agency or agencies which are authorized to do so. Should the submitter’s permission be required for specific types of sharing, electronic authorization via a ‘click-wrap’ agreement is also appropriate, provided the

Australian Customs Act 1901

Provisions regarding lodgment of entries

Section 68 requires all imported goods to be entered for home consumption or warehousing and lists the goods not subject to this requirement (including those that do not meet the entry threshold value).

Section 71A sets out the requirements for making an import declaration either by document or electronically and any conditions relating to obtaining permissions under other Commonwealth laws.

Section 71F specifies that, if a person changes any information on a declaration at any time after that declaration has been communicated to the Department, and before the goods are dealt with in accordance with the declaration, the person is taken to have withdrawn the declaration as it previously stood and any authority to deal with the goods is revoked.

Section 71L specifies the manner and effect of communicating electronically with Customs.

Section 181 specifies that only the owner of the goods, an employee of the owner, or an authorized licensed Customs broker acting on the owner’s behalf can lodge import declarations.

Source: Australian Department of Immigration and Border Protection
appropriate legal mandate has been sought to implement it. Domestic laws usually provide the primary legal basis for governing relations between agencies, while agreements, Memoranda of Understanding and Service Level Agreements (SLAs) define the levels of operational performance. In addition, Interconnect Security Agreements (ISAs) serve to define the kind of security measures that would be needed to enable secure data exchange.

If interchange is envisaged with entities abroad, then it could also involve international agreements with treaty force, including bilateral agreements, or separate protocols for amendment to existing Customs Mutual Assistance Agreements. Technical annexes and other working level documents could also provide details on data and messaging standards, service ontology and metadata registries.

The layers of the Globally Networked Customs (GNC) Utility Block template provide a basic checklist for countries attempting to establish interconnected systems with one another. Globally Networked Customs is addressed in more detail in Section 4.4.

<table>
<thead>
<tr>
<th>Name of the Block</th>
<th>AEO/Commercial Fraud/Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose</td>
<td>What the block is supposed to do</td>
</tr>
<tr>
<td>Legal Framework</td>
<td>The law, including the instrument providing the legal gateway</td>
</tr>
<tr>
<td>Entities</td>
<td>Those who can send/receive information, and the methods of identifying them</td>
</tr>
<tr>
<td>Business Rules</td>
<td>The specific rules for the UB. If not described elsewhere, include relevant protocols, standards and guidelines</td>
</tr>
<tr>
<td>Data Cluster</td>
<td>The list of data elements for the UB</td>
</tr>
<tr>
<td>Triggers</td>
<td>Events that either start the data flow, or respond to data receipt</td>
</tr>
<tr>
<td>Interface</td>
<td>How the parties in a GNC relationship are connected</td>
</tr>
<tr>
<td>Integration</td>
<td>How a GNC partner connects to its own systems</td>
</tr>
<tr>
<td>Communication</td>
<td>The electronic means of exchanging information</td>
</tr>
<tr>
<td>Advantages</td>
<td>Benefits delivered to: Customs, business and other agencies</td>
</tr>
</tbody>
</table>

Table 1: Template of a Utility Block (UB) from the WCO handbook for Globally Networked Customs.

### 4.3 Identification, Authentication and Authorization

The services accessible to users on the web portal or software client of a Single Window environment are only the proverbial tip of the iceberg. In addition, the Single Window must adopt a secure and legally sound solution in order to provide access to disparate applications and business processes of participating CBRAs, and to give Single Window users a sense of seamless access.
UN/CEFACT Recommendation No. 35 suggests the adoption of an ‘identity management’ solution. The Single Window solution needs to provide ‘rule-based and role-based’ access to heterogeneous systems. Identity management solutions that are based on open standards can promote interoperability by federating and managing identities of users across different organizations. It is also necessary to isolate and decouple the access control mechanisms from the underlying application and database resources which may be hosted on disparate platforms.

There is hardly any legislation which explicitly addresses identity management systems (European Commission (TURBINE Project) 2009). However, privacy and data protection legislation squarely applies to data held in identity management systems. A number of other regions have also pursued paths towards international standards in this area, most notably the APEC Cross-Border Data Privacy ‘Pathfinder’ programme. Be that as it may, the Single Window operator will have to meet national legislation on privacy, and commercial confidentiality must be observed.

