KYOTO CONVENTION

GENERAL ANNEX
GUIDELINES

Chapter 7

APPLICATION OF INFORMATION AND COMMUNICATION TECHNOLOGY

WORLD CUSTOMS ORGANIZATION

Version 7 March 2014

Table of Contents

1. MANAGEMENT SUMMARY

1.1. PURPOSE

The purpose of these Guidelines is to focus the attention of Customs administrations on the impact of Information and Communication (IC) technologies (or 'ICT', but sometimes also referred to called 'IT') on their business. They outline how Customs can use these technologies to enhance program delivery and plan improvements in their services to clients and trading partners. They neither pretend to provide a catalogue of the latest available technologies nor suggest hardware and/or software solutions. The focus of these Guidelines remains on the key principles governing the use of ICT in Customs Administrations.

1.2. THE STRATEGIC ROLE OF ICT

Around the world, public authorities are now expected to deliver public services electronically. For Customs, this began earlier than most other wings of the government. It was natural that Customs, with their key responsibilities for goods control, revenue collection and border enforcement, should have used automation systems, initially, to control inspection and examination of goods, and collection of associated revenues.

Customs administrations then began to use ICT to shift the focus of inspection from goods to relevant information on paper-based import and export declarations. They found that they could also reduce obligations on traders to submit numerous copies of "original" paper documents, as key information was being captured by an automated system, which could not only validate and process data but also stock them at much below the cost ofstoring paper records.

Nevertheless, in the then rudimentary state of ICT , Customs still needed the physical presentation of paper by declarants or their representatives, at a place and time convenient to, and specified by, Customs. Subsequently, with advancements in IT created the possibility of instant, direct communication. These technologies transformed the prevailing procedural structures and rules. For instance, Customs could separate release from clearance. Electronic information received well in advance of the goods could give Customs all necessary information to apply controls.

The modern Customs organization has a very high degree of dependence on the application of ICT. Demand from stakeholders for greater effectiveness in trade-facilitation and compliance continues to drive Customs into making new investments on IT basedprojects and initiatives. Advanced systems for risk management and Single Window involve sophisticated technologies, and demand large and complex investments in hardware, software and services.

In a number of Customs administrations, legacy systems continue to be used for a variety of reasons. Even though some of these systems are beyond the lifetime of support provided by its vendors, the administrations are obliged to operate them and maintain them in good shape in the interest of satisfactory performance in facilitating trade.

By some estimates, for large business organizations that are engaged in services, the operating expenditure on information technology is second only to that of human resources, accounting for between 5 and 7 percent of the total operating expenditure. (Source: Gartner consulting Worldwide IT Benchmark Service, 2011)

Traditionally, ICT has been treated as a support service or an enabler. Of late, this has changed and ICT is now recognized as the engine for producing transformational changes and a way of maintaining competitive advantage.

The executive management must grasp the processes by which IT created value for the organization. This demands the adoption of frameworks of governance that bring clarity and transparency, explaining to stakeholders the correlation between business outcome and IT investments. The achievements of ICT achievements need to be explained in business terms.

In this background, a new discipline of Information Technology Governance was born mostly out of the principles of management accounting and strategic audit, bringing with it a number of frameworks and professional competencies that fulfil the needs of management at various levels starting with the ‘board level’ down to the operational managers.

The decision making processes in relation to ICT as a strategic area within the organization has been included. Customs Administrations have to set a methodology for linking the organization’s strategic goals with the relevant IT processes needs to be explained.

This helps Customs in building capacities on the most essential IT processes. This portion should also cover relevance of Enterprise Architecture in managing strategic investment into IT.

The goal of every Customs Administration is to preserve value in the international supply chain by improving effectiveness of cross-border controls so that cargo flows are un-interrupted, borders main secure and that leakages of revenue are plugged. The managers from Customs and Trade understand this value in terms of effectiveness of controls and the efficiency of the supply chain. The goal of ICT is to support these efforts and assisting the Customs and Trade in achieving the business goals by bringing to bear ICT’s rapidly growing capabilities.

Investments in ICT have ballooned in the last decade and perceptions about thereturns on investments are not uniform. It is not uncommon for some members of theexecutive management to develop a critical attitude towards the accomplishments of IT within the organization and to display a lack of appreciation for the results achieved. Other managers who understand the overall value proposition of the investment are unable to relate them to delivered results. There is need a framework to help the executive management track the real value that investments into ICT bring and to be able to obtain credible assurance that the goals of the organization are aligned with the goals of informationtechnology projects and services. The ‘COBIT’ Framework for IT Governance and Control isa major practice that divides the entire gamut of IT governance into “Control Objectives” listed in the table below.

Plan and Organize

PO1: Define a strategic IT plan.
PO2: Define the information architecture.
PO3: Determine technological direction.
PO4: Define the IT processes, organization, and relationships.
PO5: Manage the IT investment.
PO6: Communicate management aims and direction.
PO7: Manage IT human resources.
PO8: Manage quality.
PO9: Assess and manage IT risks.
PO10: Manage projects.

Acquire and Implement

AI1: Identify automated solutions.
AI2: Acquire and maintain application software.
AI3: Acquire and maintain technology infrastructure.
AI4: Enable operation and use.
AI5: Procure IT resources.
AI6: Manage changes.
AI7: Install and accredit solutions and changes.

Deliver and Support

DS1: Define and manage service levels.
DS2: Manage third-party services.
DS3: Manage performance and capacity.
DS4: Ensure continuous service.
DS5: Ensure systems security.
DS6: Identify and allocate costs.
DS7: Educate and train users.
DS8: Manage the service desk and incidents.
DS9: Manage the configuration.
DS10: Manage problems.
DS11: Manage data.
DS12: Manage the physical environment.
DS13: Manage operations

Monitor and Evaluate

ME1: Monitor and evaluate IT performance.
ME2: Monitor and evaluate internal control.
ME3: Ensure compliance with external requirements.
ME4: Provide IT governance.

This framework is supported by a set of tools that allow managers to bridge the gap between control requirements, technical issues and business risks. It is extensive in its treatment of IT governance and covers a wide range of issues that a Customs management should have control over. The ICT Guidelines touch-up on most of these issues in different sections.

≡ improve revenue collection and trade policy administration at import and export;

≡ offer accelerated release of export and import consignments and other premium procedures to those clients they identify as most reliably compliant and so presenting least risk to revenue collection and other Customs responsibilities;

≡ respond to governmental and public concern for effective controls of prohibited goods, endangered species, intellectual property rights, etc; and

≡ ensure integrity and effectiveness in handling the movement of goods and passengers.

Modern Customs administrations need to respond to, and assist, a wide range of international trade innovations based on IT applications, including express delivery and other global multi-modal delivery services, and an increasing network of global supply, production and distribution systems relying on just-in-time logistical networks.

Keeping Customs practice in tune with such commercial developments will call for equally innovative changes in basic administrative management.

While many administrations are either using, or plan to use ICT to enhance their operations, most existing Customs procedures are still based on receiving the electronic equivalents of old documentary exchanges. Paper declarations have simply been replaced by EDI messages.

Administrations currently considering either the development or the enhancement of IT applications should be able to move a further step forward by taking account of the fact almost all the data needed by Customs are already present in the commercial information systems that have been used to service the business transaction.

They should determine how far their own needs for control data can be met from the information systems of their trading partners, once these have been audited to ensure that they are secure, can reproduce data accurately and have proper data retention and archiving facilities.

If, as is now commonplace, these ICT systems are shown to provide more accurate and readily usable data for Customs purposes than traditional paper-based exchanges,Customs administrations will be able, increasingly, to rely on audited automated systems of accredited commercial trading partners for their own revenue, trade and other data needs.

Most Customs administrations are currently obliged to handle a growing workload in processing goods and passengers with only existing or even reduced staffs. Many have already proved that recourse to ICT has improved the quality of information capture and handling and freed scarce resources to concentrate on primary enforcement tasks, especially identifying and processing suspect consignments and persons.

These Guidelines recommend that Customs using ICT should observe relevant international standards. It is essential any such standards actually employed in automated applications should be easily identifiable and available for any necessary exchanges with other administrations.

Before adopting any IC application administrations should consult potentially affected and interested parties, including especially other government departments and traders, carriers, agents, port and airport operators, to ensure the chosen solution will be easily usable by all concerned. Continued consultation, with such partners, at all later stages of system development, will enable and encourage them to design and adapt their own systemsto make and offer the best use of Customs innovations.

While the primary purpose of this Guideline is to focus the attention of all Customs administrations on the use of ICT in their own operations, administrations will need to follow, and take full account of, relevant parallel applications, linked to rapidly changing business practices, that have had, and will continue to have, profound world-wide effects on day to day government.

1.3. FUTURE TRENDS

While, in the past, the WCO has concentrated its attention on the use of ICT in conventional Customs operations, recent discussions have begun to explore their effect on the total Customs function.

It is now obvious that Customs will have to move away from the “one size fits all” mentality and move towards an open system philosophy in which they will be able to exchange information, electronically, by a range of different means with employees, commercial and non-commercial clients and, nationally and internationally, with other relevant government departments and agencies.

In planning such a migration Customs will have to take account of the fact that between one third and one half of all international trade now consists of intra-company transactions, in which materials, components, and partly processed and/or finished products, are beingmoved across national frontiers, within integrated commercial management systems and increasingly diminishing and demanding time-frames.

Other business sectors, engaged in traditional sale/purchase trading are seeking the advice and help of logistical-chain service suppliers to emulate these highly efficient seamless transaction management systems. Customs, everywhere, still treat such movements as a series of separate export or import operations. Every administration only sees and treats one half of each international transaction.

The key to greatly improved Customs control, based on a major innovative response to now well-established and rapidly spreading commercial practice lies in the design and implementation of bi-lateral and multi-lateral agreements for Customs-to-Customs mutual assistance to provide and apply unified management of an overall set of controls and, procedures.

Several Customs administrations have embarked on pilot and prototype projects, in co-operation with selected, interested traders, to explore and test the necessary data sets and communication standards, identify legal obstacles and evaluate practical cost/benefits for all participants.

Experience in these projects, so far, has shown that while necessary technologies are already available, existing international and national legal frameworks, governing the movement of goods and information will need review and eventual revision.

Just-in-time techniques have inevitably resulted in a multiplication of small, repetitive and frequent consignments. As, for Customs purposes, each consignment has to provide its own packet of relevant control data, this could have posed serious information processing problems.

Fortunately specialist carriers, in all traffic modes, are already using ICT to maximise logistical efficiency and Customs, using appropriate e-commerce (EC) systems and an expanding range of electronic data interchange (EDI) techniques, can take advantage of these well-managed data flows to feed their own risk-assessment and release procedures. Many Customs services have adopted, or will implement, EDI applications using standard message formats, principally UN/EDIFACT. In order to ensure these messages are compatible, it is recommended that all EDIFACT systems should be developed on the basisof the EDIFACT maps in the WCO Data Model.

UN/EDIFACT standards, defining data structures for virtually every type of business and government document used in the course of international trade, still have unique global authority. Extensible Mark-up Language (XML) has also grown into a mainstream standard. XML data structures and vocabularies are being nurtured by different standards bodies including the WCO. New technologies and telecommunications infrastructures, such as those offered by Internet, offer Customs low cost means of receiving and disseminating information including XML, database publishing, document publishing and electronic forms. Appropriate consultation with trading partners, will allow Customs to offer their commercial communities a wide range of information exchange options. Some of these are set out Appendix 1.

Rapid changes in technology are reshaping the way businesses are functioning today, leaving behind much of the traditional ways of delivering services by electronic means. The emphasis on 'catching-up' with technology will vary according to strategic priorities of Customs administration and each case of change in the use of IT will be driven by its own business case.

Several major changes in IT are taking place simultaneously, which will change the way services will be delivered in the coming years. Some of them are mentioned below:

1. End-user mobile devices: Firstly the end-users are better equipped with technology, with access to inexpensive devices that are more powerful than the desktops

computers of a few years ago. These devices are being produced in different sizes and shapes to meet the unique needs of users. Smart phones and tablets are two broad categories, with the tablet sometimes transformed along with a keyboard doubling-up as table top computer.

2. Ubiquitous internet: Mobile devices are now connected to the ubiquitous wireless internet and can always ‘online’. High-speed ‘everywhere’ internet on mobile devices is a reality in industrialized countries but less developed nations are also catching-up. This offers an opportunity to governments to improve access to its applications using the internet.

3. APPs are the new kinds of software that runs on mobile devices. (APP is an abbreviation for a software application.) APPs are easy to find, acquire, install, launch,operate and update. APPs thrive on economies of scale. The speed with which a consumer gets access to APPs and uses APPs has no precedents. There is a quantum enhancement to usability and user experience, There seems to be a ceaseless supply of useful and innovative new mobile APPs for all key business functions. Information shared by some WCO members suggests that it is only a matter of time before enterprise applications will be similarly enabled. To the Customs administration, this could mean instant acquisition and delivery of business solutions to the end-user.

4. User interface: Keyboard, mouse and the graphical user interface (GUI) arebeing challenged by the finger and the touch interface of mobile devices. The touch interface forces a software designer to look at ways in which business functions can be performed witha few swipes of a finger on a tablet. In other words, developers will look at applications in ways that are most convenient to the mobile user. This lowers the barriers to a user’s engagement with the application. For example, unless there is no other option, the user will not be asked to enter data, leading to a high degree of reuse of business data.

5. Context & location awareness in applications: Smart devices have now been developed that can reveal in real time the location of containers, goods, transport means, logistics workers, customs officers and other actors. This capability opens new possibilities for designing applications in such a way that the flow of information and goods always remain in tandem. The data feeds obtained from devices called sensors will also play a big role. Container tracking sensors and Radio Frequency Identification Device (RFID) on electronic seal will generate continuous streams of useful operational data.

6. Social media is a collection of internet-based applications that provides the means by which information is created and shared by users belonging to a virtual community. Social media has brought powerful changes to the way in which organization, communities and individuals communicate. Social media is being rapidly embraced by enterprises as a communication channel with clients and stakeholders. This medium provides an opportunity for customs administrations as a means to achieve regulatory transparency as well as coherence within an administration.

7. Big data: Smart devices, social business networks and sensors based data collection units get connected to enterprise systems, the latter will receive continuous streams of large-volume data. Technologies that handle such volumes of data are termed as ‘big data’, which might prove to be useful for Customs administrations to generate valuable business intelligence and contribute to improved risk management.

8. Cloud computing platform: Cloud computing has gained prominence in the area of enterprise computing. Cloud computing technology helps in packaging and presenting computing resources such as servers, storage and networking as consumable unit through the concept of virtualization in the form of Infrastructure as a Service (IaaS). Cloud computing also covers approaches such as Software as a Service (SaaS) and Platform as a Service (PaaS). Cloud computing technology has made computing resources more easily accessible and cost effective than traditional solutions. Adoption of cloud computing technologies is gaining in government, where the technology is often deployed as a 'private cloud'. This reduces the risks of data security because data resides in government operated or managed data centers. Government agencies find cloud computing attractive because of the following reasons:

a. Cloud computing technology helps avoiding capital expenditure, thereby reducing investment risks.
b. Whilst reducing costs of starting pilots and proofs of concept, it also helps test and launch new initiatives faster.
c. As soon as an application is ready for production, it becomes easy to access cloud computing enabled 'production ready' IT infrastructure.
d. Cloud computing allows Government agencies to pool IT resources, making it possible to take advantage of the technology while addressing issues of security and data jurisdiction within government.
e. With cloud computing, Customs administrations can look forward to the prospect of sourcing computing services 'on-demand' without getting involved in purchasing and running their own infrastructure.
f. Some of the services can be operated strategically by government instead of individual departments using multiple third parties.

It may however be noted that the use of cloud computing is still in its initial stages and there are major security concerns associated with the technology. Governments usually wish have full knowledge of the location of the data and complete audit-capability with regard to data confidentiality and access. Therefore, governments around the world are putting in place formal policies on cloud computing, in order to tackle the challenges posed by the technology while deriving benefits from its deployment. It is being predicted that the technology will increasingly be deployed in greenfield projects and for non-mission critical applications.

Bearing in mind these future trends, Customs should plan for changes to its ICT infrastructure.

1.4. Scope

These Guidelines have been prepared to assist Customs decide how they can use ICT to improve their services to clients and trading partners. It identifies the main areas inCustoms program delivery where the application of ICT is most likely to prove most rewarding. It suggests and describes possible trading partner interfaces, and outlines a number of factors that administrations will need to consider when developing the use of ICT. These factors include legal issues and requirements, security aspects and client consultation.

ICT enables Customs to improve control while, at the same time, enhancing facilitation. To maximise such benefits, a Customs administration planning to apply ICT will need to undertake a preliminary review of its current programme delivery procedures, bearing in mind that ICT can only provide tools to support substantive activities. It is assumed that procedures and processes will already have been re-engineered in line with the revisedKyoto Convention standards, annexes and guidelines.

These Guidelines do not cover hardware and/or software solutions, which must be selected by each individual administration keeping in mind its own special needs and the related requirements of its trading community.

The Guideline has been designed:

≡ to encourage Customs administrations to investigate and make use of ICT solutions to support their current Customs procedures and controls;

≡ to advise and encourage Customs administrations that are considering the use of automation to follow a pre-defined process/plan covering all their needs;

≡ to promote the use of international standards in the interchange of electronic data among Customs and their trading partners; and

≡ to advise Customs administrations on current and possible future developments which could improve Customs automation.

1.5. CROSS REFERENCE TABLE TO THE KYOTO CONVENTION

Provision in General Annex	Section in IT Guidelines
3.11	8, 9.3, 9.4
3.18	6.4
3.21	6.4
6.9	2, 6.6, 12.
6.10	4
7.1	2, 3, 4, 5.6
7.2	8, 9.3, 9.4
1.3, 6.8, 7.3	2, 5
7.4	8.2, 8.3, 11
9.1, 9.3	6.14

2. BENEFITS OF INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

(Transitional Standard 6.9, Standards 7.1 and 7.3).

2.1. INTRODUCTION

This section outlines the main procedural areas where the introduction of ICT byCustoms will benefit Customs and their trading partners, bearing in mind that this step can have a major influence on Customs/trade working relationships and that many of the benefits which Customs can derive from the introduction of ICT will require full understanding by, and co-operation from, their trading community.

Automation planning and development should include, and be preceded by, a detailed cost-benefit analysis, in consultation with relevant commercial interests, to check that projected solutions will be worthwhile and effective for all concerned. It has to be remembered that the introduction of certain technologies, for example EDI, by Customs, can oblige traders to invest resources in the development of the necessary interface software in their own systems, with associated additional expenditure in, for example, network traffic charges.

Bringing trade representatives, as appropriate and necessary, into the Customs planning and decision-making process can take a number of forms, but the most common measures include the establishment of a trade/Customs consultative group, supported by public meetings, information packs and newsletters. The consultative group is very important because it can enable those outside Customs who are directly affected by the proposed system influence its implementation and to acquire a sense of ownership of the eventual outcome. Such a group should be set up very early in the planning stage of the project and should meet regularly throughout its full lifecycle.

Public meetings, open to all individual traders as well as their institutional representatives offer useful means of passing information to, and receiving views from, a wide commercial constituency. They should be supported by publicly available information packs, describing the proposed system and the ways in which it could affect and change trading operations, with details of relevant trader system requirements.

2.2. MORE EFFECTIVE CUSTOMS CONTROLS

The main Customs functions are the application of effective control to prevent duty/tax evasion, repress fraud and smuggling, apply trade policies and enforce a range of public protection requirements.

In order to comply with these responsibilities Customs are obliged to intervene, routinely, in the movement of goods across national frontiers in order to examine them and/orrelevant associated information.

Given limited Customs resources and the exigencies of modern trading timetables it is normally impossible for them to produce a no-risk situation by stopping and examining every consignment that enters or leaves their territory. Customs in leading trading nations have, therefore, become expert practitioners of modern risk management techniques, carefully designed and operated to select and target suspect consignments and persons.

Risk assessment and selectivity routines to identify consignments for documentary and physical examination can be applied in a manual system, but they can be carried out on a much more consistent, reliable and better informed basis by administrations who have automated their passenger, carriers, transport means and cargo control and/or goods declaration processing.

Fresh intelligence, gathered by Customs, can be fed into the computer system to supplement basic historical data including compliance records and guide selectivity and targeting. Such systematic, accurate and timely analysis of files can greatly increase Customs chances of detecting and repressing fraudulent practices. One incidental benefit is that automation can also help identify import transactions in which the declared value of products falls outside predetermined parameters.

2.3. More efficient Customs clearance

Automation of passengers and goods processing provides:

- increased productivity for both Customs and trading partners;
- better use of official and commercial resources;
- stimulate competitors to improve their own the necessary safeguards to offer highly-compliant traders premium procedures which will improve their business operations and compliancy performance;
- reduction in costs to Customs and trading partners by
- expedited release of goods;
- more accurate and timely information;
- more reliable enforcement capabilities;
- reduced congestion at ports and airports.

Automation of Customs procedures and electronic exchange of information, such as cargo data and goods declarations, opens the way for pre-arrival and/or pre-departure information processing. The capture and verification of regulatory information in advance of the arrival of export or import consignments, at the point of physical Customs control, offers administrations time to carry out an initial risk assessment, and give electronic notification of decisions on the release status of the goods immediately on their arrival.

The skilled use of information and communication technology in co-operative arrangements between Customs, other regulatory agencies and declarants, can enable all parties to an import/ export transaction to use a Single Window process by which relevant official border agencies can share prescribed control data to provide traders with streamlined ‘one stop shop’ release/clearance processing.

2.4. UNIFORM APPLICATION OF CUSTOMS LAW

The regulations governing Customs powers and responsibilities are constantly increasing in quantity and complexity. In a manual environment Customs can find it difficult to be certain that they have taken all existing regulations into account when processing each individual import and export consignment. A well-constructed automated system, however, fully programmed with respect to all relevant regulatory requirements, can ensure that all transactions are processed in comprehensive and consistent accord with all appropriate legal requirements. This ensures a uniform application of national laws to all trading partners. Customs can also use international data standards and business modelling techniques to provide the same uniformity and equitable treatment within the business rules so that when the law changes the rules themselves are changed.

2.5. MORE EFFICIENT REVENUE COLLECTION

In many countries, import duties and taxes are the major source of government revenue and efficient, timely accounting and collecting processes are vital to the national economy. Customs automation can help meet these requirements. In a manual environment reconciliation of revenue due and paid can be slow and error-prone. Automation can identify and quantify outstanding and bad debts instantly, and at any time, for prompt appropriate action.

2.6. MORE EFFECTIVE DATA ANALYSIS

Customs are the primary source of international trade data, required by governments for economic analyses and trade policy negotiations and relied on, by businesses, to aid market surveys and guide sales strategies.

Such detailed Information, collected and held in paper-based manual systems is bulky and time consuming to evaluate and organise properly. Extracting useful related data is very labour intensive.

Automation produces up-to-date trade information as a virtual by-product of export and import processing. Customs can offer the resulting benefits to all subsequent users and can apply Business Intelligence (BI) tools , to interpret and manipulate this information to improve their own operations at national and local level, especially in respect of effective post-audit control.

Traders using IT can send error-free, timely data to Customs who can then rely on their accuracy at this and any subsequent stage of data analysis, by reason of validation and credibility checks built into the automated capture process.

2.7. EFFICIENT PRODUCTION OF EXTERNAL TRADE STATISTICS

Almost all Customs administrations are responsible for the collection of trade data used as the basis for compiling national external trade statistics and informing a wide range of important political and economic decisions. The necessary data are generally extracted from import and export goods declarations. In an automated system they can be presented immediately in a prescribed structure and format, and to a very high-degree of accuracy, while, in manual systems, they only become available at some later stage in the clearance process. Statistics produced in automated cost-effective Customs routines facilitate prompt action by other government agencies.

2.8. IMPROVED QUALITY OF DATA

Data validation and credibility checks at capture enable Customs to resolve discrepancies while goods are still under their direct control and ensure the reliability of the basic raw data entering the Customs computer system for all subsequent purposes

Data Validation, protecting a computer application from incorrect information application, is of paramount importance. Once invalid data enter the system, the results of any processing are worthless and associated investment of financial and other resources is wasted.

3. THE DECISION-MAKING PROCESS

(Transitional Standards 7.1)

Why does a Customs administration, or for that matter, any organisation, wish to introduce ICT into its operations? To increase efficiency, solve an existing problem or meet a new requirement, in Customs, for example, implementation of the revised Kyoto Convention, are some of the most usual answers. All and any of these are perfectly sound reasons for computerisation.

There are many others, some less easy to admit and formulate, but at least equally valid, such as the improvement of professional integrity.

All computerisation projects should be approached with great caution in view of the serious financial and other losses that can result from mistakes in planning andmanagement. This warning is not intended, in any way, to deter administrations from introducing computer systems, only to alert them to possible pitfalls so that, by taking care to avoid these sufficiently early in the project planning process, they can move forward with justified confidence.

Automation, from the moment senior management decides in its favour right up to commissioning and live operation calls for intensive, expert planning and control, regardless of whether the new system is being developed in-house or by external consultants.

Given the large expenditure on equipment, services and manpower invariably associated with the development and implementation of a Customs automated system (including 'Single Window' systems and interfaces other government agencies) as well as concomitant major changes in basic procedures and operating methods, every such projectis a high-risk venture.

Careful planning and control are essential to identify and evaluate the risks and uncertainties, reduce or eliminate them where possible and ensure smooth implementation without serious time or cost over-runs. Good control, the basis for sound, comprehensive planning, should enable managers to recognise any deviations very promptly and to take rapid corrective action.

3.1. CHANGE MANAGEMENT

In modern social structures, all organisations, whether governmental, profit, non-profit, health care or educational, are having to face mounting pressures of change and are expected to:

≡ Do more with less;
≡ Do it faster;
≡ Be flexible; and
≡ At the same time, maintain or improve the quality of product or service or both.

In 10 years, at least one fourth of all current knowledge will be obsolete. The life span of new technologies is 18 months and this is rapidly decreasing. The older methods of recycling, revamping or revising conventional wisdom, no longer work. Customs administrations, in particular, must change if they are to give reasonable responses to the massive, changes in international trade patterns and practices.

They need to answer four basic questions:

1. What do the clients (importers/exporters/carriers/brokers) really value?
2. Does the administration need change to accommodate those values?
3. How will change benefit the administration?
4. How will changes in Customs meet broader government needs?

3.1.1. Ten Steps in Change Implementation

Step One: Focus on the business process and not on the function

It is critical that Customs identifies the functions arising from its responsibilities, but once this has been done, focus must shift to the processes required to perform thosefunctions, because they are the means by which the organisation interacts with its clients.

Step Two: Development of a process profile

Most processes within an organisation are not documented, which makes it extremely difficult to assess improvement opportunities accurately. In documenting processes, Customs wants to aim for the 80 – 20 rule. The application of this concept is extremely powerful when applied to improvement initiatives because:

- 20% of the processes consume 80% of the resources;
- 20% of the activities within a process generate 80% of the results; and
- 20% of the problems within a process represent 80% of the opportunities for improvement.

The organisation can quickly identify the vital few resource-consuming processes by developing a process profile, with diagrams of activities and process flows,

Step Three: Process mapping

Have the processes been designed or have they evolved? In most Customs administrations, the business processes were designed years ago and there has never been time to go back and review or redesign. Anything documented has long since changed. As a result most employees have never seen a visual representation of their work and don't know what is done before or after their work. They don't know how they fit in the big picture. A process map is a visual image of the way work is performed, showing:

- How inputs become outputs;
- Who performs what activities;
- Work flow and rework loops; and
- Decisions made and supporting information.

Step Four: Measure the processes

Process measurements allow Customs to determine current performance levels and establish quantifiable improvement targets. There are seven quantitative measures for determining the effectiveness of most business processes:

1. Process cost; The total cost of each activity in a process.
2. Unit cost of process outputs; The cross-functional cost of producing tangible outputs.
3. First pass yield; The percentage of transactions that make it through the process without being reworked, revised or rejected.
4. Cost of rework; The cost of the alternate flow associated with fixing the revised, reworked or rejected.
5. Process Cycle Time; The length of time required to generate a deliverable, such as minutes, days, weeks or months.
6. Actual Cycle time; The length of time spent generating an output with no waiting or rework.
7. Hands-off; The number of hands an item goes through and the activity at each hand.

Step Five: Study other Customs Administrations processes

Ideas or proven processes in other Customs administrations can provide invaluable information and save time and possibly avoid mistakes.

Step Six: Process redesign

Using the information gathered from the previous five steps, Customs can now map out the new processes, eliminating redundancies and duplicate work activities.

Step Seven: Balance processes and technology

In most organisations, information systems are very closely tied to the way work is performed, but technology should be seen as a tool and not, in itself, a driving mechanism for change. Automating a manual process will not necessarily make a Customs administration more productive and automating an ineffective process will simply get poor results faster. Customs should ensure that in improving processes and exploiting technology, the process review should come first so that technology recommendations can be based on its findings.

Step Eight: Manage process change

There are many possible effects from change, and Customs should concentrate on those that are:

≡ Highly desirable but unlikely without specific actions
≡ Highly undesirable, but very likely without sufficient attention

Step Nine: Prepare people (staff and clients) for change

There is NO organisation/administration so bad that somebody doesn't like it the way it is. Most people resist change out of fear of what the future will bring, rather than any positive attachment to the current process. The role of those who lead change is difficult and thankless, little training is available and there are few available role models for guidance and advice. Employees may need to be led through a three-stage process before unconditional acceptance of a change initiative:

1. HEAD:
   People intellectually understand the need to change based on supporting data. As much participation as possible will aid understanding.
2. HEART:
   People are emotionally engaged in change because they see the performance possibilities.
3. FEET:
   People take personal action as a participant, not an observer.

The length of each stage will vary with the individual person and the situation.

Step Ten: Continue Process Improvement

Business process re-engineering is time-consuming, costly and strenuous. Although change is sometimes mandatory, a culture of continuous process improvement will ensure that small improvements happen all the time and big changes happen infrequently. The job tasks of every employee should include:

- Continuous assessment of the situation, measuring the process from the client's viewpoint
- Identification of improvement opportunities, concentrating on high-leverage improvements yielding the greatest return.
- Prompt action when improvement opportunities are identified and offer quick tangible results.
- Measurement of results, translating change initiatives into quantifiable results.

There are no magic formulae or quick fixes for creating and maintaining good change management. Customs should be constantly alert on the path to improvement with day -to- day challenges and opportunities.

3.1.2. WHY CHANGE FAILS

Inadequate Information and Communication - poor information sharing and communication with stakeholder is often at the root of failure in change management.

Changes take too long and cost too much – When change is spread over a long period of time, it loses focus, funding, and momentum.

The risks are unknown - All significant changes have risks. If the risks are not clearly identified, it will create a sense of uncertainty, ambiguity, and a fear of failure.

The methodology is unproven - Change is difficult and complicated, it is unlikely that change will be successful if the change process is unknown and the agents of change are learning as they go.

The resources are insufficient - Successful change requires a Resource Management Plan to ensure that the number of required resources are identified, and a Recruitment Plan to ensure the best available resources can be brought in. These resources, however, are sometimes the most difficult resources to obtain.

The focus is internal - Many changes are driven by internal, not external factors. Without focus on the external clients' requirements, there is very little chance of success.

The change is disruptive - In the past, some organisations could put some operations on hold while they implemented change. Today, however, with the unrelenting pace we are all expected to operate at, it isn't possible to stop business while changes are being implemented. This means that resource planning is critical to ensure there are sufficient resources to maintain the status quo while the new work goes on as well. No organisation (Customs administration) will succeed if change disrupts the status quo and productivity suffers, or if the employees are not involved in the change to the extent where they are not able to do either the old or the new job process well.

3.1.3. How To Ensure Change Succeeds

Accelerate the pace - People who are driving the change, as well as people being impacted by it, must see tangible results quickly.

Use a proven methodology - A proven methodology with experienced change agents removes the guesswork from the change process. The benefits are clearly defined and communicated, and people work harder to overcome barriers to change when they see their efforts result in tangible benefits.

Focus on the client - The client will be your administration's biggest critic, so if the client sees value in your change, it will succeed.

Ensure the disruption is minimised - Change not managed and not resourced can be so disruptive it can paralyse an organisation's ability to function.

In summary, in order to make sure any change that is being introduced will succeed:

- Articulation of the administration's need for change;
- Use of a structured framework;
- Creation of top notch teams to manage and implement the change;
- Selection of the right business processes for change;
- Understanding the risks and preparation of contingency plans; and
- Involvement and education of staff and clients in the change process.

3.2. Who should develop the system?

The introduction of automation into a Customs administration is a complex and highly specialised task. Assuming that there may be a lack of suitably qualified and trained staff within the department very careful consideration will need to be given to the question of who will actually do the job.

There are usually three possibilities - to recruit suitably qualified staff, train existing Customs officials or engage external consultants. There are pros and cons for each of these choices.

The recruitment of qualified computer staff presents many problems but it enables work on the project to get under way relatively quickly. Salary scales will need to be at a level that will attract personnel of the right calibre. This can be a source of tensions between the new computer experts and existing operational staff that could have a damaging influence on the success of the project.

Training of existing Customs officials as computer systems analysts, programmers and operators may offer a better solution as they will be able to bring their Customs background to bear on the problems they will encounter. It may be difficult, however, to retain such staff once they have qualified as computer professionals after considerable public expense on recruitment and training. An appropriate salary policy will be needed to prevent the drain of this expensive expertise to private companies.

The final possibility is to contract a firm of external consultants for advice and assistance in feasibility studies, equipment selection and systems design and programming.

Organisations faced with automation for the first time often opt for a “turn key” solution and seek competitive tenders, based on a Feasibility Study, for a complete operational system.

Administrations with their own specialised IT staff may call for tenders to supply hardware, systems software and communications but could prefer to develop their own application software.

In this situation tenders would be invited from:

≡ Computer manufactures with software capabilities
≡ Computer manufactures without software capabilities
≡ Software houses
≡ Systems houses
≡ Batch bureaux
≡ Time sharing bureaux
≡ A combination of the above.

The tenders to be submitted should include:

≡ An estimate for the cost of carrying out the detailed system design
≡ An estimate for the cost of the computer programming work
≡ Training costs (for users of the system maintenance)
≡ Hardware costs
≡ Communications costs
≡ Maintenance costs
≡ A timetable for implementation
≡ Details of company background and experience.

Customs managements will then need to evaluate the various proposals and select a company to design, program, test, install and implement the new system. Control by a Steering Committee is vital at each stage during the development process. The best choice to install a "turn-key" system will usually be a well-established company with an international reputation. While the "turn-key" option is likely to be expensive results will probably appear earlier than with the two other in-house solutions.

It is usually wise to establish an IT Section within the administration even when automation is being developed by external consultants on a turn-key basis. This Section, staffed by Customs officials, should link the consultants and Customs field staff. Once the system is installed and the consultants have left, the IT Section will be responsible for maintenance, so it is important Section staff receive appropriate IT training from the external consultants or another suitable source.

3.2.1. CHOOSING A CONSULTANCY COMPANY

Where Customs decide to employ consultants the selection process will demand careful consideration. A mistaken choice could commit the administration to a lengthy contract, returning very bad value for money. Most international management consultancy firms now provide computer consultancy as part of their services and such firms probably provide the safest option. Their main work is advisory, helping to choose a particular system and possibly writing the software themselves. They can also assist with putting contracts out to tender and evaluating responses. They help with staff recruitment and may arrange to stay with the administration until the system is finally implemented.

External consultants, being outsiders, can avoid getting mixed up in the internal politics of an administration which can often hamper and delay the work of internal system development teams. Besides, externals should be provided with adequate briefing and with time to acclimatize with the complexity of the Customs domain.

Good consultants are not cheap, but they can provide good value for money to administrations without the necessary in-house skills. The terms of their contract should ensure that, by the time they leave, staff within the administration's IT Division will have been trained to replace them.

3.3. THE STEERING COMMITTEE

One essential component in the planning process is a Project Steering Committee to initiate, guide and review automation projects. It should comprise line management representatives from all areas of the administration likely to be affected. The data processing manager, if one is available within the administration, should be a member, along with a senior manager from the department’s financial and accounting branch. The Chairman of the Steering Committee, preferably the Director General of Customs or his deputy, should be drawn from senior management, as automation decisions must be understood and supported at the very highest level if they are to be implemented satisfactorily.

In many administrations management representatives on the Steering Committee may not have any detailed technical knowledge of data processing problems and requirements. It may be desirable, therefore, for senior staff to attend formal IT training sessions, specially designed for management and personnel in user areas, to help them appreciate the nature of the problems likely to occur in IT operations. It may also be necessary to engage an independent consultant to sit on the Steering Committee in order to advise management at various stages of system development.

3.4. TYPES OF PLANNING

In most organisations, including Customs, planning for IT purposes can be divided into three categories:

1. Strategic planning (paragraph 3.4.1.)
2. Project planning (paragraph 3.4.2.)
3. Business Continuity Planning (paragraph 3.4.3.)

