Tax Administration Reform in India
Spirit, Purpose and Empowerment

Second Report of the
Tax Administration Reform Commission
Ministry of Finance, Government of India

New Delhi
September 2014

सत्यमेव जयते

Govt. of India
Ministry of Finance
Tax Administration Reform Commission
NBCC Plaza, 3rd Floor, Pushp Vihar, Saket, New Delhi-110017

F. No. **TARC/Report/36/2014-15** Dated **26.09.2014**

To,

Shri Arun Jaitley
Hon'ble Minister of Finance,
Government of India

OFFICE OF THE FINANCE MINISTER
26 SEP 2014
RECEIVED
26/9/14

Sir,

We submit herewith the Second Report of the Tax Administration Reform Commission (TARC).

Dr. Parthasarathi Shome
Chairman

Y.G.Parande
Member

Sunita Kaila
Member

M.K.Zutshi
Member

S.S.N.Moorthy
Member

S.Mahalingam
Member

M.R.Diwakar
Member

Preface

TARC in its first report had addressed four terms of reference. These terms of reference related to customer focus, structure and governance, people's function, dispute management, key internal processes and ICT. This report of the TARC, which is the second report, addresses two important aspects of tax administration, capacity building of the customs department and data and information exchange. The terms of reference for the TARC on these aspects are:

- *To review the existing mechanism and recommend measures for "Capacity building" in emerging areas of Customs administration relating to Border Control, National Security, International Data Exchange and securing of supply chains. (Chapter VIII in this continuing TARC report)*

- *To review the existing mechanism and recommend measures for strengthening of Database and inter-agency information sharing, not only between Central Board of Direct Taxes (CBDT) and Central Board of Excise and Customs (CBEC) but also with the banking and financial sector, Central Economic Intelligence Bureau (CEIB), Financial Intelligence Unit (FIU), Enforcement Directorate etc. and use of tools for utilization of such information to ensure compliance. (Chapter IX in this continuing TARC report)*

The importance of the customs capacity building is to be seen in terms of rapidly growing global trade, not only by rise in trade volumes but also in terms of complexity of supply chains. It may be stated that in the last 30 years, world merchandise and commercial services trade have increased by about 7 per cent per year on average. The share of developing countries in the world exports and imports is now close to 50 per cent. The growth in trade has also spurred fragmentation or specialisation in production chains, creating a network of activities. The response of the countries has been to engage in various trade treaties and harvest the competitive advantage that the global trade integration is offering. While globalization has given impetus to economic growth, customs administration, as part of the tax administration, is being engaged in multidimensional challenges. Customs administration which so far has had a traditional role of import and export processing of goods and administering export incentive schemes or duty drawback is now confronted with areas such as administering a complex web of rules of origin for granting preferential treatment in duty to imports from a particular country, developing a robust risk management system so that there is pre-arrival risk assessment and post-clearance compliance management for facilitating trade and moving towards "smart" customs. While all these measures will go to improve trade facilitation, aspects of security, which comprise another aspect of customs administration cannot be compromised. Emergence of e-commerce has created yet another dimension to global trade and presents a challenge to the customs administration while maintaining sufficient control to prevent the abuse of this channel.

All these will require a strategic reorientation of customs, shedding the overwhelmingly transactional and administrative mind-set that dominates the present thinking. Chapter VIII addresses the aspects of capacity building with a keen eye on promoting voluntary compliance with enhanced technological capabilities to control the cross border movement of goods and persons with almost no intrusion. The customs administration will also need to be more customer focused and forge closer links with trade and industry in design and implementation of policies, as part of the larger governance framework. The issues of security at the borders on illicit drug trafficking, public health and safety, and importation and exportation of environmentally-sensitive goods like CFC gases and hazardous waste will require close co-ordination by the customs administration with the specialised agencies for better compliance. Customs

administration for all these aspects will have to be engaged in a modernization process, adopting global best practices, facilitating legitimate trade, safeguarding revenue collection and securing the borders. Initiatives such as SAFE framework, mutual recognition, pre-arrival information, air cargo security, supply chain integrity and dematerialization of documents will be other parts of the modernisation requiring international co-operation and exchange of information. Customs to customs sharing of information will be crucial for such co-operation and exchange. Thus, the capacity building of the customs administration in this fast integrating world will not only be confined to People's function as already covered in Chapter IV in the first TARC report but will require modernisation of equipment, environment and, importantly, the mind-set.

Another term of reference covered in this report is on exchange of data and information. With the adoption of ICT by the Indian tax administration, large volumes of data and information are being generated. They provide opportunities to the CBDT and CBEC to harness them for analysing how to improve tax compliance and ensure better enforcement. But so far, the CBDT and CBEC as well as CEIB, FIU and Enforcement Directorate are generating data and collecting information *sui generis* and there is almost no effort to integrate them or work on a common database. Most of these agencies as reviewed in Chapter IX work on databases that are scattered and disconnected. The seamless flow of information across agencies which has become the norm in most of the advanced tax administrations remains unchartered in India. By contrast, most advanced tax administrations have recognised the importance of exchange of data and information for compliance and enforcement and have adopted collaborative mechanisms among the organisations, which can take forms varying from partnership agreements, MoUs, statements of practice, standard protocols, and others, often backed by law. The collaborating agencies exchanging the data or information apply a consistent approach with a common taxonomy and standards. Such common taxonomy is reflected within each of the three areas – data description, data context and data sharing for standardisation. The idea behind this is to create/collect data or information once while using them many times. A common database enables a "one data, many users" approach, thereby reducing duplication of efforts and minimising the cost of collecting data and time expended on it.

Towards the above framework, TARC has recommended one database to facilitate re-use of data and information to enable arriving at time-critical decisions in an expeditious manner and also to achieve seamless flow of data among participating organisations. Since data would be collected in a common framework with a common taxonomy, format and metadata, it would be ready to be used while cutting down the time and cost of data collection. Second, the use of a Special Purpose Vehicle (SPV) to harness the combined potential of the data created or collected has been recommended. This is in line with the TARC's earlier recommendation of creation of an SPV. An SPV will facilitate a single repository or storage of data with common taxonomy and standards and will receive all data and information from different entities, such as banks, financial institutions, the FIU, AIR and CIB, placing them on one platform so as to provide a common linkage between the relevant data. The recognition of PAN as CBIN, also recommended in Chapter VI in the first TARC report, will provide common identification of data so that storage, retrieval and use of data will be further eased. For the above strategy to be successful, it will be important that different agencies abandon the culture and practice of information hoarding and instead, embrace the exchange and sharing of data and information. This would be a crucial condition of success in improved exchange across silos and inter-departmental exchanges.

The TARC, keeping in line with its earlier practice, sought the views of various stakeholders, including the two Boards and CEIB, FIU and field offices and held altogether 18 meetings with them. To assess the problems facing the customs administration and to get first-hand information,

the TARC visited land customs posts at Attari on the western border with Pakistan and Petrapole on the eastern border with Bangladesh. The TARC also undertook a visit to the Chennai seaport to get first-hand experience of the working of newly installed mobile scanner to facilitate non-intrusive verification. The meetings with the DG (Systems) of the two Boards on data and information exchange were held to understand the current status and also the ambition level. Interaction with DG, CEIB and Director, FIU were to understand their role in providing crucial information and the work carried out by them. A list of such meetings is given at Annexure - I. Sri Sukumar Mukhopadhyay, ex-Member, CBEC in an interaction with the TARC provided valuable inputs on the customs capacity building. The TARC is thankful to all the stakeholders for their suggestions and also for the free and frank discussions. These suggestions formed the basis of many of TARC's recommendations. The TARC also acknowledges the support of the CBDT and the CBEC in providing information and data.

For an in-depth analysis, the TARC constituted two focus groups for the two terms of reference. These focus groups comprised officers of the two tax administrations – former as well as current – and professionals from the private sector. A list of participants in the focus groups is at Annexure - II. The input of each of the focus group members were discussed in detail within the TARC. These inputs helped the TARC to successfully thrash out many new ideas and emerge with a set of recommendations that should improve the Indian tax administration decidedly.

The TARC's recommendations were formulated at many meetings, formal and informal. A list of meetings in which TARC discussions were held is at Annexure – III. The TARC's findings, conclusions and recommendations were unanimous.

The TARC also wishes to recognize the overarching support of the Secretary to the Commission in all aspects. The Director and Under Secretary as well as other support staff were also helpful. The work of two research consultants was important for the background studies that were carried out. The editor's meticulous work at top speed was crucial. But for their intensive efforts, timely delivery of the report would not have been feasible.

Parthasarathi Shome

Dr. Parthasarathi Shome
Chairman
Tax Administration Reform Commission

New Delhi
26th September 2014

Table of Contents

Tax Administration Reform Commission

Chairman

Dr. Parthasarathi Shome	Level of Minister of State

Members- full time

Y. G. Parande	Ex-Member, CBEC
Sunita Kaila	Ex-Member, CBDT

Members- part time

M.K. Zutshi	Ex-Chairman, CBEC
S.S.N. Moorthy	Ex-Chairman, CBDT
S. Mahalingam	Ex-Chief Financial Officer and Executive Director, TCS
M.R. Diwakar	Ex-Vice President, Taxation, Murugappa Group

Secretariat

Sanjay Kumar	Secretary
N.K. Jain	Director
Sukalyan Banerjee	Under Secretary

Research Consultants

Vrinda Jaju

Prativa Shaw

Administrative Support

Tejpal	Consultant (Administration)
Jagdish	Assistant
Ankur Verma	Steno/Assistant

Tables

Diagrams

Graphs and Boxes

List of Annexures

Glossary of Technical Terms

ACBPS	Australian Customs and Border Protection Services
ACES	Automation of Central Excise and Service Tax
ACP	Accredited Clients' Programme
ACQS	Animal Quarantine and Certification Services
ADEPT	Analytics for Debtor Profiling and Targeting
AEO	Authorised Economic Operator
AERB	Atomic Energy Regulatory Board
AGIMO	Australian Government Information Management Office
AIR	Annual Information Return
APIS	Advance Passenger Information System
APTA	Asia-Pacific Trade Agreement
ASEAN	Association of Southeast Asian Nations
ASEM	Asia-Europe Meeting
ATO	Australian Taxation Office
B/E	Bill of Entry
BEL	Bharat Electronics Limited
BoI	Bureau of Immigration
BRICS	Brazil, Russia, India, China and South Africa
CAG	Comptroller and Auditor General
CASS	Computer Aided Selection System
CBDT	Central Board of Direct Taxes
CBEC	Central Board of Excise and Customs
CBI	Central Bureau of Investigation
CBIN	Common Business Identification Number
CCR	Counterfeit Currency Report
CCTV	Closed-Circuit Television
CDSCO	Central Drugs Standard Control Organisation
CEIB	Central Economic Intelligence Bureau
CFS	Container Freight Station
CHA	Customs Housing Agent
CIB	Central Information Branch
CIO	Chief Information Officers
CIS	Commonwealth of Independent States

CISF	Central Industrial Security Force
CMAAs	Customs Mutual Assistance Agreements
CMCPC	Compliance Management Centralized Processing Centre
COFEPOSA	Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974
COIN	Customs Overseas Intelligence Network
CONCOR	Container Corporation of India
CPC	Central Processing Centre
CRA	Canadian Revenue Agency
CRCA	Commissioners for Revenue and Customs Act, 2005
CT-PAT	Customs Trade Partnership against Terror
CTR	Cash Transaction Report
CVD	Countervailing Duty
DEPB	Duty Entitlement Passbook Scheme
DFIA	Duty Free Import Authorization Scheme
DFRC	Duty Free Replenishment Certificate Scheme
DFTP	Duty Free Tariff Preference
DGAD	Directorate General of Anti-Dumping and Allied Duties
DGCEI	Directorate General of Central Excise Intelligence
DGFT	Directorate General of Foreign Trade
DGIT	Directorate General of Income Tax
DGSD	Directorate General of Safeguards
DI&CI	Directorate of Intelligence and Criminal Investigation
DoV	Directorate of Valuation
DPQIS	Directorate of Plant Quarantine Inspection Service
DRI	Directorate of Revenue Intelligence
DRM	Data Reference Model
DTAA	Double Tax Avoidance Agreement
EA	Enterprise Architecture
EASIEST	Electronic Accounting System in Excise and Service Tax
ECDB	Export Commodity Database
ECIL	Electronics Corporation of India Limited
ED	Enforcement Directorate
EDD	Extra Duty Deposit
EDI	Electronic Data Interchange
EDW	Enterprise Data Warehouse

EFS	Enforcement Information System
EFTA	European Free Trade Association
EHTP	Electronic Hardware Technology Park Scheme
EOUs	Export Oriented Units
EOW	Economic Offences Wing
EPCG	Export Promotion Capital Goods Scheme
EPZs	Export Processing Zones
EU	European Union
FEA	Federal Enterprise Architecture
FEMA	Foreign Exchange Management Act, 1999
FICN	Fake Indian Currency Notes
FII	Foreign Institutional Investor
FINnet	Financial Intelligence Network
FIU	Financial Intelligence Unit
FSSAI	Food Safety and Standards Authority of India
FTAs	Free Trade Agreements
GATS	General Agreement on Trade in Services
GATT	General Agreement on Tariffs and Trade
GDSC	Government Data Standards Catalogue
GEI	Group on Economic Intelligence
GNC	Globally Networked Customs
GPRS	General Packet Radio Service
GPS	Geo-Positioning Systems
HF	High Frequency
HMRC	Her Majesty's Revenue and Customs of UK
HS	Harmonized System
IB	Intelligence Bureau
IBSA	India, Brazil and South Africa
ICD	International Customs Division
ICD	Inland Container Depot
ICEGATE	Indian Customs and Excise Gateway
ICES	Indian Customs EDI System
ICP	Integrated Check post
ICT	Information and Communication Technology
IEPD	Information Exchange Package Documentation
IGM	Import General Manifest

IOT	Internet of Things
IPR	Intellectual Property Rights
IRDA	Insurance Regulatory and Development Authority
IRS	Internal Revenue Service of USA
ISCM	Integrated Supply Chain Management
ISO	International Organisation for Standardization
ISPS	International Ship And Port Facility Security
I-T Act	Income-tax Act, 1961
ITD	Income Tax Department Application
ITD-MS	Integrated Taxpayer Data Management System
ITS	Individual Transaction Statement
KAIC	Knowledge and Analysis Centre
LCS	Land Customs Station
LDCs	Least Developed Countries
LEA	Law Enforcement Agency
LOC	Line of Control
MFN	Most Favoured Nation
MoU	Memoranda of Understanding
MRA	Mutual Recognition Agreement
NACEN	National Academy of Customs, Excise and Narcotics
NCB	Narcotics Control Bureau
NDSAP	National Data Sharing and Accessibility Policy, 2012
NEIN	National Economic Intelligence Network
NIA	National Investigation Agency
NIDB	National Import Database
NIEM	National Information Exchange Model
NII	Non-Intrusive Inspection
NSDL	National Securities Depository Limited
NTCD	National Training Centre for Dogs
NTRO	National Technical Research Organization
ODS	Ozone Depleting Substances
OECD	Organisation for Economic Co-operation and Development
OEM	Original Equipment Manufacturers
OGAs	Other Government Agencies
OLTAS	Online Tax Accounting System
OSPCA	On-Site Post Clearance Audit