Transactions could be compartmentalized for privacy purposes, or due to a lack of integration between different service providers. A Single Window environment, on the other hand, legitimately seeks to link up information about economic operators for risk profiling purposes and therefore, by design, seeks the convergence of services and workflows. Furthermore, it also seeks to maintain observability and auditability of actions by individuals: the latter are not at liberty to revoke their engagement with the identity management systems operated in the Single Window and, in any case, should not be able to repudiate their actions.

The contracts that bring users on board a Single Window system need to reconcile these opposing concerns of individual privacy and legitimate business interest. Having ‘accepted’ the terms of participation in a Single Window environment, economic operators waive their rights to privacy and commercial confidentiality to the extent that the information is for the legitimate use of CBRAs. The system operator will therefore have to ensure system security and guard against unauthorized access or use.
In view of this, and in order to ensure admissibility of Single Window submissions for legal purposes, the identifiers issued to the individual user should be linked to his or her civil identity (for individuals), or to their corporate identity (for businesses), duly issued by the State. This is analogous to economic operators being identified based on their legally assigned identifiers. In the European Union context, the ‘EORI’ number performs such a function. In Singapore, the Unique Entity Number (UEN) identifies businesses and other registered organizations and entities. CBRAs need to properly identify regulated entities in the event of having to proceed against them to enforce cross-border trade regulations. Furthermore, it is a legal person that needs to be held to account for his/her observed actions in the automated systems. Authentication and authorization are mechanisms performed by the automated system. The former is the mechanism under which the system is securely able to identify the user and to ascertain whether the user is the person he or she is claiming to be. The latter grants the level of access to the user and looks at whether the user is allowed to perform a particular operation (e.g. a submission, update, amendment or cancellation). Consistent application of identification, authentication and authorization procedures is vital for ensuring that the information system is secure and is delivering a consistent, auditable service. Single Window services grow with the trust of their users over years of secure operation. The legal validity of actions performed by users will be challenged in the absence of a legally sound mechanism of identification, authentication and authorization.

**INTERCHANGE AGREEMENTS**

Interchange agreements imply sharing of data and the eventual disclosure of private, confidential and protected information. The main points are covered in the list below.

**Identification of databases:** Through a name and a title of the database in a way that clearly defines its boundaries.

**Ownership of databases:** All interacting databases in a Single Window environment must have names, titles and ownership. This includes the specific databases of the Single Window operator.

**Creation of databases:** The legal basis for establishment of the databases - from where does the administrator draw authority to establish and maintain the database?

**Classification of information:**
- *Classification by confidentiality:* Confidential, restricted, unclassified, unrestricted, based on government information-classification scheme.
- *Classification by privacy category:* Nominal and non-nominal data.

**Authorization and access controls:** Purpose of collection, processing and usage of data and legal basis therefor. Long-term usage, especially of nominal data.

**Manner of collection of data and legal basis therefor – interface specifications:**
- Data management life-cycle policy, period of preservation; restrictions, if any, on transnational movement of data.

**Liability:** Limitations and liability coverage against exposure.

Entity Number (UEN) identifies businesses and other registered organizations and entities. CBRAs need to properly identify regulated entities in the event of having to proceed against them to enforce cross-border trade regulations. Furthermore, it is a legal person that needs to be held to account for his/her observed actions in the automated systems. Authentication and authorization are mechanisms performed by the automated system. The former is the mechanism under which the system is securely able to identify the user and to ascertain whether the user is the person he or she is claiming to be. The latter grants the level of access to the user and looks at whether the user is allowed to perform a particular operation (e.g. a submission, update, amendment or cancellation). Consistent application of identification, authentication and authorization procedures is vital for ensuring that the information system is secure and is delivering a consistent, auditable service. Single Window services grow with the trust of their users over years of secure operation. The legal validity of actions performed by users will be challenged in the absence of a legally sound mechanism of identification, authentication and authorization.
The conditions under which electronic records, electronic documents and contracts will have probative value are determined according to national legislation. Determinations in relation to digital evidence will be made in courts, where experts will have to assist judges in deciding on the evidentiary value of access logs (for instance, whether such logs were authentic, reliable and intact). In the case of electronic records or documents, valid digital signatures will have high evidentiary value.