3.4.1. STRATEGIC PLANNING

In every Customs administration there is a common set of business rules reflecting the Customs business processes. These business rules determine the execution of every process and influence the organisational set-up of the Customs administration.

The organisational set-up must guarantee that all business rules are performed in a well-controlled manner i.e. business controls, financial controls, personnel controls, PKI organisation etc. The organisational set-up influences the ICT security of the Customs administration.

Strategic planning will be concerned with the development of the administration's long-term computerisation plan. Individual applications can be automated without any long-term plan, but there can be no guarantee however that they will solve the administration's problems in the most effective manner or be compatible with any other internal systems that might be developed in future. Once an administration has embarked upon a particular course and become increasingly dependent on a computer-based system, it may find it very difficult and costly to change direction. As, in most administrations, the introduction of computers will affect more than one part of the organisation, an integrated policy is essential if automation is to proceed in a logical and coherent manner, avoiding overlapping systems and minimising cost.

The administration's long-term or strategic plan, usually part of the Feasibility Study or following immediately on its conclusions, should be submitted to the Steering Committee for comment and approval. Once it has approved the plan, the Committee will be responsible for monitoring and guiding implementation. It will assign priorities to individual project items and assess user requests for amendments or the inclusion of new projects.

The plan will set out the administration's IT policy objectives and identify the automated applications required to achieve that objective, together with a logical sequence for their development and a description of their boundaries and mutual interfaces. Technical aspects of hardware, programming languages, etc., will also be specified.

3.4.2. PROJECT PLANNING

The long-term or strategic plan will comprise several projects, each of which will require individual planning and control. Projects will usually be assigned to individual project teams with leaders reporting periodically to the Steering Committee. Some Project Committees may work under the chairmanship of the Project Leader who will report to the Steering Committee. When a Project Team has completed one long-term plan/project they will be assigned a new project by the Steering Committee.

Planning for individual projects is needed to:

- define precisely the objectives of the project and identify any constraints
- establish the boundaries of the project
- identify its relationship to other projects or systems whether existing or proposed
- establish a timetable specifying what has to be done, by whom and when, and what it will cost

The easiest way to plan and control a computerisation project is to divide it into more easily manageable phases. Most computerisation projects will consist of three essential phases:

1. project initiation phase
2. development phase
3. post-implementation phase

The initiation phase generally consists of the Preliminary Study and the Feasibility Study described in Chapter 5. This phase ends when the Steering Committee gives the go-ahead for the Project.

The development phase consists of the following steps or stages:

detailed investigation and analysis of the current system	(paragraph 5.1)
detailed system design	(paragraph 5.2)
programming	(paragraph 5.3)
hardware procurement and installation	(paragraph 5.4)
system implementation	(paragraph 5.5)
evaluation	(paragraph 5.6)

Many of the steps mentioned above are carried out sequentially, others are handled in parallel. Hardware procurement and testing, for example, will take place during the detailed design and programming phases, though hardware procurement and installation may be an individual project in its own right.

The post-implementation phase covers on-going maintenance of the system and the post-implementation evaluation.

Effective planning of a computerisation project requires an estimation of the resources to be allocated to each step and should include agreed time scales and resource allocations for completion. Progress is reviewed against the project plan at key points throughout project development. Any deviations from the plan are identified and measure taken to rectify them. The Project Leader (or Project Committee) will constantly measure progress against the plan and report to the Steering Committee at previously agreed intervals. In some instances the Steering Committee may only commit further resources to the project if the previous phases have been completed correctly and on time.

Planning a computerisation project is not any easy task. It is especially difficult in organisations introducing IC techniques for the first time. Any administration, which undertakes computerisation without a clear plan of action, both for the long-term and at individual project level, will very quickly find that it has lost its way and squandered a considerable amount of public money. While planning and control of projects will not guarantee success, they permit management to maintain a tight control on allocated resources and minimise the risk of serious cost or time over-runs.

Customs administrations are advised to consider using standard frameworks for project management, especially for managing large-scale ICT projects. In addition to traditional approaches for project management, a number methodologies and frameworks have been developed, supported by accredited experts. An example of a structured approach to project management is PRINCE2. For managing Software projects, one can use frameworks such as HERMES.

3.4.3. BUSINESS CONTINUITY PLANNING

Business Continuity planning is the overall process of developing an action plan to ensure the continuation of business in the event of unexpected unavailability of a crucial system or facility. For Customs it means the ability of an administration to maintain collection of duties and taxes, the control of goods and people crossing the border and the uninterrupted and speedy clearance of goods and people in international trade and travel.

Customs Administrations ought to worry about business continuity at all times. If Customs IT systems or processes are unable to function:

≡ Uncleared goods may clog vital parts of a country’s infrastructure
≡ Loss of risk assessment possibilities may pose a specific risk to society
≡ There may be increased attempts to import restricted goods
≡ Public and traders may be unable to obtain the information they require
≡ Tariff Calculations may be inaccurate
≡ There may be errors in revenue and duty collection and accounting

For these and many other reasons Customs Administrations need to have robust continuity plans in place. Otherwise disruption for industry and the community at large could damage the national or regional economy and restrict law enforcement and the availability of essential goods to the public.

Although business continuity planning should, as a matter of course, be an integral part of the management of a Customs administration, not every administration has such a plan in place.

A business continuity plan will require a set of contingency plans for each core business process and infrastructure component. Each plan should provide a description of the resources required, staff roles, procedures and timetables needed for its implementation. The process covers four key stages.

1. Initiation
2. Business Impact and Risk Analysis
3. Development of individual plans
4. Management of the plans

Stage 1: Initiation

- Obtain commitment from Senior Management
- Set policy and scope for business continuity management
- Establish a Business Continuity Planning Project work group
- Develop a master schedule and milestones

Stage 2: Business Impact and Risk Analysis

- Define possible failure scenarios
- Define the minimum acceptable levels of outputs for each core business process
- Assess potential business impacts and risks of these scenarios
- Identify and evaluate options

Stage 3: Develop individual plans

- Identify and document contingency plans and implementation modes
- Define triggers for activating the plans
- Assign resources for each core business process
- Obtain management approval and allocation of resources

Stage 4: Management of the Plans

- Distribute the plans to all relevant stakeholders
- Maintain strategy, plans and procedures
- Look at education and awareness, review plans and risks, test the plans and control changes to the strategy and the plans so these remain consistent with each other
- Train staff to produce the strategy and plans as well as to undertake the actions embodied within the plans
- Assure the quality and applicability of the plans in respect of adaptability, completeness, data quality, efficiency, friendliness/usability (very important as the plan will only be used in a time of chaos or disaster), maintainability, portability, reliability, resilience, security, testability and timeliness and management approval.

Customs Administrations need to obtain the commitment of Ministers and Heads of Department to the essential elements of Business Continuity Planning.

There has to be a contingency Planning Manager with overall responsibility for the business continuity plan. As the plan affects the survival of the whole organisation, this needs to be a senior person with sufficient authority to ensure things are done, to obtain and deploy required resources and co-ordinate the recovery effort. The detail of the plan must be provided from the individual business areas.

It may be necessary to assign regional or area co-ordinators to manage the recovery effort at a local level if and when the Business Continuity Plan is invoked. Individual plans will prescribe actions to counter specific risks. It is advisable to identify individuals, with the appropriate technical skills, to manage these.

Detailed Guidelines on how to undertake business continuity planning can be obtained from the WCO Business Continuity Planning Guidelines.

3.5. DEVELOPING ENTERPRISE ARCHITECTURE:

The decision to computerize involves careful planning by the different levels of the organization. Section 3.4 discusses the various types of planning including Strategic Planning, Project Planning and Business Continuity Planning. The development of the ‘Enterprise Architecture’ is a part of Strategic Planning for the introduction Information and Communication Technology. In order to support the strategic management process of the ‘enterprise’, it is necessary to produce and maintain the relevant organizational blueprints.

The aim of Enterprise Architecture is to establish direct links between the business imperatives of the enterprise and the deployment of technology. In establishing these linkages, the organization is able to seek alignment between business goals and information technology solutions. This helps in putting resources to best use and in identifying resources that are not contributing to the business goals of the organization. The absence of an architectural solution may lead to the proliferation of projects that do not meet business challenges, and to solutions that are being duplicated, infrastructure that is wasted and not playing any part in achieving business goals. Enterprise Architecture results in more efficient use of ICT ensuring improved return-on-investment (ROI) and lower total-cost-of-ownership (TCO). Investment into information technology without having the enterprise architecture view is inherently risky.

Enterprise Architecture comprises different architectural views and architectural descriptions that support the high-level planning for the solutions involving the use of Information Technology. There are different standard frameworks describing the architectural views.For example, the US Department of Defence Architectural Framework (DODAF) uses three views: i) the operations view that identifies the activities that have to be performed and who performs them. (ii) The systems view defines the systems that fulfil the operational needs focusing also on information exchanges (iii) the technical standards view defines the applicable technical standards, notations and conventions. These three views are interdependent and together contribute to the final picture.

The Enterprise Architectural descriptions include business architecture that describes the functions of the organizations and how it performs them. For example, where and how does a Customs officer check documentation and inspect goods? Who conducts desk audit of goods declarations and uses what kind of tools? How do these activities benefit the organization? Information architecture provides a complete picture of the intra and inter-enterprise flow of information. It also includes the underlying conceptual data model. The inventory of software applications that that serve the organization's business objectives and missions would form a part of the application architecture. This architectural view also describes how the applications fit-in with each other as well as with the overall business purpose of the organization. The software platform that mediates between applications – called middleware provides the software environment for the execution of applications. Technology architecture deals with these issues and drives other architectures such as security and software architectures. These architectural views can help rally divergent groupings within the organizations towards forging a consensus on the common needs. They help project participants identify with something concrete on the agreed future and course of action.

The Open Group Architecture Framework (TOGAF®) is a framework for enterprise architecture which provides a comprehensive approach for designing, planning, implementing, and governing an enterprise information architecture. The Single Window Implementation Framework, a document produced by UN/ESCAP and the UNECE has been developed based on the TOGAF Enterprise Architecture concept. TOGAF is a well-known discipline supported by a large and diverse body of practitioners

This Guideline recommends that as part of the strategic planning for automation, Customs administrations should invest in Enterprise Architecture and make available the relevant architectural views and descriptions to the project and operational planners. For a more detailed discussion on the concept and application of Enterprise Architecture the reader may refer to Chapter 8 of the WCO Capacity Building Compendium [published by the WCO in 2009] and to Chapter 6 of Volume 2 of the WCO Compendium on How to Build a Single Window Environment [published in 2011].

4. THE IMPORTANCE OF CONSULTATION

(Transitional Standards 6.10, 7.1)

Customs automated systems cannot be developed successfully without the co-operation and goodwill of a large number of people. It is particularly important to consult two groups before, during and after the development of a Customs system - .the trading community and Customs staff who will use the new system.

4.1. THE TRADING COMMUNITY

As most Customs automated systems will have a major impact on trade users consultation with them is essential to secure maximum benefits. A formal Consultative or Advisory Committee can b formed to advise on practical issues and keep trade partners informed of Customs plans. Other interested government departments, importers, exporters, carriers, freight forwarders, Customs agents (brokers), port/airport authorities, etc., should be represented on this Committee.

4.2. CUSTOMS STAFF

Any new computer system can encounter user resistance based on a natural human reaction that resists change and tries to preserve the status quo. This is best overcome and the full effectiveness of the system is best obtained by ensuring the participation and co-operation of users at all introductory stages. If a new system is wrongly used it is usually because the users do not understand it properly or do not want it to work.

If the users feel that the system does not meet their needs the cause is usuallyinadequate system investigation, or poor perception of user needs by the systems analyst. User participation in the development of the system is therefore of crucial importance since it promotes effective systems analysis and design, facilitates user understanding and confidence and can highlight potential areas of difficulty. While the need for user participation is clear, achieving it is much less straightforward.

If users are to co-operate effectively they must know that their jobs are secure. Any anxieties on this account must be allayed at the outset. Users must trust the systems analyst and have confidence in his ability. In return, the systems analyst must trust the users and be prepared to accept their ideas.

Users must be kept informed of developments during the entire duration of the project. Lack of information encourages rumours and discontent, hardly the most suitable environment for the introduction of a new computer system.

Regular contact is needed to secure user confidence and co-operation. Users should be adequately represented on project teams and committees. There should be regular working group meetings to encourage users to participate in the design of the new system. Their in-depth knowledge and understanding of existing manual systems will enable them to make important contributions in several areas, for example office layout, form design, error procedures, screen layout and report layout.

Education is also an important element in boosting user co-operation and confidence. User education can be divided into two categories, firstly general education on information technology and the basic concepts of computing and secondly detailed training on the particular system being developed. Where an external firm is developing the system, user training should be part of their responsibility.

The success or failure of a system can depend largely on user co-operation. If users are informed and re-assured and brought into the design of the system chances of success are correspondingly improved. If they are alienated the system is doomed to failure.

5. THE SYSTEM DEVELOPMENT PROCESS

(Transitional Standards 1.3, 6.8, and 7.3)

Once a particular course of action on the basis of the Feasibility Study has been decided and necessary financial authorisation has been obtained, the project moves into the development phase and develops from a concept into a system that is ready to operate. The decision on who carries out the system development phase will depend on on the strategic outlook of the Customs Administration concerning ICT procurement. existing IT personnel arrangements within the administration (see 5.1).

During this phase, as at all other stages of system development, management must exercise close control through the Steering Committee, to ensure that the project is progressing in accordance with agreed time scales and within budget. It must maintain that control over the completed development phase product, that is the computer programmes and their supporting documentation.

The computer programmes will reflect, in minute detail the procedures that are currently carried out in the manual environment so it is vital that the necessary steps are taken to ensure that they accurately reflect those procedures otherwise the final system will not meet the users' needs.

This phase of project development should be broken down into sub-phases to facilitate user participation and management control. The results of each sub-phase should be reviewed by the Project Committee and Steering Committee before approval is given to proceed to the next sub-phase. The various stages in this process are described later in this Chapter.

5.1. DETAILED INVESTIGATION AND ANALYSIS OF EXISTING SYSTEM

This investigation of existing procedures does not imply that the earlier enquiry, carried out as part of the Feasibility Study, was inaccurate, but will need to go into much greater depth to provide the basis for detailed analysis and design of the new system.

In this detailed investigation the main tasks of the systems analyst will be to interview staff at all levels within the administration and to consult procedure manuals and any other relevant and available documentation. Once in possession of all the facts, he will analyse the information he has gathered and produce a User System Specification for submission to the Project Committee and, ultimately, the Steering Committee. This document will describe, in layman's terms, the main features of the new system and how it will affect management and staff.

At this point the Project Committee will need to bring users of the system fully into the development process, to check that the information gathered by the systems analyst is accurate and that the detailed design of the new system can proceed without any need to introduce amendments at a later date. In effect the end-users of the system will have to tell the analyst whether the system he is designing meets their needs.

The User System Specification should be approved by the Steering Committee before commencement of detailed design work and, once the contents have been agreed it should not need to be updated. The User System Specification is often the users' last opportunity to request changes where the design fails to meet their requirements. Once the Specification has been accepted, it is often "frozen" so that no amendments can be accepted during the remainder of the project.

5.2. DETAILED SYSTEM DESIGN

Detailed system design begins once, following analysis, the Steering Committee authorises the development of a new system.

Authorisation will be based on the outline design of the system contained in the Feasibility Report together with the expanded statement of user requirements in the User System Specification. The design will include detailed specification of computer and manual processing requirements, inputs to and outputs from the system, computer files used to store information and segmentation of the processing into programs.

The systems analyst will produce the results of this design work in a series of documents, namely:

≡ Program Suite Specification
≡ User Manual
≡ Operations Manual
≡ Test Data
≡ Changeover Instructions

The Program Suite Specification provides the computer programmers with all the information about the computer functions that they need to write the programs.

The User Manual will instruct user departments in the clerical operations required for the successful operation of the system and the actions to be taken in the event of failure or error. The User Manual must be accessible for reference purposes throughout the operational life of the system It should always reflect the current state of the system and will, therefore, require updating when changes are made which affect user procedures. Users who have not had previous experience of computer-based systems are not usually aware of the importance of strict adherence to the instructions contained in the User Manual. Care should be taken to ensure such awareness.

The Operations Manual is the permanent reference document relied on by the computer operations department, for information on the system to be implemented and the tasks to be carried out for its routine operation.

Once the programs have been written and users are familiar with the new procedures, the system will need to be tested to ensure that it will operate successfully under all the likely conditions and that it will produce the expected results. Test Data will be required to test that the completed system satisfies developers and the users alike.

Finally two sets of changeover instructions will be required; one for user departments and one for computer operations. These will specify, in detail, the procedures required for the changeover from the old to new systems.

All of these documents will be reviewed by the Project Committee and Steering Committee before approval is given for the commencement of programming.

5.3. PROGRAMMING

The programming task will include designing the program structure, designing and documenting the detailed logic of the program, coding, preparing a test plan and test data, testing (technical part) and debugging the programs and preparing final documentation.

The starting point for programming is the Program Suite Specification which has been prepared as part of the detailed design of the system. The programmer will test his own programs to some degree but the entire system, including all the programs, will need to be tested for the functional part for user acceptance and finally approved by the Project Committee and the Steering Committee before the system can go live . From a management point of view it is vital to ensure that the computer programs are fully documented. Undocumented programs should not be accepted under any circumstances. Without supporting documentation, programs are virtually unreadable and cannot be modified except by the person who wrote them.

It cannot be stressed too strongly that documentation is a fundamental part of any program suite. There is an equal need for programmers to adhere to agreed programming standards otherwise maintenance can become a problem. It should be stressed to programmers that what is required are programs that work well and can be easily modified should the need arise.

5.4. THE PROCUREMENT PROCESS

5.4.1. PROCUREMENT

Computer hardware on which the new system will be run has not been mentioned in depth so far. Computer procurement should not take place before the Feasibility Study or the detailed analysis are carried out or after the system has been designed and programmed. If new computer hardware is required, procurement is usually carried out in parallel with the system design phase.

Administrations should not fall into the trap of acquiring expensive hardware prior to conducting a detailed examination of their computing requirements. The likelihood is that it will not meet their needs and will simply be an expensive millstone around the administration’s neck. Equally it is not prudent to delay acquisition until after the system has been programmed. This will simply prolong the implementation schedule for the automated system. Most organisations aim to have the computer hardware available and installed to coincide with the programming phase since it is at this point that the computer will be required.

Administrations should therefore undertake the process of hardware procurement in sufficient time to ensure timely availability. Acquiring a computer system means buying three basic components (hardware, software (systems and application) and communications). Some Customs administrations (especially those encountering IC technology for the first time) will opt to install an entire automated system on a “turn-key” basis. The process of acquiring hardware, system software and communications is discussed here independently of the application software and not as part of an overall package implicit in the “turn-key” approach.

5.4.2. Request for Proposal (RFP)

In order to procure the necessary equipment it is usual for government agencies to issue a Request for Proposal (RFP) to a list of vendors identified as likely to be capable of submitting a serious bid. Before that can be done however, it will be necessary to prepare a document specifying the functions that the equipment must be capable of performing. This document is known as a Functional Specification. In some cases the Feasibility Study Report may already contain sufficient detail. If it does not however it will be necessary to supplement it to ensure that it contains the following minimum information:

* Mandatory Requirements
A list of all requirements which the computer system must be capable of performing including requirements for meeting computer standards;
compatibility requirements - if the system is to be used in conjunction with another system;
upgrade capability - if the workload is likely to increase over the life-cycle of the system;
system recovery requirement in the event of system failure;
security requirements, etc.;
compilers, assemblers, other utilities.
All system software requirements should be itemised.

* Detailed Workload Requirements
A description of the processes that will be performed; input volumes; processing volumes; volume of storage; type of storage (on-line, off-line); length of storage; peak activityvolumes (for on-line systems); response time requirements (for on-line systems); turnaround time (for batch systems).

* Vendor Support
A statement of all the support requirements to be met by the vendor. This includes site planning, electrical installations, air conditioning, fire prevention, auxiliary power supply, installation schedules, pre-installation computer time, line test demonstration, on-site support personnel, training needs, and very importantly - maintenance requirements.

* Reliability
Reliability is usually expressed in terms of a percentage of scheduled operating time. If this requirement is very high, 99 %, for example, the vendor will probably have to propose a dual system. This will mean a very large cost increase, especially if the contract includes a substantial penalty clause for excessive downtime. It is therefore best to determine the amount of downtime (downtime to maintain the system excluded) that would be tolerable within the criteria for a responsive operating system. It is important to include penalty clauses in the contract to ensure that the vendor will provide adequate maintenance and equipment to stay within those established reliability criteria.

* Contractual arrangements
This should specify the formal contractual obligations, which will be entered into between the administration and the chosen vendor. It will specify such things as exact delivery dates, payment dates, penalties, resolution of disputes, after sales service, etc.

In addition to the Functional Specification which contains all the above requirements, it will be necessary to submit a number of "bench-mark" problems to potential suppliers to ensure that the equipment which is proposed to be supplied actually meets the performance standards required. A bench-mark problem is a simulated version of a typical computer application which the vendor can run on the computer to be supplied. The results will form part of his final proposal.

5.4.3. Evaluation of responses to RFP

The proposals received from the potential suppliers are evaluated by the Steering Committee (if necessary with professional advice from a consultant specialising in tender evaluations) under the following headings:

≡ Technical evaluation

≡ Cost evaluation

≡ Benchmark evaluation

Technical evaluation will call for the examination of the proposals to ensure that they meet the mandatory requirements set out in the Request for Proposal.

Cost evaluation will compare the offers of suppliers for the cost of outright purchase, lease and lease with option to purchase. The various acquisition options for each supplier need to be examined in detail in order to identify the most cost-effective solution. Live tests and demonstrations should be arranged with each supplier who passes the technical evaluation. During such live tests the benchmark data should be processed and the results should be collected and evaluated.

Only the suppliers whose equipment passes the benchmark tests and meet the mandatory technical requirements should be considered when awarding the contract. Negotiations should be undertaken with each of these suppliers with a view to assuring the best possible price.

After a thorough evaluation of all proposals, the administration should be in a position to choose a supplier and an equipment configuration. When the time comes to prepare the contract, the administration should insist that all special circumstances and offers of technical assistance and support as well as equipment maintenance are incorporated in it. If the successful supplier has promised additional support in post-installation phases, this should also be carefully defined and included.

While the normal method of paying for computer equipment has been by leasing from the manufacturer, purchase plans and various forms of lease-back arrangements with independent leasing organisations are also available. Senior financial officers should carefully examine the financial impact on the organisation of these various options. In addition, the contract should be reviewed by a legal officer to ensure that it provides adequate protection of the administration's interests.

5.4.4. Installation

Installation of the computer can be a complex and time-consuming project. It is easy to underestimate the time and resources required to carry it through successfully. Computer manufacturers can often provide a comprehensive checklist of the actions that will need to be carried out prior to delivery of the hardware. Using this as a basis, a plan should be established for the necessary pre-installation activities showing their any relevant inter- dependencies. These activities include:

≡ site preparation plan

≡ staffing plan

≡ data communications plan

≡ delivery schedule

≡ logistical support plan

Site preparation planning includes determining computer centre and tape library floor space requirements, defining heat and humidity requirements, defining electrical and telephone requirements, and defining all special computer facility requirements such as sprinkling systems, electrical interference safeguards, electronic security safeguards, auxiliary power supplies, etc. It also includes identification of such support requirements as desks, tape racks, carpets, observation decks for supervision, report preparation equipment, etc.

The staffing plan identifies all of personnel required to operate the computer centre, shows when they will be needed and what actions are required to obtain them. Personnel requirements for a data processing centre normally include a data centre manager, computer operators and supervisors, support software programming staff, data preparation personnel, technical control personnel (if the computer application includes extensive data communications) and data entry machine operators.

The staffing plan also shows when recruitment action will begin for newly hired personnel, when retraining will begin for personnel that are being retrained from existing staff, when personnel will actually be brought on board and when and how they will begin performing their jobs. The staffing plan must be co-ordinated with the computer system procurement to ensure that the personnel are available when needed.

The data communications plan depicts data transmission requirements and shows when and how the data circuits, modems and concentrators will be installed in order to support operation of the system.

A logistical support plan is prepared to show what support will be required and when to deal with personnel (recruitment), transportation and removals, installation of equipment, legal assistance, etc.

System Installation is normally the responsibility of the computer supplier. Site preparations, however, are normally the sole responsibility of the Customs administration and if the site is not ready, the computer supplier will not be liable for delay in the installation date. Also, if site preparation is not in accordance with the supplier's environmental specifications and the differences are significant, the vendor will usually not install the computer system until site corrections have been completed.

Once installed, the computer will not be considered operational until a series of tests have been carried out to ensure that it performs at a satisfactory level for a stipulated period. This acceptance testing is a critical activity requiring highly skilled personnel. Unless such personnel exist within the administration it is advisable that the task be contracted to an independent consultant. Once the computer has passed the acceptance tests it is declared "operational".

5.5. IMPLEMENTATION OF THE SYSTEM

The system development process has now reached the point where the computer has been installed and programs have been written. The next phase of the process is "implementation". This is, in effect, composed of a number of activities or stages:

≡ System testing

≡ File conversion

≡ User training

≡ Changeover

5.5.1. SYSTEM TESTING

When the programmers have completed their work the programs and documentation will be handed over to the systems team for testing the technical part. The major objective of systems testing is to find and correct any bugs (faults) which may remain in the computer programs. Some faults may be due to misunderstandings between the analyst and the user or the analyst and the programmer. If many bugs are due to incorrect specification it is a sign that the investigation, analysis and design tasks were not carried out with sufficient care or thoroughness.

A plan and a work programme for systems testing should be draw up by the systems analyst and approved by the Project Committee. Where the system is being developed for Customs by external consultants, Customs staff must be fully involved to ensure that the system meets their needs. The test data, which have been prepared by the systems analyst during the system design phase, and which will simulate as closely as possible, actual operating conditions, will be processed by the computer. The results of testing the functional part will then be compared with the expected results and any discrepancies will be followed up until the results are clean and error-free. Even when all the systems tests have been carried out to everyone's satisfaction, it may still be necessary for further testing to be carried out in a live environment.

5.5.2. FILE CONVERSION

This is the task of converting manual files into computer files, in other words converting reference and other data e.g. the Customs tariff, into computer readable form. This is a major task.

Examples of the types of computer files that might be established in a Customs system are:

≡ Tariff file

≡ Quota file

≡ Currency file

≡ Country file

≡ Importer file

When these files are established they will require constant updating until the system goes live and must continue to be updated throughout the life of a system.

The process of file conversion will usually require the transcription of the source data into a suitable form for input to the computer. After the files have been set up they must be checked for accuracy since nothing can upset the start of a new system as much as bad master file data. This entire process, which is expensive and time consuming, should be planned carefully as it is critical to the success of the whole system.

5.5.3. User training

For any system to prove effective, the people who will operate the system must be adequately trained. The analogy of "the weakest link in the chain" is most appropriate here.

Training of users may be the responsibility of the systems team (where the system is developed in-house), it may be shared with the personnel department of the administration or it may be the responsibility of external consultants engaged to develop the system.

Two types of user instruction are required:

1. Education in computers generally.

2. Training in the use of the new system.

Where users have no previous automation experience, their general education should begin as early as possible (when the Feasibility Report is approved). Training on the use of the new system should be as late as possible so that new forms and techniques will not be forgotten before implementation. The recommended maximum duration between technical training and use of the skills is two weeks.

Training in the actual use of the new system should include:

≡ General overview of the system logic
≡ Completing input
≡ Interpretation of output
≡ Limitations and constraints of the system
≡ Action to be taken on receiving error indications
≡ Practice using test data and test files

5.5.4. CHANGEOVER STRATEGY

The system has been designed, programmed and tested, the files have been converted and user staff has been trained. It is now time for the system to be used in a live situation.

There are three basic strategies for changing over to live running:

1. Parallel running

2. Pilot running

3. Direct changeover

Parallel running is often the method of choice for a computer system that is replacing, in all essential functions, a manual paper-based system. The manual system continues to operate unchanged when the computer system is first installed. The output of the two systems is compared, item by item, until all discrepancies are resolved. This method is only possible if the two systems are identical in all major output, and if staff are available for carrying on the old system while at the same time preparing the input for the new one and checking the results.

Pilot running is often the preferred method if the new system is eventually to beinstalled in a number of different locations - as occurs very often in Customs. One typical location is chosen for the pilot run, where the data processing department, especially, the systems team can concentrate their resources until the system has been proved under real life conditions and all major problems have been solved. The system can then be progressively introduced in other locations.

Direct changeover is the only alternative, if none of the other methods are suitable, to end the old system the one day and begin the new one the next. If this is to be successful, there are two prerequisites. The first is that the computer system has been very thoroughly tested before being allowed to operate on live data. The second is that there are plans for what to do if the new system fails. This may include such precautions as keeping copies of input data, listing all master files at each update, and retaining staff in the user department until the new system is proved to be reliable.

There are advantages and disadvantages with each approach. While the cost of user effort and systems effort for direct changeover is usually very low the consequences of failure can be catastrophic. The risk of failure with parallel running and pilot running is considerably lower, but both methods require more system and user effort. It may be advisable, when implementing a large system to implement it by parallel running at a single pilot location. This is probably the safest option in a sensitive area where the cost of failure could be high. Parallel and pilot running offer a low risk opportunity for testing those parts of the system which have not been tested already viz. the operator's procedures, data preparation procedures, user department procedures, etc. These procedures will have been set out in operator and user manuals by the systems analyst during the design of the system and will need to be tested under live operating conditions. When the new system (both computer and manual sub-systems) has operated satisfactorily for a reasonable period the Steering Committee will give the instruction to discontinue the old manual system.

5.6. POST-IMPLEMENTATION EVALUATION

(Transitional Standards 7.1)

A post-implementation evaluation is an essential follow-up to any computerisation project. The main reasons for conducting such evaluations are:

≡ to determine how far the automated system has achieved its intended objectives

≡ to ensure that the expected tangible and intangible benefits have been realised;

≡ to compare actual costs and benefits with those projected at the Feasibility Study stage;

≡ to identify any weaknesses in the system and recommend any necessary improvements.

Post-implementation evaluation is a vital element in effective project control. It provides Customs management with an independent justification of development costs together with a related certification of benefits realised.

Post-implementation evaluations are usually conducted on behalf of the computer Steering Committee by the Project Committee although, in some instances, an independent evaluation team may be engaged or the task may be carried out by some other Government Agency, such as the Ministry of Finance or the Treasury, that may require formal justification for the expenditure of resources. Typically, a post-implementation evaluation should becarried out approximately 6-9 months after the system has gone live. This gives sufficient opportunity for any teething troubles to be sorted out and for users to become accustomed to the changed procedures. Such evaluations should not be confined to a single occasion but should be repeated at 2-3 year intervals so that the operation of the system is kept under constant review.

Although minor design changes, improvements or adaptations can sometimes be recommended following post implementation evaluation, it is rare for projects to be abandoned or fundamentally changed unless the planning and control mechanisms have not been implemented properly.

Certain problems may be encountered during evaluation, which may make the evaluator's task more difficult. Firstly there is often a lack of proper, well-documented historic data about the old manual system against which the performance of the new systems can be measured. Some information about the manual system will be contained in the Feasibility Study Report but this is frequently inadequate. Another difficulty may arise from user's unrealistic expectations of the new system. If not properly educated in computing basics, users may sometimes believe that computers can solve all their problems at the push of a button. This rarely happens in reality. Changing user requirements may also cause difficulties. Users sometimes fail to appreciate that the computer system can only be designed on the basis of the situation as it exists at the time. If the requirements change,then computer system must be changed or redesigned.

A further problem often arises regarding the quantification of certain benefits of the system. For example, it would be difficult to quantify the benefit of Customs computerisation to the economy of a country as a whole even though it is safe to assume that some benefit will accrue. Finally, where the system is being assessed by an independent evaluator who is not part of the Customs administration, a problem may arise from lack of familiarity with the functional area under review. This can sometimes lead to misunderstandings and care should be taken that no errors of fact are contained in the evaluator's report.

In spite of the difficulties, a post-implementation evaluation brings a number of benefits. Firstly, it gives users a chance to air their views on the system and to state whether or not their needs are being met. If they have justified criticisms, the evaluator's report will provide abasis from which to rectify any shortcomings of the system. It will also provide an opportunityto examine the merits of future enhancements to the system and to assess priorities for future developments. Finally, it will provide an independent justification for development costs.

5.7. System maintenance

5.7.1. Reasons for maintenance

Nothing is permanent, especially when it comes to computers or computer systems. Changes will be required from the first day of operation. Possible reasons include:

* Previously undetected bugs are inevitable. Even if a system has been running smoothly for a number of years, there is no guarantee that no bugs exist. It could be that the particular combination of circumstances, that will bring the bug to light, just have not occurred yet. There may be a bug in year-end routines, which takes 12 months to show itself. In a new system some bugs are bound to show up for the first few cycles.

* After running and observing the system in live operation a few times, systems staff or the computer operator may be able to suggest changes to make it run faster and more cheaply. The user may find, in the light of actual practice, that forms and procedures could be improved, to make them easier to use.

* The most radical change would be the acquisition of a new and different computer, in which event a system may have to be rewritten. It is more likely that it will make sense to change the system to take advantage of a new kind of peripheral, or a new software feature.

* Changes in the volume of transactions to be processed over and above those expected. These may require hardware upgrade.

* Legislative changes; for example changes in duty rates, tariff changes (the introduction of the Harmonised System will mean extensive changes to existing systems), new trade policy (quotas, restrictions), new taxes (such as VAT) at importation or exportation.

* Implementation of related systems, for example if an administration that is already operating and entry processing system wishes to introduce a cargo control system, the entry processing system will need to be partially redesigned to include the necessary interface.

5.7.2. Types of maintenance

Almost all system maintenance work can be described in terms of the following categories:

≡ Modifications (emergency or non-emergency) requiring no major change to the logic of the system.

≡ Revisions requiring new design and programming e.g. changes to input or output specifications - new input forms, new reports.

Redevelopment requiring new systems design and extensive programming and testing, e.g. major changes to the processing logic as a result of new requirements. It might be inappropriate to deal with this under "Maintenance" as such redevelopment should go through all the phases of a new project (from feasibility to implementation).

Even minor modifications to the system should be thoroughly tested before being released for live use.

5.7.3. Responsibility for Maintenance

Where Customs systems are developed by external consultants the contract for the system should specify maintenance support at least in the short term. Customs staff (from the IT Division) should work closely with the consultants during the project development in order to ensure that they are fully conversant with all aspects of the system. The IT Division will then be responsible for routine maintenance of the live system.

For more extensive redevelopment it may be necessary to engage external consultants once again unless the IT Division is, by then, sufficiently experienced and staffed to undertake the work.

Where Customs systems are developed in-house, the Customs IT Division will usually have sufficient knowledge and experience to maintain any system they have developed.

5.8. Set up of a Help Desk

5.8.1. Customs client service commitments

The idea of a helpdesk begins with a commitment to serving clients. Customs should declare its service commitments keeping in mind the limitations of its systems. Some administrations do publish their service commitments in their **Citizen's Charters**

Who are our Clients? It is fairly easy to identify customs clients. The importers, exporters, customs brokers, passengers and warehouse keepers, carriers etc obviouslycome to mind. However, a rigorous approach to identifying all parties that interact with Customs.

Service Requirements and Delivery Channels: Service requirements identification begins on the drawing board when the services are being modelled in the design-time. Some of the 'actors' in the use-case diagrams are the recipients of the service while there are others that are its producers. The client service requirements and the corresponding means of meeting these requirements can be captured in the use-case specifications.

For example, the importers, exporters and their agents/brokers seek information on the cargo logistics, release and other commercial information (service requirement), which they want to be delivered electronically (means of service delivery).

Service Areas and Service Requests: Customs have a large clientele and an equally large responsibility. It is therefore necessary to break-up the entire domain into ServiceAreas. Each Service Area would attract a usual list of 'Service Requests', which would haveto be mapped against "Assignees" who will process these Requests. Here are a few examples to illustrate this:

While import, export and transit could be different Service Areas; a delay or a problem in receiving a drawback claim would be a Service Request.

The IT infrastructure is usually supported though a helpdesk. The IT infrastructure comes into play for ensuring that the completion of a service delivery cycle (such the issue of a release notification against a client's declaration). The entire infrastructure can be divided into service areas each of which can be mapped to a Service Request.

Service standards and Service Commitments: It is fairly easy to identify service requirements when the standards of service are known/established. Standards of service are generally derived from the client's expectations. Service standards are usually the measurable parameters of the service offering - such as waiting time for a documentary examination or time for obtaining a refund. Others service standards are intangible - such as quality of information on the website and the courtesy extended by the Customs Inspector. However, all service standards are measurable behaviour of the individual, group and systems. It is often said that service standards drive the systems design. The converse is equally true. The established systems could limit the capabilities of customs to respond. For instance, a manual procedure cannot be expected to deliver as fast as an automated system.