PAN	Permanent Account Number
PCCV	Post-Clearance Compliance Verification
PITNDPS	Prevention of Illicit Traffic in Narcotic Drugs and Psychotropic Substances Act, 1988
PMLA	Prevention of Money Laundering Act, 2002
POL	Petroleum, Oil and Lubricants
PSRs	Product Specific Rules
PTA	Preferential Trade Agreement
RAW	Research and Analysis Wing
RBI	Reserve Bank of India
RCEP	Regional Comprehensive Economic Partnership
REIC	Regional Economic Intelligence Committee
RFC	Request for Comments
RFID	Radio-frequency Identification
RFP	Request for Proposals
RMD	Risk Management Division
RMS	Risk Management System
ROC	Registrar of Companies
RoO	Rule of Origin
RTA	Regional Trade Agreement
RTK	Revenue Tonne Kilometer
S/B	Shipping Bill
SAARC	South Asian Association for Regional Co-operation
SAFTA	South Asian Free Trade Area
SAPTA	South Asian Preferential Trading Agreement
SASEC	South Asia Sub-regional Economic Co-operation
SCBTM	Secure Cross-border Transport Model
SEBI	Securities and Exchange Board of India
SEP	Single Entry Permits
SEZ	Special Economic Zone
SFIO	Special Fraud Investigation Office
SFIS	Served from India Scheme
SIEN	Secured Information Exchange Network
SIIB	Special Intelligence And Investigation Branch
SLA	Service Level Agreement
SME	Small and Medium Enterprise

SMTP	Sub-Manifest Trans-shipment Permit
SOAs	Service Oriented Architectures
SOLAS	Security of Life at Sea
SPRM	Strategic Planning And Risk Management
SPV	Special Purpose Vehicle
SSC	Staff Selection Commission
STCE	Strategic Trade Control Enforcement Programme
STP	Software Technology Park
STR	Suspicious Transaction Report
SVB	Special Valuation Branch
TAA	Taxation Administration Act, 1953
TARC	Tax Administration Reform Commission
TDS	Tax Deduction at Source
TEP	Tax Evasion Petition
TFA	Trade Facilitation Agreement
TIEA	Tax Information Exchange Agreement
TP	Transshipment Permit
TPP	Trans-Pacific Partnership
TRIPS	Trade-Related Aspects of Intellectual Property Rights
TRS	Time Release Studies
TRU	Tax Research Unit
TTIP	Transatlantic Trade and Investment Partnership
UNCTAD	United Nations Conference on Trade and Development
UNESCAP	United National Economic and Social Commission for Asia and the Pacific
UNODC	United Nations Office on Drugs and Crime
VHF	Very High Frequency
VKGUY	Vishesh Krishi Gram Upaj Yojana
WCO	World Customs Organization
WHO	World Health Organization
WTO	World Trade Organisation
XBIS	X-Ray Best Inspection System

Chapter VIII

Customs Capacity Building

VIII.1 Introduction

According to the definition adopted by the World Customs Organization (WCO), capacity building is commonly understood to mean developing or acquiring the skills, competencies, tools, processes and resources needed to improve the capacity of the administration to carry out its allotted functions and achieve its objectives.

The rapidly changing global trading environment, marked by steadily growing volumes and complexity of supply chains, and heightened security perceptions have had a large impact on the role and functions of customs administrations everywhere. On the one hand, globalisation has been an engine of economic growth, enhancing the importance of the trade facilitation role of customs and other border agencies as key determinants of a country's economic competitiveness and attraction as an investment destination. On the other, it continues to offer new opportunities for criminal organisations to engage new types of fraud and pose multidimensional challenges to customs administrations.

Customs administrations have had to respond to these challenges by redefining their roles, reorienting their strategies and altering the traditional control paradigm that had served them well in the older, more uncomplicated times. They have had to build newer technological, human and organisational capabilities and adopt governance practices congruent with modern standards to both effectively deal with risks as well as meet growing client expectations for higher service standards. In the process, the best practice customs administrations have radically transformed their structures and business processes, taking advantage of the opportunities the rapid advance of technology offers. While Indian customs too have moved forward in this direction, they still have a long road ahead, which cannot be traversed unless some key gaps in terms of capacity building are filled. This paper seeks to identify some of those key gaps and the measures needed to fill them.

It needs to be mentioned at the outset that the TARC had, in its first report, given a large number of recommendations in the areas of governance, structures and processes, people management and information and communication technologies. These recommendations have a direct bearing on the topic of this report and have to be kept in mind while dealing with the issue of customs capacity building.

VIII.2 Snap shot of customs in India

The Central Board of Excise and Customs (CBEC) has several field formations to help it discharge its responsibilities of levying and collecting customs duties and preventing smuggling under the

Customs Act, 1962. These include the 11 Customs/Customs (Preventive) zones and 35 commissionerates spread all over the country. In the ongoing cadre restructuring of the department, the number of Customs/Customs (P) commissionerates are proposed to be increased to 60. While customs commissionerates are primarily responsible for collection of customs duties and implementation of allied acts, vigil over coastal and land borders is maintained by preventive commissionerates to thwart any attempt at smuggling. However, the role of the preventive commissionerates is not limited to anti-smuggling operations only and almost all the preventive commissionerates are entrusted with the added responsibility of appraisement work in respect of goods imported/exported through smaller ports, airports, inland container depots and land customs stations, which fall within their geographical jurisdiction. The marine and telecommunications wings under the Directorate of Logistics also assist in keeping surveillance over the borders. Wherever there is no customs formation, the functions under the Customs Act are discharged by central excise officers. In some border areas, like the Indo-Pak border in the state of Jammu & Kashmir, other border enforcement agencies like the BSF are also notified under the Customs Act to discharge the functions of customs officers.

These formations manage operations in nearly 100 ports (along with the associated CFSs), over 40 international airports and over 100 inland container depots. Besides, there are about 112 land customs stations, although only a few see significant cross-border trade. At the last count, there were 387 SEZs of which 192 were operational. Besides, the central excise field formations also administer a large number of 100 per cent export oriented units (EOUs). There are also a large number border check posts and coastal units which perform anti-smuggling functions.

The organisation of the field formations is largely territorial and all key functions are located under one roof in each large customs office. The assessment work, however, is carried out in appraising groups that are organised along commodity groups, each dealing with specified groups of tariff headings; this organisation is uniform across customs locations. The officers are subject to regular rotation among jobs, which we have identified in our first report as a major factor that leads to lack of specialisation.

The CBEC is assisted in specific customs related functions by four Directorates – the Directorate of Revenue Intelligence, the Directorate of Export Promotion, the Directorate of Safeguards, and the Directorate of Valuation and one division, called the Risk Management Division.

- **Directorate of Revenue Intelligence** – This directorate is the nodal agency under the CBEC in the enforcement domain. It is responsible for gathering and dissemination of intelligence on smuggling and commercial frauds, and investigation of major cases. It has a network of zonal and regional units that operate across the country.
- **Directorate of Export Promotion** – This directorate deals with various export promotion schemes and is the CBEC's interface with the Ministry of Commerce.
- **Directorate of Safeguards –** This directorate is responsible for dealing with applications for imposing safeguard duties and recommending them where warranted to the government.

- **Directorate of Valuation (DoV)** – This directorate acts as the national resource for valuation issues to support the CBEC as well as field formations. It maintains a number of data bases that are intended to assist the assessing officers in the field, important among which is the National Import Database (NIDB). It also maintains a centralised registry of related party cases which are to be finalised in the major custom houses.
- **Risk Management Division (RMD)** – This division is responsible for designing, implementing and managing the RMS using various risk parameters and risk management tools to address the risks facing customs, i.e., the potential for non-compliance with customs and allied laws and security regulations, including risks associated with the potential failure to facilitate international trade. The RMD is responsible for collection and collation of information and development of an intelligence database to effectively implement the RMS and also carry out effective risk assessment, risk evaluation and risk mitigation techniques. In this process, the RMD closely interacts with all custom formations, the Directorate of Revenue Intelligence (DRI), the Directorate of Valuation (DoV) and the Directorate General of Audit (DG Audit). It is also responsible for managing the Accredited Clients' Programme (ACP) of the CBEC.

The growth in the volume as well as complexity of international trade has naturally led to an increase in the workload of customs. Data furnished by the CBEC shows that, from 1997 to 2014, the number of import documents processed by customs has gone up 7 times. There has been a twenty-fold increase in the value of imports from Rs.1540000 crore to Rs.30,00,000 crore. Customs revenue rose from Rs.41,000 crore in 1997-98 to Rs.1,75,000 crore in 2013-14.

With the progressive reduction in peak rates of customs duties over the years, the percentage share of customs revenue in the total tax revenue of the central government has shown a declining trend, although in absolute terms, there has been a positive growth, mainly due to increase in the volume of international trade and imports. This is indicated in Table 8.1 below.

Table 8.1: Total tax revenue of the central government and the share of customs duties

(Rs. crore)

	2010-11	2011-12	2012-13	2013-14
Total Tax Revenue	793,071.72	889,176.36	1,036,460.45	1,159,155.60
Total customs duties	135,812.51	149,327.50	165,346.22	175,056.00
Percentage share of customs duties in total tax revenue	17.12%	16.79%	15.95%	15.10%

Customs also have the responsibility for the processing of import and export goods under a number of export incentive schemes, besides the disbursement of customs duty drawback on goods

exported from the country. Table 8.2 gives the data on revenue foregone (tax expenditure) on various such schemes.

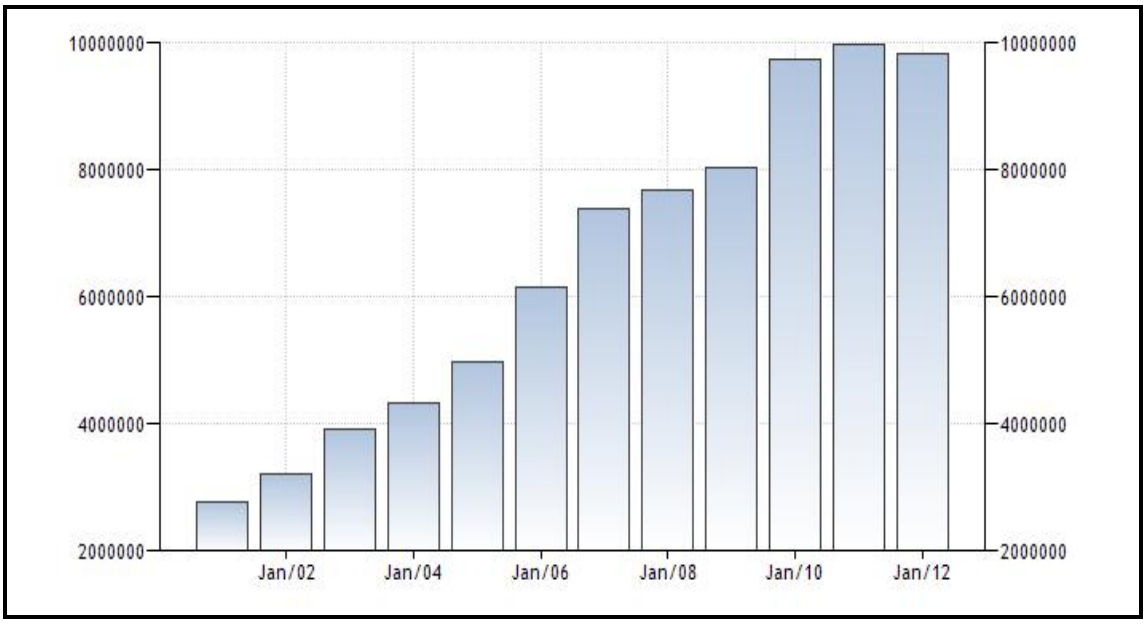
Table 8.2: Revenue foregone

(Rs. crore)

Name of Export Promotion Scheme	2008-09	2009-10	2010-11	2011-12	2012-13	2013-14
Advance Licence Scheme	12,389	10,089	19,355.28	18,306	18,971	20,956
EOU/EHTP/STP	13,401	8,076	8,579.87	4,555	5,881	5,840
EPCG	7,833	7,020	10,621.24	9,672	11,218	8,990
DEPB	7,092	8,028	8,756.55	10,409	2,709	434
SEZ	2,324	3,987	8,630.16	4560	4491	6198
DFRC	111	62	43.53	40	21	2
DFIA	1,268	1,399	1,404	1,244	1,735	3,365
Duty Free Entitlement Credit Certificate	418	234	156.39	190	142	235
Target Plus	1,220	267	374	436	592	884
VKGUY	2,059	2,869	1,788.48	2,263	2,232	2,442
SFIS	531	515	542	556	590	639
Focus Market/Product	408	829	1,757.50	3951	6,178	10,182
Total	**49,053**	**43,375**	**62,009**	**56,182**	**54,911**	**60,168**

Graph 8.1 depicts the steady growth in the number of containers handled in Indian ports.

Graph 8.1: Container port traffic in India



Source: http://www.tradingeconomics.com

There has been a steady growth in international passenger traffic. The number of passengers passing through international airports has grown from 19.42 million in 2004-05 to 46.62 million in 2013-14.[104]

The enforcement function to implement customs and allied laws on the borders is discharged by the Directorate General of Revenue Intelligence, Customs (Prev.) Commissionerates and the Special Intelligence and Investigation Branch (SIIB) in the appraising customs formations. While Customs (P) Commissionerates are entrusted with the responsibility of keeping vigil over international boundaries in their respective jurisdictions, the DRI, being the premier intelligence agency for anti-smuggling operations, keeps liaison with foreign countries, Indian missions and enforcement agencies abroad in such matters, in addition to intelligence collection and investigation of cases. DRI also liaises with INTERPOL through the CBI and it is the nodal agency for the CBEC to obtain any information from foreign customs administrations in matters of investigation. To collect intelligence, DRI relies on traditional human intelligence resources as well as contemporary technical intelligence gathering tools.