Digital evidence is an important legal issue. Where a Single Window environment is concerned, it is necessary for the country to determine what is permissible under the existing legal framework, and to propose amendments to the legislation where appropriate. An electronic submission cannot be treated as a less binding or less accurate form of submission, merely because of its modality. At the very least, data submitted in the Single Window environment should be treated as being no different to the same information submitted in a manual procedure, such as a paper-based declaration. This empowers governments to move beyond paper-type procedures to electronic or dematerialized procedures. It is also essential in conveying to users that an electronic submission must be taken seriously, and the same due diligence applied, otherwise penalties relating to incorrect or false submission of information would similarly apply.

### 4.4 Globally Networked Customs

The WCO has developed Globally Networked Customs (GNC) as an approach for Customs authorities to exchange information in a standardized way. GNC covers the sharing of Customs-to-Customs (C2C) information, logistics, risk assessment and commercial information. Although developed as an instrument for exchange of information between Customs administrations, it can also be used in the context of a Single Window as a mechanism for governments to exchange information with other governments.

Data sharing between Customs administrations must strictly abide by the rule of law, and the arrangements have to be either bilateral or multilateral. Most C2C data exchange scenarios are bilateral, except where Customs unions are involved. Information exchange under GNC works on the basis of protocols, standards and guidelines. For the standard scenarios of information exchange, the collection of documentation on protocols, standards and guidelines is called a Utility Block. The existence of fully developed Utility Blocks speeds up the framing of international agreements on exchange of information, and also facilitates the actual implementation of international data exchange. GNC is meant to ‘industrialize’ the setting up of exchange of information agreements, reducing the cost of their replication.

GNC is a voluntary arrangement. Members have to come together to negotiate areas of information exchange. For GNC to happen, countries must have enabling laws and administrative arrangements which allow them to exchange information, and must further afford adequate levels of protection to shared information. Electronic information should be shared in accordance with agreed technical and security protocols.

In the GNC framework, there are several scenarios of routine information exchange between governments. For example, documentation required in a Single Window, such as sanitary/phytosanitary certificates, test certificates, or certificates of origin, which originate in the country of export, can be shared with border regulatory authorities in the countries of import. This
means that the issuing authorities can send the documentation directly to the authorities of the importing countries. If the documentation is already available in the Single Window, this will save considerable time and effort.

4.5 Data Exchange – Push vs Pull

The way in which data is delivered between two agencies is an important consideration: whether the data needs to be fetched, or whether it is ‘dropped’ into the system, makes a difference, both technically and from a legal perspective.

Technically speaking, ‘push’ technologies involve data being sent via a message bus, through a web service, or by exposing an application programming interface (API). ‘Pull’ technologies involve connecting to the source system and pulling out the required data.

The choice between ‘push’ or ‘pull’ is typically a matter of requirements and design – both provide equally valid methods for government agencies to receive, consume, and process the data and information needed to fulfil their regulatory processes. ‘Push’-type delivery is suitable for processes that are well defined and have clear parameters (for example, regulatory processes performed through HS codes, or transactions that meet other clear pre-set criteria). The ‘push’ concept is used when the need to share the information is determined by the source system; on the other hand, the ‘pull’ concept is used when the need for the information is determined by the receiving system. The two modes are not mutually exclusive – processing workflows are typically facilitated through ‘push’ modes, while reporting processes use ‘pull’ modes. In this way, agencies scrutinize applications on a real-time basis, based on pre-set ‘push’ criteria, while receiving reports based on specified operational needs.

5. The Legitimate Use and Sharing of Data

5.1 Record-keeping Obligation

In a Single Window environment, almost all information will be digital. Thus, all evidence will be electronic. Single Window administrators will be governed by rules on data protection and the manner in which digital evidence is handled in their jurisdiction of operations. For them and their lawyers, there are important implications relating to digitally held information. ‘Personal data’ or ‘nominal data’ is a special class of data that is subject to special rules.