.

5.8.2. Does Customs need a help desk?

All organizational models that contemplate remote service delivery require remote support resources. With the induction of IT into customs, most Customs administrations need a help desk of some magnitude. The kind of helpdesk (size and output characteristics)is determined by the estimates of the level of service demands and complaints. It is normally easy to estimate the requirements of client service by category. However, it is appreciated that service levels have a certain impact on the compliance behaviour of the clients. Can Help Desks increase the effectiveness of service delivery? Surely, an effective helpdesk would alter the client's perception of the service offerings.

The monopolistic position of Customs implies that it does not have "business retention" issues (unlike the normal business organizations). Our clients cannot be lost to competition. However, our effectiveness could enhance our client's productivity and increase confidence of the businesses in the operating environment. If a piece of equipment or a part of the network becomes inoperative, it could lead to loss of productivity. The help desk could formally track this loss in order to improve productivity of the asset base both for internal and external clients.

5.8.3. DIFFERENT ASPECTS OF HELP DESK

5.8.3.1. Helpdesk as the front-office:

The term 'help desk' refers to the concept of having a single point of interface within an organization to handle service requests. In every service set-up, there would be the 'front-stage' operations and the 'back-stage' operations. The back-stage is usually a complex web of operations involved in the creation and delivery of services and is normally not visible to the internal and external clients. To the clients, the consumption of services has to be madea pleasant and fulfilling experience. The help desk, being the first contact voice, is front stageof the service that captures client requests, translates them into technical and business problems for which solutions have to be found. Thereafter, the helpdesk chases the solution by peeping into the backstage to produce the output against the request and communicates this output to the client in a language that is familiar to the client. The helpdesk activity is productive if it can resolve and close the request to the client's satisfaction. The help desk is the friendly face, which spans the boundaries of the 'business process core' of the organization. In a way, it is a communications and knowledge transfer centre.

5.8.3.2. Service Encounters & 'Moments of Truth':

The Customs organization, as a tax collecting authority and an enforcement agency is not given to please. However, it does face its 'moments of truth' in the various points of contact with its clients in the day-today operations. These 'moments of truth' constitute the overall service experience of the client. It is within the powers of the help desk staff to produce and control the service experience and level of satisfaction of the service encounter.

5.8.3.3 Service Recovery

Indeed, as the customs organization launches its automated systems to enable its services to be accessed from a remote location by the members of the trade and its internal users, helpdesk is the first and last line of defence against service failure. In the event of a service failure, usually, it is beyond the helpdesk to deal with the situation and the senior management has to step in to carry out the damage control or 'service recovery' operations.

5.8.4. HELP DESK AS A VEHICLE OF VALUE DELIVERY

Like the nature of service itself, the worth or value of the helpdesk to Customs service delivery is also is hidden and intangible. It is difficult to measure, but linkages can be established with measurable factors such as (i) business continuity (ii) complaints (iii) preferences in service options (iv) improvements in cycle times (v) loss of productivity due to technical issues.

The efficacy of the helpdesk is integral to the image of Customs as an effective service. The relevant processes and functions that are related to helpdesk but are integral to service delivery are:

≡ Help desk & website are complementary: With the popularization of the Internet as a medium, it is the administration's communication tool of the first choice for developing the informed client. It is asynchronous – the client can use it at will and on his/ her own without having to speak to anybody. The helpdesk operations and processes should complement the website and be a part of the communications mix along with the web-content and other elements of the media/publicity plan. Help-desk is often the last line of defence in a service delivery strategy but could continuously add to the FAQs and “do-it-yourself” part of the service offering.

≡ Client self-learning: Very often, customs administrations have had to struggle while introducing new remote services such as EDI or remote filing. Regardless of the training inputs given and workshops organized to train the users, there are always initial errors that cause service failure. The self-learning by clients happens in cycles of continuous learning and improvement. Client self-learning is a goal and helpdesk an integral part of the strategy.

≡ Change management: Helpdesks can play a frontline role in change management. Technology and business process guidance in a changed scenario is a challenge. Whenever it is necessary to deploy new technology/business process, the helpdesk agents would remain the centrepieces in the strategic planning activity and the overall client assistance plan. The helpdesk could work proactively in orderto minimize service activation risks even as only tested service released. Helpdesks play an absolutely vital role in the building and testing of new services and the “release to production” event. Helpdesks are able to report gaps in the end-to-end service that may have been planned.

≡ Knowledge management: Helpdesk is both a knowledge acquisition facility as well as a solutions sounding board. If a question such as “Which are the top three irritants that the users face?” is floated through the helpdesk, the problems facing the services would be known immediately. The call management facility can handle the number and level of calls in different service areas. Requests can be categorized and “solutions that worked” can be documented in the helpdesk database. This could save time for helpdesk agents and Customs clients by direct access to solutions knowledge-base.

≡ Service levels management: While helpdesk is a critical part of service-levels reporting, it often works in conjunction with other tools and sources that gather information regarding service discontinuities. Very often, automated tools are deployed to monitor the availability of the ICT devices, services and processes. They come in handy in putting together, the big picture that depicts service levels.

5.8.5. HOW TO SET UP A HELP DESK?

A helpdesks requires five components:

(1) **The IT Component:** To activate the help desk, some IT components are required. These components enable the helpdesk agents to access information that is relevant in servicing the requests in a timely manner. Today, most hardware and software components provide a facility for remote monitoring. Additionally, there is a need for telephone lines with interactive voice response (IVR) in the front end, which would be backed by a call agent. To handle proper routing of calls and management of call volumes, there are a number of solutions available, which ensure the of the helpdesk agent’s productivity.These solutions are a mix of hardware and software. Calls are to be logged, resolved and monitored for effective resolution.

The Human Component: Providers of helpdesk service are personnel that would come in contact with the clients to deliver information and services. These resources can be from within the organization or they can be outsourced.

(2) **The Knowledge Component:** Information about the critical processes that contribute to service delivery cycles must be available remotely at the helpdesk. Incidents that can lead to service failure should be mapped on fishbone diagrams (*ichikawa* cause effect charts) and all causes of service failure that arise out of equipment and software failuremust be monitored and serviced remotely from the helpdesk. Over a period of time, call resolution cycles lead to the creation of a knowledge base of successful solutions, which could be made use of in future incidents of like nature.

(3) **A helpdesk model:** It is a common tendency for a helpdesk agent to pass the buck' to another section. Therefore, the help desk model must be based on the client service premise that users must have a single point of contact (SPOC) that understands the client's needs and service objectives (which should be documented). The client may have a business issue or a communication issue and the help desk should be able to handle both through a pre-defined menu of responses and interaction choreographies and escalation matrices.

5.8.6. HOW WELL IS THE HELP DESK DOING?

The performance of the helpdesk is very difficult to measure as we are dealing with several intangible and momentary events in remote service delivery. However, we need to measure the degree of success of the helpdesks. Objective and result-oriented metrics need to be developed to gauge the helpdesk success factors. Here is an illustration:

	METRIC	METHOD OF MEASUREMENT
.	Credibility, Sincerity & Politeness	Survey among Clients
.	Response times	Call sampling, call routing and monitoring
.	Call resolution times	➢ Number of calls/ incidents ➢ Number of resolutions ➢ Time spent on calls ➢ Number of unique clients handled ➢ Gross number of first contact resolutions ➢ From time-stamps in Call Management and call logging databases.
.	Call duration Vrs idle time	Same as above
.	Effective utilisation of client training opportunities	➢ Call agent reports ➢ Surveys among Clients
.	Promotion of client self-learning	Number of FAQs; reduction in calls on the subject.

5.8.7. IMPACT OF HELP DESK ON CUSTOMS OPERATIONS

There is a need to integrate the Client Assistance programs with the helpdesk as informed clients support and enhance voluntary compliance. A professional and structured client support service can improve the levels of compliance simply by making it that much more easy for the clients to comply. Clients would then know that they have a voice and that there is someone that listens to them. Technology today can bring all information to the client's desktop but the simple reality is that clients still want to contact and communicate with human beings that can empathise and resolve their issues. The concept of a help desk always follows the need to improve support and can be used as the cutting edge for change management.

6. OVERVIEW OF MAIN APPLICATION AREAS

(Standard 7.1)

6.1. INTRODUCTION

There are many areas in which the introduction of IC technology can benefit Customs. The following section outlines the principal Customs processes and procedures on which IT can have a very significant impact. . In addition, Customs may work closely with other cross-border regulatory Agencies in order to develop a Single Window solution. (Please refer to the WCO Compendium on 'How to Build a Single Window Environment'). The main functional areas are:

- Cargo Inventory Control;
- Goods Declaration Processing (import and export, transit, inward processing etc.) including pre-arrival/pre-departure processing
- Management of Licenses, Permits, Certificates & other types of
- Release Notification;
- Customs Enforcement;
- Selectivity(including risk assessment & targeting);;
- Advance Passenger Processing (Traveller Processes);
- Revenue Accounting;
- External Trade Statistics;
- Management Information Systems (MIS); and
- Reporting;
- Data Storage;
- Trader Partner registration &Management of Authorised Economic Operator(AEO) Programs
- Office Automation;
- Customs Intra- and Extra-net.

Ideally, a Customs automated system should be capable of performing all these functions. Some countries have implemented comprehensive systems of this type, but in many others only a few functions have been automated or automation is confined to a limited number of high-volume ports, airports, etc. Many of the applications listed have a bearing on other applications. For example, data captured from goods declarations in a goods declaration processing system might be used by a revenue accounting system to produce accounts and by an external trade statistics system to produce statistics. Similarly, information stored in an enforcement system could be used by a cargo inventory control system, a goods declaration processing system or a passenger processing system for Customs control purposes. In many cases systems share hardware (central processor, VDUs, printers, telecommunication network) and computer files.

It is not always feasible or practical to develop a comprehensive Customs computer system covering all processes and procedures at once. However, when a system is being designed, every aspect needs to be identified, including processes, databases, interactions between different processes and data. The system should be designed on a modular basis. This enables distinct parts of the system to be developed at different times and integrated with other parts or other systems, as necessary.

Regardless of the selection of application for the launch of an ICT system, care must be taken to ensure that international data standards must be used. In this regard, the WCO Data Model is the most useful resource. [‘Please see Appendix 18 for the ‘Recommendation of the Customs Co-operation Council concerning the use of the WCO Data Model’]

6.2. DATA VALIDATION

Computer systems must:

≡ identify and report critical errors; and

≡ identify and report possible errors (i.e. apply judgmental criteria to the data).

Errors can be detected at two stages:

≡ The first is at input. This is sometimes referred to as the data validation or vetting stage and normally deals with absolute errors;

≡ The second is at updating when, as well as detecting absolute errors, the system may perform some credibility checking using master file data for comparison purposes.

It is possible to combine these two stages but for this the master files must be on-line at data capture.

Typical input stage checks:

Type	**Explanation**	**Examples**
Presence	Checks that all the necessary or mandatory fields are present. This is especially important if there are optional fields whichmay become mandatory if certain other optional data are supplied	The “trading partner’s number” must be present if duty deferment is claimed
Size	Checks that the correct number of characters	If the field “tariff code number”

Type	Explanation	Examples
	is present in a field	has a fixed field length of 8 characters, then the data in this field will be rejected if there are not 8 characters present
Conformance check	Checks that numbers or codes are contained within the prescribed code-list	If a list of codes has been allocated in the range 7000-7999, then anything outside this would be rejected. Country of Origin must conform to ISO 3166 Country Codes.
Character check	Fields are checked to ensure they contain only the correct type of character	If the data element "country of origin" should be in two-character alpha format, the data will be rejected if any numeric characters are detected
Check-digits	This is a self-checking number created by a mathematical formula or algorithm often known as a modulus. It is used to identify either false numbers or numbers which have transcription or transposition errors.	A trading partner registration number can be checked for validity by subjecting it to the same calculation that createdthe original check-digit
Reasonableness	Before processing, quantities are checked to see if they are abnormally high or low.	Is it reasonable for a super-tanker carrying crude oil to declare 100 tonnes?

The following checks can be done at updating time:

New records	If a complete new record is being input to the master file, there will be a check to ensure there is no duplication.
Deleted records	If a record is marked for deletion, there will be a check to see if the record exists. If it does not an error will be signalled.
Consistency	Before a master file is amended, there will be a check to ensure that the new data are consistent with those already held on the master file. For example, when the payroll master file is updated with overtime payments, a check will be made to see if the employee is entitled to overtime pay.

Other checks known as credibility checks (reasonableness is one example), which rely on pre-set parameters, are used to determine the quality of the input. These are generally comparison checks which attempt to identify incompatible data (e.g. a ship sailing from New York is unlikely to discharge its cargo at Heathrow; price of a certain commodity from a particular country lower than expected, etc.).

When an error is discovered, the normal procedure is as follows. At input to thesystem, errors will cause rejection and will have to be corrected and re-input. Credibility checks are not always fatal and processing is usually allowed to continue but the situation is reported for further investigation before final acceptance or rejection. An automated monitoring sub-system may be included to ensure that reported errors are addressed withina specified time-scale. The system may also automatically reject or accept any reported errors not addressed within the specified time-scale and produce audit reports on errors and how they were resolved.

Proper data validation ensures data quality. The above information suggests that data validation is largely influenced by ‘data types’ being used to represent information. The WCO Data Model maximizes the use of codes and identifiers and discourages the use of ‘free-text’ type fields resulting improved data quality.

6.3. CARGO INVENTORY CONTROL

The control of cargo from time of arrival until duty has been paid or secured and the goods cleared presents many problems for administrations. Customs must ensure that all cargo arriving in its territory can be properly accounted for. The process of manually matching paper-based records for this purpose is cumbersome, error-prone and labour intensive. In an automated cargo control system, manifest data and Customs declaration data can be matched automatically. Data may be amended in order to record any overagesor shortfalls following Customs examination of the consignment. Cargo data may be screened against predetermined selectivity criteria in order to alert Customs officers to high- risk consignments. Following presentation of the goods declaration for the goods in question the computer will automatically write-off the cargo inventory record or produce a discrepancy report for follow-up action. Reports of cargo not entered within predetermined time limits are usually produced for further investigation.

In certain circumstances Customs do not maintain their own computerised cargo inventory control system but rely on the automated systems of carriers, port authorities, etc. Customs maintains control over such systems by means of supervisory audit. This approach to cargo inventory control can provide a cost-effective solution for Customs, particularly as the majority of carriers and port authorities are automated.

Accepting automated pre-arrival cargo manifest information into the Customs system enables Customs to make an initial risk assessment. In many cases, where the goods are low value or unrestricted, no further assessment may need to be carried out.

6.4. GOODS DECLARATION PROCESSING (IMPORT AND EXPORT) INCLUDINGPRE-ARRIVAL/PRE-DEPARTURE PROCESSING

(Transitional Standards 3.18 and 3.21)

The processing of goods declarations for import and export is one of the major tasks facing any Customs administration and many administrations have realised major productivity gains by automating this process.

Data can be captured in the following ways:

- keying of data by Customs officers;
- keying of data through Direct Trader Input, by trading partners or bureau services; and/or
- Reading barcodes , auto-identification devices and through optical character recognition (OCR)
-
- Other sensors and location aware devices
- using data transmission.

Once the goods declaration data have been entered into the computer system, they will be subjected to a number of processes. The core processes are:

≡ data validation (see 6.2 above);

≡ classification and origin;

≡ risk assessment & selectivity

≡ value control;

≡ duty calculations;

≡ duty collection (customs duties, VAT, excise, etc.)

The implementation of an integrated tariff database will enable any restrictions or preferences linked to the declaration to be quickly and accurately identified and ensure that the correct duty rates are applied.

The accurate valuation of goods, including national and international measures, is the basis for correct duty calculation. A valuation database with up-to-date data can be used to identify acceptable values for specific goods from particular countries. The database can also highlight valuations that fall outside acceptable ranges.

Once the duty has been calculated (including currency conversion), the information can be transmitted to the revenue accounting system.

During the course of this processing the user will be notified of any errors by system-generated messages and will have an opportunity to make corrections. He will also be notified of any supporting documents which may be required before the goods can becleared, e.g. licences, certificates of origin, etc. Instead of requesting for hardcopies of supporting documents, Customs could carry out online verification of information contained in the supporting documents and if that is not possible, supporting documents may be received electronically for automated verification. (Please see WCO Recommendation on Dematerialization of Supporting Documentation. Appendix 20.)

When Customs formalities are complete, the system produces a release note (see also 6.6). Where the cargo inventory control function is also automated, the cargo data and goods declaration data can be reconciled and the cargo inventory written off.

Goods declaration processing systems can also produce periodic reports for trading partners. These may show the amounts owing under deferred payment so that funds can be transferred electronically from the trading partner's account to Customs.

Accepting automated pre-arrival/pre-departure Customs declaration information allows Customs to carry out all the necessary processing, including accounting for duties in advance of the goods arriving physically in the Customs territory or, in the case of exports, the goods leaving the Customs territory. Any errors can be notified to the trading partner in advance, thus allowing corrections to be made and reducing potential release time delays.

6.4.1 Pre-arrival/pre-departure processing

Pre-arrival/pre-departure Customs declaration information is processed using the same routines as for goods declarations as described in Section 6.4.

Customs use information received in advance of the arrival of goods to take decisions related to the admissibility and release of goods.

6.4.2 Management of Licenses, Permits, Certificates other types of authorizations. (LPCOs)

A number of commodities are subject to regulation at import and export. In order to apply and manage these restrictions, authorities issue licenses, permits, certificates etc. These documents contain the description, categories, quantity or value of commodities that could imported or exported. The life-cycle processes of LPCOs can be managed effectively through ICT systems. These processes include the issue, utilization, cancellation and expiry of LPCOs. Handling the information contained in these types of documents electronically will help improve the management of cross-border controls including non-tariff restrictions. This application is especially important in the context of the Single Window approach as several other cross-border regulatory agencies are responsible for managing the life-cycle of the LPCOs.

6.5. DATA RECONCILIATION

For Customs, automated data reconciliation or matching is one of the most important system processes, for example, between cargo inventory control and goods declaration processing systems. Any discrepancies between the matched data can be highlighted and a report on over- or under-declarations generated.

Computerised data reconciliation techniques can also be applied to the Customs procedure of "temporary admission subject to re-exportation in the same state".

As part of the automation of the revenue accounting system, the reconciliation of actual duties owed, as extracted from the goods declaration information, can be matched against receipts to produce timely and accurate accounting information. Where drawback is concerned, the accounting system can be used to validate claims.

6.6. RELEASE NOTIFICATION

(Transitional Standard 6.9)

While goods declaration processing is definitely an area suitable for automation, electronic release notification can be implemented as a separate initiative. There is much to be gained by interfacing with existing automated release systems and capturing the release for distribution via the Internet or electronic mail to one or more trading partners. Moreover,an electronic release notification system can be implemented even if all the transactions are processed on paper. Electronic release notifications could also be shared through a suitable agreement with the warehouse operators who have the physical custody of goods. The timely distribution of electronic releases can bring benefits for both Customs and its trading partners, in terms of faster release times.

6.7. CUSTOMS ENFORCEMENT

(Transitional Standard 6.9)

The advantage of using ICT for control purposes is the ability to make information easily available to all authorised Customs officials. Automation opens up the possibility of accessing information held on databases maintained by other law enforcement agencies, such as police records, immigration files, etc. The application of ICT also allows Customs officials to assess various data, such as selectivity criteria, speedily and accurately, in orderto identify their usefulness and helps them to react quickly to changing circumstances. However, an optimum balance needs to be struck between the need to enforce regulations against non-compliant trading partners and, on the other hand, the need to ensure maximum transparency for the rest.

In ensuring compliance with Customs regulations, in order to make efficient use of scarce resources, Customs must employ selectivity and risk assessment techniques. While these techniques are not necessarily dependent on information technology for their implementation, they cannot really be applied efficiently and consistently without it. In an automated environment the same selectivity and risk assessment principles can be applied to both goods and persons.

6.8. SELECTIVITY

This is the process that will determine whether or not a particular consignment or person needs looking at more closely. In an automated environment four selectivity filters can be applied, namely international, national and local profiles and a random selection system. Targeting is a part of the selectivity process involving the selection for examination/audit of a certain consignment, passenger, means of transport, transaction or entity based on risk analysis, profiling, document review, observation and questioning techniques.

The first two of these are based on a system of profiles built up from the (international) Customs knowledge base and by using data analysis systems to assess the risk of loss and non-compliance. Artificial Intelligence and Expert systems such as pattern recognition can be of great help in supporting risk assessment and profiling policy. (The identification of risk and the typical data elements used in profiles are covered in detail in the WCO Guideline on Customs Control.)

The system designer should be aware that for building up a set of profiles the system needs to be flexible and capable of handling not only simple individual data elements but relatively complicated combinations of data elements as well. Using combinations allows Customs to fine-tune its targeting capabilities. Thus, Customs might, for example, only want to select a particular commodity if it comes from a particular country and not if it comes from any other country. Appendix 2 and Appendix 3, to this document outline the conceptual approach of a selectivity system.

The principal difference between international/national and local profiling is that international/national profiles are mandatory for all Customs offices whereas local profiles only concern a single Customs office or a small group of offices. However, information from local profiles should be used as part of the general risk analysis, and where appropriate, upgraded to national status. All profiles should be reviewed on a regular basis. For security purposes, steps should be taken to identify those authorised to change profiles, at both levels.

The random selection system uses an algorithm to select a declaration for further examination by Customs.

It is also important for the system to allow for monitoring of the co-ordinated interaction between the three levels of selectivity so that the overall target for examinations is not exceeded.

The system will also have to be designed to ensure that all the data go through the international/national profiles but only the declaration data relevant to a specific region or Customs office go through the local profiles for that region or office. Facilities are often included to enable profiles to be switched off temporarily by authorised managers.

6.8.1. Risk Management

Risk Management is fundamental to the effective targeting of consignments for examination. (Methodologies needed to conduct risk management are outlined in the WCO Risk Management Compendium).

.

Selectivity profiles are only as good as the information they contain. Regular review of profiles will tell Customs officials which data elements and combinations of data elements have successfully detected non-compliant declarations. Analysis of the declaration information itself will also afford clues to trends and identify potentially high-risk consignments.

Korea's *"Integrated Risk Management System": Overview*

Risk management based on information and communication technology is essential for coping with challenges from cross-border transactions. The Korea Customs Service (KCS) selects and inspects high-risk passengers, goods and transportation based on the results of risk analysis. The KCS has traditionally conducted risk analysis for post- audit on illegal transactions and tax evasion cases, and also established a Customs Data Warehouse (CDW) in 2002. The CDW collected data not just from Customs divisions but from other government agencies such as the Ministry of Justice, National Tax Service, Ministry of Foreign Affairs & Trade, and Ministry of Land, Transport and Maritime Affairs. From 2008 the KCS started to establish an Integrated Risk Management System (IRM) with a range of functions:

- automatic integration and segmentation of data;
- providing customized information (e.g. high,mid and field level);
- circulating information and screening criteria; and
- articulating risk factors using complex target selection indicators.

(Source: WCO Risk Management Compendium 2011)

6.9. ADVANCE PASSENGER INFORMATION

Advance Passenger Information (API) allows Customs to expedite passenger processing. In order to manage the iincreased volume of passengers and a diverse range of risks tomanage it is necessary to use ICT and advance information in order to allows border agencies to undertake pre-arrival risk assessment. API enables more intelligent and efficient methods to check passengers and their baggage - combined with other information it allows for **targeted intervention** The better data that border agencies receive - the more effective the intervention. The majority of passengers can be facilitated thereby reducing demand on border agencies, airport infrastructure and contributing to a better passenger experience.

The full benefits of API cannot be obtained nor can it be used efficiently without co-operation between the border control agencies (Customs, police, immigration) and the carriers (airline and shipping companies, etc.). The WCO/IATA/ICAO Guidelines on API specify the maximum data requirements Customs should request and the standards to be used. International standard messages that allow for the exchange of API data already exist.

Apart from Advance Passenger information (API), there are also potential advantagesof using Passenger Name Record (PNR) data in fighting drug trafficking and other serious transnational crime. PNR information is the generic name given to records created by the airlines for each flight a passenger books. PNR contains information provided by the passenger and information used by the airline for their operational purposes. PNR information may include elements of information that will also be reported under API. PNR provides basic information for all the different parties within the aviation industry (including travel agents, air carriers and handling agents at the airports) to recognise each passenger ina common format, and have access to all information relevant to his/her journey; departure and return flights, connecting flights (if any) and special services required on board the flight.

The application to process PNR information should take into account that fact that the amount and the nature of the information in a PNR record can vary from airline to airline and from passenger to passenger, often depending on how the reservation was made. The maximum data elements that can be included as part of PNR reporting requirements is described in ICAO Document 9944 (also called the *Guidelines on Passenger Name Record (PNR) Data*). The WCO IATA and ICAO have agreed on a standard for reporting PNR information. The standard message is called the 'PNRGOV' message and the relevant guidelines are jointlypublished by the WCO IATA and ICAO.

Several WCO members had reported instances of the successful use of API and PNR data in targeting passengers suspected to be involved in the illicit trafficking of drugs and other contraband, and in the smuggling of terrorism- related materials. Recognizing this, the WCO has adopted a Recommendation concerning the use of Advance Passenger Information (API) and Passenger Name Record (PNR) for efficient and effective Customs Control (Appendix 19).

6.10. REVENUE ACCOUNTING

For many Customs administrations revenue collection is one of their primary functions. Therefore the automation of the revenue accounting process is an essential part of any integrated Customs IT system. A revenue accounting system must:

≡ account for all duties collected exempted/foregone and refunded;

≡ provide a mechanism for the collection and refund of duties at the time of clearance;

≡ provide a mechanism for the deferment of duty payments for a specified period.

The application of a deferred payments system requires the establishment of a trading partner registration system. This controls the guarantees and identifies the revenues payable over a specified period of time. Details of a trading partner registration system are set out in section 6.13 of this document.

In a revenue accounting system the following tasks are ideally suited to the application of IT:

≡ automated control of duty security;

≡ maintenance of the trading partners' deferred payment accounts; and

≡ production of fast and accurate revenue accounts.

At the time of clearance, duty can be collected by accepting cash, cheques, bank drafts, credit cards and debit cards from the declarant and/or by using real-time electronic funds transfer (EFT) payment methods.

Customs must be able to reconcile the actual duties collected with the total duties calculated by the goods declaration system. Typically, the system should record the actual duty amounts collected for each transaction together with the Customs applied declaration number and the means of payment. Normally, the type of duty (excise, Customs duty, export tax, etc.) with the corresponding amount is also recorded, thus allowing the Customs authority to determine for each declaration how much duty is collected for each duty type.

The acceptance of payment cards means that Customs must install the necessary technology linking the Customs offices to the banking system, in order to validate the details on the card and ensure acceptance of the total duty amounts.

The application of a deferred payments system differs significantly from the collection of duty at the time of clearance. Such systems are based on maintaining individual accounting information for each approved declarant or trading partner. Normally, a maximum limit on deferred duty is agreed between the trading partner, Customs and the tradingpartner’s bank through the issuing of a guarantee. Details of this amount, together with details of each transaction (Customs declaration number and duty payable), are maintained on a database, which is linked to the trading partners registration system. Operating and maintaining a manual system requires extensive resources and is more open to fraud and error. Moreover, it is not practical to operate a manual deferred system on a national basis (i.e. one account per trading partner to cover transactions for every location). However, with the implementation of an automated revenue collection system, a national deferred payment system can be easily administered.

In an automated environment the latest deferred account balance is always available, whereas in a manual environment this cannot be guaranteed. Furthermore, in a manual environment there will always be a risk of the deferred duty amounts exceeding the guarantee. This could expose the Customs to revenue loss. An automated revenue accounting system, on the other hand, will not allow the trading partner to exceed the guarantee limit. If the duty amounts for a particular transaction are greater than the balance of the guarantee, the system will alert Customs.

Where information is exchanged electronically, the Customs system will send a response message to the trading partner indicating that duties cannot be deferred due to insufficient credit. The trading partner would normally be able to submit a request for information concerning the deferred account balance or a statement of the account.

When the duty becomes payable, the total amounts owed by each approved trading partner together with their bank account details (account number, branch sort code, etc.) should be transferred to the relevant bank. The question of agreement between Customs and the banks on the information exchange standard and the medium (EDI, tape, disc, Internet) will need to be addressed. International standard messages designed for use in the EDI environment are available for the transmission of payment information.

6.11. External trade statistics

As the declaration database will also be the primary source of external trade statistics data, these requirements will need to be considered during the database design phase.

6.12. Management Information Systems (MIS)

Once data is held electronically, it is can be analysed using proprietary software or programs written in-house. Before choosing one of these options it is essential to undertake an analysis of the types of queries and reports required. Data analysis tools can be used to do simple things like extracting every occurrence of a name or for complex processing like merging related pieces of data from various files to produce a report not otherwise readily available.

These techniques are of great value in enforcement and fraud investigations. However, MIS can also be used by management to ensure that resources are used efficiently. Reports can be produced on the number of declarations processed in a particular Customs office, the identification of peaks and troughs in the work flow, types of consignments, etc.

6.13. Reporting

In building a Customs automation system, administrations need to develop a facility that allows for the automated production of pre-formatted batch reports on a daily, weekly, monthly, or annual basis. It may also be useful to develop an ad-hoc reporting tool that allows staff and management to create their own reports. A well-designed reporting facility allows Customs to build its own reports based on the various types of data contained in the Customs systems.

6.14. DATA LIFE-CYCLE MANAGEMENT

Administrations need to take into consideration the legal requirement for storing data. Stored data can also facilitate the reporting system designed, as well as being useful for building risk assessment and enforcement tools.

There are many ways to store data, including on magnetic disks such as hard disks and on magnetic tape. New technologies also allow data to be stored on optical disks (CD and DVD).

6.14.1. DATA RETRIEVAL

A retrieval system allows Customs on-line access to historical entry data. Entry data that were keyed or transmitted by EDI can be viewed on line at the header/trailer, sub-headerand entry line levels. A good retrieval system will allow a user to view all versions of the entry data with the current version being displayed first.

6.14.2. DATA MINING

Data mining can best be described as a business intelligence technology that employs various techniques to extract comprehensible useful and hidden information from a population of the stored data.

Data mining makes it possible to discover hidden trends and patterns in large amounts of data and for that reason is very useful for risk assessment. The output can take the form of trends or patterns that are implicit in the stored data.

6.15. TRADING PARTNER REGISTRATION SYSTEM

Trading Partner Registration Systems are often developed as part of a deferred accounting system but can be used for other purposes, for example, to identify which special facilities the trading partner has been allocated by Customs. Such a system will typically hold basic trading partner details such as:

- trading partner unique registration number (common across all agencies, where possible);
- Trading partner rating
- trading partner details (name, address, telephone number, etc.);
- bank account details (bank name, address, account number);
- guarantee amount (the maximum monetary amount guaranteed by the trading partner’s bank);

- duty debit date (date when the duty should be debited from the trading partner's bank account);

- special Customs procedure facilities (periodic declarations, bonded warehouse, etc.);

- a list of relationships with a parent company and/or branches, where these exist.

The declarant will be required to quote the registration number on each declaration. Then duty details can be matched against the correct deferred account or a particular facility or Customs procedure can be activated. Each individual account should hold the declaration number and date together with the total duty amount for the declaration. A running balance of the current guarantee amount should also be maintained.

The trading partner registration system should be accessible only by other Customs systems and in view of the significant privacy implications, Customs access should be strictly controlled with appropriate security and privileges.

6.16. CUSTOMS TRANSIT

The basic principle of Customs transit is to permit goods to move from one Customs office to another in the same Customs territory or another Custom territory without collecting the duties and taxes that may be applicable under the condition that all the requirements concerning Customs seals, time limits or security etc are met.

Electronic Data Interchange would improve efficiency and effectiveness of Customs Transit. Transit and transhipment movements can be more easily controlled in an automated environment. The declaration information can be captured at entry and matched and written-off when the goods leave the Customs territory. Basic validation and credibility checks are carried out on the data and a unique declaration number is allocated by the system. At the point of departure Customs access the original details using the unique declaration number.

The use of automation allows any incomplete or mismatched transit movements to be identified in a timelier and more efficient manner.

Transit control could benefit greatly from the exchange of information between Customs administrations. The timely sharing of such information would help to reduce the opportunities for transit fraud. The benefits of using IC Technology in national transit equally apply to international transit.

Currently there are on going developments concerning the use of EDI in the transit procedures. Two recent examples are the EC's New Computerised Transit System (NCTS) and the system being developed by the International Road Union the Safe TIR. A standard for electronic TIR (eTIR) has been developed by the UN/ECE.

6.17. OTHER APPLICATIONS

(Transitional Standards 9.3 and 9.4)

In addition to the application areas already mentioned, other Customs functions that can be automated include:

- the refund of Customs duties already paid (drawback);
- quota administration;
- administration of Customs fines, penalties, etc.;
- binding tariff information (BTI);
- classification decisions;
- warehousing,;
- clearing of declarations (manifest lines cleared by subsequent declarations, transport declarations cleared by arrival, etc.).
- human resource management applications

6.18. OFFICE AUTOMATION

Like all organisations, Customs must carry out a number of administrative functions. Office automation provides uniform support for the more general and routine office processes listed below:

Basic process	**Office process**	**Support**
Registration of letters, documents, etc.	Data registration Data collection	Database package Tracking software
Storage and distribution	Archives Retrieval Reproduction Word processing Verbal communication Electronic document management	Scanning/key word generator optical disk/database storage Key word search on optical disk/database access Electronic distribution using external e-mail, fax, production of optical disk, automatic printing on network printers Word processor Telephone
Communication and planning	Data communication	E-mail and electronic calendar, fax, telephone

Basic process	Office process	Support
Information usage	Information analysis Arithmetic functions	Query-tools spreadsheet
Presentation	Data presentation	GUI (Graphic User Interface) Integrated software packages

Office automation must include a balanced package of tools, selected to meet the requirements of the end user. It is important to introduce a standard office automation environment, normally consisting of, at least, a Graphical User Interface (GUI), a word processor, and a spreadsheet package.

The telephone as an IC technology tool can be of great value. More and more Customs administrations are introducing telephony infrastructures to support their program deliveryand provide their customers with answers to program-related questions. This is a valuable technological tool that can be introduced into a program without major costs to an administration.

6.19. CUSTOMS INTRA- AND EXTRA-NET

The emergence of internet technologies has also had an impact on the Customsservice itself. Customs is becoming increasingly part of the e-Government concept byoffering all its services to its customers through the Internet. e-Government is about internal as well as external communication and has great potential for significantly rationalising the dissemination of official information, both internally and externally. If implemented properly the concept of online Customs could significantly improve the service to traders and the general public. However, as with the introduction of information technology in general, the fullbenefits of an automated system can only be realised if the internal procedures and processes are reviewed and, where necessary, amended or even abolished prior to its implementation.

A Customs Internet web site with general public access will help the administration to facilitate access to, and dissemination of, Customs regulatory information in the public domain, particularly for travellers and participants in international trade. The web site will alsoensure that the relevant regulatory information is being made available to the public in a cost-effective and easily accessible manner.

An organisation-wide Intranet will ensure access to all systems from a single terminal (PC) and central access management for all relevant tools and databases. The Intranet, where all the information and documentation received and prepared by the organisation is electronically available, will reduce the paper flow and paper storage requirements and improve the internal workflow.

In 1999, the WCO Council adopted a Recommendation on the use of the World Wide Web for Customs. This was a very important first step in the process of encouraging Customs administrations to get on-line (see Appendix 10). As of November 2003, the WCO web site had established links to more than 140 Customs administrations world-wide.

7. OUTSOURCING IN CUSTOMS

7.1. OVERVIEW

Outsourcing occurs when an organisation purchases products or services or delegates some of its functions to an external entity, rather than performing the same work within its own facility. Such entities are usually specialists for such outsourced service or product or activity.

7.1.1. OUTSOURCING, OFF-SHORING AND IN-SOURCING

Off-shoring is another term used in the context of outsourcing, when the activity identified for outsourcing, is performed in another country. Outsourcing can be done within aswell as outside the country.

Any function that is not a core competency could be sourced to others that have such competencies. Sometimes, in order to prevent loss of control of an activity, organisations induct external resources on a contract basis that then become part of the team. The objective in such a situation is to use the skills of the external resource who, while not on the department's payroll, is likely to share the department's values and culture and will be deeply involved on a day-to-day basis. Such activity is called in-sourcing, which is different from outsourcing. It is commonly held that activities or services that are outsourced should not have a strategic value to the organisation and to attract competencies that have strategic importance, in-sourcing is a better idea.

7.1.2. THE GROWTH IN OUTSOURCING

The growth in outsourcing in recent years is partly the result of a general shift in business philosophy, prompted in good measure, amongst other things, by the advent and use of Information and Communication Technology and the need for an 'IT specialist' who may not be part of the main or primary function of the organisation.