Areas of major concern on the outright smuggling front are the attempted smuggling of gold, narcotics, fake Indian currency notes (FICN), red sanders and ozone depleting substances (ODS), and on the commercial fraud side, undervaluation, mis-declaration of goods, misuse of exemption notifications, misrepresentation of country of origin of goods and related misuse of exemption under free trade agreements (FTAs) and misuse of various export promotion schemes. Statistics in

[104] *Source: AAI traffic news*

Tables 8.3 to 8.5 indicate trends in outright smuggling of goods and commercial frauds detected by the DRI and other customs formations during the last three years.

Table 8.3: Outright smuggling cases detected by DRI and other customs formations

(Rs. crore)

Commodity	2011-12	2012-13	2013-14
Gold	46.43	99.35	692.35
Foreign currency	35.55	9.96	14.49
Narcotic drugs	1711.93	969.16	451.98
Electronic items	189.98	71.66	37.85
Computers/parts	4.99	18.6	0.46
Fabric/silk yarn etc.	158.79	49.89	24.03
Bearings	6.10	0.32	0.47
Diamonds	24.66	9.46	6.62
Indian currency	18.2	4.87	5.20
Watches/Parts	7.3	8.88	1.17
Machinery/Parts	133.71	69.5	563.18
Vehicles/Vessels/Aircrafts	415.4	306.08	472.89
Indian fake currency	2.64	2.24	1.13

Table 8.4 compares the frauds detected by DRI and other customs formations, show-cause notices issued in these cases in FY 2012-13 and 2013-14 and the amount of duty alleged to have been evaded in these cases.

Table 8.4: Commercial frauds and duty evasion cases detected by DRI and other customs formations

Nature of fraud	2012-13		2013-14	
	No. of cases	Duty or export benefit involved (Rs. crore)	No. of cases	Duty or export benefit involved (Rs. crore)
Undervaluation	513	524.27	315	680.27
Mis-declaration	368	507.24	428	1015.88
Misuse of DEEC/Advance Licence Scheme	34	229.92	5	17.43
Misuse of DEPB Scheme	24	30.12	26	30.47
Misuse of EPCG Scheme	25	78.85	22	96.68
Misuse of EOU/ EPZ/SEZ Scheme	9	98.88	12	100.38
Misuse of Drawback Scheme	98	28.52	59	45.41
Misuse of end-use & other notifications	94	11.95	75	443.20
Other	322	597.81	972	2341.54
Total	**1487**	**2207.55**	**1914**	**4769.26**

Table 8.5 gives an account of the actions initiated – number of persons arrested, number of persons detained under COFEPOSA/PITNDPS and number of prosecutions launched. It needs to be noted that the cases mentioned for prosecution launch may not pertain to the FY mentioned, as normally there is some lag between the detection of cases and the launch of prosecution.

Table 8.5: Arrests, preventive detentions and prosecutions initiated by DRI

Action initiated	2011-12	2012-13	2013-14
No. of persons arrested	278	207	475
No. of persons detained COFEPOSA/PITNDPS	18	17	11
No. of prosecutions launched	22	25	16

VIII.2.a Procedure for import/export of goods

The import/export customs clearance process is handled in an automated environment through the Indian Customs EDI System (ICES), which works in conjunction with the e-Commerce portal of the CBEC, ICEGATE, and the customs' Risk Management System (RMS). The process is described in brief below.

i) Clearance at the Gateway Ports/Airports

The carrier of goods, i.e., shipping line/airline electronically files an import general manifest (IGM) before arrival in case of imports and an export general manifest (EGM) after departure in case of exports in the ICES either through the service centre or ICEGATE.

The importer is required to file electronically a bill of entry (B/E) containing a declaration of goods imported. Similarly, for export of goods, the exporter is required to file a shipping bill (S/B). On filing of B/E or S/B and self-assessment by the importer/exporter, the documents gets transmitted to the Risk Management System (RMS) by ICES. The RMS processes the data through a series of steps and produces an electronic output for the ICES to determine whether a particular B/E or S/B will be taken up for verification of assessment or examination or both by customs or be cleared without any customs intervention after payment of duty, if any. Also wherever required, RMS provides instructions to appraising/examining officers to help them discharge their functions. The accredited clients (ACP clients) are given assured facilitation and their consignments are interdicted for verification of assessment or examination by customs only rarely on a random basis.

Post-clearance compliance verification (PCCV) is done to confirm the correctness of the duty assessments. The objective of the PCCV is to monitor, maintain and enhance compliance levels, while reducing the dwell time of cargo. The bills of entry are selected for audit by RMS after clearance of the goods and directed to the audit officers for scrutiny. The number of bills of entry taken up for PCCV may be adjusted locally in the custom house in tune with available manpower resources. Normally, it is kept at 20- 30 per cent of total import consignments. In respect of ACP clients, an onsite post-clearance audit programme has been launched under which the audits are to be done by the central excise/service tax officers in the premises of these importers, along with central excise/service tax audit.

ii) Clearance at the ICDs/CFSs – Transhipment of import/export consignments between Gateway Ports/Airports and ICDs/CFSs:

Indian customs provide trade with the facility to complete all customs formalities relating to import/export goods at their door steps instead of their having to go to the gateway ports. For this purpose, inland container depots (ICDs) and container freight stations (CFSs) have been opened in the hinterland all across the country. The import/export goods move under bond between gateway ports and ICDs/ CFSs and are transported by agencies like the Container Corporation of India (CONCOR) or other private operators. The IGM filed by the carriers of goods from foreign ports to Indian gateway ports consist of a sub-manifest transhipment permit (SMTP) portion, which is treated as request for transhipment of goods from gateway ports to the designated customs port(s) in the hinterland. The containerised cargo sealed with the shipping agents seal or customs seal (if shipping line seal is found broken or tampered with at the gateway port) are transhipped under a continuity bond along with a bank guarantee submitted by the transporter. The transhipment permit (TP) information is electronically transmitted to the transporter undertaking the transhipment, the custodian of the gateway port and the ICES location at the destination port and it automatically converts into an IGM at the destination port. On the arrival of containers at the destination port, the transporter electronically submits the container arrival report to the ICES, which is then matched with the transhipment message received from the gateway port and a 'landing certificate' message is generated and transmitted to the gateway port for closure of the IGM lines. Thereafter, the imported cargo is cleared on filing the bills of entry from the ICD/CFS as per the rules. A similar procedure, mutatis mutandis, applies for transhipment of export cargo from ICD/CFS to the gateway ports.

The implementation of the Risk Management System (RMS) was one of the significant milestones in the e-Governance initiatives of the CBEC. It allowed the CBEC to move from a regime of virtually 100 per cent assessments and examination to a selective, risk-based approach to assessment and examination of cargo and the ability to release a large number of consignments without much human intervention. The objective was to strike an appropriate balance between trade facilitation and enforcement and optimise the utilisation of human resources. Further, under the Accredited Client Programme (ACP), importers, who have qualified to be accredited clients based on their past compliance record, are granted assured facilitation and except for a small percentage of consignments selected for assessment and/or examination by customs on a random basis by the RMS or cases where specific intelligence is available or where a specific pattern of non-compliance is required to be addressed, no assessment or examination is done.. There are approximately 300 ACP clients registered with the Risk Management Division (RMD) of the Directorate of Systems. Although the implementation of the RMS, together with the accredited clients programme, significantly enhanced facilitation and reduced the dwell time of cargo, these benefits lately seem to have lost momentum owing to certain factors that we deal with later in the report.

As the TARC noted in Chapter VII of its first report relating to ICT implementation, while the ICEGATE, ICES and RMS together have made significant contributions in the improvement of

the customs processes, the ICT coverage remains partial and does not cover all business processes, many of which remain in a paper environment.

Apart from ICT, customs have also taken major steps to modernise by investing in non-intrusive inspection systems such as container scanners. While a system has been developed and deployed in the *Nhava Sheva* port for risk-based selection of containers for scanning, it is yet to be integrated with the ICES, leading to the two operating in separate silos. A more detailed discussion on this follows later in this report.

VIII.3 Emerging trends in the global economy and the changing role of customs

The World Customs Organization (WCO), in its Customs Environment Scan 2013, presents the following picture of the emerging global trends in international trade.

The world has become ever more interconnected and interdependent through expanded cross-border flows of goods, services, people, transport, capital, information and technology. Globalisation makes it easier to conduct international business than in the past, and provides economies with the opportunity to fast-track development goals through increased international trade.

World merchandise trade has grown faster than growth in global GDP. This trend is likely to continue and global trade growth is projected to increase at 4.5 per cent in 2014 while global GDP growth is estimated at 2.6 per cent.

While China, the United States and the European Union (considered as single entity) are the largest players in international merchandise trade, developing economies and the Commonwealth of Independent States (CIS) have collectively increased their share and, in 2012, they accounted for nearly half of world merchandise trade.

In 2012, more than 80 per cent of world merchandise trade was carried by sea as measured in weight with a growth rate of 4.3 per cent. Containerised trade accounted for 16 per cent of global seaborne cargo by weight, and more than half by value. The air transport industry carried only 43 million tonnes in 2011 as compared to 8.7 billion tonnes carried by the marine transport industry, but it accounted for 35 per cent of the global trade in value terms. Despite a slight contraction in air cargo traffic, the express cargo segment showed a growth of 24.8 per cent and 10.2 per cent (as measured in RTK[105]) in 2010 and 2011 respectively. The international express sector is expected to register an annual growth of over 5 per cent consistently through to 2031. It may be added that the growth of e-commerce has a strong correlation with the growth of express cargo as this, together with the postal channel, is the primary mode for delivery of goods, bought over the internet, to consumers overseas.

International trade has also become more regionalised. The 2012 trade statistics indicate that 50.7 per cent of world exports were to countries in the same region. Thus, multilateralism seems to be

[105] Revenue-Tonne-Kilometer means weight multiplied by distance for charged cargoes.

losing ground and giving way to regional trade agreements. Intra-regional trade remained high in Europe (68.6 per cent), Asia (53.4 per cent) and North America (48.6 per cent), but low in South and Central America (26.9 per cent), the CIS (18.5 per cent), Africa (12.7 per cent) and the Middle East (8.6 per cent).

Regional Trade Agreements (RTAs) have proliferated over the last two decades. According to the WTO RTA database, 251 RTAs concerning merchandise trade existed as of December 2013, of which 144 RTAs entered into force in and after 2003. Among the RTAs, free trade agreements (FTAs) are most common, accounting for 87.6 per cent of the total RTAs in force. Given that a number of FTA negotiations are currently underway, including "mega-FTAs", in particular the Transatlantic Trade and Investment Partnership (TTIP) between the EU and the United States and the Trans-Pacific Partnership (TPP) between the US, Canada, and 10 countries in the Asia-Pacific region, it appears that the trend in favour of FTAs will continue for the time being.

With the increasing dominance of large multinational firms that operate as global networks across national borders, intra-firm trade and trade between related parties has witnessed a steady increase. According to an OECD estimate in 2011, such trade accounted for one-third of world merchandise trade.

New technologies, outsourcing, integration of global financial markets and advancements in transport and logistics has transformed the international supply chain. Trends such as the fragmentation of production across national boundaries pose complex challenges in relation to issues of origin and international trade statistics.

There has been a steady growth in export processing zones. In 2006, it was estimated that there were 3,500 export processing zones (EPZs) in 130 countries, employing around 66 million people. EPZs accounted for more than 20 per cent of total exports from developing economies, although this varies from country to country.

The increase in illicit drug trafficking is an issue of great concern to the international community. Illicit drugs pose a grave threat to public health and safety and the trafficking in such drugs undermines economic development and international stability. The UNODC (2013) indicated that maritime seizures for drug trafficking amounted to 11 per cent of all cases, but each maritime seizure was on average almost 30 times larger than seized consignments trafficked by air. As a result, the share of maritime seizures jumped to 41 per cent in quantity terms. It is estimated that customs is responsible for more than half of all drug seizures worldwide.

The issue of security of global trade and international supply chains has attracted considerable attention in the international community in the light of the increasing threat of international terrorism after the 9/11 attacks in 2001. The acquisition of weapons of mass destruction or the strategic goods used to develop or deliver them threatens both national and international security, and a major proliferation event could have a catastrophic impact on global supply chains. Faced with this concern, the WCO introduced the Strategic Trade Control Enforcement Programme

(STCE) in 2013 to better assist members to identify and seize strategic goods which could pose a serious threat to global supply chains and to international security.

Cross-border movement of dangerous goods that undermine public health and safety is a global problem. The dangers posed by certain counterfeited or substandard goods like medicine, tobacco products and batteries to the health and safety of citizens have been well recognised.

The importation and exportation of environmentally-sensitive goods like CFC gases and hazardous waste, etc., has become an issue of increasing concern for customs administrations. Cross border movement of such environmentally-sensitive goods is subject to a variety of multilateral environmental agreements and the role of customs with respect to such goods is to ensure compliance with the trade-related provisions of these multilateral agreements.

The emergence of e-commerce is creating a global, virtual and borderless marketplace. This has a direct correlation with the growth in express cargo and postal channels and presents a challenge to the global customs community of handling growing volumes of expedited clearances while maintaining sufficient control to prevent the abuse of this channel. For example, the WCO Illicit Trade Report indicated an emerging trend in seizure cases, namely, an increase in IPR-infringing goods transported in small consignments handled by express companies and by post.

Customs import duties remain a significant source of government tax revenue in many developing countries although their share has declined as tariff rates have dropped through multilateral, regional, bilateral and unilateral initiatives. A WCO survey indicated that tax evasion was the first enforcement target for nearly 70 per cent of customs administrations. A WCO report estimated that customs collected more than 10 per cent of total government tax revenue in at least 90 per cent of the countries, more than 20 per cent in at least 74 per cent of the countries, and more than 50 per cent in at least 18 per cent of the countries (in India, as noted above, customs duties represent 15-17 per cent of total central tax revenues). Revenue loss, caused by under-invoicing, smuggling, origin fraud, misclassification, transfer pricing, etc., significantly undermines national economic development and competitiveness.

Globalisation also has implications for how customs define "border" in the context of customs control. Increased emphasis on supply chain security, the need to regulate economic activities in the continental shelf and exclusive economic zone, etc., means that it stretches overseas for some purposes, while greater emphasis on post-clearance controls and emergence of SEZs, inland ports, etc., means that it extends to the hinterland. Similarly, "security" in the customs context would go beyond the aspects of physical security and embrace wider issues of the economic security of a country, protection against health and safety hazards, etc. In framing its recommendations, the TARC has kept these dimensions in view.