If the procedures for safe handling of data are compromised, or the Single Window administrators handle data in a non-compliant way, the government or other trade entities will not be able to
receive appropriate legal remedy. This is because potential violators will be able to question the validity of stored digital records and escape conviction. Justice will not be served.

In Single Window implementation, data and documents are not just held by participating government authorities, but also by private sector entities and their service providers. The policies, rules and regulations in relation to privacy, data protection and data retention will apply equally to entities in the private sector. Record-keeping requirements may have their origins in multiple pieces of legislation. For example, in some jurisdictions, Customs law may require records to be stored for a period of five years. Other laws, such as tax laws, may require an additional period of storage. If the records are kept in electronic format, then additional requirements may be prescribed.

5.2 Technological Challenges: Cloud Computing

Rapid technological changes have transformed the way in which data is accessed and used. In the manual era, data was in manual files held locally in each office. With the fast-paced development of computing and communications, data can be processed through filtered searches and transferred effortlessly over the internet. More and more nominal data is held in a distributed fashion and is exposed to unauthorized access.

Cloud computing systems involve virtualization of computing resources. The key aspects – data communication, data processing and data storage – are virtualized, such that the organizations using the cloud are unaware of the specific resources being used by their software applications, or of where the data is held physically at any given point. The core benefit of cloud is that it allows system resources to scale up quickly to process huge volumes of data, without being constrained by physical system upgrades. As a result, no one can pinpoint exactly where the data is stored or on which server. However, one can define the cloud so that it is ‘localized’ within a specific country (i.e. restrict storage of the data to being within the country).

With cloud services, users are able to pay only for what is used, or to subscribe to a certain bandwidth or storage, upgrading when they need more. This provides flexibility.

With the advent of cloud computing, there is potentially a dynamic allocation of computing resources distributed across jurisdictions, raising legitimate questions about how digital evidence will be brought to bear in legal proceedings. In cloud computing, digital data processing is

---

Measures to ensure usability of data kept under record-keeping rules

The following is an extract from section 240 of the Australian Customs Act 1901, explaining the requirements of record-keeping. Rules protect the ability to access records in order to verify compliance.

“Subsection 240(5) A person referred to in subsection 240(4) must:

(a) keep the document in such a manner as will enable a Collector readily to ascertain whether the goods have been properly described for the purpose of importation or exportation, as the case requires, and, in the case of goods entered for home consumption, properly valued or rated for duty; and

(b) if the document is in a language other than the English language—keep the document in such a way that a translation of the document into the English language can readily be made; or

(c) if the document is a record of information kept by a mechanical, electronic or other device—keep the record in such a way that a document setting out in the English language the information recorded or stored can be readily produced.”
highly distributed. In such a situation, locating, extracting and analysing digital evidence is extremely complex. Forensic investigations involving cloud computing are difficult and time-consuming.

Traders using a Single Window are subject to data requirements relating to record-keeping. Laws requiring record-keeping of past data sometimes also provide for the manner of its retention from the point of view of accessibility and legibility, or specify that it should be capable of being processed for post-clearance compliance verification. If records are kept in a cloud computing environment, then – as with any technology or platform – the fundamental principle of ensuring due care in protecting the confidentiality, integrity and availability of data applies.

Challenges in a Single Window environment grow significantly because the obligations or policies in terms of data retention, open publication, or protection against personally identifiable information (PII), etc. will be different for each agency.

As a trade facilitation measure, it is suggested that record-keeping obligations of Customs and all other participating agencies be made uniform, so that businesses are not burdened with a variety of policies and mandates.

5.3 Data Back-up, Data Archiving and Data Retention

Data archiving is meant to handle only a valid search for data. Archived data serves as a repository of data that may be stored for a long period of time. While it is not critical to be able to restore archived data to be read or used in the software application that produced it, it is vital to be able to search as part of a formal process and to produce results that can be presented as evidence in a court of law. The key to archiving is that archived data cannot be altered.