Consequently organisations have tried to identify a "core competence", a unique combination of experience and expertise that relate to the main business of the organisation.

All operational aspects of the organisation are aligned around the core functions and any activity or functions that are not necessary to sustain the core business are then outsourced.

Today, outsourcing is embraced not only by industries and companies but has also entered the field of government business.

The functions of an organisation can be outsourced either entirely or selectively. Total outsourcing may involve dismantling entire departments or divisions and transferring the complete responsibility for a product or service or function to an outside vendor. Selective outsourcing on the other hand may target a single task or function, for which better skills exist outside the organisation and can therefore be handled more efficiently by an outside specialist.

The decision to outsource is a strategic one as it impacts the organisational design and identifies the basic organisational choice of the functions for which internal expertise is developed and nurtured and those for which such expertise is purchased. The reasons for outsourcing may not only include reduction of costs, but also re-orientation of resources to areas that are of prime concern of the organization and aligned with existing and core competencies. For non-core functions it makes business sense to utilise better skilledhuman resources available outside the organisation in the interest of effectiveness andefficiency.

In fact, it is said that the real benefit comes from being able to redeploy the resources functions of higher value to Customs and perhaps by focusing on the core competencies of Customs officers

7.2. Outsourcing in Customs: Potential Areas of Outsourcing: Core versus Non-core Activities

The role of Customs in International Trade has been an evolving one. Increasingly global trade relies upon the rapid movement of goods and service across borders. Trade facilitation is seen as an important element of a country’s economic policy.

Use of advances in Information and Communication Technology allows business processes to be rearranged in a flexible manner. Trade expects better services with the ability to conduct businesses from their offices.

Customs plays a pivotal role in the International Supply Chain. The need to reduce transaction costs and just in time inventory management, so as to ensure competitiveness, is increasingly expected from Customs. Customs has to fulfil these expectations through delivery of services in a timely, efficient manner.

In recent years, the growing emphasis on the need for security and for ensuring secure trade has compelled Customs to redefine its ways of conducting business. Customs therefore have to evolve a methodology not only to meet the divergent demands of enforcement and facilitation in a most cost effective manner, but also to deliver quality, problem free service to the international trading community and ensure seamlessmovements of goods and service across borders. Customs’ role therefore has been enlarged to include that of a service provider.

While Customs is not expected to outsource its core functions relating to security, enforcement of restrictions and prohibitions, protection of society, collection of revenue; for the delivery mechanisms, outsourcing can be a supplement to in house capabilities. Most delivery of service entails use of ICT requiring the need of IT professional skills, which is not the area of Customs’ expertise. In fact outsourcing as an option becomes necessary where quality of service is paramount. Outsourcing in such a context not only ensures efficiency but also value additions for Trade. Some of the Customs’ activities which can be outsourced leaving customs to concentrate on its core functions could be the following:

a) Management & Operation of the Customs IT Infrastructure
b) Information dissemination
c) Website maintenance
d) Facilities Management
e) Application management and maintenance
f) Call Centre and Helpdesk services
g) Publicity and Public Relations
h) IT Security & Audit in the areas of security assessments, security policy and managed and monitored services and security of buildings

7.3. Benefits of Outsourcing

7.3.1. Back to core business

By outsourcing non core functions to an external entity, Customs can focus on its areas of core competence and fulfilment of its mandate to manage enforcement and facilitation. It enables use of knowledge and expertise not available in the department and contributes directly to the quality and efficiency of service that is expected by the international trade community.

7.3.2. Accountability

Outsourcing is predicated on the understanding -shared by business and vendor alike- that such arrangements require quality service in exchange for payment. This accountability, defined through service level agreements is both practical and legal, with financial implications. The same is not possible when the service is provided by internal resources.

7.3.3. Quality

By not committing internal resources to tasks for which in house skills are not available, issues of poor attitudes and poor performance are avoided.

7.4. Challenges of Outsourcing

7.4.1. Quality of Service issues

In any situation where tasks or activities are outsourced, the danger of poor quality control is always present. This is particularly true if an activity is to be carried out both by Customs and the vendor and responsibilities are divided. Outsourcing works best when an activity, complete in itself is outsourced so that the responsibility rests with only one agency. More importantly, a vendor’s flexibility to quickly adapt to changes in law and procedure arising out of policy announcements affects both the delivery of service as well as the cost of service. The challenge lies in determining the sort of outsourcing relationship which will best meet needs and specifying it in terms of service level agreements.

Another important aspect of outsourcing, generally overlooked, is that the overall responsibility for the service delivered by the vendor remains with Customs. There is no abdication of responsibility simply because the task has been handed over to another agency. The vendor is providing the service to the clients on behalf of Customs and close involvement between Customs and the vendor is essential for maintenance of delivery standards. Regular performance assessment of the vendor has to be a recurring exercise.

7.4.2. Human Resources issues

There are arguments against outsourcing from a human resources perspective. There is a fear that outsourcing will result in a loss of institutional knowledge and decrease staff loyalty. Unless the outsourced service is a commodity -a regularly available, or an easily substitutable service- doing it within the organisation is preferable.

If human resources are key to the organisation's success there is every reason to invest in them. Investment in re-training of staff is worth more than the savings that will be generated out of reduced costs in outsourcing. Trained and aware human resources will keep alive the knowledge of operations within the organisation.

It is further argued that in-sourcing options could be considered where there is temporary unavailability of skills.

Both outsourcing and off-shoring also present a challenge from the point of view of the flight of jobs across national borders.

However, outsourcing can also reduce the workload on employees, particularly when Customs are constantly faced with an increase in responsibilities without an increase in human resources. By freeing the Customs' Officer from tedious tasks, more career development opportunities are possible

7.4.3. Security Issues:

Outsourcing of services creates flows of information and knowledge out of the organisation. Security concerns arise when sensitive client data or information is passed without authorisation in violation of domestic legislation. Protection of data and privacy may not be a violation of the same gravity in the offshore site. Theft of data could cause monetary harm to the client and may impose unacceptable legal liability to the outsourcing organisation, including outright fraud. Limiting access on information resources to the vendor poses a technical challenge. Compromises may lead to unacceptable harm to the organisation.

It is necessary that logical access to information be restricted to identified personnel and should be relative to their responsibilities. Appropriate controls need to be carefully calibrated to ensure access on a need-to-know basis i.e the principle of denial of access to all information unless absolutely for the performance of the vendor's personnel should be followed rigidly. Access to information also needs to be periodically monitored and audited.

7.5. Conclusion: Finding the right balance

With the constant increase in responsibilities, the constraints of costs and human resources, the need for specialized technical skills required to deliver quality service, and the opportunities presented by advances in Information Technology, outsourcing is the way for the future.

For successful outsourcing, it is necessary to define the Department's needs and to identify a vendor that can effectively integrate all the outsourced business functions so that there is no need to find individual vendors for each function.

Outsourcing should not be looked as merely a task delegated to an external entity but a mutually beneficial partnership, where both Customs and the vendor are involved on a day to day basis in ensuring delivery of services in terms of predetermined standards on a sustained basis.

The outsourcing contract should clearly define responsibilities and performance criteria, outline confidentiality rules and ownership rights to new ideas or technology. Service Level Agreements (SLAs) are one tangible measure of job performance. The contract should also include the means of severing the relationship if the service does not meet expectations

8. INTERFACES BETWEEN IT APPLICATIONS

Customs should develop information systems on the basis of an integrated information architecture that could consist of the following application sub-systems and relevant databases. When interfaces are developed within sub-systems operated by the Customs Administrations, it leads to a tighter integration between the various organizational functions. In order to build a Single Window environment for trade, it may be necessary to build interfaces with systems belonging to other government agencies concerned with cross-border regulatory controls. Systems interfaces may also be developed to support information exchange with other Customs administrations (eg under Globally Networked Customs.)

The following is a list of subsystems of an automated system in a Customs administration.

Application sub-systems:

≡ Import declaration processing system

≡ Export declaration processing system

≡ Transit declaration processing system

≡ Excise declaration processing system

≡ Excise movement and control system

≡ Drawback system

≡ Risk management system

≡ Enforcement system

These information systems support the basic Customs procedures for goodsprocessing. Interfaces are needed to enable them to communicate with each other. For example, transit systems need interfaces with the export and import systems.

Administration databases

≡ Trading partner registration database
This database may consist of trading partner data, guarantees given - for what purpose, up to what amount, by which bank – and special Customs arrangements, such as simplified procedures

≡ Integrated tariff database (nomenclature)
Including national and international measures

≡ Revenue accounting database

≡ Selectivity database

≡ Declaration databases

≡ Deferred payment database

The information architecture should guarantee the common use of stored data within Customs. Each database may be used by several application sub-systems.

For the purposes of database management it is recommended that data which are closely related to each other be stored in a single database. This means that the primary data and the relevant management data should be stored in the same administration database, wherever possible. The identification of data relationships and data organisation should be part of the initial systems analysis.

It is recommended that in developing information systems the logistical part of the Customs procedures (processing) be separated from the data relating to the Customs application (files, databases). This facilitates the re-use of functional components and makes the maintenance of the information systems more efficient and effective. Appendix 4 gives an example of the relationships between some of the main processes and databases.

In a Single Window environment interfaces are often to connect Customs systems with those operated by other government agencies. (Please refer to the WCO Compendium on How to Build a Single Window Environment). Electronic interfaces could also be built in order to communicate with other customs administrations. For an initial description of GNC please refer to Section 9.3.

8.1. Service Oriented Architecture

The ease with which different applications are developed and integrated depends on the way in which they were constructed and assembled. Each application or module supports a set of services to perform core regulatory functions of import export & transit and trade facilitation.

Service-Oriented Architecture (SOA) begins with a strong focus on the business services. It is does not focus on the technical infrastructure (servers, storage etc) and its associated technical services. SOA is an architectural approach and is technology neutral. This architectural approach is strongly rooted in business services and therefore it is a reasonable choice for architecting IT solutions where different application components are to be integrated.

Service Oriented Architecture can facilitate the implementation of change in information systems, as well as link-up different modules or functionality. Traditional IT systems were pieced together by rigidly integrating hardware, software and networking making it difficult to implement. Service Oriented Architecture advises the building of software applications using components that are easy to assemble and build. These building blocks are not pieces of software but are business services that are performed in order to fulfil business needs. Commonly used services can be re-assembled to create new services. Organization for the Advancement of Structured Information Standards (OASIS) developed a standard Reference Model for Service Oriented Architecture (OASIS Technical Committee on SOA, 2006).

The concept of re-usable service components is extremely useful. In spite of differences in areas of regulation, most cross-border regulatory agencies require common business services. These relate to inspection of cargo, crew and means of transport, documentary examination, recording of test results, drawing of samples, computation of duties and taxes, risk assessment framework etc. These service components are re-usable firstly in the sense of business operations and then in the sense of the underlying software service components. While the subject of inspection may vary between government agencies, the stages of process are the same, while the parameters for calculation of duties, taxes and fee may vary, they are all linked to the process of levy and collection. Payment services can be abstracted into utilities that can service all payments arising in the course of cargo clearance.

The Information Technology (IT) components that underpin the reusable services are building blocks that are loosely coupled. This enables re-use of the component. Such loose coupling minimizes the impact of change. Service Oriented Architecture relies upon common parlance use of terms. Where the service consumer (being a software component) requests for a service from a service provider (another software component). The exchange service request and service response is driven by messages and the quality of service is governed by service contracts between the interacting service components.

These characteristics require a ‘service’ to be a self-contained unit whose performance does not depend on the state of other services. It is a logical encapsulation of self-contained business functionality. This autonomous nature of a service component allows software developers to remove it, make changes and plug it back without impacting other components. Services can be orchestrated. This implies that services can be rearranged or re-ordered to suit business purpose. This is of considerable value in handling business processes in a Single Window environment.

A service communicates with another service using messages. For services to be working together, messages should be interoperable and should operate across platforms. These messages should be able to describe and discover services. These should be reliable and secure and based on industry standards.

One way of achieving interface between different existing applications is to modifythem to be part of a Service Oriented Architecture (SOA). This is called “SOA Enablement”. Itis recommended for building the integration between applications.

9. INFORMATION EXCHANGE

(Standards 3.11, ~~and~~ 7.2 and 7.4)

The key to trade facilitation and an efficient global trading system is an interconnected electronic data exchange environment. The imperatives of economic growth and expansion, combined with the emergence of new approaches to security and environmental protection, call for more efficiency in how we deal with trade transactions. Customs administrations and other regulatory authorities should~~must~~(NZ, TH) therefore minimize cross-border trade constraints via the use of modern information and communication (NZ) technology and application of uniform global standards. Over the years, however, there has been little co-ordination in the development of automated systems. As a result, thousands of pieces of data in hundreds of different formats have created barriers to international trade. An average international trade transaction involves 27 to 30 different parties, and some 40 documents with 200 data elements – of which about 30 are repeated and 60-70% are re-keyed at least once. To address such issues, the WCO Data Model, among other international instruments and standards, is one of the key solutions for achieving optimized electronic data exchange, providing a global standard for cross-border data requirements needed for the release and clearance of goods, and helping administrations conform to international standards. Use of the Data Model as the international data exchange standard could potentially result in significant savings in costs and time for governments and trade.

9.1. INFORMATION EXCHANGE WITH TRADING PARTNERS

The idea information exchange between Customs and it trading partners has now evolved into the ‘Single Window’ approach. In recent times, Single Window to international trade and cross-border regulatory exchange has gained prominence. The Single Window concept deals with regulatory controls through the eyes of the trader and views all interactions between trade and regulatory agencies without regard for the internal divisions within government. This approach clearly brings out all the procedural redundancies, duplication in the filing of information and the wastefulness involved in the overall effort in fulfilling cross-border regulation. From this analytical approach arise a set of solutions that greatly simplify government-trade interface by reorienting procedures and reorganizing regulatory data requirements.

There are different types of interaction between Customs and its trading partners. However, the principal information exchanges between Customs and its trading partners relate to the importation and exportation of goods.

There exist a number of standard ways to arrange electronic information into computer files. This is referred to as syntax standards. The most commonly used syntax standards is called UN/EDIFACT, United Nations Directories for Electronic Data Interchange for Administration, Commerce and Transport. XML (extensible Markup Language) has grown in usage since the growth of internet technologies. There are regional and industry-sector standards such as ‘ANSI X.12’ and ‘CargoIMP’. Also prevalent are non-standard proprietary message syntaxes. Proprietary syntaxes are considered costly since would require industry to allocate fresh resources to understand and use it.

From ancient times, Customs have applied cross-border controls by requiring and using facts about transportation, cargo handling, supply chain locations, goods items, packaging, inspection, valuation, duties & taxes etc. Despite remarkable growth of technology, and innovations in Customs procedures and business processes, Customs continues to deal with more or less the same basic business information. These pieces of information have been captured systematically in the WCO Data Model.

The WCO Data Model is a set of carefully combined data requirements that are mutually supportive and which will be updated on a regular basis to meet the procedural and legal needs of cross-border regulatory agencies such as Customs controlling export, import and transit transactions. The instrument is developed and maintained by the WCO Data Model Project Team and is promoted through partnerships with WCO Members, InternationalOrganizations and the Private Sector.

The WCO Data Model presented as a library having two main parts. The first part is a collection of standard components. The second part is a collection of 'Information Packages'. Information Packages are built using data model components and represent the usage of data in business processes Information Packages provide electronic templates for information exchange. They can also be used to illustrated business functions. Appendix 1- Information and Telecommunications Structures for Electronic Commerce describes Information Packages in detail.

(Components 1 and 2: Flexibility in declaring/acquiring data for Customs processes/procedures and data quality, Concept No. 7, Data Issues, Proponents: EU, IN and UG)

[Within the scope of information exchange, and in line with the principles governing it, Customs should endeavour to acquire data **[at the earliest possible stage without compromising the data quality (IN)** ~~**earliest possible stage in the supply chain**~~**]** from a wide range of relevant sources, economic operators, and traders, such as e-platforms, vendors, intermediaries, etc. In addition, Customs should aim to acquire data from cross-border regulatory agencies via the Single Window environment. It is important, however, that re-use of data be considered where possible instead of repeatedly seeking the same information from economic operators and trading partners.]

9.2. INFORMATION EXCHANGE WITH OTHER GOVERNMENT AGENCIES

(Standard 7.4)

Many kinds of data flow between Customs and other Cross-border Regulatory Agencies (CBRAs), for example, trade statistics and information on quantitative quotas, restrictions, preference agreements, etc. Where government offices cannot be co-located, computer interfaces can reduce delays in exchanging information.

Where trading partners can electronically submit import/export licences, sanitary/phytosanitary certificates, etc. issued by other agencies, the computer interface enables instantaneous communication of the approval of those permits to Customs.

A “Single Window” scenario for trading partners, with all regulatory data being transmitted once only to a single regulatory entry point, would expedite the clearance process for all consignments. However, to ensure the success of such a scenario the trading partners would have to have access to all the related regulatory requirement information and it would have to be exchanged electronically. Therefore, when designing IT systems, Customs should consider not only the interfaces with trading partners but also those with other government agencies.

The development of Customs/trading partner interfaces and Customs/government administration interfaces can be facilitated by using international standards for information exchange. If trading partners operate the same standards, the software costs associated with electronic information exchange will be considerably reduced.

To support capacity building efforts, the WCO has developed a Compendium on “How to Build a Single Window Environment”. The Compendium comes in two volumes. Volume 1, called the ‘Executive Guide’, deals with aspects of Single Window that are of concern to senior management. Volume 2 is called the Professional Practice Guide and is a collection oftools and techniques to support technical experts working on projects to establish a Single Window.

9.3. INFORMATION EXCHANGE WITH OTHER CUSTOMS ADMINISTRATIONS

(Standard 7.4)

Information and Communication Technology offers a Customs administration, ns to the capability of exchanging data with other Customs administrations.

The WCO Initiative on Globally Networked Customs (GNC) undertook a comprehensive analysis of the potential to rationalize, harmonize and standardize the secure and efficient exchange of information between Customs administration. connectivity', The analysis concluded that maximum benefits of Customs-to-Customs cooperation can be more effectively delivered by streamlining exchange of information processes which can benefit other stakeholders as well.

A standardized approach, using generic templates and blueprints, facilitates and enhances these processes by speeding up the drafting and implementation of information exchange agreements. In addition, the compilation of a catalogue of documented arrangements in a standardized form, each of which can be replicated with minimum effort, allows for the scope, growth and reach of Customs networks to accelerate.

At bilateral, multilateral, and plurilateral levels, Customs administrations would continue to work toward arrangements and agreements that fully allow for sharing of information in the most effective way possible. Information exchange would follow two tracks
- one dealing with enforcement-related information and others dealing with information about commercial flows of cargo.

There is already a Customs Enforcement Network, which helps rapidly disseminate sensitive, non-nominal enforcement information. There are numerous examples of functioning bilateral and regional exchanges of information between multiple Customs administrations. The Globally Networked Customs initiative has used the concept of ‘Utility Block' to describe Customs-to-Customs information exchange.

A Utility Block is a specific part of the Customs business process, explained in simple yet comprehensive terms covering describes strategic aims for policy makers, business processes for managers, legal issues for lawyers, functional approaches for operational staff, and technical specifications for Information and Communications Technology specifications. Utility block is constructed and reviewed by experts using a standard development template. It focuses on the needs of a specific part of the Customs business process, includingrelevant data elements. For example, Authorized Economic Operator (AEO), commercial fraud, transit, etc.

Breaking down Customs business processes into individual Utility Blocks allows Customs authorities to be selective about what business process and associated information they choose to share with their partner(s), and to more quickly facilitate those networking arrangements. Sharing of advance information, mutual recognition of Authorised Economic Operators (AEOs), mutual recognition of controls, co-ordination of transit controls and cross-border sharing of one country's export cargo declaration to be used in the country of import are some of the examples of ‘Utility Blocks' under construction.

The use of the WCO UCR number for Customs could also be of great help in facilitating international information exchange (see Appendix 9). As the name suggests, this reference number would be carried right through the life-cycle of a transaction and would provide a unique key for the identification of that transaction by all the trading partners. Customs should consider making provision for this data field when designing their transaction databases.

International information exchange may raise certain legal and procedural issues which may need to be addressed. Administrations who embark on such projects should involve the relevant national legal experts at an early stage to ensure that any legislative changes required are introduced in good time.

(Components 1 and 2: Flexibility in declaring/acquiring data for Customs processes/procedures and data quality, Concept No. 7, Data Issues, Proponents: EU, IN and UG)

9.4. Data Quality

Data quality remains a challenge for both Customs administrations and the private sector. Improvement of data quality underpins the concept of balancing improved supply chain security and greater trade facilitation. Automation is one of the keys to improving data quality, and its implementation should be a priority for all stakeholders. Additionally, the WCO Council has adopted a Recommendation on the Guiding Principles for Data Quality (June 2015). The WCO has also developed a list of acceptable and unacceptable goods descriptions that provides consistent language which can help to improve data quality.

Customs administrations should work with stakeholders and other relevant government agencies, as appropriate, to improve the timeliness, completeness and accuracy of data, with a view to supporting robust and effective risk management techniques and facilitating legitimate trade.

Cross Border Regulatory Agencies (CBRAs) have adopted a variety of ways of measuring and assessing data in terms of its quality, requiring that the data be accurate, timely, and complete. [For example, the Advance Passenger Information (API) should~~must~~ accurately reflect the data in the passenger's official travel document. The API must be provided to the CBRAs within the required timeframe.] (JP)

Legislation and guidance should be in place for clarity of understanding between the CBRAs and stakeholders. Constructive engagement with industry and/or trading partners is essential. There should be a common understanding and clarity between stakeholders regarding the definition and scope of data to be exchanged and the list of expected data elements. In the area of API, initiatives are being explored to increase the accuracy of API through the use of Radio Frequency Identification (RFID) chip readers within smartphone applications, digital travel credentials, and other uses of biometrics and verified identities.

Commented [PD1]: 31st RKC/MC Meeting:

JP: subject to further discussion and suggested to consider a better alternate example.

Further suggested that the new updates relating to Data Quality covered under Concept 7 as well as under ACI concept need to be reviewed together and consider as to how it can updated in both the Chapters in terms of specificity and general context.

10. COMMUNICATIONS

(Standard 7.2)

Customs engaged in the process of introducing an electronic information exchange system should recognise that success will depend on its availability and accessibility. This can only be guaranteed through the use of fully recognised international standards at all appropriate levels of system development. There are four areas of interest relating to international standards.

10.1. DATA TRANSFER OPTIONS

There are three main data transfer options:

1. physical delivery of magnetic media such as tapes and disks via postal/courier services;

2. point-to-point data transmission;

3. communication networks, which provide store and forward and other value-added services.

Tape/disk

This method is slow as it requires the media to be physically exchanged by post, or by the trading partner calling at the Customs office. Media exchange can be seen as the first step toward the implementation of EC. International standard messages, as outlined in the WCO Customs Data Model, can still be used. Implementing such a system can give Customs and its trading partners valuable practical experience in the application of electroniccommerce.

Point-to-point

Modems are used to connect two computers over telephone lines or satellite links so that they can communicate. Traditional telephone lines are intended for voice rather than for computer communications. Consequently, modems and telecommunications software are required before information can be exchanged.

If dedicated leased lines are used instead of regular dial-up telephone lines, the sending and receiving computers may use a communications controller instead of a modem. The essential difference between having a dial-up line and a leased line is speed. Dial-uphas a much slower transfer rate, which makes it suitable for low-volume use only.

Communication networks

The typical scenario for a communication network is for each of the trading partners wishing to exchange information to have an electronic mailbox, managed by thecommunication network. Electronic messages are transmitted over the communication network from mailbox to mailbox. This means that, unlike point-to-point, where both systems have to be available and open to receive data at the same time, the transmission and temporary storage of information is separated from the application system. If for some reason the Customs system is not operational, trading partners can continue to send information to the Customs mailbox.

A Value Added Network (VAN) is a third-party communication network that can accept a message from any computer hardware and software configuration and deliver the message to a receiver that uses different hardware and software. A VAN can provide not only communication services but also EDI translation and security services. Most VANs cansupport a wide range of communications protocols. Since the technology of communications and protocol conversion can become extremely complex, a VAN offers a true value-added service by handling this aspect of the communications between pairs of trading partners, or within groups of trading partners, with dissimilar computer configurations.

Customs will need to examine the most effective ways in which to receive information. Many countries lack VAN services but do have Internet services. These tend to be cheaper than VANs but for the time being there are security implications and service-level concerns to be considered.

Apart from Value Added Networks, Administrations are already turning to the Internet as the primary medium of exchanging information.

10.2. TELECOMMUNICATIONS

At the telecommunications level, Customs needs to ensure that the protocols used for physical connectivity are recognised ones, such as International Standards Organization (ISO) X21, X25, X400, etc. Standards also exist for Internet protocols such as TCP/IP and Hyper Text Transport Protocol (HTTP). Telecommunication service providers, VANs and Internet service providers generally apply these standards. .

10.3. MESSAGING

(Standards 3.11 and 7.2)

The issue of electronic information standards is one on which Customs has been able to exert a more direct influence. For a number of years Customs has been engaged in the development of electronic message standards through the United Nations. These UN/EDIFACT messages have become the international standard used in EDI. The WCO has developed the WCO Data Model. The WCO Data Model has been optimized electronic data exchange. It is a universal language for cross-border data exchange. It provides a global standard for cross-border data requirements needed for the release and clearance of goods, containers, means of transport and people;

UN/EDIFACT and other EDI messages can be sent over the Internet as attachments to standard Internet e-mail using Simple Mail Transfer Protocol (SMTP). These e-mails can be secured through digital signatures using Secure/Multipurpose Internet Mail Extensions (S/MIME).

The development and rapid expansion of the Internet has opened up new possibilities for information exchange. Consequently, new information exchange formats will become de facto international standards through global use, for example, electronic forms, hypertext mark-up language (HTML), eXtensible Markup Language (XML) and a global repository, open document architecture (ODA), etc. While many of these are still under development, Customs looking at future electronic information exchange will need to take these formatsinto account in their business strategies.

The Internet enables SMEs to inquire about the goods status and/or the status of their goods declaration at Customs, while creating opportunities for e-pay and the archiving of electronic documents.

Electronic Data Interchange (EDI) is a set of electronic data exchange protocols for conducting structured inter-organization exchanges. The original standards defined the method for packaging the UN/EDIFACT transactions sets in a MIME envelope. However, with the growth of internet, and the demand for vendor-neutral, inter-operable services new standards were developed called EDIINT (EDI- Internet Integration) with focus on security issues such as message privacy, authenticity, integrity and non-repudiation. The internet Engineering Task Force managed the development of these standards, which initially emerged as Request for Comment (RFC) documents containing 'Applicability Statements'.

AS1 - Applicability Statement that describes how EDI messaging can be delivered on the Internet standards for MIME and SMTP. Messaging is secured through digital signatures and encryption of exchanged information. AS1 allows for secure internet-based exchanges.

AS2 - Applicability Statement that describes how EDI Messaging can be delivered in real-time using exchange of information between to process of web-based HTTP and MIME. This method uses digital signature of exchanged data, but both the session and the exchanged data files are encrypted. AS2 makes real-time secure exchange between web- based applications.

AS3 - Applicability Statement that describes how EDI or XML data can be transmitted over internet in a secure manner based on file transfer protocol (FTP). Security is achieved through encryption of the FTP session, encryption and signature of the exchanged data files.

Of late, a new AS4 standard has emerged that uses web services as the core messaging technique, while ensuring that the security features required for messaging on the internet are maintained as with AS2 and AS3.

----

11. ICT SECURITY

The business conducted by government and industry has changed dramatically over the past 10 years. Use of the Internet and community access to low-cost ICT is opening up systems to communication with a broader range of people with a growing knowledge of how to use and manipulate ICT.

While these changes have brought many benefits in terms of speed and access, they have also heightened awareness of the security risks to which our communications, our systems and our holdings are exposed.

The growing incidence of computer fraud and the possibility of systems being sabotaged or accidentally breaking down are some of the challenges that any administration employing ICT must face in managing its systems and associated business processes.Corruption or breach of Customs ICT systems can cause serious disruptions to trade and revenue collection. In more extreme circumstances they have the potential to compromise national security.

It is particularly important for Customs administrations to identify the risks and develop an integrated approach that addresses not only the physical and technical vulnerabilities but also the question of governance (i.e. procedures and business arrangements) needed to assure a high standard of ICT security.

Experts have advocated a risk management approach to managing information technology security risks. Customs administrations should obtain information and tools to help effectively identify and manage risks associated with their information & communication technology(ICT) assets. Risk assessment involves the identification of threat or vulnerability to ICT assets along estimation of of the likelihood and impact of a security breach. Competence in the assessment of risks to information security is key to management of information security. Risks can occur to IT assets through fire, flood, loss of access, cyber attacks, breach of access, data loss etc. A risk management approach helps identify these risks and prepare the organization to mitigate these risks and respond appropriately.

Information Security Management System (ISMS) is covered by ISO27001, which sets out the requirements of such a system. The standard has a specifies risk assessment to be carried out before any controls are selected and implemented. A risk management based approach has been elaborated in ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management. Every control must be justified by a risk assessment. The risk assessment, when carried out for each ICT asset within scope, enables budgeted countermeasures that are commensurate with the loss or harm that likelyto result from a breach of security on the asset. This principle of IT security management should be embodied in the IT security policy discussed in section 11.2 below.

The serious nature of security risks to ICT assets deserves the attention of higher management in customs as important legally protected data, information about transactions involving monetary implications and risks to national security, public health and safety. Customs cannot afford to lose or have such information exposed. Given the impact of breach or loss of information assets including loss of public confidence, the strategic management of risks to information security should be the responsibility of the executive management.

11.1. ICT SECURITY – DEFINITION AND GOAL

ISO 27000:2012 (*Information technology - code of practice for information security management*) defines Information Security as the

> "…preservation of confidentiality, integrity and availability of information"

where **confidentiality** is "ensuring information access only to those authorised"; **integrity** is about "safeguarding the accuracy and completeness of information and processing methods"; and **availability** ensures only "authorised users have access to information and associated assets".

11.2. ICT SECURITY POLICY

One way of achieving this goal is to publish an ICT security policy so as to ensure that every member of the staff is aware of the issues involved and of his or her personal responsibilities.

The policy should demonstrate the management's approach and commitment to ICT security and spell out what the administration expects of its staff. The roles, responsibilities and obligations of users should generally also be defined.

Although it is possible simply to inform clients of ICT policy, it may be more appropriate to develop user agreements that clearly set out the client's obligations and responsibilities.

However, the ICT security policy will not in itself deliver "confidence, integrity and availability". In any developed ICT installation, a complex set of procedures, technicalsolutions, legal requirements and policies, management processes and business considerations will be required to underpin the administration's general ICT security policy.

11.3. ICT SECURITY – CONSIDERATIONS

Note: For a more rigorous treatment ICT Security please refer to standard (Code of practice for information security controls or CoP: ISO/IEC FDIS 27002:2013).

ICT security covers all the following aspects of a Customs administration's activities:

≡ Organization of information security,

≡ Human resource security,

≡ Asset management

≡ Access control,

≡ Cryptography,

- Physical an environmental security,
- Operations security,
- communications security
- systems acquisition, development and maintenance,
- Supplier relationships,
- Information security incident management,
- Information security aspects of business continuity management (BCM)
- compliance.

These aspects are thoroughly covered by ISO 27002:2013 and it is recommended that Customs administrations carefully examine the considerations and explanations contained in that standard.

The following headings, drawn from ISO 27002:2013, will help to identify the broad areas that should be considered within any ICT security framework.

Organization of information security

Organisational security is the management framework for initiating and controlling security within the administration. It should cover the roles, responsibilities and the segregation of duties.

It involves both the establishment of an internal management infrastructure to assign and maintain security responsibilities and roles and the consideration of specific controls for the contact with authorities, for the contact with special interest groups and the information security in project management.. It also covers service providers, for example, outsourced ICT service provision..

The use of mobile devices and the ability of teleworking should be covered here.

Human resource security

Security clearances and staff training are important to assure an appropriate level of trust and sound practice. In addition, confidentiality agreements and specific terms and conditions of employment may need to be considered, depending on the nature of the information and the access that employees have to the system.

Compliance with security requirements should be assessed under procedures for monitoring and reporting security breaches.

This includes specific controls for the screening, the terms and conditions of employment, during employment, the management responsibilities and the awareness, education and training.

Asset management

To protect its ICT assets, including information holdings, the administration needs to have both a means of accounting for assets and information and a means of classifying them in order to establish appropriate levels of protection.

Assets may include both the physical infrastructure and the databases, files and software applications that may be housed in the physical assets. Each asset has to be determined the ownership, the acceptable use and the return. An Inventory of all assets is mandatory.

Information needs to be classified not only in terms of its security treatment but also in terms of its security rating. This rating will determine the protection afforded to the information (such as by whom and under what circumstances it may be viewed) and may even determine the types of physical assets (hardware, installations, etc.) in which it can be stored or through which it can be transmitted. The information should be labelled.

Media that contains information needs to be handled correctly. The management of removable media, the disposal and the physical transfer should be described.

Access control

Control over access to information is the key to establishing secure and trusted systems.

Access needs to be based on the administration's business requirements to ensure that only those with appropriate authority are able to view or transmit certain information. These requirements are generally documented as part of an “access control policy” which establishes the terms and criteria for determining access to systems and information.

In addition to the way in which access controls are to be administered, agencies will need to address:

≡ who is responsible for authorising access
≡ the rules governing the granting of access
≡ the levels and types of access to be made available, and
≡ the privileges associated with the various levels and types of access.

Access management rules may also be needed to decide such matters as the time that can elapse before an idle session is automatically closed, the preconditions for accessing areas of the system and even changes in permissions, which may be automatic or subject to management decision.

Network access controls and monitoring of access are also important because network connections can represent a significant risk to security. Important aspects of network access include the means by which:

≡ users are authenticated
≡ terminals and other entry points are identified and logged, and
≡ pathing of users is enforced.

A detailed discussion of the authentication of users and the options in common use can be found in Section 10.4 - Authentication.

The responsibilities of the user and the system and application access control should be covered in this section as well.

Cryptography

Cryptography should be proper and effective used to protect the confidentiality, authenticity, the integrity and the non-repudiation of information.

The use of cryptography should be described in a policy as well as the management of the cryptographic keys.

Physical and environmental security

In developing a physical and ICT security policy, it is essential to include any possible physical risks to which buildings housing ICT, the ICT equipment itself or the ICT working environment may be exposed.

Countermeasures may range from the establishment of perimeter security to security check points, clear desk and screen policies, power supply backup, secure cabling, security measures and procedures for off-site equipment. The selection and use of anycountermeasure will depend on the specific risks, the mix of equipment and the physical environment.

Operations security

To ensure that the Customs administration's processing facilities are properly secured, it is essential to establish appropriate procedures.

This covers a broad range of issues, including:

- documentation and application of operating procedures
- change management
- procedural measures needed to separate different ICT environments such as testing and production environments
- forward planning for capacity, acceptance of new systems or upgrades
- protection against malicious software
- housekeeping
- backup and
- logging and monitoring

Communications security

- network management and controls
- segregation in networks
- information transfer and agreements on information transfer
- electronic messaging

Further details concerning information and software exchange are provided in Section 10.4 – Authentication, which covers many of the factors that agencies need to analyse in order to assure the integrity of the information and establish the identity of the communicators.

Systems acquisition, development and maintenance

Security should be intrinsic to systems design. This includes infrastructure, business applications and supporting business procedures.

When changing, selecting or accepting software, precautions include avoiding covert channels (a hidden "access door" that would allow unauthorised access) and Trojan codes. Access control for code changes, use of trusted suppliers, code inspection and product testing are just some of the possible strategies. Ensure that data for testing is accurately protected.

Supplier relationships

The relationships to the suppliers should regard the following:

- security policy for supplier relationships
- addressing security within agreements
- technology supply chain
- monitoring and review supplier services
- managing changes to supplier services

Information security incident management

Security incidents must be managed. The responsibility and the procedures have to be described. The reporting of events and weaknesses should reach management as quickly as possible. Information security events should be assessed, responded and evidence shouldbe collected.

The lesson learned from each event should reduce the likelihood or impact of future incidents.

Information security aspects of Business Continuity Management

The consequences of failure, whether by security lapse or disaster, should be considered before a business continuity plan is developed and tested.

As with any aspect of security planning, the business continuity measures adopted will depend on the risks identified, the likelihood of those risks materialising and the consequences for administration business. For many Customs agencies, a failure in the delivery of services might not only disrupt trade, but could impair national security by weakening targeting, screening, profiling and communication facilities.

To ensure the availability of information processing facilities those should be implemented with sufficient redundancy.

Compliance

Measures for ensuring that the administration complies with any legal or contractual requirements to which it may be subject should be considered, as well as compliance with its internal security policies and frameworks.