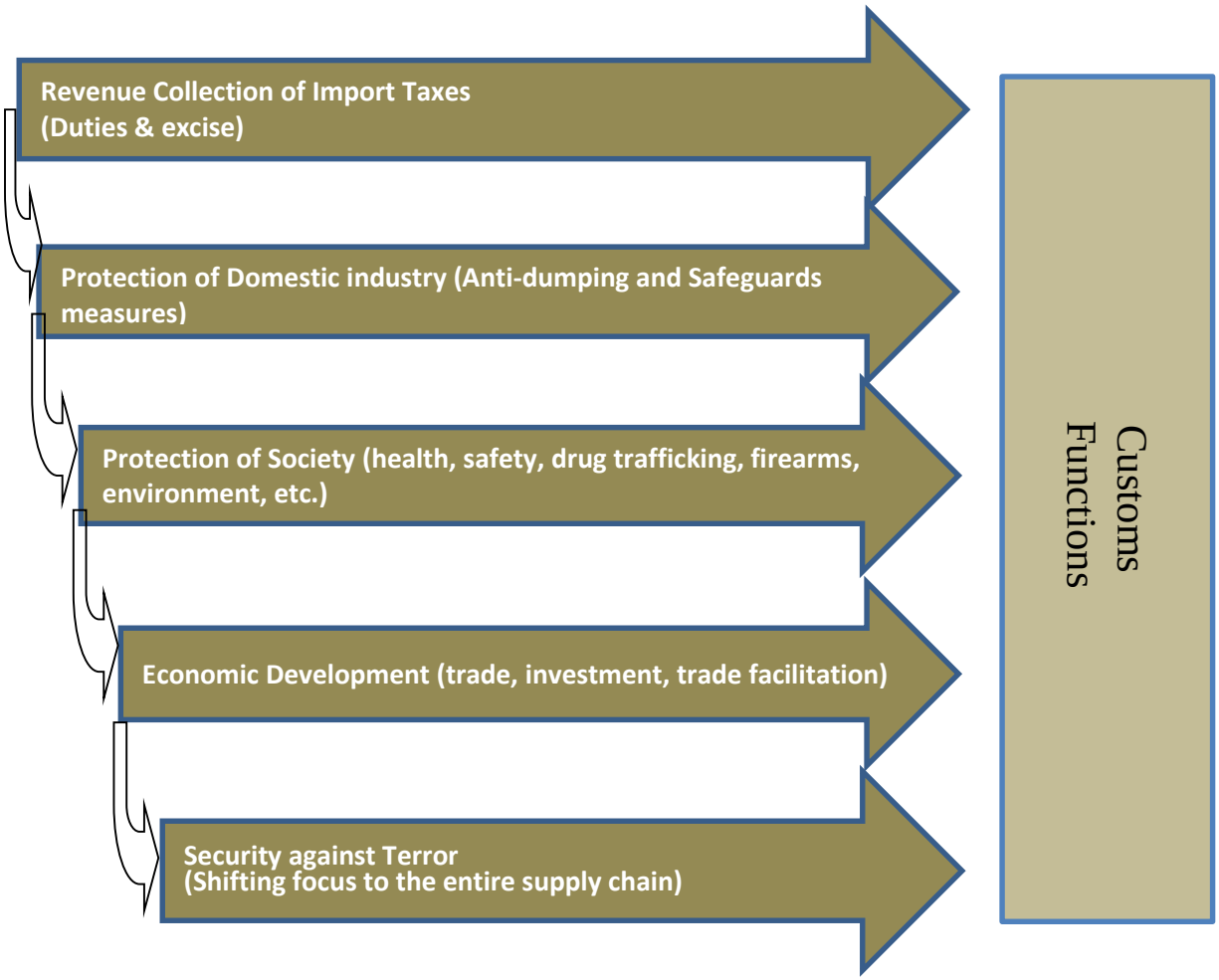
VIII.3.a Emerging role of customs and changing customs control paradigm

The trends delineated above pose complex challenges to a customs administration and necessitate a fundamental re-examination of its role, strategies and organisational structures and processes.

Effective exploitation of the rapidly developing ICT and other technologies, on the other hand, offer new capabilities for overcoming these challenges.

Diagram 8.1 depicts how the role of customs has evolved over time.

Diagram 8.1: Evolution of role of customs



In the face of the growing complexity of the challenges before them and the greater need to facilitate legitimate trade, customs administrations globally are getting "smarter". They are investing heavily in technology, simplifying processes and recognising information as the primary lever of control. They have moved away from the "gatekeeper" approach and the control mechanisms they employ are no longer built around the traditional means of checking individual transactions and routine physical examinations – measures that introduce high costs and unpredictability in the cargo clearance process. They rely on advanced risk analysis to intervene by exception at the pre-clearance stage and effective post clearance audits as the chosen control mechanisms. They also place strong emphasis to customer focus – building partnerships with industry, facilitating compliant traders, simplifying procedures and educating industry and the community on compliance requirements through easy to use and exhaustive documentation and other communication channels.

With emphasis shifting from static border control to supply chain security, most customs administrations are building strong capacities to effectively implement programmes like the WCO's SAFE Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework), including Authorised Economic Operator (AEO) programmes and mutual recognition programmes. This represents a more evolved approach to compliance management, which seeks to address risks by forging partnerships with willing and compliant traders who maintain prescribed standards of compliance and work with customs to get their records and processes validated.

For effective control, the best practising administrations have adopted sound risk management frameworks that focus on compliance improvement by using a mix of appropriate customer service and enforcement interventions. Their HR policies tend to focus on competency building and specialisation among staff and leadership in key areas.

The risk assessment is also shifting from being rooted in historic records to a more dynamic, self-evaluating, predictive and continuously improving system. There is also growing realisation that the risk management philosophy needs to be a whole-of-government approach to border management with all other government agencies (OGAs) embracing the global trade facilitation agenda.

It is increasingly recognised that the key to effective tax administration is a system that encourages and incentivises a culture of voluntary compliance by the taxpayer. Hence there is a pronounced emphasis on good governance, accountability and transparency. The functioning is within the framework of clearly articulated strategic plans and performance goals. An increasing number of administrations also regularly publish data on their performance and regularly obtain customer feedback.

In short, to cope with diverse emerging challenges faced by them, customs administrations have moved from the traditional administrative approach to a more strategically oriented and wholesome compliance management approach aimed at maximising voluntary compliance and founded on robust and reliable risk management.

In terms of the core customs clearance process, their approach broadly has been to delink issues relating to duties, tax, etc., from the clearance decision, which revolves primarily around what are called "admissibility" issues (security, health and safety, contraband etc.), which risks necessarily involve pre-clearance treatment. Duty or tax related issues are usually handled in a post-clearance environment. Further, compliant traders are also allowed duty payment on a periodic basis, based on a return that they are required to file. Thus, in such cases, release of goods has been delinked from duty payment and globally, the customs assessment and duty payment process has moved much closer to the one already widely in vogue everywhere, including in India, in relation to assessment and payment of taxes.

Table 8.6 gives a broad comparison between the Indian situation and global trends in customs administrations.

Table 8.6: Comparison in Indian customs administrations with global trends

Customs Role	Indian Customs	Global Trend
Revenue Collection	• Transaction base assessment • Duty collection before release • Poor audit-based control • Examination of goods as part of assessment • A plethora of notifications and procedures adding to complexity, uncertainty and unpredictability in assessments and clearance.	• Periodic return-based filing and assessment of duty • Clearance of goods from customs custody not linked to payment of customs duty • Deferred duty payment linked to periodic return filing • Strong post-clearance, audit-based control • Larger emphasis on risk-based examination of goods with an aim to confirm the correctness of disclosure
Protection of economic interests of domestic industry	• Ministry of Commerce comes up with decision on levy of anti-dumping duty on imports • Directorate of Safeguards, under the CBEC, decides on levy of safeguard duty • Process of investigation and levy of anti-dumping, safeguard duties etc. is not robust and lacks transparency • No institutional mechanism for country of origin verification • Inadequate risk management in relation to origin risks and lack of specialisation in the area.	• Robust process for investigation and levy of anti-dumping and safeguard by Department of Commerce – International trade Administration • Strong institutional mechanism for country of origin verification by the donor country with an aim to protect domestic industry against origin frauds – around 45% failure rate of import origin verifications in Korea in the year 2013 • Specialisation in Origin Administration/Management
Protection of Society	• Combating smuggling • Administration of narcotics and psychotropic substance regulation • Control on import of hazardous products, agricultural products	• Strong intelligence driven risk assessment • Technology and analytics assisted early identification of threats

Customs Role	Indian Customs	Global Trend
	• Inadequate use of ICT and analytics. • Lack of adequate coordination with other governmental agencies in relation to border procedures	• Single window, co-ordinated implementation of all allied laws • Integration of other regulatory agencies with customs administration • Strong canine enforcement programme against drug trafficking, e.g., the US has the largest number of working dogs
Economic Development	• Poor focus on trade facilitation measures which is said to result in 15% cost disadvantage to Indian goods in global trade • Outdated physical controls over goods and premises • Absence of origin verification agency leading to possible loss on account of misuse of free trade agreements • Inadequate compliance guidance to trade	• Trust based system with strong customer focus • Very strong focus on trade facilitation • Document and self-declaration based system with very strong audit-based controls • .Active programmes for trade assistance and guidance
Security	• Poor implementation of AEO programme • No traction on mutual recognition agreements • Lack of security focus in customs administration	• Strong focus on security • Institutionalising customs to business partnership on security • Co-ordinated border management with involvement of various agencies and co-ordination bodies • Strong implementation of mutual recognition agreements

The impression of there being a large gap between the current state of customs administration in India and international best practices is reinforced by some of the key feedbacks the TARC got from consultation with various stakeholders, which is summed up below:

i) Indian customs lack confidence in administering a document-based or digital footprint-based controls; hence they go by the dated process of physical control for collection of duty.

ii) Although there has been an improvement in terms of quick releases under programmes like the ACP and AEO, there is a high degree of unpredictability in the release processes and uneven quality in performance across different customs formations.

iii) Differences in assessment practices continue across different locations, adding to unpredictability on the one hand and allowing dubious traders to take advantage of weak points on the other.

iv) There is absence of a proactive approach in issuing clarifications on doubtful or contentious issues. This leads to lack of clarity and consistency and avoidable disputes.

v) There is a marked absence of judicial discipline and respect for precedent, which results in a plethora of avoidable disputes.

vi) There is marked risk aversion to taking decisions that are in favour of the taxpayer

vii) The approach is not very taxpayer friendly, particularly at the frontline levels, and customs is widely perceived to be adversarial in attitude and lacking in a positive and helpful approach.

viii) The concept of self-assessment has not been internalised by officers at operational levels.

ix) Trade facilitation is not owned as important action point by Indian customs. Each forward step is often followed by a backward step – resulting in Indian customs border being an unpredictable element in the global supply chain.

Customs are also not regarded as being responsive to emerging needs and opportunities for industrial growth. For example, although the country has the potential to be a choice destination for exhibitions, seminars or other international events, its realisation is inhibited by the discretionary nature of controls on temporary imports and inconsistent practices. India is widely considered as a temporary import unfriendly country. Some of the notifications issued in this regard have been written in 1994 and 1995 and do not seem to have been reviewed to suit contemporary needs.

VIII.4 Way forward

VIII.4.a Governance

The starting point for capacity building in the CBEC must thus begin with an assessment of the "as is" situation and the development of a clearly articulated vision and strategic plan that is aimed at rejigging its governance and placing it among the "best in class" customs administrations. The plan should set out clearly the strategic goals of the CBEC and the implementation strategy to achieve them. It should also focus on putting in place appropriate service standards and performance standards that are measurable so that progress can be reviewed on an ongoing basis. And the implementation needs to be backed by a robust performance management framework using which the CBEC can continuously track and improve its performance and benchmark itself regularly with best international practice in the spirit of continuous improvement.

This will require a strategic reorientation of customs, shedding the overwhelmingly transactional and administrative mind-set that dominates thinking. The strategy must be centred on measures calculated to promote voluntary compliance and leverage technological capabilities to enhance its ability to control the cross border movement of goods and persons with as little intrusion as possible. It will need the customs to get far more customer focused and forge much closer links with trade and industry in designing and implementing policies. It will need to undertake a much more intensive stakeholder engagement to promote voluntary compliance and move in the direction of a partnership-based, collaborative approach towards good corporate citizens who have the capacity and commitment to share responsibility for compliance. In Chapter III of its first report, the TARC had set out the key principles and values that should form the foundation of the structures and processes of governance and recommended a functional restructuring of the organisation to suit contemporary and emerging requirements. These will have to form the fulcrum of the customs' strategy.

The strategy should reflect the changing role of customs, looking beyond exclusive revenue orientation, and focus on capacity building in emerging areas such as the AEO programme and SAFE frameworks, RTA administration, and proper application of trade remedies, non-tariff barriers, environmental and safety issues, border functions relating to Intellectual property rights etc., which are dealt with in this report.

The strategy should also recognise the vital importance of facilitating legitimate trade in enhancing the international competitiveness of the country. As noted earlier, the forces of globalisation have transformed manufacturing and led to increased movement of intermediate goods across national borders. Increasingly, a manufactured item will involve raw materials and components that have moved back and forth among multiple countries before emerging as a final product in one jurisdiction. Supply chain economics have become a key factor in today's manufacturing and trading environment, with emphasis on lowering costs and managing just-in-time inventories and any undue break in the supply chain can have serious consequences on the viability of a business. Unpredictability and delays in border procedures therefore directly affect the investment climate of a country and far greater understanding of the consequences of their actions and a much greater sense of responsibility in the exercise of authority needs to be exhibited by customs officers at all levels. It, therefore, should aim at developing systems, structures and processes that ensure that the response of the CBEC is consistent and uniform across the spread of the organisation, whether it is in the area of customer services or enforcement.

Again, as noted in Chapter VII of the TARC's first report, ICT needs to be far more deeply embedded in the governance structures and processes in order to reflect the realities of the digital world. A cornerstone of the customs strategy, therefore, will have to be an ambitious plan to become a fully digital enterprise. The importance of this cannot be overemphasised as ICT is the key enabler for the organizational transformation that is needed. The TARC had, in Section VII.6 of that chapter, suggested a roadmap for the journey towards the "digital by default" status.

Thus, there must be a clear articulation of the customs vision that focuses on the following.

- Delivery of customer services according to declared standards and with respect for taxpayers rights
- Standardisation and simplification of processes, minimising discretionary controls which pose moral hazard in international trade
- Effective use of ICT and other technologies
- Active participation in the economic development of the country by improved facilitation performance and reduction in transaction costs
- Active participation in the protection of national security at the border alongside other security agencies
- Continuous improvement by sound performance management and by testing policies, notifications, circulars and procedures, etc., against the vision.
- Sound integrity management coupled with transparency in reporting performance

This entails changes in its control paradigm, which must shift from a transaction based approach characterised by high levels of pre-clearance interdiction to intelligence-led, risk based interventions by exception, with supply chain management and post-clearance audits as the primary tool for compliance management. Unless this happens, CBEC cannot hope to achieve comparability with the global best practices in customs administration. There is no choice but to do this as it will be well-nigh impossible for it to fulfil its mission with the traditional methods of routine transaction-based processing of import and export documents in the face of growing workload. It must take bold decisions to move away from the traditional approach if customs are to transform themselves into facilitators, rather than inhibitors, of the country's economic growth.