The process of archiving, and the technology used, are equally vital. Technically, an archive is understood to be unalterable storage. Data storage drives that are termed ‘write once, read many times’ (WORM) are often used for archiving.

Data retention refers to the availability and persistence of data in the hands of the authority that asked for it. Data

European Union: Privacy and data protection as a basic right of citizens

The right of protection in respect of one’s personal data is mentioned in Article 8 of the EU Charter. All EU Regulations must comply with these laws:

- Right to the protection of personal data
- Right that such data be:
  - Processed fairly for specified purposes
  - Processed based on consent of the person
  - Processed as laid down by law
- Right of access to personal data
- Right to have it rectified

Compliance is subject to control by an independent authority.

Source: EU legislation
retention applies to both live and archived data. It is easier to understand compliance requirements in relation to data archiving and data retention if electronic data is treated in exactly the same manner as manual information.

Legal issues surrounding data retention pertain to personally identifiable information, which is afforded a degree of protection. Protection of personal data implies that authorities receive personal data lawfully; that the data requested is only as much as is required to fulfil legal obligations; and that data is not processed in a manner incompatible with the purpose for which it was required. It should be accurate and kept up-to-date. Technical and operational measures should be in place to prevent unauthorized access. Retention of data increases the risk of unauthorized disclosure.

5.4 Destruction of Data

Data that need not be retained should be destroyed. There should be appropriate security policies and procedures in place to ensure that electronic records are not tampered with. These are briefly discussed in Section 6 below. Data should be stored in back-up facilities at secure locations that are entirely removed from the main processing centres, in order to protect against the dangers of simultaneous loss through disaster. The owners of data assets should have an obligation for data custodians to periodically review the data and information in their custody to ensure that it is actually destroyed when the data retention period has expired. Due to the fact that there are technical means to retrieve data from electronic storage devices, even after it has been deleted, professionals should be engaged to destroy data in a certifiable way.

SINGLE WINDOW: RESPONSIBILITY OF USERS & PARTICIPATING ENTITIES

All users and participating entities of the Single Window have an obligation to protect personal privacy, commercial secrecy and security of data. The traders, transporters, warehouse operators, logistics service providers and intermediaries and regulatory agencies expect that the data provided to a Single Window will be protected and handled appropriately.

How can users and participating entities protect data?

- By knowing how the Single Window classifies data according to privacy and confidentiality.
- By understanding the types of data handled by them in their day-to-day business.
- By appreciating privacy and commercial secrecy concerns of all data they come in contact with.
- By applying data access and data sharing policies and principles.
- By understanding legal obligations and adhering to accepted privacy laws and principles.
- By taking responsibility for their actions and omissions.
6. Data Security and Preservation

The Single Window relies on the bedrock of secure and protected information systems. Single Window systems can be at great risk without appropriate data security policies, security-related roles and responsibilities, a risk management approach, a security audit framework, and a proper data archiving and retention policy.

6.1 Documented Security Policy

To ensure a reliable data security framework, it is necessary to adopt appropriate technical standards, such as ISO/IEC 27001 on information security management. This family of standards will help a Single Window operator manage the security of all its information assets. The implementation of a security framework should be reviewed through audit, active monitoring, and security scanning, carried out by an independent specialized organization. The professional information systems auditors rely on use comprehensive checklists and proven methodologies to carry out security audits.

6.2 Classifying Data Assets

In auditing the security of Single Window systems, an exhaustive list is prepared of all data assets in databases, records contained in the electronic messages received by/sent to the systems, and other computer files stored in the systems. Information contained in these assets is classified and given a security rating. The classification and rating will determine the kind of protection afforded to the information. This will help in assessing data implementing access authorization profiles.

6.3 Following a Risk Management Approach

Experts have advocated a risk management approach to managing data security risks. Risk assessment involves the identification of threats to data assets, or the latter’s vulnerabilities, by estimating the likelihood and impact of a security breach. Risks can occur to data assets through fire, flood, loss of access, cyber attacks, breach of access, data loss, etc. A risk management approach helps identify these risks, and to prepare the department to mitigate them and respond appropriately. The ISO 27001 standard specifies that risk assessment be carried out before any controls are selected and implemented. Every control must be justified by a risk assessment. The risk assessment, when carried out for each IT asset within scope, enables budgeted counter-measures that are commensurate with the loss or harm that is likely to result from a breach of security of the asset.