Relevant considerations include copyright, protection of organisational records, management of records as admissible evidence and monitoring of audit logs. (More Information Required).

11.4. AUTHENTICATION

11.4.1. WHY AUTHENTICATE?

Within the paper-based world, there are long-accepted processes and conventions for authenticating identity and documents. For example, written signatures, witness signatures and seals are methods that have been used to authenticate identity. While not foolproof, legal and forensic methods of “proving” the authenticity of an entity’s identity and association with its transactions have developed over a long period of time and have been well tested through national judicial systems.

These methods are not necessarily transferable to the electronic world, and new methods of authentication need to be assessed and adopted.

The challenge of authentication is even greater in the electronic world because of:

- the breadth of access provided by ICT
- the increasing volume of transactions, and
- the ‘distance’ from the client (both geographically and in terms of relationships) that electronic transacting encourages.

This is particularly significant for Customs administrations in their compliance and enforcement roles. Any failure to link an individual firmly to his electronic identity, documents or declarations would undermine the standing of evidence in legal proceedings. It might also expose Customs systems to the potential for fraud or misuse of identity, thereby undermining confidence in an organisation’s systems and standing.

11.4.2. THE ELECTRONIC ALTERNATIVES

There is a wide array of options available for authentication purposes. These vary considerably with respect to the degree of assurance of identity offered and the degree of reliability with which a party can be linked to its message.

Authentication methods range all the way from a simple password system to thecomplex systems provided by public key cryptography. Each method or technology has its own strengths and weaknesses. The various methods available are briefly surveyed below.

Passwords, PINS and User IDs

The commonest method of authentication for computer systems today is the password. Although currently there are a number of authentication methods and techniques in use, such as token based, biometric-based and knowledge-based authentication, User ID and passwords authentication involving text (alphanumeric) is still common. Therefore, this section discusses good practices concerning password quality.

The password relies on being a secret known only to the holder and issuer with access being allowed only where the user’s password matches the issuer’s records. As with many authentication systems, it depends on users maintaining security around their online identity – their password.

From a technical perspective, the password model is susceptible to "brute force" such as "dictionary" attacks. These usually involve repeated and automated attempts at gaining unauthorised access through trial and error. For this reason, password systems are reliant on the security of the channels through which the password is communicated and on the security practices and arrangements of the issuer.

At best a password system authenticates the identity of the user. It does not authenticate the material being sent or address the integrity of the message content.

While password systems have the advantage of low-cost implementation, they are best suited for one-off use or for use in circumstances where the data or system to be protected has a low security threshold.

Password systems can be made more secure by combining them with other security and authentication methods such as encryption, user IDs or challenge and response.

Good password management practices are essential. Management policy decisions will determine the effectiveness of any password system and the degree of support that is needed to maintain users. These decisions may include simple security policies on such matters as:

≡ the length, composition and life span of passwords

≡ the number of failed log-in attempts permitted

≡ the procedures and processes for issuing, reissuing and suspending passwords, and

≡ ensuring that users are kept aware of the need to protect their password properly.

One-Time Use Passwords

One-time use passwords get around the main drawback of conventional password systems, namely, the fact that the password can be lost, stolen or sometimes cracked and then used repeatedly without authority.

A one-time password system generates a unique password for each session. This is normally achieved through a connected piece of hardware that automatically generates a password. The Customs administration's system knows which passwords or sequences are associated with which users and will allow access only where there is a match.

This approach has the disadvantage of requiring all users to purchase, or be supplied with, the necessary hardware and software. A broad-based roll-out could be expensive and might be more suitable for discrete groups of users. A weakness that this system shares with other authentication systems is that it too relies on the security practices employed bythe users to maintain control over their password device and the means of accessing it.

Challenge & Response Systems

Challenge and response is commonly used in combination with other methods such as passwords.

The concept involves the user providing answers to a question or a series of questions to which only the user is likely to know the answer. In some versions of this approach, the user may even be asked to suggest the question. The questions are then used to “test” the identity of the individual when, for example, user records need to be amended or a new password needs to be issued. Challenge and response can also be used as an additional authentication check when logging on.

Depending on the administration approach and requirements, challenge and response can prove complicated in operation. The management process for dealing with it may involve significant cost and have ongoing resource implications for the administration.

Cookies

Cookies are tokens placed on a user’s computer that can be used to recognise a user’s machine.

As a means of user authentication, cookies work on the assumption that each machine is only used by a single entity. They cannot therefore be viewed as a reliable means of authenticating a particular identity.

Because cookies can be used to track an individual’s browser habits, there may also be serious privacy issues that emerge where they are misused. Cookies can also be stolen and used to gain access to an administration's systems by fraud. Moreover, they have low levels of user acceptance.

Biometrics

Most authentication methods do not associate a physical identity with the user when he or she accesses the administration’s systems. Biometrics seeks to address this by providing a direct link between the known physiological or behavioural characteristics of an individual and the user.

Digitally encoded and unique voice patterns, finger or palm scans, retina scans or face scans, for example, are compared each time a user seeks access to the system.

Biometrics relies on the user having access to scanning hardware each time he accesses the administration’s systems. It also relies on the security of the digital code that represents the individual’s identity.

Apart from being expensive, the broad application of biometrics might encounter difficulties in gaining user acceptance of some of the biometric scanning methods employed – for example, in many cultures, iris scanning can be viewed as intrusive.

Conventional Encryption

Conventional cryptography is commonly known as “symmetric cryptography”. Symmetric algorithms involve the sender and receiver using the same key (a computer file with a unique identifying code also known as a secret key). In a very simple example, if the message to be transmitted was the number 20, the sender and receiver could agree that the algorithm that they would use would be to subtract the key from the message. Both parties might then agree that the key would be the number 2. The sender encrypts the message to the number 18, sends it, and the receiver decrypts it by adding the key to obtain 20 again. As long as a strong algorithm is used and both parties keep their keys safe, good levels of confidentiality can be attained. Symmetric algorithms also provide fast processing times.

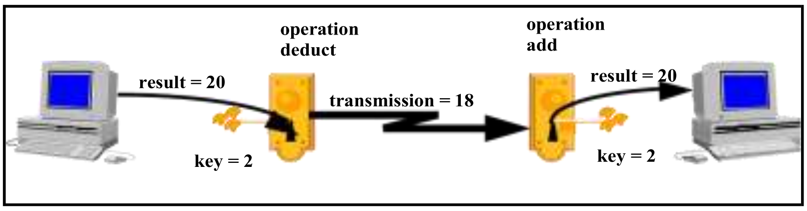


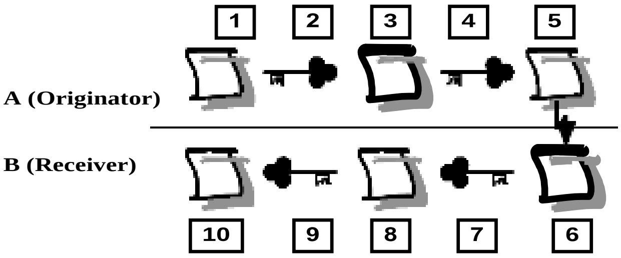
Figure 2: Elements of a system using symmetric keys

The principal weakness of this system, however, is in the issue and distribution of the keys that identify the user and the issuer to each other. Not only must a separate set of keys be agreed with each user, but the keys need to be physically provided to the client tomaintain some certainty of identity. Where courier services and third parties are used to deliver the key, the security of identity can be compromised. While symmetric algorithms provide fast processing times for encryption and decryption, the key management needed to assure authentication can prove costly and inconvenient for broad-based use.

Public key cryptography (digital certificates)

The problems of key distribution associated with conventional encryption are solved by public key cryptography. Public key cryptography uses separate pairs of keys for authentication (or signing) and encryption (or confidentiality). The key pairs are referred toas public keys and private keys. Public key cryptography is often referred to as ‘asymmetric’,as the public and private keys are different.

The private key is known only to the owner, whilst the public key can be published and known by anyone. A message encrypted using the public key of the receiver can only be decrypted using the corresponding private key. In the RSA standard (named after the inventors), the keys are constructed by manipulating two very large prime numbers but the mathematics behind the algorithm are too complicated to be discussed here. Thus, anyone can encrypt a message to the intended receiver, as long as they know his public key. The drawback with using asymmetric rather than symmetric keys is that the computations take longer.



1 = Document in clear text not electronically signed
2 = Private key of A to encrypt the control value of data + time stamp (= digital signature) (Integrity)
3 = Document in clear text electronically signed
4 = Symmetric algorithm to encrypt the content (Confidentiality)
5 = Document encrypted and electronically signed
6 = Document equals 5
7 = Symmetric algorithm to decrypt the content (Confidentiality Check)
8 = Document equals 3
9 = Calculate control value of data + time stamp; public key of a to decrypt received control value; match both values (Integrity Check)
10 = Document equals 1

Figure 3: Workflow of a public key encryption system

While asymmetric cryptography solves some of the problems that may be encountered with key distribution, it still relies on the user maintaining proper security over his keys. It also raises questions about how user identity is validated at the time the key is issued.

Public Key Infrastructure

Public Key Infrastructure (PKI) seeks to address unresolved problems in conventional asymmetric cryptography. Using asymmetric cryptography as its technical base, PKI provides a framework for securing message content, authenticating the sender and validating his identity.

These goals are achieved through the introduction of a digital certificate. A digital certificate is an electronic document signed by a trusted Certifying Authority, which identifies the key holder and the business entity (where appropriate) he represents. It binds the key holder to a key pair by specifying the public key of that key pair.

PKI involves a complex of legal and organisational elements to operate effectively. These, together with the working of PKI, are considered in greater detail in section 10.9.

PKI offers strengths in the areas of authentication, message integrity, confidentiality and non-repudiation within a single solution.

One area of vulnerability, however, is the reliance on third-party processes for checking identities and issuing certificates based on those checks. This can be remedied by tightening specifications or performing the function within the administration, but only at extra cost.

Another weak spot is the certificate holder's own security and management practices. If the owner loses (or allows others to use) his certificate, then its authentication can no longer be relied upon.

Transport Layer Security - (TLS)

The Secure Sockets Layer (SSL) protocol is a set of rules governing the authentication of servers (such as web servers) and encrypted communication between clients and servers. The protocol was developed to secure the transmission of data over the Internet. The authentication process under SSL uses public key encryption and digital signatures to confirm that a server is the server it claims to be. It does not authenticate the user. Once the server has been authenticated, the client and server use symmetric key encryptiontechniques to encrypt the information they exchange. A different session key is used for each transaction. This impedes a hacker's ability to decrypt messages. Subsequently,Transport Layer Security (TLS) was developed as an upgrade of SSL, Version 3.0

It should be stressed that SSL and Transport Layer Security (TLS) only provide confidentiality and integrity for the server. They do not provide non-repudiation and unless supported by a combination of appropriate private key protection and user willingness and ability to validate digital certificates, they do not provide effective authentication. SSL is well known because of its use in Netscape Navigator and Internet Explorer web browsers.

In May 1996, development of SSL became the responsibility of an international standards organisation, the Internet Engineering Task Force (IETF), which develops many of the protocol standards for the Internet. TLS, an enhanced version of SSL, was released in early 1999 and has been upgraded to TLS 1.2. Transport Layer Security is a widely used technology and versions of the product may be suitable for use by Customs agencies.

11.4.3. WHICH METHOD?

"Which authentication solution is required?" is an important question, but there is no single correct answer. The approach adopted should be determined by the outcome of a risk assessment and made subject to the preparation of an associated business case. Thechoice of any method or combination of methods will depend on the risks and consequences that an administration may face if an identity should prove false or if transactions andinformation are repudiated. It will also depend on the relative costs and the businessenvironment within which the administration operates.

11.4.4. ACCEPTABLE RISK

There are already a number of well developed processes for identifying, assessing and managing risk. One of the first of these was the Australia and New Zealand standard AS/NZS4360.1999 (www.standards.com.au). This may also be found in ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management Wherein section 3.14 on Risk Evaluation, which is defined as a process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable [SOURCE: ISO Guide 73:2009], There may be other national standards available and it is recommended that agencies consider referring to these documents when assessing their risks.

To identify and assess risk in context, agencies should consider:

- the environment within which they operate - including any political, economic, technical, business and legal aspects that affect their operations
- their clients and their relationship with them
- the types of transactions undertaken, and
- their business requirements and operations.

In this way the administration will gain a broad picture of where its risk areas lie. For example, the political environment may require the administration to provide the public with broad access to on-line transactions. The administration will therefore need to deal with different groups of clients, including some with whom it has long-standing compliance arrangements and others who may only transact once. A regulatory administration's legal environment may oblige it to rely on its transactions as legal evidence for prosecution purposes, thereby imposing a non-repudiation requirement. The weaknesses and threats identified in the light of these considerations are effectively the risks that the administration will need to assess.

The assessment of the risks identified generally involves considering the consequences of each risk and the likelihood of its being realised – the more serious the consequences and the greater the likelihood of realisation, the less acceptable the risk willbe. After that, risks can be prioritised, existing counter-measures can be assessed and new ones identified as necessary. The complete elimination of risk is unlikely and prohibitively expensive. The assessment must recognise that not all authentication solutions are totally reliable and secure. Every method of authentication can be compromised given sufficient skill and resources, or due to poor security procedures, practices or implementation.

Setting up a highly secure, but expensive, automated system may in fact buy only a marginal advantage over other alternatives in terms of deterrence or risk reduction and may not justify the extra cost.

The aim is to ensure that risks are reduced to acceptable levels and threats aredeterred by the measures adopted. For example, an administration may have found that in its electronic transactions it is potentially exposed to the risk of repudiation because it is unable to assure itself of the identity of the entity with which it is communicating. It believes that the consequences could be serious – identity fraud, loss of revenue and illicit trade. Deciding that it needs the highest level of authentication and security available, the administration considers a PKI solution but with strengthened evidence-of-identity requirements and tighter controls over certificate revocation. However, the digital certificates are now four times more expensive, few vendors will consider supporting the administration's requirements and the administrative effort and cost are significantly increased.

On looking more closely at the likelihood of the risks being realised, the administration notes that its client groups have different characteristics and represent different aspects of its business. It notes that most of its transactions are with trusted clients with whom it has strong compliance arrangements and transparent procedures. For these clients at least the administration can address its risks by taking a far less costly and elaborate approach.

11.4.5. COMPARING AUTHENTICATION METHODS

In identifying appropriate solutions for managing risk, agencies will need to assess and compare authentication methods. A number of these methods are identified in paragraph 10.4.2, where their respective strengths and weaknesses are also indicated.

In comparing these and other methods it is important to keep in mind that there is no single solution and that it is possible to use a combination of methods to achieve higher levels of authentication and security. For example, in conducting simple low-value financial transactions it is not uncommon to use PIN and passwords in combination with some form of cryptography. Similarly, challenge and response is often used not as a primary means of authentication but rather as a secondary check when updating user information in low to moderate risk transactions.

Each method should be measured against the administration's requirements and the risks identified. An appropriate method can then be selected based upon how accurately it meets the administration's requirements and how well it reduces the administration's risk to an acceptable level. Alternatively, several methods may be used at the same time, in which case it will also be necessary to determine how well they operate in combination.

11.5. NON-REPUDIATION

Non-repudiation is an issue of particular concern to Customs agencies, which usually have regulatory, revenue collection and border management roles. Reports, declarations and the production of documents are often required under force of law and penalties for breaching the provisions are often prosecuted in court.

Customs agencies therefore need seriously to consider the extent to which they are able accurately to associate transactions and message content with a particular sender.They also need to consider how they can ensure that once under their control the informationis not corrupted or transformed in a manner that would make it inadmissible as evidence.

11.5.1. NON-REPUDIATION DEFINED

There is an inherent and often unarticulated problem with the notion of 'non- repudiation'. In a technical sense, the word is taken to mean the use of cryptographic procedures by a relying party to provide evidence that a message could only have been sent by the signatory and nobody else. This generally means that technical procedures must be used to identify the signatory, ensure the integrity of the message and establish a link between the signatory and the message. This process can also be extended to include linking the message to the recipient. However, from a legal perspective, the concept of non- repudiation does not exist. In certain circumstances, irrespective of the evidence gathered by such cryptographic procedures, it is still possible for a person to deny the legal consequences of a transaction. In effect, it is only possible to limit the opportunities for repudiation.

Despite these anomalies, non-repudiation can generally be defined as: "the reasonable assurance that an entity can be clearly linked to a transaction for the purposes of binding it to the legal consequences of that transaction."

The purpose of non-repudiation is to ensure technical and legal certainty. Whiletechnical and business requirements may drive the development of non-repudiation policies,it is also a legal issue. Non-repudiation should be considered in the light of the possible future legal consequences.

11.5.2. NON-REPUDIATION IS NOT A STAND-ALONE ISSUE

Non-repudiation is only one of the issues which an administration will need to consider in developing a transaction system or conducting electronic transactions. Non-repudiation policies and processes should be regarded as part of a risk management approach which addresses a number of other, equally important issues including (but not limited to):

≡ privacy

≡ cost (to the Customs administration and to clients)

≡ usability

≡ security

≡ national legal requirements applying to government agencies in general (for example, any general legislation covering privacy, freedom of information, record keeping, etc.)

≡ legal requirements applying specifically to Customs (e.g. legislation relating to Customs and Excise or, in some cases, national security).

The specific non-repudiation policy and legal/technical solution adopted by an administration will depend on that administration's requirements in relation to these issues.

11.5.3. LEGAL CONSEQUENCES OF REPUDIATION

There cannot be a single non-repudiation policy or a single legal, business or technical solution to limit repudiation that applies to all agencies. The architectures, policies and processes which agencies adopt to avoid repudiation will vary depending on their business requirements and the kind of legal consequences they intend their transactions to have.

Broadly speaking, the legal consequences of transactions will fall into four categories, all of which have application to Customs agencies:

Criminal Offences:

Applicable to regulatory or compliance transactions. Agencies will need to consider the criminal standard of proof (beyond reasonable doubt), the requirement for trial by jury, and the specific forensic requirements of criminal prosecutions.

Civil Proceedings:

Applicable to commercial transactions (i.e. the administration is either buying or selling goods or services). Usually these will be proceedings under the law of contract, although other remedies might apply, e.g. some countries may have specific legislative trade provisions. In cases of this type, agencies may be able to specify alternative forms of dispute resolution such as arbitration or mediation.

Administrative Law Proceedings:

Applicable where the transaction leads to a decision being made against the client. Some countries may have appeal tribunals or courts that review such decisions. Issues suchas the need to ensure natural justice for the client will be relevant here.

Executive Action:

Sometimes the Customs administration's most effective remedy may be to deny the client the opportunity to deal with it electronically in the future. This does not rule out repudiation of the particular transaction. However, in some cases the prospect of losing access may deter clients from attempting to repudiate. The client may not have any right of appeal against the administration, but where appeal tribunals, ombudsmen or other legal review bodies exist, administrations must be able to justify their actions.

An administration must take into consideration the level of acceptable risk of repudiation for the transactions it manages. In assessing that risk, consideration should also be given to the balance between cost and the effective delivery of business objectives.

The solution will vary considerably depending on the types of transaction involved and the associated risks. With simple financial payments there may be little need for non-repudiation, demonstrating remittance and receipt being the two main risks. The need for non-repudiation will be much greater when accepting security or declarations in which the entity must be specifically bound.

Similarly, solutions will differ markedly depending on the technology adopted by the Customs administration. An administration using PINs and passwords, for example, may need to undertake its own authentication involving internal procedures and rely on a single agreement with users. On the other hand, an administration using PKI is more likely to be reliant on third parties and will use a complex set of agreements extending beyond the user.

11.5.4. ASSURANCE

Essentially, non-repudiation is an exercise in risk management. The level of assurance that an administration requires with respect to identity, content or process is a reflection of the risk of a client repudiating a transaction and the consequences that repudiation might bring.

Successful enforcement of an electronic transaction will require evidence to be gathered (in a form admissible in court, where necessary) regarding many aspects of the transaction, including:

- the evidence of identification (EOI) process
- how the identity of the sender of an electronic transaction was assured (e.g. access controls-pins, private keys, etc.)

- whether the administration imposed any conditions of use
- the information provided to clients regarding access controls and possibly education and other representations or instructions
- the particular authentication technology used (archiving, legacy systems may be required)
- the version of the end user software used by the client
- the way the software was being implemented at that point in time, and
- evidence of the time at which the transaction took place.

11.5.5. GROUNDS FOR REPUDIATION

The grounds on which a client might attempt to repudiate a transaction can be categorised as follows:

- **Electronic transaction-specific grounds**: Client claims that the transaction, or part of it, occurred without his or her knowledge or approval (i.e. forgery). This usually involves a challenge to the integrity or appropriateness of the procedures or the technical infrastructure within which the transaction was conducted.
- **General legal grounds**: Client admits that the transaction has occurred but claims that he or she is not legally bound by it.

Electronic transaction-specific grounds may include allegations that:

- the transaction has been forged or altered in transit by a third party – either by crypto-analytic attack or through loss or compromise of client's key, token, etc.
- the transaction has been forged or altered after receipt by the administration or by a rogue employee or external attacker gaining access to the administration's system
- the client's identity is false due to failure of the registration/EOI process.

The general legal grounds on which a client may attempt to repudiate a transaction will depend on the kind of legal effect the administration intends the transaction to have. Some examples are given in Attachment A to this chapter.

It should not be assumed that for electronic transactions non-repudiation requires only technical solutions. For example, it may be appropriate for a transaction to be designed with off-line steps to minimise the risk of repudiation. Thus, a client might be required to print a form from a web site, complete it and mail, fax or deliver the completed form to the administration concerned.

One likely general legal ground for repudiation is that the client was not fully aware of the content of the transaction to which he or she allegedly assented. To a significant extent, the solution to this lies in the technical design of the system, which must allow content to be fully displayed and, if necessary, scrolled through before the client can push an "agree" or "send" button.

11.6. IDENTITY ASSURANCE

Evidence of Identity

While the issue is essentially one of authentication, the evidence used in establishing an electronic identity (EOI) and the processes used in verifying that evidence form the indispensable basis for linking an entity to its transactions. Failure at this primary level increases the risk of transactions based on identity being successfully repudiated.

The administration should assess the EOI requirement against its own need to authenticate identity and avoid the repudiation of transactions. As the consequences of repudiation become more serious, higher levels of validation and evidence will be required.

A further complication arises when authentication methods involving third parties (such as under a PKI) and specific agreements are needed to establish a third party's liability for assurance of identity. However, these issues are addressed under the Gatekeeper Framework for the operation of Certification Authorities.

Evidence of Authority

Evidence of authority to undertake transactions is particularly important where agents or employees of an entity carry out transactions. It is easy to repudiate a transaction when there is no clear link between the electronic identity and the authority for its use.

The use of legal agreements to establish an electronic identity is important in this respect. At what point they are established, whom they bind and the form they take are all influenced by the type of transaction and by the administration's particular business processes and system choices.

The Framework

Assurance of identity relies on clients having appropriate control of verification tools (such as pins or private keys) and on access to these being restricted to the proper person. In this respect, the question of responsibility for the use of identity needs to be considered, both in terms of the owner's responsibility for securing his identity and in terms of thesafeguards which an administration's systems and procedures provide for protecting that identity. These responsibilities are commonly established in agreements between the parties.

How identities are stored (e.g. on dedicated tokens such as smart cards or directly on computer disk drives, where applicable) and client awareness of the need to ensure records are securely stored are other issues that agencies should consider.

11.7. CONTENT ASSURANCE

Assurance of Integrity

During the life of a transaction the content will be accessed, manipulated, actioned and stored. Throughout this life-cycle, the originator's content needs to be identifiable and reproducible as the original transmission. If an administration is unable to reproduce the content and demonstrate its integrity through the processes it used to conduct the transaction, its actions may be open to challenge and the content subject to repudiation.

Of critical importance is the link between the electronic identity and the content of a transaction. Without this, any attempt to limit repudiation for a transaction will fail. How this is managed will depend on the technical solution adopted by the administration. An electronic certificate forming part of an e-mail with an attached content could easily be separated and administrative procedures may be required to ensure that the original and complete communication is preserved. A completely automated transaction process may simply require the maintenance of detailed electronic logs of transmissions, access and authorised changes.

Keeping the parts together

Transactions may often involve a number of component electronic communications and decisions. It is important that all components of a transaction are tracked and remain linked to that particular transaction. Where not all the components can be retrieved to provide evidence of the entire transaction, the integrity of the transaction may be called into question and part or all of it may be repudiated.

Appropriate procedures, such as logging and annotation, need to be considered.

Storage and Reproduction

There are a number of issues connected with the storage and reproduction of transaction material that affect repudiation.

The integrity of the storage facility, the form in which a document is stored, the management and updating of cryptographic mechanisms, where these are used, and the relationships maintained between data being processed all have a bearing on the strength of the evidence limiting repudiation.

11.8. PROCESS INTEGRITY

Management Framework

The design of any business process includes elements which assure the quality and hence the integrity of both the process and the material being processed. These correspond to the points in the process most relevant to limiting repudiation. Commonly they involve matters of governance such as the identification of decision-making responsibilities and the processes for authorising and reviewing access.

As these processes concern the integrity of the transaction, they are central to the assurances needed to avoid repudiation and will constitute an important source of evidence if the administration is required to defend itself against claims of internal fraud or negligence.

System Rules and Architecture

When considering the reliability of material, courts may examine the integrity and capabilities of the electronic systems used. In this context, the range of issues important in limiting repudiation will include the system rules, software rules and architecture.

Electronic systems operate within a framework of rules – predetermined decisions that affect the action taken in connection with each transaction. These rules may addressmatters ranging from the terms and scope of access through to what is logged or archived, when and in what form. They will need to be reviewed from the perspective of the assurances they provide.

11.9. PUBLIC KEY INFRASTRUCTURE (PKI)

PKI is one of the more complex methods of authentication. As the name implies, PKI is less a “single solution” than an “infrastructure” centred on public key cryptography andinvolving both an organisational structure and a legal framework. Therefore, unlike many other solutions, PKI aims to offer a “complete” package, integrating technologies and processes in order to assure authentication and integrity and reduce the potential for non- repudiation.

While it has yet to enter into common use, it is emerging as one of the stronger solutions for organisations that require high levels of assurance. As Customs agencies are very likely to have such a requirement, PKI has been selected here for separate and detailed discussion.

11.9.1. BACKGROUND

The decision of a Customs administration to enable traders, customs brokers, carriers and other regulatory agencies to carry out their import and export clearance tasks securely over the Internet or with the help of value added network service providers (VANs) involves issues of IT security discussed in the preceding sections.

The Internet is an inherently open system. Its strengths are built around this openness and its low cost and ease of access, which make it an inexpensive medium for transacting Customs compliance-related business. However, its openness can also be a major threat for users.

The open nature of the system makes it relatively easy for web-sites and Internet communications to be compromised and the IT assets of a Customs administration used for EDI messaging are exposed to such threats. In considering mitigation strategies, it is necessary to refer to the standards which various bodies are developing. Doing business on the internet poses four generic kinds of risk. These pertain to (a) the privacy of the message, (b) its authenticity, (c) its integrity and (d) non-repudiation. Public Key Infrastructure (PKI), based on the technology of public key cryptography, provides a means of mitigating these risks.

The EDIINT standards were developed by the Internet Engineering Task Force (IETF) to address issues relating to secure communication techniques for EDI messaging over the Internet. These standards identify PKI as one of the technology enablers for addressing these security concerns.

11.9.2. PKI Defined

Public Key Infrastructure (PKI) can be defined as the architecture, organisation, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. It includes a set of policies, processes, server platforms, software and workstations used for the purpose of administering digital certificates and keys. A public key cryptographic system works with the help of asymmetric crypto-systems algorithms.

11.9.3. Conventional and digital signatures compared

The challenge for PKI is to translate the trust conventions of the physical world and make them work in online transactions. Signatures are not the substance of the transaction. Signatures only represent an event in a transaction. Signatures impart certain characteristics to the objects involved in the transaction. More precisely, a paper signature authenticates the signer (or signatory) and the signed document. Thus, the signer leaves a distinctive mark and his writings become the signature, which then becomes the evidence connecting the signer and the signed document. The signer of a paper document is aware of the significance of the act of signing and the finality associated with the event of signing. By common law and custom, the very act of signing implies that the signer duly approves the contents of the document being signed. Signed documents represent distinct “states” or “finalstages” in a transaction and the convenience associated with having crossed through certain final stages or states.

Conventional signatures are paper-based and therefore, in the absence of paper, the characteristics of the paper-based signature have to be built into the digital signature. PKI technology enables the generation of signatures, the verification of signatures and archiving of the verified documents/records, as well as providing evidence whenever necessary. An actual PKI implementation must therefore address these aspects.

11.9.4. The operating life-cycle of a digital certificate

Under PKI a person may apply for a digital certificate by first generating a key pair comprising a public key and a private key. He or she must then fill out an application form for a digital certificate for signature and/or authentication purposes and send it to a Certificate Authority

The Certificate Authority receives the application form, verifies whether the key pair submitted by the applicant forms a valid cryptographic key pair, checks the correctness of the information supplied by the applicant and then issues a digital certificate, which is signed by the Certificate Authority itself.

The public key is published in a directory, which will usually comply with the International Telecommunications Union (ITU) X.500 standard. The applicant keeps the corresponding private key secure for use in connection with encryption and/or signing and/or verification operations.

The certificate will be valid only for a certain period of time and may therefore require periodic renewal. For certain specified reasons – chiefly the reported misuse or compromise of a private key - the Certificate Authority may suspend or revoke a digital certificate. The operating life-cycle is described in form RFC 2527 of the Internet Engineering Task Force (IETF).

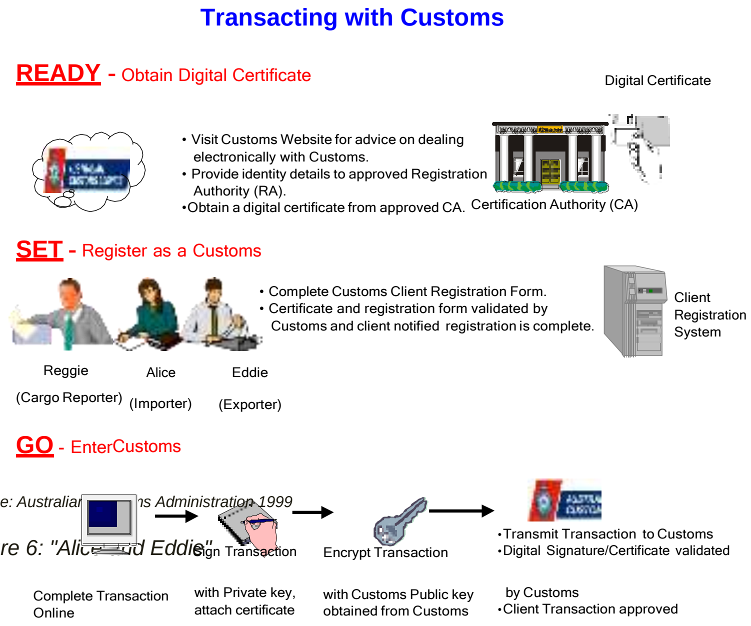
11.9.5. IMPORTANT CONSIDERATIONS IN IMPLEMENTING PKI-BASED SOLUTIONS

In view of the advantages offered by PKI technology, Customs administrations may wish to consider using PKI-based systems in designing and implementing their EDI messaging solutions. This involves providing comprehensive capability for handling digital certificates and signatures in Customs business processes and IT systems.

PKI implementation has the potential to build capacity in connection with the secure storage of electronic data as well as the transmission of electronic information using digital (signature) certificates. However, before proceeding to implementation, agencies should first consider the scope for their PKI. This normally involves preparing a “scoping document” that lists the objectives, assumptions and goals and any limitations that need to be placed on the project.

It is important to consider limitations to avoid the project expanding unnecessarily into areas the administration has already ruled out for implementation. The scoping document may include illustrative scenarios showing how the administration might use digital certificates for authentication, secure messaging and signature purposes. For a simple illustration see figure 6 below.

Specifically, steps should be taken to ensure that the overall e-commerce and EDI solution implemented by the administration is PKI compliant and PKI compatible.



Transacting with Customs

READY - Obtain Digital Certificate

Digital Certificate

- Visit Customs Website for advice on dealing electronically with Customs.
- Provide identity details to approved Registration Authority (RA).
- Obtain a digital certificate from approved CA.

Certification Authority (CA)

SET - Register as a Customs

- Complete Customs Client Registration Form.
- Certificate and registration form validated by Customs and client notified registration is complete.

Client Registration System

Reggie (Cargo Reporter)
Alice (Importer)
Eddie (Exporter)

GO - EnterCustoms

Complete Transaction Online

Sign Transaction with Private key, attach certificate

Encrypt Transaction with Customs Public key obtained from Customs

- Transmit Transaction to Customs
- Digital Signature/Certificate validated by Customs
- Client Transaction approved

Source: Australian Customs Administration 1999

Figure 6: "Alice and Eddie"

11.9.6. USING DIGITAL SIGNATURES IN EDI AND XML MESSAGING

The World Wide Web Consortium (W3C) and the Internet Engineering Taskforce (IETF) are working on a digital signature standard for Extensible Markup Language (XML) messaging. UN/CEFACT and OASIS are working on integrating SOAP (Simple ObjectAccess Protocol) with Attachments specifications into the ebXML specifications (www.ebxml.org). This will result in an open, global standard for reliably transporting electronic business messages over the Internet.

The ebXML messaging specifications themselves encompass a set of services and protocols that allow a client to request services from the servers over commonly used application level transport protocols such as Simple Mail Transfer Protocol (SMTP), Hyper Text Transfer Protocol (HTTP) and others. EbXML allows for a general-purpose message involving a message header that supports multiple payloads, while providing for digital signatures within and among related digital messages of any specification.

UN/EDIFACT messaging provides for the use of digital signatures along with the electronic messages. In addition, the UN/EDIFACT messages provide for import and export of public keys (provided for by the UN/EDIFACT KEYMAN messaging format). As with other forms of messages, administrations will need to consider the issues involved in the logging and archiving of these messages, so as to maintain data security in order to manage the consequences of repudiation

11.9.7. CERTIFICATE AUTHORITY AND THE LEGAL FRAMEWORK

After deciding on a PKI-based solution, the Customs administration would have to consider several technical and legal issues that arise in the course of any PKIimplementation. As indicated above, PKI requires a system for the generation and maintenance of digital certificates. This is normally achieved through the establishment of a Certificate Authority.

A Certificate Authority is an entity that attests to the identity of a person or an organisation. The Certificate Authority's chief function is to verify the identity of entities and issue certificates attesting to that identity. Digital certificates are a way of verifying a person's (or a company's) identity. The digital equivalents of identity cards, they help to establish the desirable security characteristics for transactions over the Internet.

The national legislative framework available in respect of PKI, which should specify the technical as well as the legal requirements, has an important bearing on:

≡ the manner in which digital certificates are issued by a Certificate Authority

≡ how a Certificate Authority manages the life-cycle of a certificate, and

≡ what technical standards have to be applied.

For a model legislative framework, administrations might like to consider the guidelines presented in the UNCITRAL model law on the subject (http://www.uncitral.org/en-index.htm) UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001).

Among other things, the legislative framework might cover:

≡ the manner in which digital information is to be authenticated by means of digital signature and the admissibility of such signatures as evidence in a court of law.

≡ the process of creation of a digital signature

≡ the process of verification of digital signatures

≡ the technical standards applicable to these processes

≡ the licensing of Certificate Authorities, and

≡ the security policy guidelines applicable to the operation of a Certificate Authority.

In the absence of a general, overarching legislative framework, administrations might consider entering into bipartite or tripartite agreements with users and service providers, very similar to the agreements in vogue in the VAN environment but with account for the PKI enabled technology platform.

11.9.8. PKI and Customs: The Key Issues for Consideration

Administrations might wish to consider whether they are in a position to perform the functions of a Certificate Authority or whether any other public/government or private agency offers public certification services of acceptable quality. Different countries have different models enabling Certificate Authorities to function, subject to their respective legislative frameworks, as chains (or hierarchies) of trust. Irrespective of the model selected, and the choice of Certificate Authority, there are several decision points that are likely to emerge in accepting the digital certificates issued by a Certificate Authority.

Attachment A to Chapter 11

Examples of legal grounds for repudiation in Australian criminal and civil proceedings

1. ***CRIMINAL***

1.1 Forensic failure (probably the most common cause of failure in criminal prosecutions) - either: sufficient persuasive evidence is not available (failure of logging, archiving, etc.); or evidence is inadmissible (problems with investigative or evidence-gathering activities, or legal problems with the admissibility of computer records).

1.2 Lack of mental element:
Individual (applicable to general offences such as fraud - may not apply to agency-specific statutory offences, e.g. under the Customs Act); or
Corporate - if applicable, corporate intent must be inferred from the intent/conduct of officers and agents.