With the implementation of the risk management system (which included the introduction of post-clearance audit), the introduction of the accredited clients programme and the legal changes in the Customs Act, 1962, in 2011 to introduce the principle of self-assessment, Indian customs have taken the first necessary steps towards modernisation. The launch of the AEO programme was the next step in this direction. The CBEC also clearly acknowledged the crucial importance of facilitation in its operations when it, vide circular F.N. 450/20/2007 – Cus IV dated Sept. 2, 2011, laid down, for the first time, facilitation targets.

While the implementation of RMS has enabled it to resort to targeted selection of consignments, enhancing the level of facilitation of legitimate trade while subjecting riskier transactions to closer scrutiny, customs in India have not developed an enterprise risk management framework in the context of which tools like the RMS need to be operated. The TARC has noted the absence of such a framework in Chapter III of its first report and recommended the creation of a functional vertical for strategic planning and risk management. As the TARC had noted in the first report, the usual tendency in organisations, including the CBEC, is to focus only on operational risks, resulting in inadequate preparedness to cope with challenges that threaten their mandate. That recommendation is reiterated in the present context too.

The various interactions that the TARC had with stakeholders, including departmental officers, gave it the unambiguous impression that the spirit of the compliance philosophy that underlies the principle of self-assessment has clearly not been internalised in the department, particularly at the operational level. The TARC believes this to be partly due to weak and inconsistent articulation of the strategic and operational goals and poor communication across the organisation. It is also due to a pervasive transactional mentality even in the leadership. Radical improvements are needed on both aspects. As the TARC noted in its first report, self-assessment marks a fundamental change in the relationship between the government and the citizen (or the taxpayer). It is founded on voluntary compliance and on trust as the first principle of administration, and a shared responsibility for compliance. In essence, the administration, while devolving the responsibility for compliance with laws to the affected citizen or business, assumes responsibility for creating conditions in which the taxpayer is enabled to fulfil his responsibility. This responsibility does not seem to be adequately owned at any level in the organisation. For instance, the TARC heard repeatedly during its interactions with stakeholders that there is a marked reluctance on the part of field officers and the CBEC to clarify contentious or doubtful issues when clarification is sought, leading to uncertainty and divergent practices and feeding into avoidable disputes, which add to costs for traders. In Chapter V of the TARC's first report, it has cited international best practices and highlighted the need for the CBEC to proactively step in and issue clarificatory circulars using the provisions of Section 151A of the Customs Act. The implementation of this recommendation will go a long way in meeting a frequently expressed need by importers/exporters.

It is equally necessary to undertake periodic review of every circular, notification etc. to examine its relevance and contemporaneity in the context of changing environment. The use of sunset clauses is a valuable way to ensure such reviews and should become a regular practice in CBEC. Another recommended practice is to consolidate the instructions/circulars etc. periodically and publish comprehensive compendia subject-wise, superseding the previous versions. This will ensure clear and user friendly guidance to trade as well as officers[106].

With the introduction of self-assessment there is also a need for CBEC to develop and make available detailed guidance in the form of self-assessment check lists in important areas which can assist the importers/exporters in achieving compliance.

In order to enhance the certainty for the taxpayer, the provision of advance ruling is an important tax payer service. In view of its current weaknesses, in Chapter V of its first report, the TARC had given recommendation for revamping the advance ruling mechanism. This is relevant in the customs context also because provision of advance rulings is an important requirement under the Revised Kyoto Convention.

Another key input the TARC heard was the lack of user friendly access to updated notifications, rules, regulations, etc., on the official website. In Chapter VII of the first report, the TARC had

[106] Many years ago, there was a practice in the CBEC of issuing a "Pink Book" that was a compendium of instructions on tariff classification etc. This enabled officers to get reliable guidance at one place. This practice appears to have fallen into disuse and there have been only sporadic attempts to consolidate instructions. In the current context, of course, such compendia need to be made available digitally to both officers and the trade.

recommended adoption of a maturity framework for continuous enrichment and improvement of the CBEC website, by improving navigability, searchability and ever improving user friendly features, and adoption of "what is not on the website does not exist" policy, which will meet this long-felt need. This means conscious adoption of a policy that no law, notification, circular can take effect unless it is first published on the official website. It also entails a sound content management process for constant updating that ensures that everyone, whether a customs officer or a trader, can fully rely on the information on the official web-site. And this with a degree of robustness that eliminates the need of the "disclaimer" that typically occurs on such websites. The website should be the official face of the department without any caveats.

Measures like this will go a long way in promoting voluntary compliance and contribute to transparency, predictability and certainty in the application of laws and procedures. The CBEC needs to adopt such modern best practices and put resources behind these programmes.

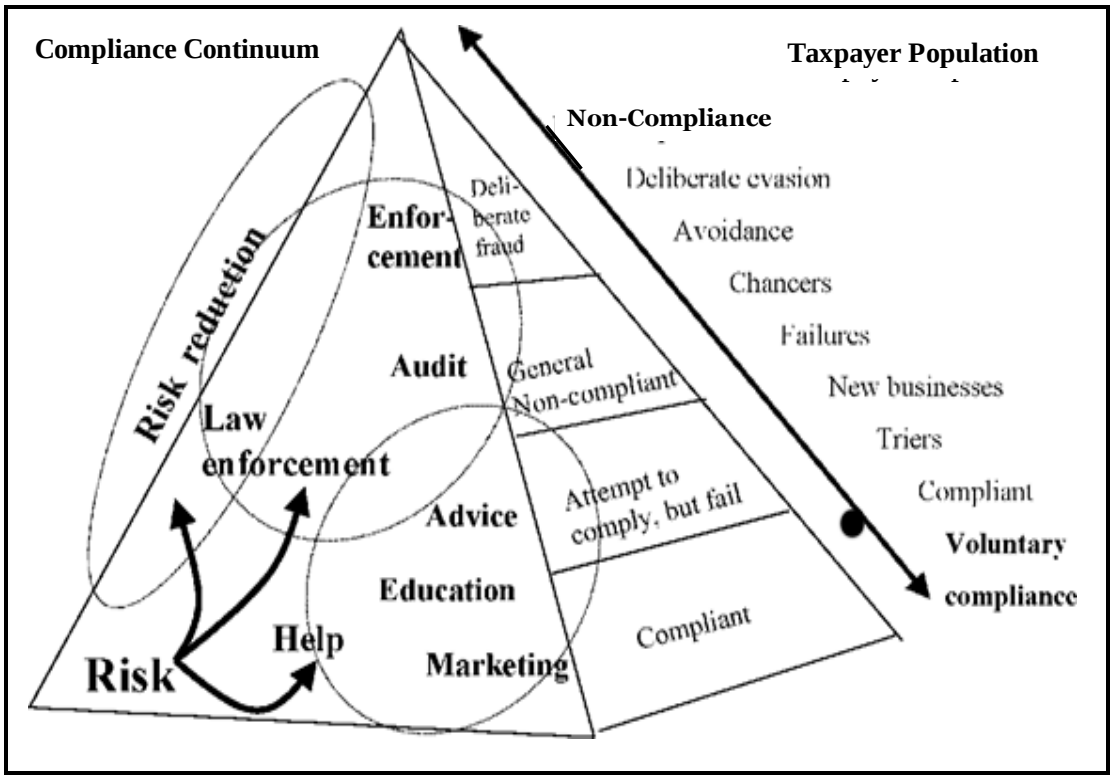
One of the key factors that inhibit the full implementation of some of the initiatives is the general absence of a programme management approach. In Chapter VII of its first report, the TARC had identified this as a critical deficiency in the context of ICT implementation. This point is equally valid in relation to the other areas of importance such as the AEO programme and post-clearance audit programme. For successful implementation of such key initiatives, the CBEC needs to adopt such an approach. This will necessitate a well-defined process and methodology that places the particular programme in the overall strategic plan of the CBEC, clear articulation of objectives and goals, a clear programme and process ownership and allocation of roles and responsibilities, planning and deployment of resources, and a rigorous performance measurement and evaluation to assess the outcomes, so that further improvements can be made. Such evaluations are indeed a prominent missing link in the programmes implemented so far. The ACP was launched as a flagship facilitation programme of the CBEC in 2004. However, there has so far been no systematic evaluation of the programme to assess its impact and to effect improvements. The same is true of the post-clearance audit programme.

The CBEC also needs to develop a robust risk management framework that dynamically addresses all dimensions of risk and enables it to build the required capacities to face emerging challenges effectively and efficiently.

VIII.4.b Upgrading the risk management in customs

Diagram 8.2 is an illustration of a dynamic risk management framework.

Diagram 8.2: Dynamic Risk Management Framework



Source: Risk Management Guide for Tax Administrations, Fiscalis Risk Analysis Group, European Commission

As can be seen, differentiated strategies and interventions need to be adopted in relation to different segments of clients whose behaviours range from voluntary compliance to deliberate non-compliance, in order to promote compliance and reduce risk. At one end of the spectrum are clients who are highly compliant in that they exhibit both the capacity and commitment to compliance. The approach towards them has to be highly facilitative and partnership oriented, with the full range of facilitation benefits extended. At the other end are those that exhibit extreme disregard for law. The approach towards them has to be enforcement oriented with frequent checks and application of strong sanctions to deter non-compliance. In between is a wide range of clients who exhibit varying degrees of compliance, towards whom the approach has to be calibrated according to their behaviours and motivations and key factors in their environment that affect their attitudes towards compliance. It has necessarily to be an appropriate application of enforcement and audit interventions combined with encouragement through help and guidance, in the case of those who are not inclined towards non-compliance but lack the capacity in terms of knowledge or resources to achieve full compliance. The goal of strategic risk management is to progressively and consistently move the client population towards the compliant end of the spectrum, thereby improving the overall compliance environment.

Critical to the success of such a framework is robust and effective segmentation of taxpayers. This needs to be analysis and evidence based and not merely opinion or perception based. It can only

be achieved through extensive research and analysis, with multidisciplinary skills such as those of data analytics, social scientists, customer service specialists and domain experts being brought to bear on the task. And such research needs to be seen as a continuously evolving process, rather than as a one-off project.

The key point to be borne in mind is that risk management is not just about having good processes. It is a way of thinking that moves a customs administration toward proactive – rather than reactive – approach. Risk management in customs, including intelligence and operations, must rest on an effective regulatory framework, which should be aimed at encouraging voluntary compliance. Although the basic thinking underpinning risk management may remain the same, its cyclical nature allows constant improvement. This may mean reconfiguring estimated risk levels, introducing new technologies, creating new capacities or sharing more risk with other supply chain participants.

Measurement and feedback are a key component of risk management, which should essentially be seen as an iterative process. Key risks need to be identified on the basis of analysis of data and other evidence and treatment plans designed and implemented. This should be followed by an evaluation of the measures taken and this should be fed back into risk management. For example, if non-compliance, say, in the form of erroneous classification of a particular good, is detected across many locations and across different segments of taxpayers, it might reflect a commonly shared interpretation of the relevant entry rather than a deliberate attempt at evasion. In such a case, the appropriate treatment of the risk would appear to be a clarification setting out what the department regards as the correct interpretation. In other situations, responses could be different depending upon the nature and gravity of risks, their impact and the perceived motivation of the concerned parties and could lead to enforcement actions. In still other situations, the risks could be addressed through public education and outreach programmes, investment in technology and development of the relevant competencies and so forth. In important areas, compliance improvement plans need to be developed, communicated effectively and implemented, and their results measured and evaluated and the process continued in a cyclical fashion.

The creation of the functional vertical in the form of Strategic Planning and Risk Management (SPRM) Directorate, as recommended by the TARC in Chapter III of the first report, will enable the CBEC to impart a strategic dimension to its efforts by anticipating major challenges, and responding ahead of time so that threats to compliance are effectively mitigated. An important function of this vertical should be to continuously scan the environment for emerging trends in terms of business practices, technologies, etc., and prepare the organisation by planning the required human, organisational and technological capacities to either cope with the threats to its mandate or to exploit the potential emerging trends may offer.

The CBEC will also have to build a far greater capacity for use of data analytics for more effective risk management. In Chapters III and VII of the first report, the TARC had highlighted the crucial role that data analytics plays in better policy making and effective risk management, and recommended the setting up of a Knowledge and Analysis Centre (KAIC), comprising a range of data and analytical skills to support strategy, policy making and operations. Apart from this, the

TARC had also emphasised that a high degree of analytical ability will have to reside in the functional verticals as well.

VIII.4.c Closer strategic involvement in development of trade policies

Greater emphasis on analysis will enable the CBEC to play a meaningful and constructive role in the government's trade policies as well. For instance, there is an urgent need for a cost benefit analysis of all FTA's to be done; this has not happened .While we do know the steep increase in imports from our FTA partners simply because of the huge market access we are offering, little fact based analysis is done about the exports from our country to these FTA partners. With more such pacts on the anvil, such as the Regional Comprehensive Economic Partnership (RCEP) involving the 10 ASEAN Member States and ASEAN's free trade agreement (FTA) partners viz. Australia, China, India, Japan, Korea and New Zealand, such research is of critical importance. It is in view of the growing importance of this area that later in this chapter we have recommended the setting of the Directorate of Origin that will devote focused attention to this area.

Similarly, even though the SEZ scheme does not come under the purview of Customs directly, there is an urgent need for cost benefit analysis. While customs have some idea about the customs duty foregone there is an absence of reliable and comprehensive data about the excise duty and service tax that are not collected. There has been no empirical study done of the benefits which the country has had because of the SEZ scheme while there have been instances of clandestine diversions into DTA or mis-invoicing of goods.

By basing their arguments on research and evidence, customs can contribute to shaping of the country's trade policy with greater persuasiveness and credibility. At present they are perceived as excessively revenue driven and ignoring the wider interests beyond revenue. Often they may have a valid argument; however, because it is not backed by adequate analysis and evidence they are not able to argue persuasively.

VIII.4.d Strengthening of Risk Management Division

In the specific customs context, it is the Risk Management Division (RMD) that will have to take a key role in this respect. It needs to be substantially revamped and strengthened to enable it to assume a more active strategic as well as operational role in customs risk management and to achieve greater integration of customs processing with intelligence driven risk management. At the strategic level, its research output should support the CBEC in developing programmes and policies as outlined earlier. At the operational level, it needs to build the technological and human capacity to use advanced analytical tools to engage in predictive analysis and improve risk assessment to sufficient levels of accuracy to allow virtually all legitimate traders to continue their business without intervention, and to allow for the remainder to be targeted. It should also be enabled to develop new algorithms and invest in sophisticated search and match technologies that will improve its ability to identify both individuals and cargo for interdiction.