6.4 Data Security Assurance Process

The data security assurance process is designed to answer the following questions:

- Who in the Single Window organization provides assurance that the data assets of all classes covered by the Single Window have been afforded adequate levels of security?

- What enables him/her to declare/certify all systems are (and remain) secure, and all data assets are intact?
These are important questions for senior management to address when putting a Single Window system in place.

6.5 Informed User Base

Single Window functionaries (CBRA officials, ‘privileged’ users and users from external trade) should be given written instructions in relation to data security and privacy. Other end-users of the system should also be provided with security instructions. In addition, Single Window administrators should periodically publish security bulletins. A written, comprehensive security policy should be complemented by regularly trained and well informed users.

6.6 Ensuring Business Continuity

A business continuity plan should be developed and tested in order to tackle the consequences of failure, whether arising from a security lapse or other source. When systems become unavailable and manual clearance is resorted to, this causes not just a disruption in services, but could also pose a risk in terms of weakening targeting, screening, profiling and communication facilities.

6.7 Preventing Cyber Attack

In this hyper-connected world, cyber security is of great concern to governments and businesses alike. Bad elements are constantly engaged in attacking cyber assets all over the world. In particular, major government and private sector systems are vulnerable because of the potential for great damage and loss. Protection of the cyberspace implies the protection of critical national infrastructure, which is the priority for any government. Many governments in the advanced economies have created capabilities for defence against cyber attacks. These capabilities include constant monitoring of trends in cyber attacks and deployment of counter-measures. ‘Cyber attack prevention and response centres’ have been established to this end. These centres work closely with government and private ICT infrastructure providers so as to bolster their cyber security preparedness. Cyber security is driven by risk assessment and by mitigation of known threats. An effective response to a cyber security incident is critical, as timely and appropriate action will help to contain the damage, recover the system and regain public confidence. Single Window systems are definitely vulnerable and should not work in isolation when it comes to dealing with cyber attacks. As part of their security policy, they should also participate in national programmes and processes that help prevent and protect attacks on their ICT assets.

6.8 Using Digital Assets in Formal Legal Proceedings

Availability and use of audit logs is an important consideration in data security. The audit logs maintained in a Single Window system will ultimately help deal with legal, quasi-judicial and formal internal proceedings. The extent to which the activities to access data can be logged, and whether such activity and access logging is kept active, are important questions. The data on audit logs should be protected for any future use in investigations or in formal proceedings.

Audit trails (or activity logs) and data validation should be built into the Single Window as a design feature. These are generally based on business requirements and may relate to the need to identify
whether a piece of information has been changed or corrupted, or to the quality and admissibility of electronic evidence in a court of law.

When designing the system for the lodgment of declarations, care should be taken to establish the process to achieve non-repudiation of source. Audit logs are typically preserved for communication and electronic files of lodged declarations, along with log records of receipt of signed and verified files (where digital signatures are applied to electronic declarations). Hence, it is important to ensure that audit logs are not tampered with.

Periodic audit is carried out to ensure that protection, archiving, retrieval and presentation processes are intact. Test checks have to be performed to verify that the electronic records can be used as evidence in formal and legal proceedings.

**6.9 Common Vulnerabilities**

Increasingly, employees access the internet using low-cost solutions, e.g. office modems, mobile internet, wifi or bluetooth. Single Window systems become vulnerable when they are opened up to communication technologies which are available to almost everyone. The security risks posed by such access to communication networks, systems and data assets, and the potential for compromise of the network due to such technologies, are real and should be addressed through appropriate mitigation strategies.

Incidents of data theft and computer fraud are increasing, especially through the use of portable media, pen drives and other devices. The impact of data theft on Single Window data and operations should also be assessed. There is a risk from access of portable media (USB drive) onto CBRA premises, with the potential for such devices to cause data theft and to introduce malicious software into the Single Window system.