1.3 Defences such as insanity, automatism (unlikely in this context).

1.4 Defendant is under the age of criminal responsibility (10 years old in NSW) (unlikely - indicates serious EOI failure).

1.5 Allegation of identity theft (which has occurred regardless of the implementation of appropriate registration/EOI processes).

2. ***CIVIL***

(Note: The following examples relate to the scenario of a contract between agency and client. There are other possible civil actions, e.g. an e-mail giving bad advice leads to an action in tort for negligent misstatement, but these seem unlikely in the context of agency transactions.)

2.1 Failure to form binding contract (failure of click-wrap process) or insufficient evidence of process. Includes:
- client assent not clearly demonstrated by process; or
- terms and conditions not adequately disclosed.

2.2 Failure to form binding contract for non-process related reasons, including lack of consideration or lack of intention to create legal relations. May also include remedies allowing rescission without fault, e.g. mutual mistake (but unlikely).

2.3 Wrongdoing by receiver (or in some cases a third party). Various remedies allow a court to set aside a transaction, including duress (physical or economic), unconscionable conduct, misleading or deceptive conduct (TPA s. 52), Yerkey v. Jones, etc.

2.4 (Individual client only) Consumer protection remedies such as NSW Contracts Review Act.

2.5 (Organisation client only) Individual representative/agent has acted without authority.

2.6 Identity theft (same as 1.5).

2.7 Client is under 18, or otherwise lacks contractual capacity.

11.10 IDENTITY MANAGEMENT

The object of identity management is the verification of the identity of an entity that seeks remote access to an information system, claims to be the author of an electronic communication, or signs an electronic document. In information systems, online identities are 'electronic'. In face-to-face interactions, an identity is verified through visual checking of the attributes of the identity. Similarly, online electronic identities need to be verified thoroughly before a person or an entity is permitted to participate in electronic transactions. Section 11.6 discusses issues of identity assurance. There is however a need to address the security and business challenges posed by the operational use of electronic identities and this section discussed these challenges of managing electronic identities from a life-cycle perspective.

Extensive use of ICT has led to the proliferation of in-house applications and networks. To access an application or network, a dedicated identification and authentication system has to be used. Over time, multiple and often mutually-incompatible identity systems tend to develop and grow. Users of ICT are not capable of handling multiple electronic identities and may falter in maintaining high password quality discussed earlier in this Chapter. Users will accumulate many passwords, making account and password management very complicated, rendering authentication solutions complex, and leaving too many dead and orphaned user accounts. This scenario would invariably result in gaps in security and auditability, making ICT systems vulnerable to password theft and consequent exploitation by criminals. The principles and practices of Identity Management are aimed at providing solutions to the ongoing management of electronic identities in an environment where users have to access multiple..

OECD has provided a working definition of Identity Management as follows:

“ Identity Management is the set of rules, procedures and technical components that implement an organisation’s policy related to the establishment, use and exchange of digital identity information for the purpose of accessing services or resources. Effective Identity Management policies safeguard digital identity information throughout its life cycle – from enrolment to revocation – while maximising the potential benefits of its use, including across domains to deliver joined-up services over the Internet.

[“The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers” (June, 2009), OECD Working Party on Information Security & Privacy].

Identity management is an important component of Information security. This component helps in dealing with the following challenges:

It helps in providing physical and logical access control to information systems. These controls form the basis for ensuring that only authorized persons accesses the relevant data and perform permitted operations on the data.

It is concerned with protecting individuals against unauthorized access to personal information and identity theft while using online electronic identities. These individuals seek assurances that their electronic identities will not be misused or compromised in the process of using them in electronic transactions. Therefore, Identity Management helps protect their online privacy.

With the rapid growth of online services, it is challenging for the individuals to handle the access procedures as defined separately by each service. For instance, the need to remember and operate separate user IDs and passwords for each service is burdensome and is inherently insecure. For the service providers, the challenge arises from the fact that the requirement of individuals to be identified by each online service leads to the proliferation of the personal information of the individual in different IT systems, opening-up the possibility of data breaches and the attendant liabilities.

Identity Management involves two basic processes, namely, identification (identifying the person) and authentication (verifying that the person is who he or she claims to be). Identification involves the association of a person with attributes that describes the person. These attributes are based information about the person. They can be physical (biological characteristics) or documentary (documents assigned to or associated with the person, such as passport or ID cards). Attributes that help distinguish between persons helpsidentify the persons efficiently and attributes identifying a person uniquely are called unique identifiers. The process of capture of identity information is called enrolment. Enrolment is a one-time process for vetting or proofing the identity of a person. Enrolment is done with the purpose of using the information in the future in order to authenticate it. Assurance levels of the identification process increase with the number and variety of attributes collected. Correspondingly, there is increased risk of misuse of this personal and private data collected at the time of enrolment. The fewer the attributes collected at the time of enrolment, the lower the risk of breach of privacy.

Verification of collected attributes can be done online (confirming visually that the attribute belongs to the person being identified) or offline (sending a Personal Identification Number or PIN by registered mail). The accuracy of personal information collected depends on the reliability of data and the dependability of the person or system ascertaining the measure of the attribute. Personal information such as height can be measured reliably andis not likely to vary. On the other hand, fingerprint verification depends on the trustworthiness of the system in recording the attribute and verifying it for the future. Verification depends on the type and source of identity information being verified, the processes involved in verification and the trustworthiness of the verification system.

The identification process concludes with the issuance of credentials (User ID Password, smart card tokens etc). Some of the credentials are based on biologicalattributes of the individuals.

Directory services are used in order to store and manage accounts, identity information and access credentials. In the absence of 'federated identity' systems, information about credentials is maintained in separate directories for separate applications. With federation of identities, it would be easier to maintain the policies for the management of entitlement of electronic credentials. Activities related to user account management, identity life-cycle management and access management are greatly simplified.

Federated identity management involves 'third parties' for account management, authentication and access management. Using federated identity solutions,the overloading of users with multiple user IDs and passwords is avoided. The third party identity management solution acts like a one-stop shop for the user and the system being accessed. The third party is the 'identity provider', the user of the 'subject' who wishes to access an information system provided by a government or a business called the 'relying party'. It is not necessary for the 'third party to be a different business entity but it is clearly a distinct role. There are legal risks associated with federated identity management solutions such as the risk of loss of privacy involving the unauthorized access to identity attributes of the user. The compromise of a user's credential information would lead to risks of false authentications, unauthorized access and consequent liabilities arising from system break- ins. These risks have to be mitigated through appropriate countermeasures.

In conclusion, these Guidelines recommend Customs administrations to follow sound principles and solutions for Identity Management as they improve security and reduce time lost in unproductive activities associated with user management.

12. LEGAL ISSUES

(Standard 7.4)

12.1. INTRODUCTION

It is not possible to give specific guidance on legal issues that will be equally valid for every Customs administration because each administration operates under a different legal system and on a different legal basis. The guidance offered here is intended to give the reader an initial understanding of the commonest legal issues. Guidance on the legal implications of automating Customs procedures should be sought from the relevant expertsin the early stages of a project.

When dealing with legal issues, remember that laws have different areas of applicability, for example:

- International Conventions (e.g. the revised Kyoto Convention);
- Supranational laws (e.g. EC legislation, with implications such as direct applicability and primacy);
- National laws with general applicability, which can affect entities inside and outside the Customs domain (e.g. privacy laws, e-commerce laws, digital signature laws, data protection laws);
- National laws with specific scope, such as national Customs law, which affects only those within the Customs domain; and
- Customs procedure law, which is limited to a Customs procedure (e.g. there may be a Customs transit law).

Legal issues are occasionally cited as insurmountable obstacles to the implementation of some proposed system option. An increasing number of member administrations has found that changing the legal requirements need not be a difficult and lengthy process.

12.2. SUITABILITY OF EXISTING LEGISLATION

When a Customs procedure is to be computerised, the vast majority of existing legislation is unlikely to require amendment. However, automation may have the effect of simplifying the procedure, which may need to be reflected in the legal provisions. Definitions of responsibilities may need to be changed, including the point at which payment is due, when a declaration is considered to have been made, etc.

12.3. TYPES OF LEGAL ISSUES

In an electronic environment, the legal issues that need to be taken into consideration when a new system is introduced can be divided into groups, for example, as indicated below. It should be noted that groups of this kind are always artificial and are created only for presentation purposes. In practice, the grouping does not have any legal value and issues overlap from one group to another.

≡ EDI issues (formalistic requirements, i.e., provisions requiring the use of paper,a document, a signed document, etc., and requirements relating to the use and acceptance of electronic data as evidence);

≡ Security-linked issues (format and media for storage of data, authentication, integrity, non-repudiation, acknowledgements, etc. and also evidential issues);

≡ Data protection issues (restrictions on data access, restrictions on the transfer of data between agencies, etc.);

≡ Other issues, such as confidentiality, operational responsibilities and obligations due to the use of the electronic data exchange system, fall-back provisions, legal provisions which prevent the use of encryption, etc.;

≡ How to introduce the new system, whether by means of an agreement (e.g. an Interchange Agreement, which raises other contractual issues) or on the basis of the administration's status as an authority by establishing provisions to be obeyed and accepted.

12.4. SIGNATURE

Despite the existence of sophisticated data exchange systems, the import/export process sometimes remains at least partly paper-based due to the legal and operational requirements of national Customs authorities. In some existing Customs IT systems, signature requirements necessitate the presentation of hard-copy declarations to Customs in addition to electronically transmitted data, thereby blocking the advance towards a "paperless" environment. Such legal barriers need to be overcome if the full benefits of Customs automation are to be realised.

Effective techniques are available for replacing the hand-written signature in a Customs automation environment. Passwords, personal identification numbers, identification cards or badges, etc. and digital signatures can be used to authenticate an electronic message and identify its origin. They are already being used extensively in other sectors, such as banking, as well as by an increasing number of Customs authorities.

There are two possible approaches to digital signature law:

≡ specify the precise technical mechanisms to be used (e.g. which algorithm, how it is to be applied, etc.); or

≡ specify that the choice of a suitable mechanism is the responsibility of the Customs.

The second option has the advantage of not requiring changes in the legislation if Customs decides to switch from one mechanism to another.

12.5. ADMISSIBILITY

Legal obstacles still exist with regard to the admissibility of computer-readable data as evidence in court proceedings. The WCO, in a resolution passed in 1986, called on its member administrations to put pressure on the appropriate national authorities in order to bring about the necessary legal changes. These would not only provide for the admissibilityof computer-readable data as evidence in courts of law but would also make provision for the authentication of such computer-readable data by means other than hand-written signature (see 11.4 above). These legal reforms are necessary not only from the Customs viewpointbut also from the viewpoint of the trading partners in general.

Where such legislation is introduced, steps should be taken to ensure that the automated system is capable of providing evidential material in the manner prescribed.

12.6. DATA PROTECTION AND PRIVACY

Although enforcement systems are generally exempted, Customs IT systems usually fall within the scope of data protection and privacy laws, which may apply to natural persons only or to both natural persons and legal entities.

When privacy and data protection legislation is being drafted, Customs administrations should try to ensure that its provisions do not compromise their ability to protect revenue, trade or other State interests by restricting their powers to retain information and exchange it with other interested parties (both national and international). Privacy considerations will become important once Customs begins to deal over public communications networks, such as the Internet, and share information on its clients with third parties.

It is also in the national interest that Customs should have the right of access to trading partners' computer systems for verification and audit purposes. Customs should ensure that this right is not restricted by new legislation.

When new IC technology is being introduced, privacy and data protection legislation should be examined to ensure that the proposed system will satisfy all the requirements.

The following documents provide further information on the legal basis for paperless trade.

(i) UNCITRAL Model Law on Electronic Signatures with Guide to Enactment 2001 [United Nations 2002]

(ii) United Nations Convention on the Use of Electronic Communications in International Contracts [United Nations, 2007]

(iii) Promoting Confidence in electronic Commerce- legal issues on the international use of electronic authentication and signature methods [United Nations 2007]

13. Audit of Internal Controls in Information Systems

(Transitional Standard 6.9)

13.1. Background

Computer systems audit provides assurance that a particular activity or process is performing as intended. Systems audit, as the name implies, means looking at the entire processing cycle rather than just at the transactions themselves. It does not rely on a fully visible audit trail and substantive testing of all or a significant number of transactions, as in a manual system, to provide assurance about the workings of a particular application or installation. Instead, systems audit attempts to use the inherent properties of computer processing to maintain user confidence.

If it can be established that the process itself is reliable and accurate and that the controls which govern it are sound and being complied with, then safe assumptions can be made regarding the quality of the output. The great strength and, paradoxically, weakness of computer systems is that once set up, they perform the same task in the same way every time until a change is made. Thus, if they have been programmed correctly, the output will always be accurate, and if not, it will always be wrong!

Customs can apply computer systems audit techniques both to external trading partner systems and to its own in-house applications. Using these methods provides assurance with respect to the integrity of the systems and identifies weaknesses, which must be addressed in order to restore confidence. The following section concentrates on Customs in-house systems audit.

13.2. Development audit

Computer systems audit can be of great benefit in the development stage of a new application. In the Customs environment there will always be a need to implement new applications as quickly as possible because of new legislation. However, the requirement for speedy implementation has sometimes led to auditability being overlooked or only partially addressed. Poor auditability means at best inadequate or at worst non-existent controls and hence unreliable data.

Therefore, whenever a new application is introduced, the planning team should ideally include a computer auditor to ensure that the question of controls and audit trails is not overlooked. This auditor can provide test data upon which realistic testing of the system can be based. Subsequently, auditors will always be able to confirm the processing of data from inception to final recording and to trace transactions in the reverse direction as well. Thus, if audit considerations are taken into account when a new system is first installed, the subsequent audit and control of that system will be much more effective and reliable. It will also be more cost effective to build these features in from the outset than to attempt to introduce them at a later stage.

The principal steps that make up the systems audit approach are outlined in thefollowing paragraphs:

13.3. PLANNING

Planning is critical to the success and credibility of an audit. It gives direction and identifies the scope of the audit or the ultimate goal against which to measure its effectiveness. Where new systems are concerned, there is usually a preliminary feasibility stage. The basic question that a feasibility study has to answer is: Can it be done?

Thus the planning stage will determine amongst other things:

≡ The objectives; the auditor must have a clear idea of what his involvement is intended to achieve. It must also be clear to those to be audited and fellow members of the development team.

≡ The scope; this sets the boundaries of the audit by specifying which areas and which systems will be included.

≡ The risk areas; this should attempt to identify areas where failure could create significant or catastrophic consequences and on which the auditor can target his or her efforts.

≡ The conduct of the audit, including preliminary and exit meetings with the auditee; the ground rules should be set out in advance to prevent misunderstandings or problems during the audit and let the auditee know what to expect at the audit's conclusion.

≡ The duration of the audit; a specified period of time should be allocated to the audit so that the auditee can organise his/her work around it.

≡ The resources needed to undertake the audit; an appropriate number of auditors should be assigned to the audit, depending on the size and/or location of the system(s) to be audited and the availability of key personnel.

≡ The availability of key personnel for interview purposes; it is even more important to ensure that key personnel are fully aware of when the audit is due to take place and when the auditor will need to speak to them. Thus, their agreement should be sought well in advance of the audit, whenever possible.

Finally, the auditor should ascertain the extent to which changes in the system, or the operating organisation, have affected previous audit knowledge. For existing systems there is likely to be a store of audit information which can provide the auditor with useful knowledge about the system and its performance in the past. If, however, there have been significant changes, the reliance that can be placed on this previous information will be much diminished.

13.4. ENQUIRY OR FACT GATHERING

These tasks can be performed by using a combination of methods, mainly the following:

13.4.1. INTERVIEWING

By talking to personnel at all levels in the management chain, including application users, data processors and system designers, if possible. From these interviews the auditor can determine how the system:

≡ is perceived to work (usually a management view)

≡ actually works (people using the system)

≡ is supposed to work (designer/user specification)

13.4.2. EXAMINATION OF DOCUMENTATION

The auditor may refer to:

≡ user specifications, which detail what the user wanted the system to do

≡ design/system specifications, which detail the solution provided by the design team

≡ test schedules: used to record the range and scope of testing. To ensure that a system is able to cope in all circumstances, is accurate, robust, has the appropriate capacity to deal with unexpected peaks and has effective error trapping and reporting mechanisms

≡ trial/parallel running results: these are the findings recorded during the live running of a new system, either at a pilot site or in parallel with an existing system

≡ user guides: these are instruction manuals on how to use the system and should be easy to read and comprehensive in scope

≡ fallback/security measures: these should specify the procedures for disaster recovery and protection of the system at both application and hardware levels

≡ archiving policy: this will specify how often data should be backed up (security copies), how long it should be kept, and where and how it should be stored, e.g. off-site in a fireproof cabinet

This evidence, which is not exhaustive, can identify both internal and operationalcontrols or the lack of them. The auditor can also deduce a great deal from the state (or even the lack) of system documentation, which, for example, may be out of date or incomplete. Proper configuration management and document management controls can provide the auditor with further evidence concerning the health of the system and the amount of confidence that can be placed in it.

13.5. RECORDING THE AUDIT RESULTS

The auditor will record his findings by using narrative text and diagrams. There are many flowcharting conventions and standards, each usually designed to portray a particular aspect. They include:

- program flowcharts
- system flowcharts
- overview or block diagrams
- database schemas

The auditor will often compare his own flow diagrams with the site flowcharts to detect any omissions or anomalies. Typical diagrams might look like the extracts in Appendix 5 and Appendix 6. This stage usually concludes with the formal confirmation, by the auditee, of the auditor's understanding of the system, before the process moves on to the next phase.

13.6. EVALUATION

By reviewing and evaluating the evidence gathered the auditor can begin to detect actual or perceived weaknesses in the internal controls. The evaluation process will enable the auditor to plan tests and determine the areas in which to apply them. This will help to establish the effectiveness of the controls and the credibility of the output.

13.7. CONFIRMATION OF AUDIT FINDINGS

This activity is carried out at every stage of the audit. Confirmation can be obtained in the fact gathering stage by observation; as a result of the evaluation stage; by inspecting records, output reports, etc.; or even by re-performing the processing cycle.

The inspection of documentation, whether computer-generated or manual transaction records, will include confirmation of completeness, accuracy and authority. Where there is a visible audit trail, it will be followed to ensure that there are no breaks.

Where there is no audit trail or where it is impractical to follow the trail because of the volume of transactions, advanced IC techniques can be used. These advanced techniques include writing special programs to interrogate data held on magnetic media. The programs can be written on an ad-hoc basis using the same language as the application software, or proprietary file interrogation software can be used.

In addition to straightforward testing and confirmation of transaction totals, tax calculations, discounts, etc., the uses of these methods also include testing for unusual data combinations, which would be almost impossible using manual techniques. Often auditors will leave a set of test programs, sometimes known as audit packs, on the system to be run on each audit. These packs can be adapted by changing the parameters, etc. but only have value if the system remains unchanged.

These advanced methods are mainly employed in those situations in which an error could have significant consequences, such as a serious shortfall in duty or tax payments or incorrect statistical information leading to balance-of-payments problems, etc.

13.8. REPORT

The outcome of the audit will usually be a report to senior management which will make recommendations as to how identified weaknesses can be eliminated or controls can be tailored to make them more effective. Controls may even be discarded if they are seen to be irrelevant in a particular situation.

Recommendations are not mandatory but are usually, even if eventually rejected, given very serious consideration since in certain circumstances the consequences could be disastrous.

13.9. POST AUDIT REVIEW

After implementing a new system or making a significant change to an existing one it is customary to review how the system is working. This review is carried out after an agreed period and is intended to show if the system is working as specified and designed or if there are shortcomings and lessons to be learned for future projects. Similarly, if a computer system has been audited and particular recommendations were made concerning its operation, a post audit review will determine whether or not those recommendations have been implemented. If the recommendations have been implemented, it will determine their effects and if they have not, then the reasons why not.

13.10. CONCLUSION

Once a system has been recorded and evaluated and any amendments to improve control have been implemented, it may be expected to perform reliably until the next significant change is made. Periodic audits should be conducted to confirm that nothing has changed and that the controls built into the system continue to be administered and applied.

14. COMMON PROBLEMS

14.1. INTRODUCTION

Prior to the implementation of any automated system consideration should be given to those areas which might become problematic during the development of the project. Strategies should be developed to ensure that potential problems, whether organisational, procedural or resource-related, do not cause a project to fail.

Any automated process implemented by any Customs administration will need to be supported. Administrations that are considering developing automation may also wish to create an appropriate organisation to support any initiative they undertake. All the activities and related costs associated with managing and directing information technology initiatives; designing, developing and implementing new or enhanced automated applications; and operating, maintaining and supporting these automated applications are important and should be taken into account. See appendix 8: Information Technology Function Logic Chart.

14.2. CULTURAL RESISTANCE

The Customs community may view automation as a potential threat to their jobs and resist implementation. Through suitable education, training and incentive programmes Customs can eliminate this resistance and turn the Customs community into a more effective workforce. Ensuring that information about project plans, scope, etc. is made generally available at a very early stage will help prevent rumours from spreading and reduce uncertainty. This can be achieved by publishing regular project reports and involving those personnel who will be directly affected by the project.

14.3. AUTOMATION OF SOURCE DATA

Lack of automated source data may make automation unattractive to certain Customs trading partners. For example, if the commercial documentation has not been transmitted electronically, then the trading partner cannot use this information as a basis for the Customs declaration. A possible solution to this problem is the use of service bureaux for data input. These bureaux could be run either by Customs or by private companies. In the case of private companies the bureau service should be sanctioned by Customs to ensure that data capture standards meet requirements. Another solution might be to purchase all the equipment for trading partners, as well as Customs, through a supplier credit programme, which could include a substantial discount for the purchase of hardware and equipment.

14.4. LACK OF INFRASTRUCTURE

An inadequate telecommunications infrastructure could pose a problem for automation. In such a situation, data could be exchanged by disc rather than over public networks. The potential for using satellite communications should also be examined.

Access to an uninterrupted power supply may also be problematic for some administrations. In those cases in which systems must be available all the time, the cost of installing a power generator should be included in the project resource requirements.

14.5. CUSTOMS LEGISLATION

Instability in the Customs legislation could make full-scale Customs automation impractical in a single project. Rather than automate an entire system, which might soon be obsolete, it is better to take a modular approach by automating activities and adding them to a core system as needs dictate or as legislative stability allows. An example might be the initial implementation of a duty payment and collection system to which other systems could subsequently be added. Resources could also be dedicated to streamlining an existing manual process to eliminate redundancy in the system.

14.6. RESOURCE AND EXPERTISE LIMITATIONS

If resources are limited, projects should be prioritised according to productivity and efficiency gains in order to optimise resource expenditure. For example, Customs might consider automating the most labour-intensive procedure first to increase productivity.

A Customs authority may not have the in-house expertise required for project implementation. Engaging outside experts requires planning in terms of costs and, perhaps more importantly, in order explicitly to define the role of the consultant(s).
Chapter 16

x x x

Appendix 1 - Information and Telecommunications Structures for Electronic Commerce

1 About E-Commerce

What is electronic commerce? For the purposes of this section, e-commerce is defined as "The process of electronically exchanging information to facilitate the trade of goods and services. An essential component of this process is the integration of business procedures with the appropriate technologies."

The term "electronic commerce" has come into use relatively recently leading some to suppose that it is a new way of conducting business. However, many organisations, including Customs, already utilise aspects of "electronic commerce" in their current operating environment. Information is routinely exchanged electronically between business partners using EDI, e-mail, fax, etc. Essentially "electronic commerce" means doing organisational business electronically. It may perhaps be defined more formally as "a way of conducting business by utilising computer and telecommunications technology to exchange data between independent organisational computer information systems".

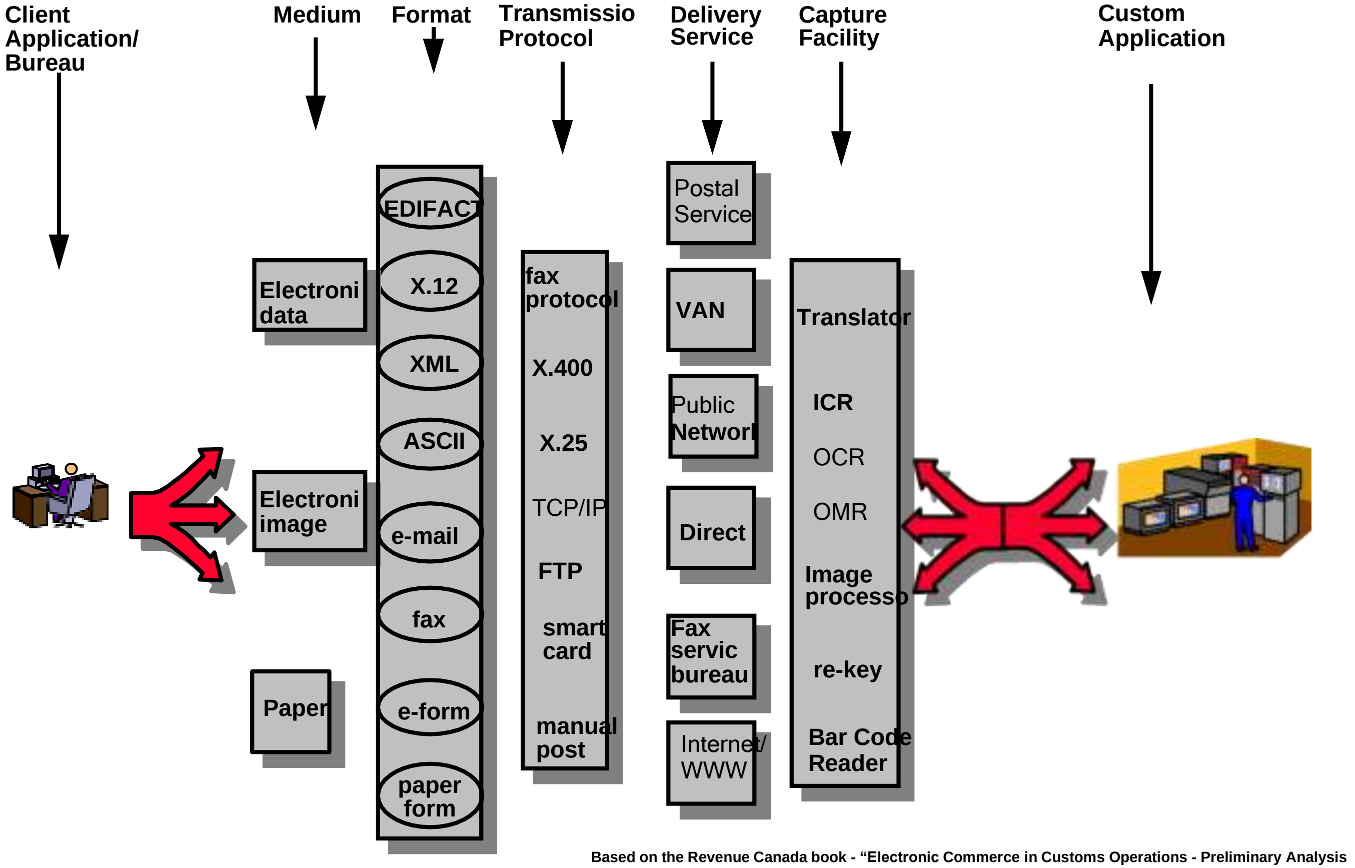
Electronic commerce covers EDI, but it also goes beyond that to encompass all other available technologies that can be utilised for transferring information from one trade participant to another. It is important to remember that information consists of structured data (using standard message formats, direct database record transfer, bar codes), images (unstructured text and pictures) and sound (voice mail, etc.). Today's Customs administrations need to examine the impact that these other technologies can have on their operations. In particular, they need to determine if the use of these technologies can provide cost effective solutions and a more facilitative and flexible service for both the trading community and the other agencies with which they may need to exchange information.

Electronic commerce has already taken a solid hold within Customs. The extensive use of EDI techniques by administrations relates principally to the clearance of goods for import and export. The large-scale transfer of cargo information and goods declaration data from traders to Customs is ideally suited to the application of EDI techniques. It is envisaged that this application of electronic commerce will continue to show a strong growth pattern over the coming decade. However, as the role of Customs expands and as new ways of performing old tasks emerge, there will be an increasing need to exploit some of the other possibilities afforded by the use of electronic commerce in its broadest sense.

The word "e-commerce" is being used as an umbrella term to describe various electronic relationships, all with their own rules and characteristics. The wide range of possible configurations includes business-to-consumer (B2C), business-to-business (B2B), and the three e-government issues, namely, government-to-business (G2B), government-to- citizen (G2C) and government-to-government (G2G).

Electronic Access Channels:

The Diagram below provides a summary of the various access channels that can be provided to the user of services offered by Customs through electronic commerce means.



Client Application/ Bureau

Medium

Electroni data

Electroni image

Paper

Format

EDIFACT

X.12

XML

ASCII

e-mail

fax

e-form

paper form

Transmissio Protocol

fax protocol

X.400

X.25

TCP/IP

FTP

smart card

manual post

Delivery Service

Postal Service

VAN

Public Networl

Direct

Fax servic bureau

Internet/ WWW

Capture Facility

Translator

ICR

OCR

OMR

Image processo

re-key

Bar Code Reader

Custom Application

Based on the Revenue Canada book - "Electronic Commerce in Customs Operations - Preliminary Analysis

Information Exchange Standards

Information exchange standards In the WCO Data Model the focus is on the high-level semantic meaning of data and how to arrange interoperability between government and business. There are three levels of abstraction about a data model, external, physical and conceptual.. The WCO Data Model focuses on the highest level of abstraction, namely the conceptual data model.

WCO Data Model as a Conceptual Data Model

The least abstract models, called External Models, describe specific implementations of a Goods Declaration and the reporting of a Manifest. Typical examples are the CUSCAR message conforming to the WCO DM V.3, and a GOVCBR message conforming to WCO Data Model. .

Physical Models are more general because they describe a set or class of instances, but they still capture the technology in which the instances were implemented. A typical example is the Message Implementation Guide (MIG) for implementing a CUSCAR message, which is included in the WCO Customs Data Model Handbook Version 1.1 released in November 2003.

Conceptual Models remove the implementation technology to emphasise the concepts and meanings that define some classes of document instances. This highest level of abstraction is newly introduced in WCO Customs Data Model Version 2.0. Typical examples are the UML Class Diagrams for all document types, the UML Class Diagrams for a single document type, and the inventory of all 450 data elements collectively known as the WCO Data Model Data Set.

Necessity of the Conceptual Model

Customs business, like most other business areas, does not change as rapidly as technology. If the WCO Data Model is only described in any specific technology (e.g. through a Physical Data Model such as EDIFACT), it will be necessary to define the Data Model in each upcoming technology. Even then, it will be very difficult, if not impossible, to guarantee that the Physical Data Models in different technologies are equivalent.

By establishing a Conceptual Model and capturing all business rules in the Conceptual Model, Trade will be able to implement customs documents in whichever technologies (i.e. Physical Data Models) that fit its needs.

Other benefits of establishing a Conceptual Model

There should be less confusion because the semantic meaning and presentation rules of a data element are preserved in different Physical Models, which are derived from the same Conceptual Model. For example, the class “Transport Equipment” means “the physical resources needed to contain or restrain consignment(s) for transportation” and includes the same class attributes whether the class is used in Import Declaration, Export Declaration, Export Cargo Report, Import Cargo Report, Conveyance Report and Transit Report.

Interoperability with data models of Other/Participating Government Agencies and Trade is much easier by having one single meaning for each data element across all customs documents. For example, the UN/CEFACT transport term “Transport Equipment” can be directly mapped to the WCO Data Model class “Transport Equipment”.

In Version 3.0, the benefits of the development of a conceptual model are apparent. WCO Data Model. Since the publication of Release 3.3 into two parts:

122.

(i) **The standardized components** (the Data Set, information models, business process models, code lists) and

(ii) **Information Packages** (Message implementation Guidelines & XML Schemas reflecting electronic data exchange templates to suit the needs of a business purpose).

An 'Information Package' addresses the means by which the standardized components of the WCO Data Model have been put together and are used in order to meet the needs of a given business purpose. Information Packages mainly contain templates for electronic data exchange but can also be used to explain the business meaning behind the structured information used in information exchange. Information
Packages were previously called "Electronic Messages". These templates are of numerous types including cross -border regulatory declarations (import, export, cargo report at import, cargo report at export, transit declaration etc.) & Government-to -Business Responses and Government to Government exchanges.

Further, Licenses, Permits Certificates and other types of "single window" exchanges were included in Release 3.3.

Data Model Information Packages can be seen as having a hierarchical structure. The WCO Base Information Packages includes the basic transaction patterns in a Single Window environment inter alia:

• Business-to-Government messages such as IM (Import Goods Declaration),
EX (Export Goods Declaration), CRI (Cargo Report Import), CRE(Cargo Report Export), CONV(Conveyance Report), TRT(Transit) advance information etc;

• Government-to-Business messages such as Notification of Release or Declaration status messages;

• Any-to-Any exchanges concerning licenses certificates, permits and other types of authorization

• Government-to-Government messages concerning guarantee management for temporary admissions and other types of exchange.

The Base Information Packages reflects the maximum data requirement in a given context of use. Building on these packages, the DMPT as part of its work on implementation support, developed commonly used formats, calling them "Derived Information Packages". Typically, these so-called "Derived Information Packages," are based on globally standardized electronic templates such as the
electronic International Maritime Organization (IMO) FAL forms, the EU Single Administrative Document, CITES e-Permits, the WTO Valuation Declaration, Guarantee Management in the context of TIR Carnet etc.

Members and other organizations that are already using or are in the process of implementing the Data Model in real world data exchanges may go even further in terms of local “customization” and produce a so-called "My Information Package". This highly specific information package aims to explain the manner in which the individual components of the WCO Data Model have been adopted or used in their particular business contexts in a particular implementation. It can be developed more easily by drawing-upon a ‘Derived Information Package’ that is similar. For example, a Member using a Customs declaration form based on the ‘Single Administrative Document’ can produce its own ‘My Information Package’ starting from the corresponding Derived Information Package published by the WCO. Similarly, a Member can produce a ‘My Information Package’ covering requirements for national cargo reporting requirements.

Such a package can explain how the national requirements relate to the IMO FAL Forms as well as to the WCO Data Model.

The production of a ‘My Information Package’ would be the concern of the Members and organizations using the WCO Data Model. The DMPT is working on the question of how a national usage of the WCO can be represented in a standard “machine readable” WCO XML template. Such a template would not only make it possible to produce a spreadsheet comparing the national usage of different elements of the WCO Data Set, but it would also allow the data from a “My Information Package” to be copied automatically into a solution provider’s tools and thus facilitates the faster introduction of practical solutions for data exchange.

Information Exchange: Changing landscape

In the earlier EDI scenario this information is supplied to Customs using such international standard messages as:

CUSDEC: UN/EDIFACT Customs Declaration Message

CUSCAR: UN/EDIFACT Customs Cargo Report Message

CUSREP: UN/EDIFACT Customs Conveyance Report Message

CUSRES: UN/EDIFACT Customs Response Message

CUSEXP: UN/EDIFACT Customs Express Consignments Message

In the EDI environment there are currently several other international UN/EDIFACT messages available for use, for example, CUSDEC and GESMES (for statistics), PAXLST (for crew/passenger lists) and SANCRT (for various licence and certificate requirements).

Currently, the WCO Data Model includes an EDIFACT message GOVCBR, which covers most requirements of cross-border regulatory agencies. An administration could potentially use GOVCBR for all its messaging requirements instead of maintaining numerous mappings of theEDIFACT messages.

Transaction Patterns:

Information exchange between trading partners involve different transaction patterns (based on ebXML taxonomy). These include:

(i) Make an offer- Accept an offer:
[Example: Customs enrols a trading partner on to its internet based application by offering a list of terms and conditions of use, trading partner accepts those terms and conditions.]

(ii) Request Information - Provide Information
[Example: Trading partner requests for information on duties and taxes for an item s/he intends to import. Customs provides the information.]

(iii) Request for Confirmation- Receive a response of confirmation (or rejection)
[Example 1: Trading partner submits a declaration seeking the release of goods. Customs confirms or denies the release of goods

Example 2: Trader files a guarantee and seeks confirmation of registration of the guarantee. Customs registers guarantee and confirms.]

(iv) Raise a Query – receive an answer
[Example: Customs raises a query with the Trading Partner seeking further clarification on the nature of the product being imported and receives an answer.]

(v) Issue a Notification to a trading partner
[Customs notifies a trading partner regarding the status of his fiscal accounts.]

(vi) Distribute tailored information to trading partners
[Customs distributes information to all trading partners regarding the status of their respective goods.]