As has been mentioned above, feedback and re-evaluation is a critical component of the risk management process. This does not seem to be happening adequately. The RMD needs to

undertake constant evaluation of the performance of the RMS to ensure that there is sharpening of the risk rules, targets or interventions inserted by the national and local risk managers to improve the quality of matches with suspect profiles. This will ensure that a large number of consignments are not unnecessarily checked, thereby adding to delays in clearance and associated costs on the one hand and waste of customs resources on the other. Under the current system, the local risk managers at the custom houses have the ability to insert targets and interventions for their respective locations. Experience has been that these tools have been used without adequate care and competence, leading to a large number of consignments getting unnecessarily assessed and examined by officers. To check this, RMD needs to be empowered to assume a greater national role and exercise greater control over local risk managers by issuing appropriate directions to ensure that the quality of performance is maintained and it is consistent across the country. Ideally, the local risk managers should step in only when there is a particular risk specific to their location or where they have reliable local intelligence as many of the key risks are national in character. It should be the RMD that primarily controls the system in order that a national consistency is maintained and interventions are purposeful, based on proper analysis and evaluation.

With the installation of the first container scanners in *Nhava Sheva* port, a risk management module for risk based selection of containers for screening was implemented. It was a standalone module, which was not integrated with the ICES, with the result that the officers processing the consignments in ICES do not have access to the images of screening. Now that these scanners are being installed in different ports, container selection should be put on a much more robust footing. It should be integrated with the risk management system and the ICES. The CBEC should progressively move away from a purely local approach towards a national approach that will ensure that risk management techniques are applied consistently across the country. It should move towards setting up a national targeting facility in the RMD along the lines many customs administrations, such as those in the US, Australia and New Zealand, have set up. The facility should be linked to all the ports and take in scanning feed from them. The decision on whether to clear a container or examine it should be taken by specially trained staff and communicated to the customs in the port. In course of time, the facility should also house the representative of other border agencies as a co-ordinated risk management framework is evolved by customs so that co-ordinated decisions can be taken.

VIII.4.e Revamping the core customs clearance process

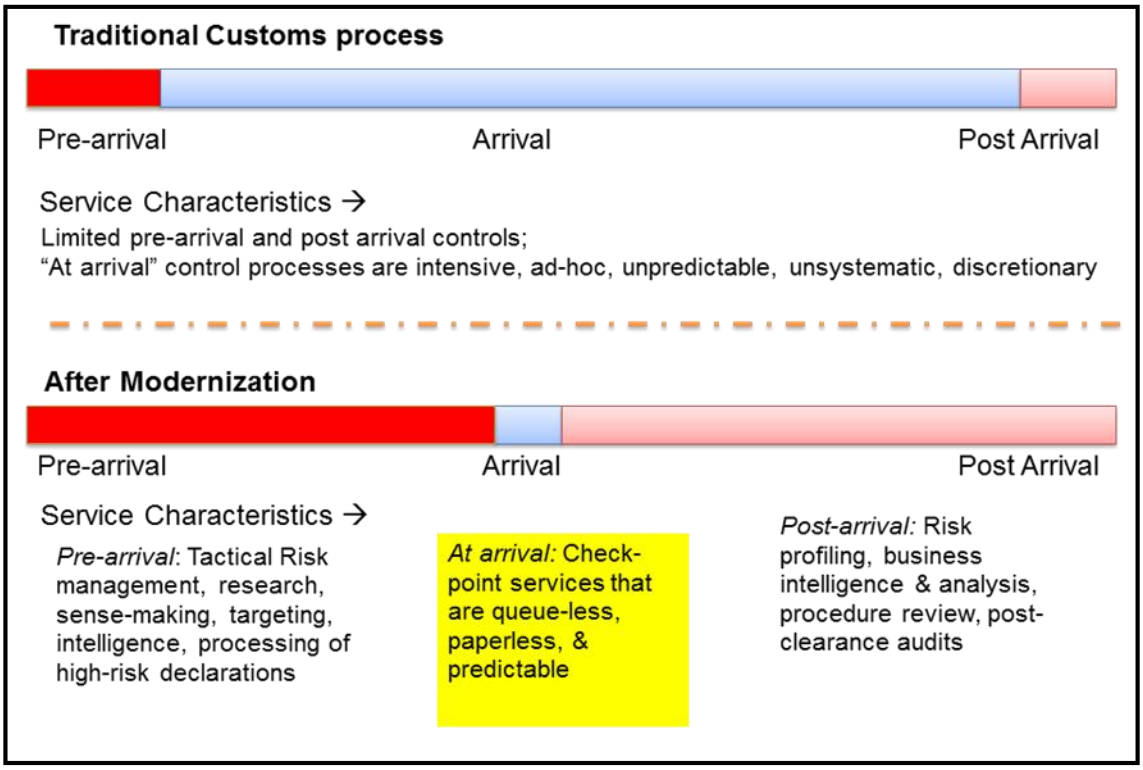
The customs clearance process in India continues to be in the traditional mould even after the introduction of the self-assessment and risk management system. There are a large number of consignments that are assessed and examined on arrival, leading to goods taking a relatively longer time for clearance than in many other countries. Data provided by some stakeholders indicates that the time taken for customs clearance in Australia, Germany, Netherlands and Singapore ranges between 1 to 3 hours where cargo is not selected for inspection and 24 to 72 hours where it is selected for inspection. There is far greater reliance on advance submissions of cargo and goods declarations and a much smaller percentage is selected for examination at ports.

The processes in advanced countries are more or less in the following order:

- Pre-loading risk assessment based on advance information for security purposes (the **admissibility decision**) (Separate carrier and/or importer security filing practices).
- Pre-arrival goods declarations for the **release decision;** physical release of goods for import or export.
- Post-release filing of all clearance details and **clearance**, when all duties, taxes, etc., are settled.

Diagram 8.3 depicts the pre and post-modernisation customs control paradigm.

Diagram 8.3: Pre and post-modernisation customs control paradigm



To make sure that the 'at arrival' is generally paper-free, the following must happen:

- The response to a goods declaration is a release decision, delivered electronically, which can be printed out (like the boarding pass) and may contain a bar code or QR code.
- The supporting documents, where required, are submitted digitally as scanned copies or e-documents. Strict checks are performed on the identity of the vehicles and people involved in the physical delivery.
- Physical inspection of documents or goods is by exception and is primarily designed to confirm the accuracy of declarations.

The physical process of cargo delivery for import, export and transit in modern customs administrations must be as orderly and predictable as that of a passenger checking in at an airport to board a flight.

The CBEC should aim at aligning its operations with this process and minimise pre-clearance intervention so that cargo moves seamlessly through Indian ports and airports. They should also aim to follow the international norm of separating duty payment from release. They can introduce this in a calibrated manner, starting with trusted partners such as AEOs. For the rest, they must progressively reduce pre-clearance checks, finally limiting them only to very high risk importers such as fly-by-night operators who are difficult to trace once the goods are cleared.

This would imply a change in the control paradigm of the CBEC to align it with international best practices. As in developed administrations, cargo will need to be stopped primarily to address risks that bear on admissibility issues, such as security, hazardous goods, etc., of the type that require that the cargo needs to be stopped at the border. Ordinarily, there should be no stoppage of cargo for duty related issues that can be handled in a post-clearance environment. The cargo examinations should be targeted, designed primarily to confirm the declarations and with a much more thorough examination of selected cases which should form a much smaller percentage of total consignments (unlike the current situation where a large number of consignments get selected for examination but are subjected to 5 to 10 per cent examination). The facility for examination at the importer's warehouse should also be extended on a selective basis where the movement of cargo is adequately secured through means such as track and trace technologies. This will decongest ports and airports and enhance their cargo throughput, thus saving wastage of substantial resources.

But for this to happen there is need for tremendous investment into pre-arrival risk assessment and post-clearance compliance management. This necessitates that the CBEC puts in place a regime in which advance filing is the norm and ensures that the data quality of the declarations is of the requisite standards. TARC's consultations with stakeholders indicate that even though the legislative framework exists, error free advance filing is far from being a reality, leading to the necessity of amendments which are time consuming and which delay the process of clearance of goods from customs. One factor that was mentioned to the TARC was that in India the responsibility for filing import general manifest in advance was divided between the carrier and agents and the latter were allowed to file house level details, whereas internationally it was the carrier who bore the responsibility squarely. Without going into the specifics of the issue, which the CBEC is best placed to judge, TARC would only wish to emphasise that error free advance filing is a critical requirement for the success of pre-arrival risk assessment that will enable smooth passage of compliant cargo through the Indian port and airports. Hence, the CBEC needs to adopt measures that will ensure the creation of such an environment.

It needs no elaboration that a major focus of customs checks is revenue and there is a perception that relaxation of these checks would lead to loss of revenue. It is often argued that the compliance environment in India is very different from the advanced economies where such measured are adopted. It appears to be a misconception that advanced nations can afford these processes because

revenue is not a concern. As noted earlier, 70 per cent of the customs administrations surveyed by the WCO listed duty evasion as their key priority. As far as Europe is concerned, nothing is further from the truth. With VAT at 21 per cent, the risk of loss of revenue is often very high in some EU countries and this is managed through a very strong system of controls that are not applied only when goods arrive (as in traditional customs administrations) but across the entire breadth of the supply chain process. There is direct communication between customs and tax authorities and multiple syncs of transaction data. Besides, customs administrations of Western Europe have very sophisticated revenue accounting systems with very well developed internal controls. These systems take into account advance payments, deferred payments, transactional payments and guarantees of different types that may apply to different classes of clients or transactions. These systems provide for strong revenue oriented controls and that is the direction in which India must progress.

The argument that the compliance environment in India is unsuitable for processes similar to advanced economies also begs the question whether the current methods of control are able to effectively counter non-compliance in the form of under invoicing or over invoicing. Any objective analysis will return a negative answer. First, the general experience is that the extra revenue generated through enhancement of assessable values is marginal to the total revenue collection and generally does not exceed about one per cent of the total revenue. Secondly, this extra revenue does not necessarily represent the correct amount due. This is because importers often agree to pay the extra duty if the cost of delay in clearance due to demurrage etc. or the urgency of their requirement exceeds the additional duty demanded by customs, and not because the demand is legally sustainable. Thirdly, the poor success rates in appeals where importers choose to contest such assessments reflect poorly on the quality of customs orders in such cases. And lastly, such cases usually do not comprise more than 10 per cent of the total transactions scrutinised by officers. In substance, this would imply that a large number of transactions that are directed by the RMS to officers did not actually require their attention. To that extent there is wastage of resources for customs as well as importers, who suffer cost due to delays and unpredictability in clearance. While this underlines the need for sharper edge to risk management system, as mentioned in the previous section, it also highlights the necessity for customs to revisit rationale of the entire process.

It is equally important to bear in mind the fact that the current process, which is a gatekeeper type operation, gives rise to frequent opportunities for rent seeking behaviour on the part of errant officials creating a serious moral hazard for the organization. If proper analysis is done, it will show that the opportunity cost of using the bulk of resources in routine administrative tasks, when there are more important demands on resources, far outweighs the possible revenue loss.

If the compliance environment is perceived to be very adverse, the leaders of the customs administration need to ask themselves what they are doing about it. Quite apart from the fact that such perceptions are not based on any studies on compliance measurement, they can exert a positive influence on the compliance environment by improved governance and accountability, strategic interventions such as improved customer services, greater consistency, clarity and transparency in approach, and better targeted enforcement.

The other area of the core process that is acquiring greater importance is the clearance of express consignments. As has been mentioned earlier, the growth of e-commerce has led to increasing use of express cargo as also postal channels that deliver consignments directly to the customers. The CBEC had undertaken a project in a PPP mode with the Express Industry Council of India to automate this process. It is learnt that it has not been fully implemented yet. It is necessary that the implementation is completed at the earliest as the volumes in this category are bound to increase. There is an equal necessity to automate the postal clearance process. Globally, express clearance is now being seen as a sub-set of the customs clearance process. The automation of this should therefore also ensure that these different modes are brought within a common risk management framework. This will enable customs to meet genuine needs of industry as well.

Currently, the knowledge about different industry sectors, groups of commodities, etc., is acquired by appraising officers only in the course of their working. While some are good at picking it up, many others are quite indifferent. The practice of recruiting expert appraisers that was in vogue a couple of decades ago has been discontinued and later, even the direct recruitment of appraisers has been discontinued. This has resulted in drastic fall in the levels of knowledge and ability. Posited against the growing volumes and complexity of imports and exports, and the continuing expansion of ports, inland container depots, etc., the shortage of knowledge and skills leads to increasing thinning of its resources; this is a major challenge before the CBEC. It, therefore, needs a strategic response.

The TARC believes that the response should be for the CBEC to move towards the centres of excellence concept and use the potential of ICT to cope effectively with the challenge. Even a broad analysis will show that a few groups of commodities contribute a large share of customs revenue. Steps should be taken to ensure that officers develop deep knowledge and expertise in the relevant commodities and the task of compliance verification in relation to the relevant discipline is assigned to such teams, who will assume this responsibility across all customs locations instead of being limited to individual locations. In other words, the CBEC should move to a model of centralised processing for compliance verification. There are different options which could be considered and it does not necessarily mean that a single central facility has to be set up. Even the current ICT infrastructure, wherein all locations are networked, has the potential to enable this with appropriate legal and administrative changes. The commodity groups can be divided among the major custom houses and international air cargo complexes and highly trained teams with the requisite expertise assigned national responsibility for transaction-based compliance verification. The function of physical inspection and examination of cargo that requires the physical presence of officers will continue to be performed at the respective locations and will be driven by clear risk-related instructions.

This will lead to the following benefits:

- Consistent application of the required high-level knowledge and skills across the country
- Consistent performance and delivery standards for legitimate trade enhancing predictability and certainty in clearance

- Suppression of the tendency of aberrant traders to exploit the weak links in the customs set up
- Enhanced accountability and manageability for the CBEC contributing, among other things, to better integrity management

This will entail a number of other steps, such as changes in HR policies for nurturing specialisation, robust knowledge management systems, etc., that had been highlighted in the first report of the TARC. It will also necessitate the creation of a supporting legal and administrative framework.

An important requirement will be complete digitization of the entire process of clearance. This will require determined efforts to implement the system fully. The ICT system should be the sole channel of communication between customs and trade. Currently, there are areas where manual interventions are made even where the system has a provision for on line interaction[107]. Such deviations will have to be firmly eliminated.