. Using Internet and E-Commerce techniques, and following one of the above transaction patterns described above, it is easy to give the trading partner exclusive access to his own domain in the Customs database. Information can be provided by the database publishing method. Typically, access to the following data will be allowed:

≡ trading partner registration database (the balance of the current guarantee amount, party name and address details)

- administrative messages (information about system changes, updates, etc.)
- goods status (goods released, held for examination, request for more information, uncleared declarations)
- anti-dumping/countervailing duty rates
- error statistics
- currency rates
- tariff database (nomenclature and harmonised tariff schedule details)
- quota rates
- region/district/port codes
- country codes
- foreign port codes
- amount and status of refund
- Customs fines and penalties (paid over a certain period)
- binding tariff information (for goods subject to import/export)

However, before access to this information is allowed, a number of issues need to be addressed, particularly the question of copyright, privacy & data protection and fees.

The issue of copyright, in the information made available to the public, is very important, especially with regard to such information as harmonised tariff schedules. Individual Member administrations will need to address the question of the right to publish updated tariff schedules. Customs should also ensure that they have permission to publish information received from other organisations. Internet technology makes it possibleto hyperlink from the Customs web site to the web sites of other (government) agencies.

The question of collecting or charging fees for making certain information available should also be addressed. For example, most national administrations charge trading partners for their tariff schedule publications and updates. In an electronic environment administrations will have to decide whether or not such fees should be charged. Before Customs disseminates information free of charge it should take into account the origin of that information and whether its owner normally charges for its dissemination.

The question of privacy & data protection needs to be addressed adequately while allowing access to customs databases. Nominal data and commercial data submitted to customs in confidence be subject to national legislation on privacy and data protection.

Allowing Customs to access trading partners' databases can increase the efficiency of cargo and passenger processing. Accessing an airline's passenger database, for example, can help to identify passengers for further control prior to their arrival. Similarly, accessing a shipper's database will allow Customs to identify high-risk consignments.

Codes

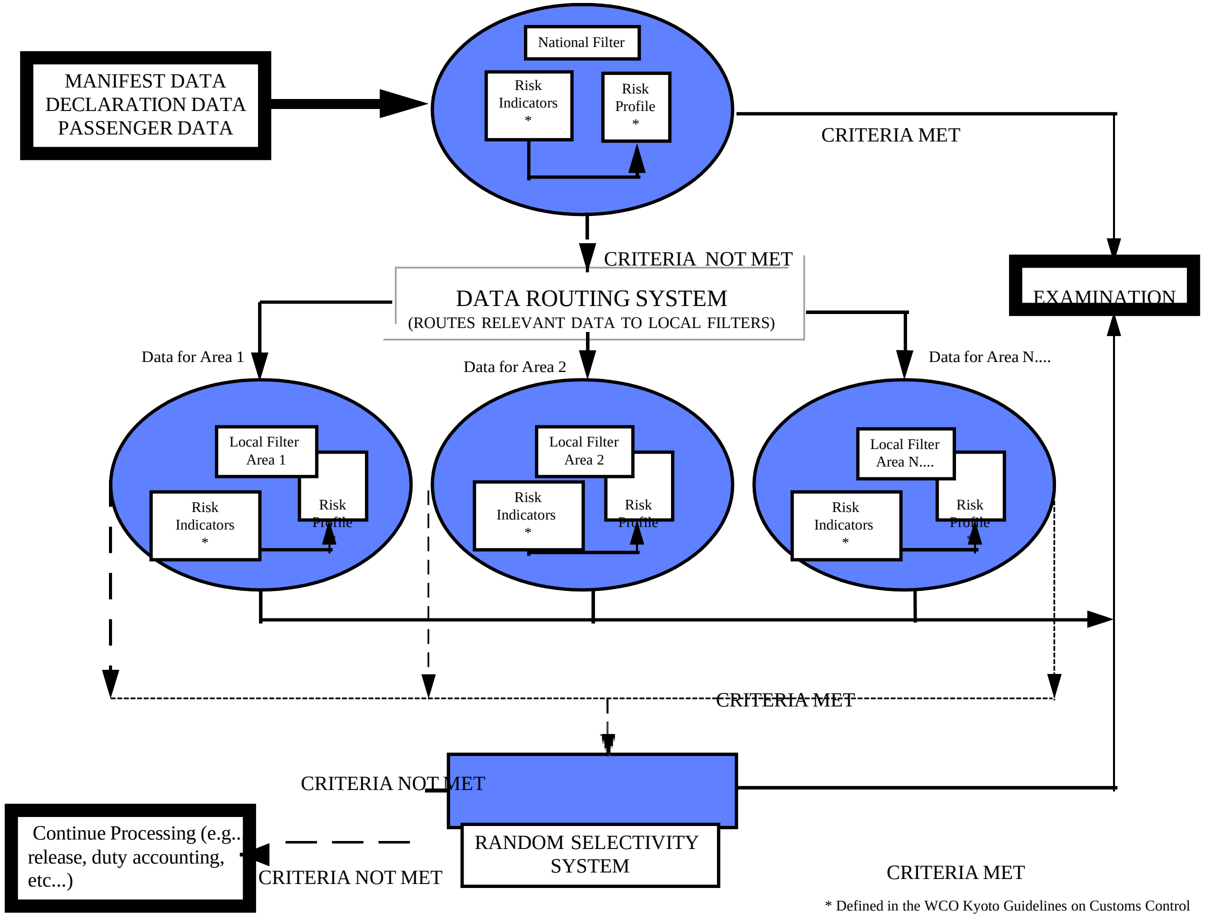
(Standards 3.11 and 7.2)

In information exchange codes and identifiers hold a very important place. The WCO recommends the use of international codes, such as ISO country and currency codes, UN transport codes, the WCO Convention on the Harmonised Commodity Description and Coding System, etc. (see Appendix 9). The use of available international codes will maximise the openness and accessibility of Customs systems. The harmonised use of codes at application level will do much to facilitate international trade. It will help simplify systems development for trading partners and other government agencies that wish to communicate with Customs. It will also make the exchange of information between Customs administrations more viable.

Recommendations

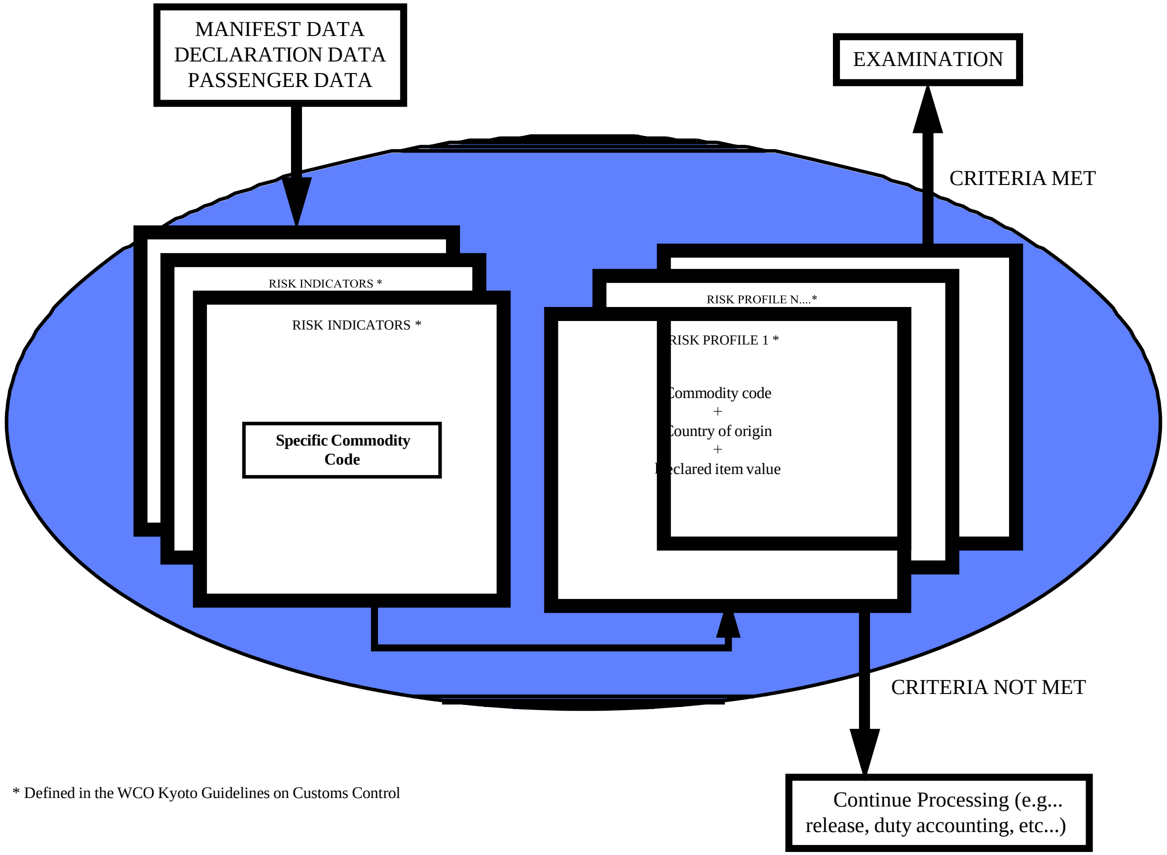
To implement e-commerce technologies successfully, in addition to its information systems infrastructure, Customs will need to have the necessary community consultation, operational and human resource capabilities in place. Firstly, the Customs administration will need to have a very clear picture of its internal capabilities as well as the expectations of external parties. This will require consultation with the various departments that make up the administration and with those external parties that will eventually participate in e-commerce with the Customs. Secondly, after reviewing the legal and policy implications, the Customs administration should draw up an e-commerce strategy and a draft implementation plan for endorsement by its top management and the external parties involved. Thirdly Customs should strive to align its requirements based on the WCO Data Model and produce national 'My Information Packages', providing the transparency necessary to bring down costs of of doing business .

Appendix 2 - Local Selectivity Process



* Defined in the WCO Kyoto Guidelines on Customs Control

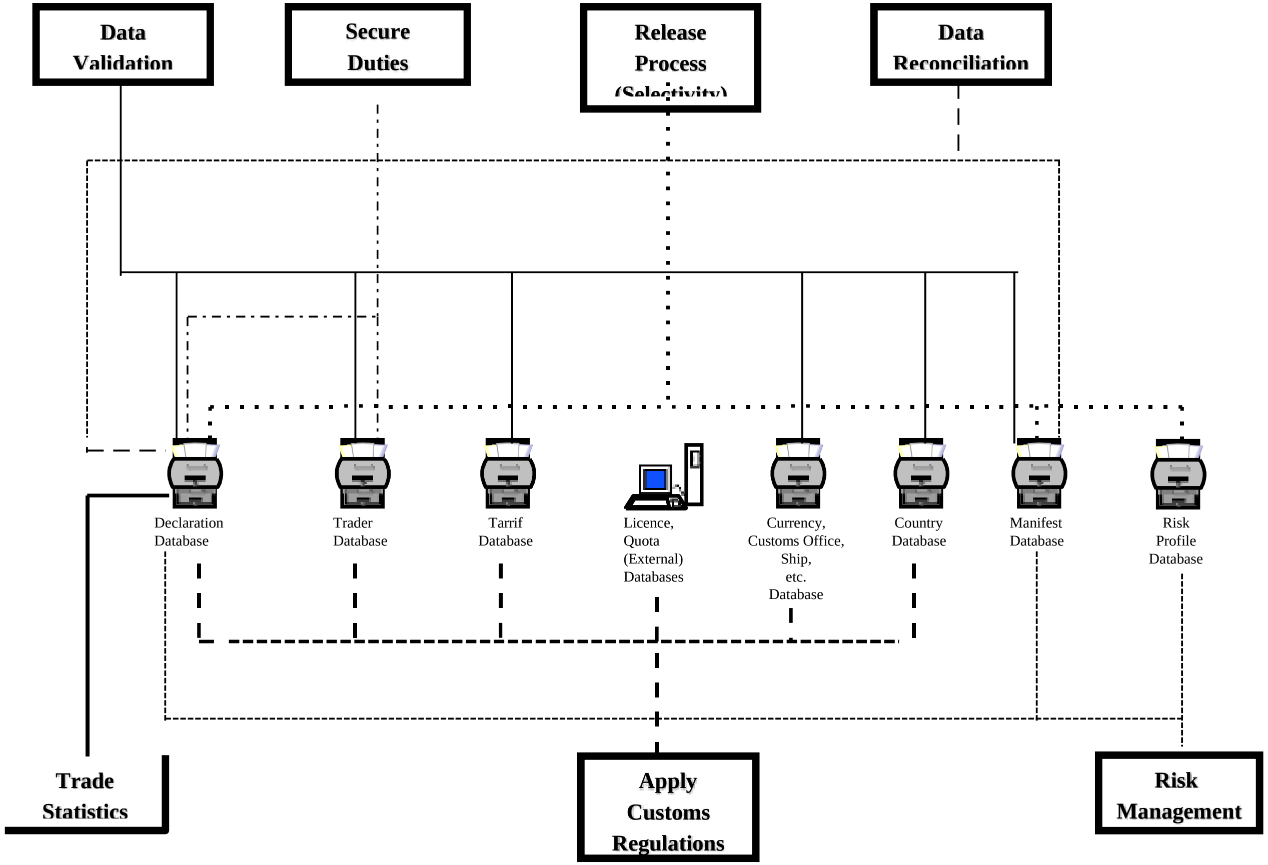
Appendix 3 - Selectivity Profile Filter System



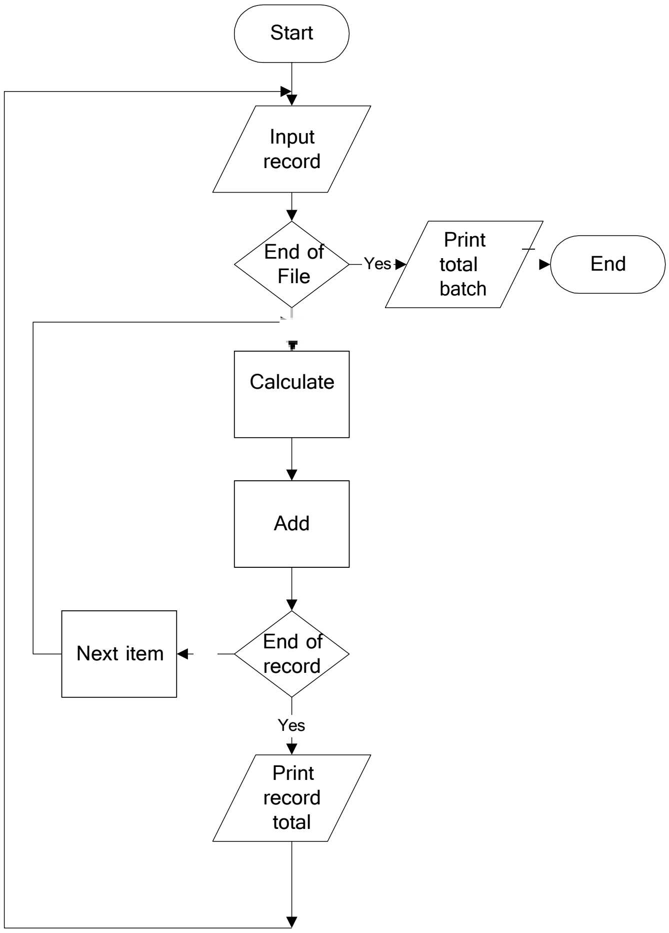
* Defined in the WCO Kyoto Guidelines on Customs Control

x x x

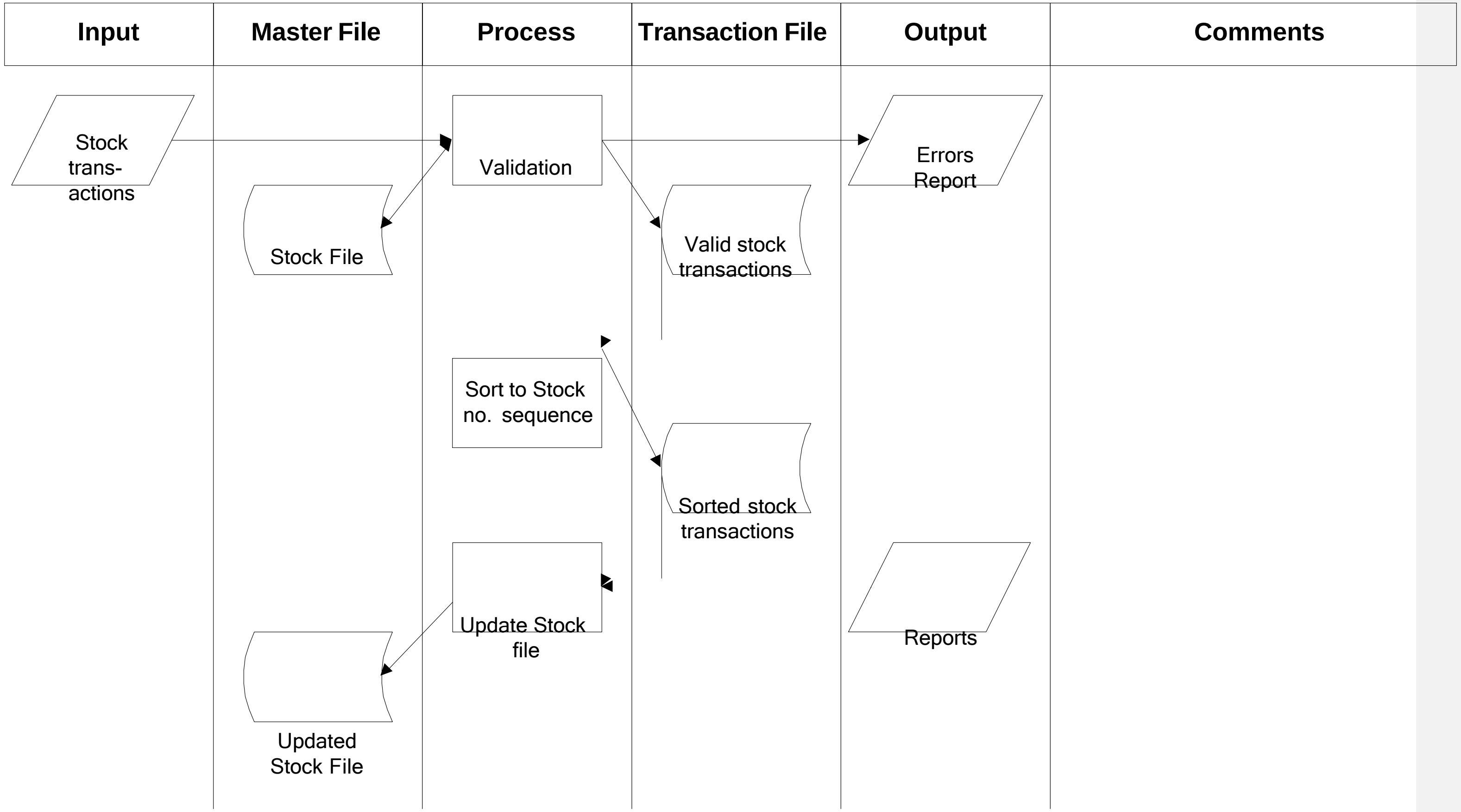
Appendix 4 - Example Customs Process/File Access



Appendix 5 - Program Flowchart



Appendix 6 - Computer Run Chart



Appendix 7 - Glossary of terms and abbreviations

application A program or suite of programs written for a specific user activity.

authentication In data security, controls that either prevent or detect the tampering and/or accidental destruction of data,including message sender and receiver identity.

biometrics Biometrics are automated methods of recognising a person based on physiological characteristics (www.biometrics.org)

block diagram A diagram of a system in which the principal parts are represented by suitably annotated geometric figures to show both the function of components and their inter-relations.

central processor The unit containing the circuits that control and perform the execution of instructions.

cookie Tokens placed on a user's computer that can be used to recognise a user's machine. (www.techweb.com/encyclopedia)

communication network A system of interconnected communication facilities.

communications controller An intelligent unit which provides line oriented interface functions, e.g. error detection, synchronisation, between a group of modems and a computer or communication network processor.

computer interface A shared boundary between two related components.

countermeasure An action taken to counteract a danger, threat, etc.

CPS Certificate Practice Statement

cryptography The conversion of data into a secret code for transmission over a public network.(www.techweb.com/encyclopedia)

data capture The act of entering data by means of peripheral devices e.g. a keyboard.

data processors Someone who performs operations on data to achieve a desired objective.
134.

database A collection of inter-related data stored so that it may be accessed by authorised users with simple user-friendly dialogues.

database schema A map of the overall logical structure of a database.

dial-up line A telecommunications line for computer to computer communication which requires the sender to physically dial a telephone number before communication between the two systems can be initiated.

digital signature A property private to a user or process that is used for signing messages over a communications link.

Direct Trader Input A system in which declarations are input into the Customs computer system by the declarants themselves, from terminals normally situated in their own offices or via commercial third-party networks.

document Any medium (including magnetic tapes and disks, microfilm and EC messages) designed to carry and actually carrying a record of data entries.

DTI See Direct Trader Input.

EC See Electronic Commerce.

EDI See Electronic Data Interchange.

EDI translator A device that converts information from application format to the agreed EDI format for sending and vice versa for receiving.

EFT See Electronic Funds Transfer.

Electronic Commerce A way of conducting business by utilising computer and telecommunications technology to exchange data between independent organisational computer information systems

Electronic Data Interchange The transmission of data structured according to agreed message standards, between one computer system and another, by electronic means.

electronic forms A document in which certain items have been pre-coded and into which variable information is entered.

Electronic Funds Transfer An automated system for transferring funds from onebank account to another using electronic equipment and data communications

Examples: e-money, debit card, credit card, Electronic Bill Presentment Payment (EBPP)(www.ebilling.org)

Electronic Funds Transfer security / protocols / systems Secure Sockets Layer (http://home.netscape.com/eng/ssl3/ssl-toc.html)

Secure Electronic Transaction (www.setco.com) or (www.setco.org)

I-Pay (www.I-Pay.com)

MicroPayments (www.w3.org/ECommerce/Micropayments/#About)

Open Electronic Wallet System (www.PCSCworkgroup.com)

electronic mailbox A place to store message packets at intermediate points prior to further transmission. Incoming messages are stored in the addressee’s mailbox and retrieved later by the addressee.

encryption Reversible transformation of data (called "plaintext") into a form (called "cipher text") that conceals the data's original meaning to prevent it from being known or used.
(www.techweb.com/encyclopedia)
(http://www.sans.org/resources/glossary.php)

feasibility stage The stage in the implementation of a system in which the proposed system is evaluated for technical and financial considerations. It is used as the basis for deciding whether to proceed to the next stage.

flowchart A pictorial representation of a process (logical or physical).

Graphical User Interface A program interface that takes advantage of the computer's graphics capabilities to make the program easier to use. Well-designed graphical user interfaces can free the user from learning complex command languages. On the other hand, many users find that they work more effectively with a command-driven interface, especially if they already know the command language. Microsoft Windows is an example.

GUI See Graphical User Interface.

hardware Physical equipment such as disk drive, PC or printer.

HTML See HyperText Markup Language.

HyperText Markup Language The language used to create pages on the Web. Pages are written in regular text and then HTML tags are applied to format the text to display it with WWW browser software. Tags include formatting options, links to other pages, graphics. HTML is machine independent.

ICT See Information and Communication Technology

IETF Internet Engineering Task force (http://www.ietf.org/)

information exchange In the context of this document it is the electronic exchange of information between computer systems.

Information and Communication Technology The management, acquisition, processing, storage and dissemination of vocal, pictorial, textual and numeric information by a micro-electronics based combination of computing and telecommunications.

integrity The preservation of programs or data for their intended purpose against loss or corruption.

international standard A formally recognised global standard agreed through a recognised international standard setting body, e.g. ISO, UN/ECE, etc.

Internet An international open computer network environment linking computers from educational institutions, government agencies, industry etc.

ISO International Standards Organisation. (www.iso.org)

IT See Information and Communication Technology.

leased line A line hired by a subscriber for his or her exclusive and permanent use.

Management Information System A system designed to provide management and supervisory staff with required data that is accurate, relevant and timely, sometimes on a real-time basis.

MIS See Management Information System.

modem MOdulator-DEModulator - a device that modulates the transmitted signal and demodulates the received signal, e.g. a modem is used to convert a digital signal from a computer into an analogue signal for transmission, usually over a telephone network.

non-repudiation The ability to prevent a sender or receiver of a message denying responsibility for sending or receiving the message.

ODA See Open Document Architecture.

on-line A system in which the data or instructions are inserted directly from the point of origin and the output data is transmitted directly to the appropriate recipient.

Open Document Architecture Architecture aimed at 'blind information interchange' This means that two systems can interchange documents, maintaining their layout and revisability without any prior knowledge other than that both systems support a particular standardised profile of the international ODA standard. ODA offers an architecture, which can cope with the majority of documents likely to be found in office environments.

PIN Personal Identification Number

PKI A PKI is an automated system that manages the generation, maintenance, and delivery of encryption and digital signature keys. Both key types, encryption and digital signature, have two related components: a public-key component that is accessible to all users, and a private-key component that must be secured from access by others. The public key and other identification information are stored in a digital certificate that is digitally signed by a Certification Authority (CA). The digital signature of the CA on the digital certificate binds the identity of the end-entity with its public-key. It also guarantees that the public key has not been tampered with.

protocol A formally specified set of conventions governing the format and control of inputs and outputs between two communicating systems.

secure sockets layer See SSL

SMIME Secure Multipurpose Internet Mail Extension (www.ietf.org/html.charters/smime-charter.html)

SMTP Simple Mail Transfer Protocol (http://www.techweb.com/encyclopedia/)

software The programs, procedures, routines and possibly documents associated with the operation of a data processing system.

source data An invoice, form, voucher or other form of written evidence of a transaction from which the basic data is extracted for processing.

SSL Secure Sockets Layer. A protocol developed for transmitting private documents via the Internet. (http://www.sans.org/resources/glossary.php)

telecommunications network See communication network.

TLS A protocol that ensures privacy between communicating applications and their users on the Internet. (www.sans.org/resources/glossary.php)

transport layer security See TLS

trojan codes A malicious code hidden inside a legitimate piece of software.

turn-key system A complete system of hardware and software delivered to the customer ready-to-run. This normally includes the installation, adjusting and testing (technical) of the system by the supplier. Just "turn the key" and go.

UN/EDIFACT United Nations/Electronic Data Interchange For Administration, Commerce and Transport.

UNCITRAL United Nations Commission on International Trade Law. (www.uncitral.org)

user specification The formal report identifying, in detail, all the requirements specified by the user of a computer system under development.

Value Added Network A communication service using communications common carrier networks for transmission and providing added data services with separate additional equipment. Added services may include store and forward message switching, terminal and host interfacing.

VAN See Value Added Network.

VDU See Visual Display Unit.

virtual shop A shop that may not exist in reality but made by software to appear to do so.

Visual Display Unit A device which permits the user to input information to a computer via keyboard, light-pen or touch-screen facilities and to view the computer output, text or graphics on a cathode-ray tube screen.

World Wide Web The graphical layer applied above the Internet. Where the standard Internet is text only, the Web is graphical in nature. Text and graphics, stored on servers, are transmitted via the network to client browsers where they are displayed.

WWW See World Wide Web.

X.21 General purpose interface between data terminal equipment and data circuit terminating equipment for synchronous operation on public data networks.

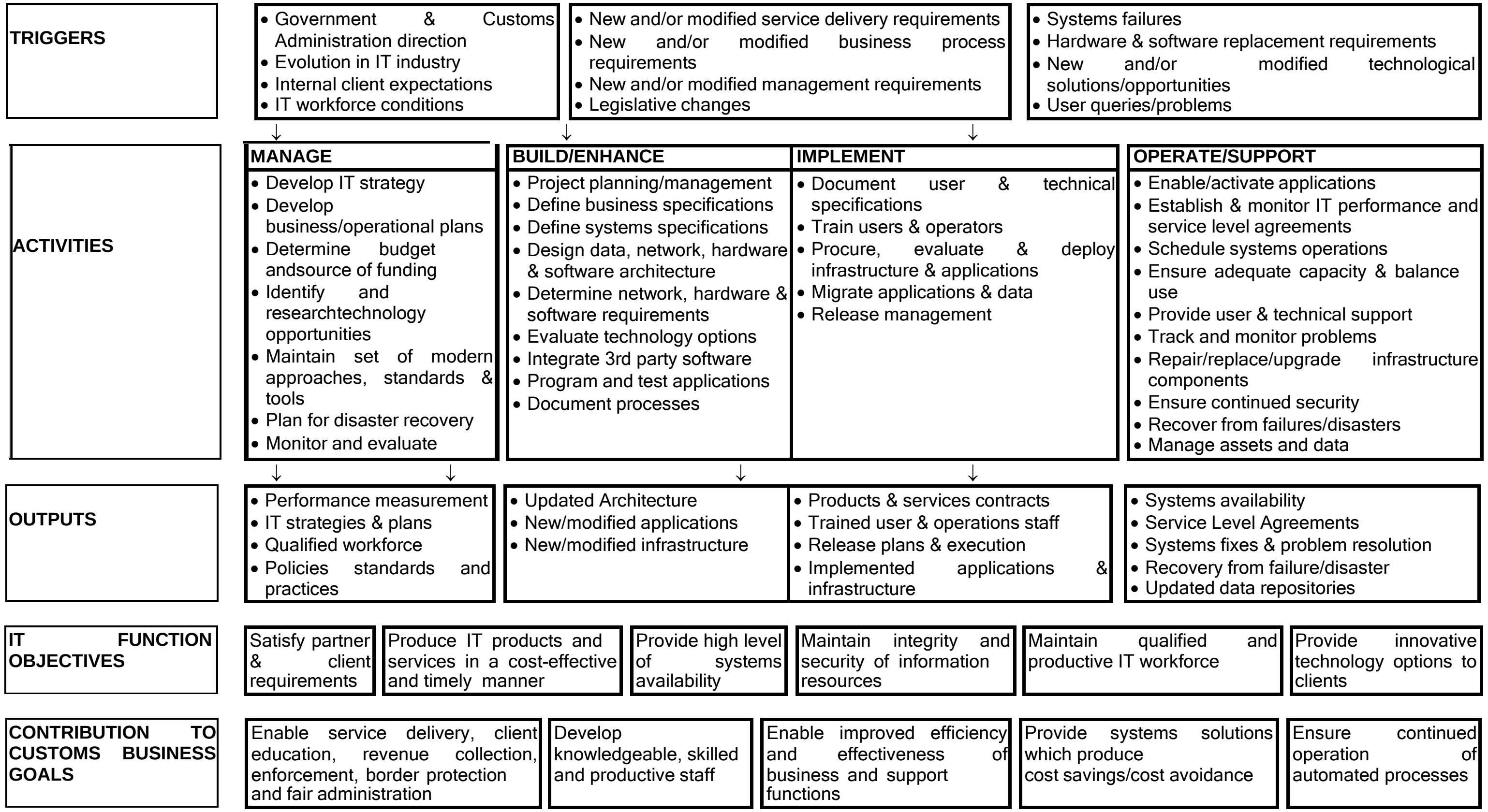
X.25 An interface between data terminal equipment and data circuit terminating equipment for terminals operating in the packet mode on public data networks.

X.400 Message handling facility.

X.509 A certificate (see PKI) used to verify certain information exchanged over a network (e.g., the internet). It contains the key holder's public key and some identifying information which confirms that both the key holder and certificate issuer are who they say they are. Certificates are stored on publicly accessible directories, like the X500 directories

XML eXtensible Markup Language (www.xml.org)

Appendix 8 - Information technology function logic chart



TRIGGERS

- Government & Customs Administration direction
- Evolution in IT industry
- Internal client expectations
- IT workforce conditions

- New and/or modified service delivery requirements
- New and/or modified business process requirements
- New and/or modified management requirements
- Legislative changes

- Systems failures
- Hardware & software replacement requirements
- New and/or modified technological solutions/opportunities
- User queries/problems

ACTIVITIES

MANAGE

- Develop IT strategy
- Develop business/operational plans
- Determine budget andsource of funding
- Identify and researchtechnology opportunities
- Maintain set of modern approaches, standards & tools
- Plan for disaster recovery
- Monitor and evaluate

BUILD/ENHANCE

- Project planning/management
- Define business specifications
- Define systems specifications
- Design data, network, hardware & software architecture
- Determine network, hardware & software requirements
- Evaluate technology options
- Integrate 3rd party software
- Program and test applications
- Document processes

IMPLEMENT

- Document user & technical specifications
- Train users & operators
- Procure, evaluate & deploy infrastructure & applications
- Migrate applications & data
- Release management

OPERATE/SUPPORT

- Enable/activate applications
- Establish & monitor IT performance and service level agreements
- Schedule systems operations
- Ensure adequate capacity & balance use
- Provide user & technical support
- Track and monitor problems
- Repair/replace/upgrade infrastructure components
- Ensure continued security
- Recover from failures/disasters
- Manage assets and data

OUTPUTS

- Performance measurement
- IT strategies & plans
- Qualified workforce
- Policies standards and practices

- Updated Architecture
- New/modified applications
- New/modified infrastructure

- Products & services contracts
- Trained user & operations staff
- Release plans & execution
- Implemented applications & infrastructure

- Systems availability
- Service Level Agreements
- Systems fixes & problem resolution
- Recovery from failure/disaster
- Updated data repositories

IT FUNCTION OBJECTIVES

Satisfy partner & client requirements

Produce IT products and services in a cost-effective and timely manner

Provide high level of systems availability

Maintain integrity and security of information resources

Maintain qualified and productive IT workforce

Provide innovative technology options to clients

CONTRIBUTION TO CUSTOMS BUSINESS GOALS

Enable service delivery, client education, revenue collection, enforcement, border protection and fair administration

Develop knowledgeable, skilled and productive staff

Enable improved efficiency and effectiveness of business and support functions

Provide systems solutions which produce cost savings/cost avoidance

Ensure continued operation of automated processes

Appendix 9 - WCO Recommendations on IT

RECOMMENDATION OF THE WORLD CUSTOMS ORGANIZATION[1] CONCERNING A UNIQUE CONSIGNMENT REFERENCE (UCR) FOR CUSTOMS PURPOSES (26 June 2004)

THE WORLD CUSTOMS ORGANIZATION

HAVING REGARD to the global nature of international trade

DESIRING to contribute to the security and facilitation of the international movement of goods through Customs and other administrative procedures and to reduce the burdenassociated with international trade procedures to a minimum

DESIRING to increase the effectiveness and efficiency of Customs Administrations in dealing with international trade transactions

RECOGNIZING the increasing importance for international Customs co-operation to ensure better Customs compliance and facilitation of legitimate trade

RECOGNIZING the efforts and investments made in particular by the private sector in modern logistics, inventory control, manufacturing and information systems

TAKING ACCOUNT of existing standards developed by the International Standards Organization (ISO) and the United Nations on unique numbering systems

RECOMMENDS that Members of the Council and members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions, should adoptand implement a Unique Consignment Reference (UCR) in close consultation with their trade bodies and transportation industries which should be,

- used for all international trade transactions;

- applied at consignment level, with a consignment being identified as "the total number of items specified in the commercial contract between the supplier and the customer and transported in a single or in multiple shipments";

- used as an access key for audit, consignment tracking, information consolidation and reconciliation purposes;

- able to uniquely identify data related to individual international trade transactions between a supplier and a customer at both the national and international level for a sufficient period of time in accordance with national data retention rules;
- associated with other relevant trade or transport references to establish an origin to destination information and documentation trail for the individual consignment, in case

[1] Established in 1952 as the Customs Co-operation Council (CCC), hereafter referred to as the Council

that the UCR, as defined in the accompanying Guidelines is not already used as the transport reference;

- issued for all consignments by or on behalf of the party having initiated the international trade transaction

- used in all relevant communications by all parties involved in the entire supply chain with regard to Customs and all other relevant regulatory agencies ;

FURTHER RECOMMENDS that the Unique Consignment Reference as specified in this Recommendation and its accompanying Guidelines be structured in accordance with :

ISO Standard 15459 Part 1 and Part 2 on unique identification (The ISO license plate) and future updated versions;
or where this standard is not yet applied

other relevant standards or industry specific reference numbers not exceeding 35alphanumeric characters enabling a unique origin-to-destination information and documentation trail of the entire international trade transaction.

REQUESTS Members of the Council and members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions which accept this Recommendation to notify the Secretary General of the Council of the date from which they will apply the Recommendation and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members of the Council. He will also transmit it to the Customs administrations of the members of the United Nations Organization or its specialized agencies and to Customs or Economic Unions that have accepted this Recommendation.