This will also need a pronounced thrust on dematerialisation of paper documents and making them available to officers digitally wherever they are needed, coupled with a document management system that will free up a lot of space. Such solutions are widely available and a large number of organisations, in the private and public sectors, including banks and financial institutions, have implemented them. The directorates of systems and logistics will have to jointly work together to implement it on a nationwide basis in the CBEC.

The CBEC also needs to undertake periodic reviews of key business processes, in the spirit of continuous improvement, to simplify and streamline them and enhance their efficiency and effectiveness. Some of the difficulties expressed by stakeholders in the TARC's consultations related to the absence of such reviews and the lack of standardisation with different practice in matters such as bonds, bank guarantees etc. being followed in different regions. As recommended in Chapter VI TARC's first report, the CBEC needs to develop standard operating procedures and publish them in manuals covering all key areas. In Chapter III of that report, the TARC has also recommended the setting up of the Directorate of Business Excellence for continuous improvement.

If the primary mode of customs control has to shift from pre-clearance interdiction to post-clearance audit, substantial capacities need to be built in this area. If the unproductive pre-clearance interventions are minimised, sufficient resources can be generated for audit.

Typically, audit takes two forms – desk based scrutiny of identified transactions post-clearance, which happens in the office, and focused scrutiny of accounts and related business records, which happens in the business premises of the traders (described as on-site post-clearance audit, OSPCA).

[107] One such area which was mentioned to the TARC was in relation to replies to queries raised by officers. The TARC was given to understand that the practice followed was to first show the reply to appraising officers physically before and getting their clearance before submitting it into the system. This is a completely unnecessary physical interaction.

Both need to be risk based and based on sufficient knowledge of business and accounting practices on the part of officers.

It is also important to understand the proper role of scrutiny, whether pre- or post-clearance, of a transaction in the self-assessment paradigm. Rather than an act of assessment, it should be perceived as a method of risk treatment conducted either before or after the clearance of goods, depending on the typology and gravity of risk. It needs to be borne in mind that the post-clearance audit is as much an audit of the RMS as it is of the importer's compliance. It is therefore important that its results feed back into the RMS for improving its performance. As far TARC is aware this loop is missing and needs to be put into place.

One of the important functions assigned to auditors, when the desk based post-clearance audit programme was implemented, was the check on data quality. The instructions specifically required them to pay attention to this even if there were no other compliance issues and give a feedback to importers for improvements where necessary. The RMS has tools that help officers to monitor whether the importers comply with such advice or not. It is not known whether this is actually being done. In an environment in which information is the key lever of control, the effectiveness of customs control is critically dependent on the quality of the data in the declaration filed in its system and CBEC needs to actively focus on such interventions to ensure that deficiencies in data quality are made good and the data in its systems becomes highly reliable over time.

It is reported that there are large pendency of transactions selected for post-clearance audit in custom houses. This needs urgent attention. A major goal of risk management is to match work to available resources. Implicit in this is the principle that all transactions need not and should not be scrutinised. The CBEC also needs to examine both the quantity and quality of the selected for audit having regard to evaluation of risks and limit them to acceptable numbers so that compliance verification happens in a purposeful manner with a clear focus on addressing identified risks.

As far as OSPCA is concerned, it is entrusted to central excise officers. Apparently, very few audits have happened as yet. However, the stakeholder feedback indicates that officers sent for audit lack enough knowledge about customs issues. There is need to ensure that the officers are properly trained before they are assigned this task.

In the current set up, there is an absence of programme ownership and a very weak link between policy and implementation. In Chapter III of its first report, therefore, the TARC has recommended strengthening the functional vertical for audit and achieving an integral link between policy and delivery and that would be the first step towards capacity building. The ownership of the post-clearance audit programme needs to be clearly vested in this vertical. Further, as noted by the TARC in that report, specialised knowledge about key industries needs to be built and sustained within this function. With the shift of emphasis from transactional compliance to supply chain security, skills in the domain of systems audit and certification also need to be nurtured in the organisation.

There is also a need for capacity building in handling related party transactions. The significance of this can be gauged from the fact that according to a WTO estimate, they account for over 30 per cent of global international trade, and with the growth of multinational corporations, this will only increase. Currently, this issue is handled by the special valuation branches (SVB) of specified major custom houses. As the TARC noted in section VI.11 of the first report, the process is out of line with global practices and India is the only country that follows the "gatekeeper" approach. The process is far from satisfactory either from the importer's or the department's perspective. There are huge pendency in SVB cases and the quality of decisions also leaves much to be desired. Further, the requirement of the extra duty deposit (EDD) continues to be a major irritant to trade. It is reportedly being routinely increased from 1% to 5% at the slightest delay on the part of importers. On the other hand, customs are reportedly not discontinuing it (as they are required to do under extant instructions) when decisions are not taken within three months of the importers furnishing their responses. Stakeholders have mentioned to the TARC that the refunds of EDD, when cases are finally decided, are also beset with difficulties, as the process is not captured in the EDI system and the original documents are frequently lost in customs. As things stand, the EDD appears to serve little purpose and the CBEC needs to seriously consider dispensing with it.

Customs need to accept the principle of self-assessment in letter and spirit, to move to a risk-based approach in this regard and make post-clearance compliance verification the chosen mode of valuation control. The Directorate of Valuation, which is already notified as the nodal agency to control the SVB process, should be strengthened to play a more active role in such audits and should be converted into a centre of excellence in valuation by staffing it adequately and building strong valuation expertise. It is often assumed that the customs services of a country already possess the necessary capacity in this respect, usually because these services have a history or tradition of applying customs tariffs to imported goods. However, it is not a good policy to make assumptions about the capacity of a customs service without taking a good look at the actual state of affairs on the ground. In India, a survey conducted in 2004-05 as part of ARTNeT/RIS study on trade facilitation identified customs valuation as the key problem for the trading community.

In addition, it should take responsibility for actively providing detailed guidance to importers through lucid and clear publications that set out detailed guidelines relating to the valuation regime, including documentation requirements (as recommended in Section VI.10 of the first report), so that there is reduction in the opacity of the customs' approach and importers are better prepared to address issues in collaboration with customs. The practice statement No. B_IND 08 dated April 12, 2013 issued by the Australian Customs and Border Protection Service (ACBPS) is a good example of this practice[108]. In fact, such user friendly guidance is regularly issued by ACBPS relation to key issues in the area of valuation such as valuation of automobile imports[109], valuation

[108] http://www.customs.gov.au/webdata/resources/files/B_IND08Valuation-TransferPricingPolicy.pdf, accessed in September, 2014

[109] http://www.customs.gov.au/webdata/resources/files/ValuationImportedRoadVehicles.pdf, accessed in September, 2014

of free of charge goods,[110] etc. This is a practice followed by many customs administrations and CBEC will do well to emulate it.

There is also need for greater collaboration with transfer pricing authorities on the direct taxes side so that documentation requirements are harmonised to the extent possible.

Importers should also be enabled to make a *suo motu* declaration even during the validity of the SVB order where the factual matrix underlining the original decisions undergoes a material change.

One aspect that seems to have attracted little attention on the part of customs in relation to valuation is the aspect of countering trade based money laundering (TBML). And this is because of the predominantly transactional focus that the current control regime is characterised by.

TBML is being increasingly recognised as a major issue internationally and a number of studies show the growing threat to national economies it poses.[111] TBML is generally undertaken by mis-invoicing of goods imported into or exported from a particular country. Generally, goods are

a) undervalued as imports to send out money from the country
b) under-valued as exports to receive money into the country
c) over-invoiced as imports to receive money into the country and
d) under-invoiced as exports to send out money from the country

Such trade mis-invoicing has adverse effects not only from a money laundering perspective, it also helps traders avail of illicit tax incentives and by-pass capital controls. There are a number of indicators that can point to potential TBML risks. These include the following:

a) payments to a vendor made by unrelated third parties
b) payments to a vendor made via wire transfers from unrelated third parties
c) payments to a vendor made via checks, bank drafts, postal money orders or travellers checks from unrelated third parties
d) suspected or known use of shell companies and related accounts
e) unexplained, repetitive or unusual patterns of wire activity
f) false reporting such as commodity misclassification, commodity over-valuation or under-valuation

[110] http://www.customs.gov.au/webdata/resources/files/ValuationofFree-of-chargeGoodsApril2011.pdf, accessed in September, 2014

[111] Money Laundering Vulnerabilities of Free Trade Zone, Financial Action Task Force, 2010, APG Typology Report on Trade Based Money Laundering, Asia Pacific Group on Money Laundering, 2012

g) carousel transactions: the repeated importation and exportation of the same high-value commodity

h) commodities being traded not matching businesses involved

i) unusual shipping routes or transhipment points not making economic sense

j) packaging inconsistent with commodity or shipping method

k) double-invoicing

l) discrepancies between invoiced value of the commodity and the fair market value

m) payment for goods either in excess or below known market value

n) size of the shipment inconsistent with the average volume of business

Studies have also shown that areas like duty remission schemes, free trade zones, etc., are particularly vulnerable to this abuse.

Because of its predominant revenue orientation, customs tend to focus primarily on undervaluation of imports to prevent revenue leakage, and overvaluation of exports to prevent unlawful availing of export benefits. Again, because of their transaction oriented focus, they often miss the indicators of potential fraud, which can only be discerned with pattern analysis and integration of customs data with data from the financial flows around the concerned business entities. Countering such frauds will require very close and active co-operation, and ongoing information exchange between customs, the FIU, the Enforcement Directorate and the Reserve Bank of India. The DRI and RMD need to be tasked for this purpose.

VIII.4.f Passenger processing

With the adoption of liberalised green channel, the airports are one area in which the CBEC has won universal acclaim. However, as the continuing seizures of contraband show, airports continue to be vulnerable to smuggling and movement of undesirable persons across the border and a strong ICT based risk management system needs to be put in place. The Advance Passenger Information System (APIS) was conceived by the CBEC for meeting this need, to be executed in close cooperation with the Bureau of Immigration (BoI). However, it has not made much progress as it is learnt that the required data sharing between the customs and BoI is yet to be put on a firm footing. The CBEC also does not seem to have placed adequate human resources at the disposal of the Directorate of Systems to enable development of the system. It is in the national interest that the APIS is developed and deployed as early as possible in active cooperation with the BoI. The system should be based on advanced technologies, such as entity analytics and identity management which are constantly improving the ability of border agencies to identify high risk passengers. The government needs to ensure that like many inter-agency issues, this too does not become a victim of absence of healthy collaboration and co-ordination.

VIII.4.g Customs role in trade facilitation and co-ordinated border management

The objective of trade facilitation is simplifying, rationalising, modernising and harmonising trade procedures with a view to

- expediting release and clearance of goods under import, export and transit
- reducing transaction cost and
- bringing greater transparency and predictability to traders

With the lowering of tariffs, removal of QRs and the recognition of the benefits of international trade to national economies, the focus of customs administration has shifted to trade facilitation. The role of trade facilitation in the competitive ability of nations to attract foreign investment has been widely acknowledged and given traction by World Bank publications like "Ease of Doing Business" and Logistics Performance Index.

While discussing trade facilitation, a few key issues need to be kept in mind. First, the discipline of trade facilitation is not limited merely to the border procedures but encompasses the wider regulatory environment of a country. Although customs are the most prominent agency at the border, it is not their actions alone that impact on trade facilitation, which gets affected by the actions of a large number of other agencies who are tasked with regulation in the areas such as standards, environmental issues, public safety etc. And the increase in growth and complexity of such regulation is a factor that any policy on trade facilitation has to take into account.

Even within customs, the complexity of law and procedures has a direct impact on the administration's ability to facilitate legitimate trade. For example, although the range duty rates is said to have been considerably reduced as measure of customs reform, in actual practice there is still a large number of effective rates through exemption notifications. Further complication is added when such notifications are based on a variety of factors such as end use conditions, composition of goods etc. which lead to disputes relating to classification etc. necessitating frequent interface with customs officers and bringing in discretionary element in the decisions. While tax policy *per se* is outside the mandate of TARC, this is being stated to underline the fact that such policy reform is also an essential ingredient in the trade facilitation initiatives of an administration.

There is nevertheless considerable scope for the CBEC to improve its governance and simplify and streamline processes and procedures within these constraints and that ought to be a key priority for it. Even though the agreement on trade facilitation (TFA) being negotiated under the WTO and endorsed at Bali in December, 2013 is still some way from coming into effect, customs and other agencies need to be prepared for its implementation. Besides, there are strong autonomous drivers that necessitate according a very high level of importance to trade facilitation.

The TFA contains about thirty-five multilateral disciplines that would help improve the border trade procedures involved in import, export and transit of goods, and bring further transparency in trade administration. These disciplines include, inter alia, publication of relevant trade-related

information such as laws, rules and procedures; review and simplification of formalities and documentation; special facilitation for perishable goods; system of administrative appeals and review; pre-arrival processing of import documents; application of risk management for customs controls etc. The TFA will have to be implemented mainly by customs. Some of the provisions will also be implemented by some other agencies involved in the release and clearance goods at international borders such as plant quarantine, port authorities, the Drug Controller, the Food Safety and Standards Authority of India (FSSAI), etc.

It also needs to be stated that trade facilitation and enforcement need not necessarily be seen as competing or conflicting considerations. Improved governance, some aspects of which have been touched earlier in this chapter, contributes to improved facilitation which in turn contributes to improved compliance. And that is also the object of effective enforcement. Facilitation and enforcement therefore need to be seen as complementary, rather than conflicting, considerations. Programmes like the AEO programme, which is discussed later in this chapter, are a key element in the strategy for improving overall compliance and much greater focus needs to be put in making them successful so that resources can be devoted to areas where sharper enforcement is needed.

One of the issues repeatedly highlighted in the TARC's consultations with stakeholders was that there is no identified programme ownership for trade facilitation and often, the facilitation under the RMS is impeded by a high level of interventions driven by pressures of revenue targets etc. It was mentioned that facilitation, which used to be as high as 70-85 per cent of the total clearances, has dwindled to around 40 per cent. It is indeed a pity that the CBEC, which vide its circular dated September 2, 2011, had issued instructions to fix facilitation targets as 80 per cent, 70 per cent and 60 per cent for ICD sectors to be achieved within six months of that instruction, has allowed this regression to happen. This clearly highlights the absence of a sense of ownership on the part of the CBEC.

The other difficulty mentioned was in relation to ACP clients who had received show cause notices from customs. It was reported that as a result of these notices, in many cases, the accreditation was withdrawn leading to loss of facilitation for clients who were otherwise compliant. It is well known that a "show cause notice" culture has unfortunately developed in the department in the last many years. We have dealt with the deleterious effects of ill-considered and avoidable litigation and disputes in Chapter V of the TARC's first report. As things stand, there would hardly be a significant business in India which is not a recipient of a tax demand or notice from either customs or excise departments. Many such notices are questionable and turn on questions of interpretation rather than being cases of evasion meriting penal action. The CBEC needs to take a robust and pragmatic view in such cases and not deny facilitation in a wooden manner where there is no reason to suspect deliberate intent at fraud or evasion.