FURTHER REQUESTS the Secretary General to work with relevant international organizations such as the United Nations Economic Commission for Europe to ensure that this Recommendation is being reflected in their respective instruments and recommendations.

x
x x

Appendix 10 - WCO Recommendations on the use of web sites by Customs administrations

CUSTOMS CO-OPERATION COUNCIL

TC2-3855

RECOMMENDATION OF THE CUSTOMS CO-OPERATION COUNCIL CONCERNING THE USE OF WORLD WIDE WEB SITES BY CUSTOMS ADMINISTRATIONS (26 June 1999)

THE CUSTOMS CO-OPERATION COUNCIL,

DESIRING to facilitate the international movement of goods and people through Customs,

DESIRING to facilitate access to, and dissemination of, Customs regulatory information in the public domain, particularly for travellers and participants in international trade,

CONSIDERING the importance of making relevant regulatory information available to the public in a cost-effective and easily accessible manner,

HAVING REGARD to the widespread acceptance of the Internet and World Wide Web (WWW) as a means of communication and information dissemination,

HAVING REGARD to growing use of the Internet and WWW by Customs administrations,

RECOMMENDS that Members of the Council and members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions, should implement a Customs World Wide Web site for their administration,

FURTHER RECOMMENDS that Members of the Council and members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions, should make available on Customs administration web, sites, where practical or feasible, the data content as specified in the Annex to this Recommendation,

REQUESTS Members of the Council and members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions which accept this Recommendation to notify the Secretary General of the Council of the date from which they will apply the Recommendation and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members of the Council. He will also transmit it to the Customs administrations of the members of the United Nations Organization or its specialized agencies and to Customs or Economic Unions that have accepted this Recommendation.

*

* *

Annex to the Recommendation on Customs Web Sites

Basic information to be made available on Customs web sites

Information for travellers

- General overview of Customs
- Comprehensive details of duty-free allowances
- Comprehensive details of prohibited goods for import and export
- Information about Customs channels (dual-channel system)
- Penalties for Customs offences
- Contact information (including e-mail address) for further information
- Links to other relevant sites, especially immigration and agriculture
- Multiple language versions of the information.
- Access to official publications

Comprehensive details of duty-free allowances

Details on duty-free allowances should cover all products, including quantities and maximum values. The conditions under which duty-free privileges are given should be covered such as origin of the journey, length of stay, the age of the traveller, etc. In some cases, especially where economic zones are concerned, different allowances are available depending upon where the journey has originated and these differences should be clearly indicated.

Comprehensive details of prohibited goods for import and export

Goods that are prohibited or restricted should be clearly identified, e.g. arms and ammunition, live animals, certain types of plants, ivory, currency, etc. Penalties for breaches of the legislation should also be highlighted.

Information about Customs channels (dual-channel system)

Information on how the dual channel system works and how passengers declare goods to Customs on arrival should be presented. This should include examples of Customs forms to be completed.

Penalties for Customs offences

A comprehensive set of information should be given, indicating what penalties a traveller should expect to receive if caught deliberately breaking the law.

Contact information (including e-mail address) for further information

Customs contact information for travellers, especially a public e-mail address, should be given to allow the public to make specific enquiries.

Links to other relevant sites, especially immigration and agriculture

Links to other government web sites such as immigration, tourism and agriculture should, where possible, be established to help visitors obtain complete information on all regulatory requirements necessary upon arrival in the country.

Multiple language versions of the information

Tourism is a very important part of the economy for many countries. Significant numbers of visitors may not speak the native language of the country they are visiting. The Customs administration should have information available for travellers in a number of other languages.

Access to official publications

Access to various official publications, brochures, etc. should be made available for downloading or ordering through the web site. Consideration should be given to the format used for documents being made available for downloading.

Information for traders

- General overview of Customs
- Overview of Customs procedures and legislation
- National legislation including Customs regulations on all the Customs procedures
- Tariff and duty information
- Currency rates of exchange
- Details of prohibitions and restrictions
- Details of how to complete a Customs declaration
- Classification decisions
- Penalties for Customs offences
- Contact information (including e-mail addresses)
- Links to other government agencies
- Access to official publications

Overview of Customs procedures and legislation

This section would give a general overview of the various Customs procedures and the legislation under which they operate. It should be considered as a broad introduction to Customs business. Links to the more detailed explanations of particular procedures or sections of national legislation should be established.

National legislation including Customs regulations on all the Customs procedures

Placing the texts of national legislation covering international trade (imports, exports, transit, etc.) on the WWW is a basic requirement of a Customs web site. However, in most cases the legislation is in plain text without any hypertext links. To make this more useful to traders, Customs administrations should establish, where possible, hypertext links to important references throughout the body of the documents.

Search engines should also be made available on the web site to allow users to conduct key word searches.

Tariff and duty information

Basic information on tariff and duty rates for various classes of goods should be made available. Access to a complete electronic version of the national tariff would be the most useful. However, at the minimum a copy of the paper version of the tariff should be made available in a “pdf” format (portable document format). This would allow the trader to download the document for viewing and printing only.

Currency rates of exchange

A list of the official currency rates of exchange for Customs purposes should be a basic element included on the web site.

Details of prohibitions and restrictions

Details of prohibited or restricted goods, goods covered by quota and similar prohibitions or restrictions should be highlighted. Special conditions for the importation or exportation ofsuch goods should be clearly indicated.

Details of how to complete a Customs declaration

A user guide on how to complete a Customs declaration is most useful to traders and improves the quality of data input to Customs systems. Most Customs administrations already have this type of guide in paper form. Customs administrations should convert this guide into a format that could be placed on the web, and such a “training guide” should be developed into a comprehensive interactive programme.

Classification decisions

Traders frequently need information about classification issues. All official classification decisions therefore should be made available on the Customs web site, thereby reducing the need to directly contact Customs officials for the information.

Penalties for Customs offences

A comprehensive set of information should be given indicating what penalties a trader should expect to receive if caught deliberately breaking the law.

Contact information (including e-mail addresses)

As with the information for travellers, contact details (including e-mail addresses) for Customs officials dealing with specific issues should be given.

Links to other government agencies

Links to such other web sites as the Ministries of Trade and Finance and the national Chamber of Commerce should be included.

Access to official publications

Access to various official publications, brochures, etc. should be made available for downloading or ordering through the web site. Consideration should be given to the format used for documents being made available for downloading.

Developing computer applications on the web

The information being made available to traders and travellers may become static, i.e. the readers can receive the information and print it, but generally cannot integrate it into their own applications. Customs administrations should develop interactive applications that can be used either by external clients or internal staff members.

x

x x

Appendix 11 - WCO Recommendations on the WCO Data Mapping Guide

CUSTOMS CO-OPERATION COUNCIL

TC2-3845

RECOMMENDATION OF THE CUSTOMS CO-OPERATION COUNCIL[*]
CONCERNING THE USE OF THE WCO DATA MAPPING GUIDE
FOR CUSTOMS UN/EDIFACT MESSAGES
(21 June 1995)

THE CUSTOMS CO-OPERATION COUNCIL,

DESIRING to facilitate the international exchange of data between Customs administrations and between Customs administrations and trade users,

CONSIDERING that UN/EDIFACT messages can be used independently of the application area and that their widespread use in international trade will greatly facilitate movement of cargo,

FURTHER CONSIDERING that it is desirable that an internationally agreed and universally applicable set of rules for the usage of Customs UN/EDIFACT messages be applied in Electronic Data Interchange,

RECOMMENDS that Members of the Customs Co-operation Council and all members of the United Nations Organization or its specialized agencies and Customs or EconomicUnions should adopt the WCO Data Mapping Guide for UN/EDIFACT messages as the standard reference document for the development of all Implementation Guides forUN/EDIFACT messages utilized by Customs in exchanging data electronically between Customs administrations and between Customs administrations and trade users,

REQUESTS Members of the Customs Co-operation Council and members of the United Nations Organization or its specialized agencies and Customs or Economic Unionswhich accept this Recommendation, to notify the Secretary General of the Customs Co-operation Council of the date from which they will apply the Recommendation and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members of the Customs Co-operation Council. He will also transmit it to the Customs administrations of the members of the United Nations Organization or its specialized agencies and to Customs or Economic Unions that have accepted this Recommendation.

x
x x

[*] Customs Co-operation Council (CCC) is the official name of the World Customs Organization (WCO)

Appendix 12 - WCO Recommendations on data requirements for API

CUSTOMS CO-OPERATION
COUNCIL

TC2-3844

RECOMMENDATION OF THE CUSTOMS CO-OPERATION COUNCIL CONCERNING ADHERENCE TO STANDARDS IN RELATION TO DATA REQUIREMENTS FOR ADVANCE PASSENGER INFORMATION (API)
(6 July 1993)

THE CUSTOMS CO-OPERATION COUNCIL,

NOTING the compliance risk posed by airline passengers especially with regard to drug trafficking and international terrorism,

NOTING the use of Electronic Data Interchange (EDI) by both carriers and Customs authorities and the potential benefits that use of this technology can bring,

RECOGNIZING that the electronic transmission of passenger-related data can result in the more rapid clearance of passengers and can have important control benefits for Customs authorities,

HAVING REGARD to Annex J.1. of the Kyoto Convention which requires, inter alia, computer applications implemented by Customs authorities to use internationally accepted standards,

DESIRING specifically to simplify and harmonize interface arrangements between (air) carriers and Customs authorities, particularly as regards the use of standard data elements, codes and message syntax,

RECOMMENDS that Members of the Council and members of the United Nations Organization or its specialized agencies and Customs or Economic Unions, should adhere to the standards set out in the Joint CCC/IATA Guideline on Advance Passenger Information, and any future updated or revised versions of these standards, for the electronic exchange of passenger data,

REQUESTS Members of the Council and members of the United Nations Organization or its specialized agencies and Customs or Economic Unions which accept this recommendation, to notify the Secretary General of the Council of the date from which they will apply the Recommendation and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members of the Council. He will also transmit it to the Customs administrations of the members of the United Nations Organization or its specialized agencies and to Customs or Economic Unions that have accepted this Recommendation.

x x x

Appendix 13- WCO Recommendations on the use of the UNTDED

CUSTOMS CO-OPERATION COUNCIL

TC2-3842

RECOMMENDATION OF THE CUSTOMS CO-OPERATION COUNCIL CONCERNING THE USE OF THE UNITED NATIONS TRADE DATA ELEMENTS DIRECTORY (UNTDED)

(26th JUNE 1990)[*]

THE CUSTOMS CO-OPERATION COUNCIL,

DESIRING to facilitate the international exchange of data between Customs administrations and between Customs administrations and trade users,

CONSIDERING that it is desirable that internationally agreed and universally applicable data element names, data element descriptions and character representations should be used in such trade data exchange,

CONSIDERING that it is desirable that the same names, descriptions and representations should be used for data elements irrespective of the context in which trade data is being exchanged (e.g. between exporter and carrier, exporter and importer, importer and Customs, etc.),

NOTING that these standard data elements can be used with any method of data interchange, on paper documents as well as with other means of data communication, can be selected for transmission one by one, or used within a particular system of interchange rules, e.g. UN/EDIFACT,

FURTHER NOTING that a subset of UNTDED constitutes the EDIFACT DATA Elements Directory (EDED) also recommended by the Customs Co-operation Council specifically for use in electronic data interchange (EDI),

CONSIDERING that the Directory has been accepted by the International Standards Organisation as an international standard, Sections 1, 2, 3, 4 and 9 of the Directory constituting International Standard ISO 7372,

RECOMMENDS that Members of the Council and all members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions should use the data element names, descriptions and character representations contained in the United Nations Trade Data Elements Directory (UNTDED) and future updated versions of this Directory in trade data exchange between Customs administrations and between Customs administrations and other trade users.

REQUESTS Members of the Council and all members of the United Nations Organization or its specialized agencies and Customs or Economic Unions which accept this Recommendation, to notify the Secretary General of their acceptance, of the date from

[*] Note : This Recommendation supersedes the Council Recommendation of 21 June 1988 concerning UNTDED.

which they will apply the Recommendation, and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members. He will also transmit it to any Customs administrations of non-Members or any Customs or Economic Unions which have accepted this Recommendation.

x

x x

Appendix 14 - WCO Recommendations on the use of EDIFACT rules

CUSTOMS CO-OPERATION COUNCIL

TC2-3841

RECOMMENDATION OF THE CUSTOMS CO-OPERATION COUNCIL CONCERNING THE USE OF THE UN/EDIFACT RULES FOR ELECTRONIC DATA INTERCHANGE

(26th JUNE 1990)[*]

THE CUSTOMS CO-OPERATION COUNCIL,

DESIRING to facilitate the international exchange of data between Customs administrations and between Customs administrations and trade users,

CONSIDERING that it is desirable that an internationally agreed and universally applicable set of rules for the structuring of such data should be used in the electronic data interchange,

NOTING that the United Nations Economic Commission for Europe (UN/ECE) has developed a comprehensive set of standards, directories and guidelines for use in electronic interchanges known as UN/EDIFACT (Electronic Data Interchange for Administration, Commerce and Transport) and defined in the Annex to this Recommendation,

AWARE that the UN/EDIFACT standards, directories and guidelines can be used independently of the application area and that their widespread use in international trade will greatly facilitate the movement of cargo,

NOTING that certain elements of the UN/EDIFACT rules are in the nature of standards which must be strictly adhered to for successful data interchange to occur (e.g. the EDIFACT Syntax Rules),

FURTHER NOTING that certain other elements of the UN/EDIFACT rules are in the nature of guidelines, use of which is highly recommended (e.g. message design guidelines),

RECOMMENDS that Members of the Council and all members of the United Nations Organization or its specialized agencies and Customs or Economic Unions, should apply the UN/EDIFACT rules as defined in the Annex to this Recommendation, and future updated versions of these rules for the preparation of electronic messages to be interchanged between Customs administrations and between Customs administrations and other trade users,

REQUESTS Members of the Council and all members of the United Nations Organization or its specialized agencies and Customs or Economic Unions, which accept this Recommendation, to notify the Secretary General of their acceptance, of the date from

[*] Note : This Recommendation supersedes the Council Recommendation of 21 June 1988 concerning the EDIFACT Syntax rules.

which they will apply the Recommendation and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members. He will also transmit it to any Customs administrations of non-Members or any Customs or Economic Unions which have accepted this Recommendation.

*

* *

DEFINITION OF UN/EDIFACT

UN/EDIFACT: United Nations rules for Electronic Data Interchange for Administration, Commerce and Transport. They comprise a set of internationally agreed standards, directories and guidelines for the electronic interchange of structured data, and in particular that related to trade in goods and services, between independent computerised information systems.

Recommended within the framework of the United Nations, the rules are approved and published by the UN/ECE in the United Nations Trade Data Interchange Directory (UNTDID) and are maintained under agreed procedures.

UNTDID includes:

- the EDIFACT Syntax rules (ISO 9735);
- Message design guidelines;
- Syntax implementation guidelines;
- the EDIFACT DATA Elements Directory, EDED (a subset of UNTDED);
- the EDIFACT Code List, EDCL;
- the EDIFACT composite data elements Directory, EDCD;
- the EDIFACT standard segments Directory, EDSD;
- the EDIFACT UNSMs Directory, EDMD;
- Uniform Rules of Conduct for the Interchange of Trade Data by Teletransmission (UNCID);
- Explanatory material, as appropriate.

x

x x

Appendix 15 - WCO Recommendations on the use of codes for data elements

CUSTOMS CO-OPERATION COUNCIL

TC2-383

RECOMMENDATION OF THE CUSTOMS CO-OPERATION COUNCIL CONCERNING THE USE OF CODES FOR THE REPRESENTATION OF DATA ELEMENTS

(20 June 1996)[*]

THE CUSTOMS CO-OPERATION COUNCIL,

DESIRING to facilitate the interchange of data among Customs administrations and between Customs administrations and participants in international trade,

CONSIDERING that it is desirable that internationally agreed and universally applicable codes should be used for the representation of data elements in such interchange of data,

HAVING REGARD to and supporting International Standards adopted by the International Organization for Standardization (ISO) concerning the use of codes or coding structures for the representation of data elements,

HAVING REGARD to and supporting Recommendations adopted by the Working Party on Facilitation of International Trade Procedures of the Economic Commission for Europe (ECE/UN) which recommend the use of codes or coding structures for the representation of data elements for international trade purposes,

CONSIDERING that the codes or coding structures referred to in the Annexes to this Recommendation provide a suitable basis for the representation of data elements in the interchange of data,

RECOMMENDS that Members of the Council and members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions, should use the codes or coding structures specified in the Annexes to the Recommendation and future updated or revised versions of these codes or coding structures for the representation of data elements in the interchange of data among Customs administrations and between Customs administrations and participants in international trade whenever there is a need for a coded designation,

POINTS OUT that acceptance of this Recommendation requires the acceptance of the Recommendation and of at least one Annex thereto, and that each Annex shall be taken to be a separate Recommendation,

[*] This Recommendation supersedes the Council Recommendation of 22 May 1984 on the use of codes and incorporates Recommendations T2-3831 (ISO-aplha-2 country codes) and T2-3832 (Mode of transport codes)

REQUESTS Members of the Council and members of the United Nations Organization or its specialized agencies and Customs or Economic Unions, which accept this Recommendation, to notify the Secretary General of the Council of the date from which they will apply the Recommendation and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members of the Council. He will also transmit it to the Customs administrations of the members of the United Nations Organization or its specialized agencies and to Customs or Economic Unions which have accepted this Recommendation.

*

* *

ANNEX I

Persons

1. Recommended coding structure

With regard to the design of a code for persons (e.g. suppliers, consignors, exporters, consignees, importers and declarants, etc.), the general guidelines concerning the coding of persons which have been prepared by the CCC Working Party on Customs applications of computers should be used.

These general guidelines, which have been developed in order to provide practical assistance to Customs administrations at the national level and which are compatible with International Standard ISO 6523 (Data interchange - Structure for the identification of organisations), are contained in the File on the computerisation of Customs operations.

2. Summary description

The general guidelines promote the use of a uniform approach to the coding of natural and legal persons involved in international trade operations and of interest to Customs (e.g., importers, exporters, Customs clearance agents, etc.). In particular, the guidelines deal with the function of codes, persons identified, the choice of codes, the length and format of codes, the identification of other elements, the identification of foreign suppliers, the use of check characters, and criteria and systems considerations to be taken into account in the development of codes.

As indicated above, the guidelines are compatible with International Standard ISO 6523 which specifies the following structure for identifying organisations for data interchange purposes: (a) an International Code Designator (ICD) (fixed-length four-digit code); (b) an organisation code; and (c) an organisation name. The organisation code consists of up to 14 characters that uniquely identify an organisation within an organisation coding scheme. The organisation code can involve the use of alphabetic, numeric or alphanumeric characters and it is recommended that the code should contain a check character which can be included within the organisation code or in a separate field.

ANNEX II

Container identifiers

1. Recommended codes

Attention is drawn to the ISO code contained in International Standard 6346 (Freight containers - Coding, identification and marking) for the representation of data concerning freight containers used in modes of transport other than air transport, and to the code developed by IATA for the representation of data concerning air freight containers.

Whenever container identification data are captured and processed by Customs, it is recommended that 17 characters should be provided for in ADP systems and associated documents in order to accommodate the ISO code (a possible total of 17 characters) and current and future versions of the IATA code (9 and 12 characters respectively).

2. Summary description

A. ISO code

International Standard 6346 establishes a 17-character alphanumeric marking code system for freight containers and provides unique international identification by means of an owner code, a serial number, and a country code, a check-digit system for verifying the accuracy of the recording of the owner code and serial number, and information concerning container size and type characteristics.

B. IATA code

The code developed by IATA for the representation of data concerning airfreight containers currently comprises 9 alphanumeric characters (unit type, size and compatibility, serial number, and owner code). In 1990, the IATA code will consist of 12 alphanumeric characters including a check digit.

ANNEX III

Dates

1. Recommended code

The representation provided for in ECE Recommendation No. 7 (Numerical representation of dates, time, and periods of time) which is based upon, inter alia, International Standard 2014 (Writing of calendar dates in all-numeric form) and 3307 (Information interchange - representations of time of the day) should be used for the representation of calendar dates and the time of day (e.g. departure date and time, arrival date and time, contract date, exchange date, Goods declaration acceptance date, clearance date, etc.).

2. Summary description

ECE Recommendation No. 7 (Numerical representation of dates, time, and periods of time) is based upon, inter alia, International Standards ISO 2014 and 3307.

ISO 2014 concerns the writing of dates of the Gregorian calendar in all-numeric form, signified by the elements year, month, day, and recommends that all-numeric dates should be written in the following order: year-month-day (i.e. YYYYMMDD) and should consist of four, two, and two digits to represent the year, month and day respectively.

ISO 3307 is designed to establish uniform time representations based upon the 24-hour timekeeping system. It provides a means for representing local time in digital form for the purpose of interchanging information among data systems. Local time is defined as clock time in public use at the point of origin. In the 24-hour timekeeping system, local time may be expressed by combinations of the time elements hours, minutes and seconds, for example, hours and minutes (HHMM).

With regard to calendar dates, attention is drawn to the fact that ECE Recommendation No. 7 recommends the use of only two characters to represent the year (i.e. YYMMDD).

ANNEX IV

Currencies

1. Recommended code

The ISO three-letter alphabetic currency code contained in International Standard 4217 (Codes for the representation of currencies and funds) should be used for the representation of currencies.

2. Summary description

ISO 4217 provides the structure for a three-letter alphabetic code and an equivalent three-digit numeric code for the representation of currencies and funds.

The first (left most) two characters of the alphabetic currency code in ISO 4217 provide a code unique to the currency authority to which it is assigned. Wherever practicable, it is derived from the ISO alpha-2 country code contained in ISO 3166 (Codes for the representation of names of countries) which is recommended by the Customs Co-operation Council and by the Working Party on Facilitation of International Trade Procedures of the Economic Commission for Europe (ECE/UN). The third (right most) character of the alphabetic code is an indicator, preferably mnemonic, derived from the name of the major currency unit or fund. In non-banking applications, the first (left most) two characters are sufficient to identify a currency. The numeric currency code is derived, where possible, from the United Nations Standard Country or Area Code.

Recommendation No. 9 adopted in February 1978 by the Working Party on Facilitation of International Trade Procedures of the Economic Commission for Europe (ECE/UN) recommends the use of the ISO three-letter alphabetic currency code for the representation of currencies for international trade purposes.

ANNEX V

Country Codes

1. Recommended codes

The International Standards ISO 3166 alpha-2 codes for the representation of countries, referred to in UN/ECE Recommendation No. 3, should be used for the representation of countries in international trade.

However, it should be noted that acceptance of this WCO Recommendation does not preclude the use of other codes referred to in ISO 3166 for the representation of names of countries for certain applications (for example, the ISO alpha-3 country code for machine readable passports, as laid down in the CCC/IATA Advance Passenger Information Guidelines). Acceptance of the Recommendation also does not preclude the use of non-ISO codes for national purposes or for internal purposes in the case of countries belonging to a Customs or Economic Union.

2. Summary description

The ISO alpha-2 country code consists of a two letter alphabetic code.

ANNEX VI

Descriptions of goods and tariff or statistical headings

1. Recommended coding structure

The Harmonized Commodity Description and Coding System should be used.

2. Summary description

The Harmonized Commodity Description and Coding System is a six-digit multipurpose nomenclature for transportable goods, which meets simultaneously the needs of Customs authorities, statisticians concerned with external trade or production, carriers and producers. The Harmonized System is suitable for automatic data processing and transmission and provides a common terminology and code specifically identifying 5019 groups of goods resulting from a detailed expansion of 1241 four-digit headings. The latter result from a very extensive revision and updating, not only in detail but also in structure, of the Customs Co-operation Council Nomenclature (CCCN). The Harmonized System can be further subdivided, where necessary, to meet national or international requirements.

ANNEX VII

Customs procedures

1. Recommended code

The general guidelines and one-digit code developed by the CCC Working Party on Customs applications of computers should be used for the representation of Customs procedures. The general guidelines and the one-digit code are contained in the File on the computerisation of Customs operations.

2. Summary description

The code for the representation of Customs procedures developed by the CCC Working Party on Customs applications of computers is a broad level one-digit code within which the principal Customs procedures are identified and within which users can develop unique codes to meet national or international requirements.

ANNEX VIII

Units of measurement

1. Recommended codes

The codes contained in ECE Recommendation No. 20 (Codes for units of measurement used in international trade) should be used for the representation of units of measurement.

2. Summary description

The unit of measurement codes developed by the ECE consist of a fixed-length (three letter) alphabetic code, and a fixed-length (three-digit) numeric code.

ANNEX IX

Mode of Transport Code

1. Recommended codes

The codes contained in ECE Recommendation No. 19 (Codes for mode of transport and the corresponding means of transport used in international trade) should be used for the representation of modes of transport.

2. Summary description

The mode of transport codes developed by the ECE consist of a single digit numeric code. However, provision is made for the possibility of a second numeric digit where the basic code needs to be sub-divided.

x x x

Appendix 16 - WCO Recommendations on customs information processed by computer

WORLD CUSTOMS ORGANIZATION[*]

RECOMMENDATION OF THE WORLD CUSTOMS ORGANIZATION CONCERNING THE ELECTRONIC TRANSMISSION AND AUTHENTICATION OF CUSTOMS AND OTHER RELEVANT REGULATORY INFORMATION

(16 June 1981 revised 24 June 2005)

THE WORLD CUSTOMS ORGANZIATION,

DESIROUS of enabling Customs administrations and international traders to make greater use of their computer systems, by making it possible for declarants to transmit Customs information to the Customs by electronic or other automatic means,

CONSIDERING that automated data processing, e-commerce incl. Electronic Data Interchange (EDI) and security techniques make it possible to transmit, validate and authenticate computer processed Customs regulatory information (such as Goods declarations, manifest data, licence information, etc.) other than by paper documentation and a handwritten signature; that these methods include the use of unique passwords linked to the declarant and transmitted with the information, software keys for the encryption of data and the generation of electronic signatures; that, in accordance with the provisions of national legislation or under the terms of an undertaking signed by the declarant, the use of such security techniques for the transmission of Customs information may be regarded as just as binding upon the declarant as a handwritten signature on paper documentation,

TAKING INTO ACCOUNT the "Recommendation on the authentication of trade documents by means other than signature", also adopted in March 1979 by the above-mentioned Working Party, which points out that the general adoption of electronic or other automatic means of data transfer require changes in existing national laws and international Conventions and in current commercial practice concerning signature,

AND FURTHER TAKING INTO ACCOUNT the “Model Law on Electronic Commerce” of the United Nations Commission on International Trade Law (UNCITRAL), adopted by the United Nations in December 1996 and the UNCITRAL “Model Law on Electronic Signatures” adopted by the United Nations in December 2001 as useful references for the development of national e-commerce and digital signature legislation,

RECOMMENDS that Members of the Council and members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions, should:

1. Allow, under conditions to be laid down by the Customs authorities, declarants to use various electronic media (including values added networks, Internet, wireless

[*] Established in 1952 as the Customs Co-operation Council (CCC).

networks, disc, tape, etc.) for the transmission of Customs regulatory information to the Customs authorities for automatic processing and to receive an automatic response to such information, from the Customs;

2. Accept, under conditions to be laid down by the Customs authorities, Customs regulatory information from declarants and other government agencies, which is transmitted by use of electronic media, validated and authenticated by security technology, without the need to produce paper documentation with a handwritten signature;

3. Ensure, where governments do not operate an electronic "Single Window" for declarants to submit regulatory information for international cross-border transactions only once to a single access point, that requirements and technical specifications concerning the authentication of electronic exchanges of regulatory information are co-ordinated among all government agencies involved;

4. Accept, where legal recognition of electronically transmitted Customs regulatory information is not yet resolved, that the Customs should authorize declarants, under conditions to be laid down by the Customs or other competent authorities, to produce Customs regulatory information on plain paper;

5. Accept, where EDI security and automated processing techniques are used but where, due to legal constraints, the production of paper documentation and hand written signatures are still required, the periodic submission of paper documentation or their storage on the premises of the declarant, under conditions laid down by the Customs;

REQUESTS Members of the Council and members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions which accept this Recommendation to notify the Secretary General of the Council of the date from which they will apply the Recommendation and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members of the Council. He will also transmit it to the Customs administrations of the members of the United Nations Organization or its specialized agencies and to Customs or Economic Unions which have accepted this Recommendation.

x x x

Appendix 17 - WCO Recommendations on the use of CCC/IATA standards

CUSTOMS CO-OPERATION
COUNCIL

TC2-3843

RECOMMENDATION OF THE CUSTOMS CO-OPERATION COUNCIL CONCERNING THE USE OF THE CCC/IATA DATA INTERCHANGE STANDARDS

(21 June 1988)

THE CUSTOMS CO-OPERATION COUNCIL,

NOTING the high level of automation in the airline industry and the increasing number of Customs administrations which are introducing computer techniques,

NOTING the growing use of Electronic Data Interchange (EDI) in world trade and the benefits of a paperless trading environment,

AWARE that the interfacing of the automated systems of airlines and Customs administrations results in the reduction of the paper burden,

RECOGNIZING that the interfacing of automated processing of cargo-related data can result in rapid clearance of air consignments and have important benefits from the Customs control point of view,

HAVING REGARD to Annex J.1. of the International Convention on the simplification and harmonization of Customs procedures (18 May 1973) which requires, inter alia, computer applications implemented by Customs authorities to use internationally accepted standards,

DESIRING specifically to simplify and harmonize interface arrangements between airlines and Customs authorities particularly as regards the use of standard data elements, codes and message syntax,

RECOMMENDS that Members of the Council and members of the United Nations Organization or its specialized agencies and Customs or Economic Unions, should use the standards set out in the CCC/IATA Data Interchange Standards Manual and future updated or revised versions in establishing interfaces between the automated systems of Customs and airlines,

REQUESTS members of the Council and members of the United Nations Organization of its specialized agencies and Customs or Economic Unions which accept this Recommendation, to notify the Secretary General of the Council of the date from which they will apply the Recommendation and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members of the Council. He will also transmit it to the Customs administrations of the members of the United Nations Organization or its specialized agencies and to Customs or Economic Unions that have accepted this Recommendation.

APPENDIX 18: Recommendation of the Customs Co-operation Council concerning the use of the WCO Data Model

(27 June 2009)

THE CUSTOMS CO-OPERATION COUNCIL,

DESIRING to facilitate the international exchange of data between Customs administrations and between Customs administrations, Cross-Border Regulatory Agencies, trade users and other relevant parties involved in cross-border transactions and cross-border movement of goods,

CONSIDERING that it is desirable to use international standards in defining data elements and elaborating electronic messages to be used in such cross-border transactions,

CONSIDERING that the WCO Data Model

i. represents a maximum set of data required for the pre-arrival/pre-departure information, the cross-border release and clearance of goods and means of transport for import, export and transit purposes,

ii. has been developed using harmonized sets of data requirements drawn from members Customs Administrations and several Cross-Border Regulatory Agencies, and

iii. is based on widely used and recognized international standards,

RECOMMENDS that Members of the Council and all members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions should as far as possible:

1. Adopt the WCO Data Model for the identification and definition of all cross-border regulatory data requirements related to pre-arrival/pre-departure formalities and procedures for import, export and transit.

2. Use the WCO data elements, their names and reference numbers (WCO ID's), the data element descriptions, the character representations (including the suggested code lists) in describing and composing electronic messages.

3. Use the standard electronic messages described in the WCO Data Model in Government to Government and Business to Government /Government to Business electronic messages.

REQUESTS Members of the Council and members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions which accept this Recommendation to notify the Secretary General of the Council of the date from which they will apply the Recommendation and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members of the Council. He will also transmit it to the Customs

Administrations of the Members of the United Nations Organization or its specialized agencies and to Customs or Economic Unions which have accepted this Recommendation.

APPENDIX 19: Recommendation of the Customs Co-operation Council concerning the use of Advance Passenger Information (API) and Passenger Name Record (PNR) for efficient and effective Customs Control

(June 2012)

THE CUSTOMS CO-OPERATION COUNCIL,

NOTING the continued and growing threat posed by serious transnational crime, inter alia illicit trafficking in drugs and other contraband, which are of serious concern to social well- being and safety and to the prosperity of nations around the world,

NOTING the continuing growth in the volume of cross-border travel movements and the challenges this creates for the facilitation of legitimate travellers,

HAVING REGARD to provisions of the revised Kyoto Convention[2] , specifically Chapter 6 of the General Annex on Customs Control and Chapter 1 of the Specific Annex J on Travellers,

RECOGNIZING that Customs administrations have the prime responsibility for controlling cross-border movements of goods, means of transport and people, and thus they are best placed to prevent, detect and suppress illicit trafficking in drugs and other contraband at the border before they disperse into the territories,

NOTING the incidents of close linkages between serious transnational crime and terrorism, and the need to mitigate perceived risks posed by travellers,

RECOGNIZING that the proper balance between the needs of Customs enforcement and the facilitation of legitimate travel can best be achieved if Customs enforcement is intelligence-based, and that the use of API and/or PNR for risk assessment would greatly assist Customs administrations in developing and exploiting the best possible intelligence for the control of travellers,

DESIRING to harmonize the interface arrangements between Customs administrations and business, particularly as regards the electronic transmission of API and/or PNR data in line with internationally standardized data elements and messaging formats,

BELIEVING that effective border control against serious transnational crime, inter alia illicit trafficking in drugs and other contraband, can be greatly assisted by co-operation between Customs administrations and other competent border control agencies at the national and international levels, and that exchange of information can significantly aid risk assessment and targeting and, as a consequence, improve the facilitation of legitimate travel,

[1] Customs Co-operation Council is the official name of the World Customs Organization (WCO).

[2] International Convention on Simplification and Harmonization of Customs Procedures (as amended).

RECOMMENDS that Members of the Council and Customs or Economic Unions should:

1. ensure that prevention, detection and suppression of serious transnational crime, inter alia illicit trafficking in drugs and other contraband, be promoted and remain as one of thepriorities of the Customs authority's enforcement strategy and programmes;

2. seek the fullest co-operation of airlines and the other international passenger transport businesses to assist the Customs in fulfilling its mission;

3. utilize advance information, namely API and/or PNR, for the risk assessment of travellers and :

- establish legal authority to acquire access to, or require to transfer, use and store API and/or PNR data along with the conditions thereof and scope of data required to this end, and put in place mechanisms for the protection of the pertinent data,

- adhere to the technical standards, formats and procedures set out in the internationally recognized guidelines, and

- to the extent possible, take part in the work for devising or updating international technical standards, formats and procedures as well as best practices in the application thereof;

4. promote co-operation with, and extend support to other Customs administrations, within the national legal framework, including the exchange of intelligence and experience in theuse of API and/or PNR with a view to further efficient and effective identification of potentially high-risk travellers.

REQUESTS Members of the Council and Customs or Economic Unions which accept this Recommendation to notify the Secretary General of the Council of the date from which they will apply the Recommendation and of the conditions of its application.

APPENDIX 20: Recommendation of the Customs Co-operation Council on the Dematerialization of Supporting Documents

(June 2012)

THE CUSTOMS CO-OPERATION COUNCIL,

ACKNOWLEDGING that the Customs administrations by and large have introduced automated systems for cargo clearance and have committed to apply information technology to support Customs operations, where it is cost-effective and efficient for Customs and for the trade,

CONSIDERING that the use of paper-based documentation in international trade is expensive, time-consuming and prone to error and malpractice,

HAVING REGARD to provisions of Chapter 3 of the General Annex to the revised Kyoto Convention[2] with regard to electronic lodgement of the supporting documents with Customs,
RECOGNIZING the rapid development of cost-effective, secure and trusted solutions for electronic document management and repository services, and extensive adoption of these solutions by the industry and administrations,

RECOGNIZING that international organizations, government agencies, and industry associations are increasingly introducing standard formats for electronic documents such as licences, certificates, and permits, and are promoting their use in the entire course of the international trade transaction,

AIMING to promote paperless transactions for Customs clearance as an alternative to paper-based documentary requirements,

DESIRING to reduce the cost of trade and to simplify trade procedures by alleviating the burden of delivering, storing, and presenting original paper-based supporting documents during Customs procedures, and

DESIRING to enhance Customs control through the effective use of automated verification and by adopting the principle of risk management,

RECOMMENDS that Members of the Council and all members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions should as far as possible :

(1) identify supporting documents that are normally required to accompany the cargo and goods declarations and examine the need for those documents for Customs clearance with a view to eliminating them;
(2) discontinue the requirement of presenting supporting documents in hard copy, if they have already been presented in electronic form;
(3) process the release and clearance of cargo based only on electronic declaration and automated verification;

(4) enable automated Customs clearance systems to automatically verify information contained in dematerialized supporting documents where such information is accessible electronically in :

(a) Other government agencies' databases
(b) Single Window environments (and Cargo Community Systems)
(c) Private repositories.

REQUESTS Members of the Council and members of the United Nations Organization or its specialized agencies, and Customs or Economic Unions which accept this Recommendation to notify the Secretary General of the Council of the date from which they will apply the Recommendation and of the conditions of its application. The Secretary General will transmit this information to the Customs administrations of all Members of the Council. He will also transmit it to the Customs administrations of the Members of the United Nations Organization or its specialized agencies and to Customs or Economic Unions which have accepted this Recommendation.

x
x x

[1] Customs Co-operation Council is the official name of the World Customs Organization (WCO).
[2] International Convention on Simplification and Harmonization of Customs Procedures (as amended).