In Chapter II of its first report, the TARC had recommended the setting up of a separate functional vertical for taxpayer services with a clear customer focus. The facilitation programme of customs should be located in this function and should be driven centrally in a cohesive manner. A national trade facilitation committee, with adequate stakeholder representation, should be set up and empowered to review the facilitation performance of customs and suggest measures for

improvement. This will in any case become a binding requirement as and when the trade facilitation agreement comes into force. Local trade facilitation committees should continue to deal with and resolve local issues.

CBEC also needs to deepen and widen direct engagement with the industry both to communicate the benefits of its programmes in the area of facilitation and to gain better understanding of their needs and concerns. Typically, it is the agents who interact with customs on behalf of their clients in the industry. Often their own interests are in conflict with initiatives to simply processes and the message that the CBEC wishes to communicate to the industry does not get properly conveyed. There is a need to bridge this gap and promote greater involvement of senior leadership of businesses in the reform process and facilitation programme. While the onus is also the business leadership to participate in such engagement, which currently is very unsatisfactory, CBEC can take proactive steps by launching outreach programmes with the cooperation of industry bodies, giving wide publicity to its schemes, generally intensifying its communication efforts and creating institutional mechanisms for greater private sector participation. The facilitation committees if used purposefully will be an important element in this effort.

There is equally a need to improve visibility and transparency in the reporting of performance in the area of facilitation. Time release studies (TRS) is an important tool in this regard. There was earlier a practice to measure dwell time of cargo and it is not known if it continues. However, the data was limited to customs processing and was never published; it was used by officers internally to track performance and effect improvement. Its use depended upon how much interest the local commissioner took in such issues.

It is desirable that the CBEC follows the international best practice by undertaking TRS and publishing the results. A number of customs administrations, such as those in Australia and Japan, now regularly undertake TRSs and publish their results.

TRS is a comprehensive tool for and method of measuring the actual time required from arrival of goods to its release including in its ambit not only customs clearances but also clearances from other border agencies. There are detailed WCO guidelines available to conduct these studies that can be adopted. TRS will have a number of benefits including process diagnosis, benchmarking and performance improvement besides enhancing the transparency of the entire gamut of border operations.

Dwell time studies of the CBEC involve making use of the time stamp available in the EDI system and using it to calculate the time taken for release. However, no other government agencies (OGAs) or the trading community are involved in the study. The EDI system has time stamps for all activities relating to imports from the time of arrival of the goods to their release in the system. The entire time period when the goods arrive till they leave the customs area can be taken from the system. However, to conduct a comprehensive TRS, time stamps from the EDI system as well as detailed reasons for delay at any stage and feedback would be required from the OGAs, CHAs, assessing/shed officers, etc. This can be done by circulating a detailed questionnaire to ascertain

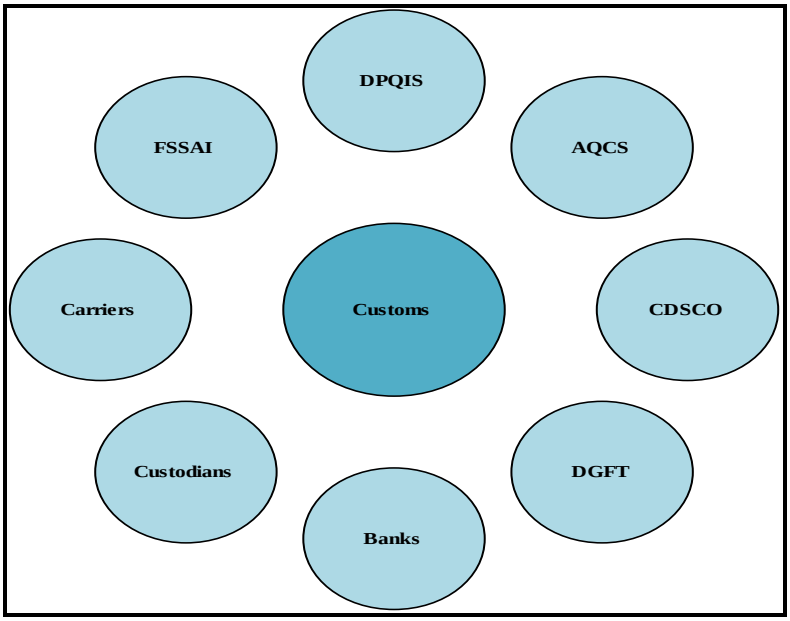
reasons for the delay for selected consignments. Various local factors can also have an impact on the time taken. Thus, there could be different reasons for delays at different customs stations.

The TRS published by the Australian Customs from 2007[112] are a good example of the best practice in this area. The CBEC should immediately put in place a mechanism for conducting such studies on a one or two-yearly basis.

VIII.4.h Co-ordinated border management and single window

Customs can bring about substantial reduction in customs clearance times by improving risk management, reducing pre-clearance interventions and shifting their control paradigm to a predominantly post-clearance environment. However, customs are not the only players in the area of border management and customs facilitation alone is not enough. There are several statutes administered by OGAs to regulate the type and quality of goods entering the country. Typically, these statutes cover areas relating to food safety, environment, hazardous goods, plant and animal quarantine, dual use goods, quality standards, etc. These statutes are the responsibility of different regulatory agencies, each of which has a different mandate with regard to goods and people crossing the borders. At present, these agencies work independently, with their own statutes, procedures and staffing, without regard to the consequences of multiple interventions on the same goods at the borders. The result is delays at the borders and increased transaction costs to trade, making it uncompetitive. Diagram 8.4 gives a sense of the complexity of the border eco-system.

Diagram 8.4: Border eco-system



The OGAs follow the general disciplines of WTO while imposing regulatory requirements. However, unlike customs, their focus is not so much on simplification and modernisation of the procedures and systems adopted by them. Besides, while customs administrations have access and

[112] http://www.customs.gov.au/site/page6067.asp, accessed in September, 2014

assistance from multilateral organisations such as the World Customs Organization (WCO), the OGAs do not majorly benefit from international guidance. In its Border Management Modernization Handbook, the World Bank notes that "in contrast to customs agencies that are linked into the WCO, most of these (other government) agencies are not connected through an intergovernmental body that acts as a focal point for the development of international instruments and the sharing of good practice approaches."

The problems associated with the functioning of multiple agencies at the borders in a un-co-ordinated manner include

- repeated inspection of goods by different agencies
- excessive document submission requirements
- non-transparent rules and procedures and
- separate infrastructure for these agencies and the consequent costs

A high degree of co-ordination is needed to reduce and eliminate the delays and costs associated with uncoordinated working. The co-ordination needs to be improved both vertically, i.e., between the central ministry/HQ and the field agency for each OGA (e.g., between the Ministry of Agriculture and Plant Quarantine) and horizontally, i.e., between customs and the OGAs. The vertical aspect is relevant in evolving processes and systems that facilitate compliance with OGA laws, including improvement in the transparency of the functioning of the OGAs and introducing modern concepts such as automation, risk management and cross-border mutual recognition in the working of these agencies. Considering that customs are the first point of contact and follow procedures that are internationally aligned with the Revised Kyoto Conventions, it is necessary that they are involved in the dialogues at the inter-ministry/HQ level. The horizontal aspect is relevant since customs, being the most visible agency at the border and the agency that gives the final clearance to cargo, taking into account the clearances given by other agencies, is best placed to co-ordinate among the OGAs.

Customs also need to build capacity in terms of greater understanding of the regulatory requirements of OGAs bearing on import and export of goods. This is particularly important in respect of requirements of agencies which are not present at the border. Examples are agencies such as the Bureau of Indian standards, Ministry of Environment etc. This is important as absence of such understanding on the part of customs officers can lead both to unnecessary references to such bodies leading to avoidable delays on the one hand and weak enforcement on the other.

Some of the steps already taken to improve co-ordination are implementation of an electronic message exchange system (ICEGATE), setting up of integrated check posts where all the OGAs sit under one roof to discharge their functions and organising interactive sessions between regulatory agencies and trade to educate trade on the regulatory requirements and to provide feedback from regulators on issues affecting trade.

To further improve the efficiency of functioning of OGAs as well as the co-ordination amongst them, it is necessary that the OGAs are persuaded to develop a risk management approach to testing and certifying consignments. In fact, interventions should be based on an integrated risk management framework which addresses the concerns of all border agencies. Customs can take the lead to develop such a system. The OGAs should also be part of the Trade Facilitation Committees set up in each commissionerate and attend meetings regularly to interact with trade.

Co-ordinated border management would lead to:

- efficient delivery of services at the border by reducing redundancies and resolving contradictions
- ensure better use of resources, including human and ICT
- better risk management
- faster clearance times and
- reduce the need for elaborate border infrastructure for each agency

In their interaction with TARC, many stakeholders pointed to the lack of adequate capacity, in terms of lack of adequate staffing and lack of automation in some of the OGAs. It was mentioned that the concerned officials were not available at the port/airport and often a single office catered to multiple locations, necessitating the importers/exporters having to travel long distances. This was mentioned as a major contributor to delays. The fact that most of the processes were paper based, and processes had little emphasis on facilitation, was mentioned as another irritant. This underlines the necessity of capacity building in the OGAs as well concurrently with that in customs.

The Finance Minister had announced implementation of the Indian Customs Single Window Project in his budget speech 2014. The enhanced co-ordination among OGAs with customs acting as the lead co-ordinating agency is a step towards supporting single window development, leading to improved border management at an operational level.

It needs to be realised, however, that the creation of a single window is long process requiring willing and committed collaboration between different government agencies as also between government and business. Typically, and this can be said to be particularly true of India, government agencies operate in silos and turf issues bedevil efforts at collaboration across organisational boundaries. Besides, a single window needs to be created in a heterogeneous environment in which different agencies operate at different levels of automation and follow processes that are not necessarily aligned with others. Hence, a ‘one size fits all’ solution is unlikely to meet the requirement and different approaches may need to be adopted in respect of different agencies. Hence, implementation of the concept will necessarily involve long periods of study, planning and phased implementation. The DG (Systems) and the other agencies will need dedicated project teams of adequate size, which need to see the project through and remain stable

through the implementation. And they cannot succeed unless there is a clear administrative, legal and political mandate to the project.

The benefits of a single window facility cannot be fully realised if the effort is not accompanied by process re-engineering of the back-end processes in each of the participating agencies. If the full benefits of trade facilitation are to be fully realised, all must commit to delivery of services against defined and published service standards and operate within a coherent and consistent facilitation and risk management framework, co-ordinated by the lead agency, which in this case is customs.

For a single window facility to become a reality, therefore, the necessary legal and administrative framework enabling and empowering customs to play an effective co-ordinating and facilitating role needs to be put in place. While the CBEC needs to build capacity for leading the effort by putting adequate skilled resources dedicated to this task and strengthening the directorate of systems, the action for legal and administrative empowerment and enablement lies at a higher governmental level and needs to be taken expeditiously.

VIII.4.i Cross-border co-ordination in border management

The manner of improving co-ordination among the border agencies is one dimension of the issue. The other dimension is the need for co-ordination with the border agencies of neighbouring countries at land borders to eliminate or at least reduce duplication of processes/procedures by sharing information. This co-ordination between border agencies across borders can be more meaningful if there is a high degree of inter-agency co-ordination behind the borders.

The General Annex of the Revised Kyoto Convention, to which India is a party, recommends joint controls. The transitional standard 3.4 calls upon contracting parties to operate joint customs controls at border crossings, and standard 3.5 calls upon parties to plan for juxtaposed customs control at new border crossings.

Such cross-border co-ordination in border management will reduce the time and costs involved in inspection and clearance of cargo at land borders and will also cut down on investments needed borders to develop land customs stations on both sides of the border.

An issue to be addressed in the case of joint control is the legal mandate for the customs administration of India to operate and discharge its official functions on the territory of another country (the provisions of Customs Act, 1962, extend to the whole of India). To start with, the joint customs controls could be operationalised at locations in India where India is developing integrated check posts (ICPs) with considerable investment. The customs of a neighbouring country could function from an earmarked area of the ICP. This would lead to better co-ordination on operational issues between the two customs administrations and lead to better utilisation of resources.

Pending this development, there should be an institutionalised system of holding border meetings between neighbouring countries. The operational issues that arise at land customs stations could

be discussed and resolved, if there is better access and communication between the customs officials of both sides, including through face-to-face meetings.

At present, having such a meeting would involve a laborious process of preparation as it would require passport, visa as well as all approvals associated with foreign travel. This, in turn, would mean that whole process/preparation will have to commence sufficiently in advance, which detracts from the regular usage of this mechanism and rules out its use to resolve an emergency.

The CBEC may consider putting in place a system (after inter-ministerial consultation) proposing movement of designated customs officers between the land custom stations/integrated check posts in India and neighbouring countries to hold border meetings to help in expeditious resolution of operational and day-to-day issues.

Such a facility may be limited to identified officers (led by customs and consisting of relevant OGAs) and their movement limited only up to the LCS/ICP in the territory of the other country for a duration of not more than 3 hours. Prior intimation of the details of officers being issued the Single Entry Permits (SEP) for the first time should be given to immigration/security agencies.

This mechanism, if instituted and used regularly, would promote better co-ordination at the borders and would build the confidence needed to operationalise a more advanced form of joint control in the future.

VIII.4.j SAFE framework of standards

The terrorist events occurring in the United States on September 11, 2001, and terrorist threats across many regions have brought the issue of the security of international transport and supply chains into sharp focus. The World Customs Organization (WCO) acted by organising and convening a series of joint customs and business task force meetings aimed at responding to the terrorist challenge. Based on recommendations of the Task Force, the WCO Council, at its 2005 session, adopted the SAFE Framework of Standards to Secure and Facilitate Global trade (SAFE FoS). A vast majority of member administrations, including India, have since expressed the intention of beginning the process of implementing the SAFE Framework provisions.

Like the Customs Trade Partnership against Terror (CT-PAT) implemented by the US and Canada, the SAFE Framework is a minimum set of standards to be implemented at various stages in accordance with each administration's capacity and legislative authority. Further, capacity building is the key to globalising customs standards on security and facilitation. The WCO has devised a comprehensive capacity building initiative called the Columbus Program to assist countries with the SAFE Framework implementation. It includes diagnostic missions to assess a country's ability to implement the SAFE Framework, developing and supporting national business cases and action plans for large scale capacity building, partnering with donor governments and trade to influence and support customs development, conducting regional workshops in advance of diagnostics and co-ordinating WCO donor member projects.

SAFE FoS is developed on the following four core principles/elements.

- The commitment to harmonise the advance electronic cargo information requirement on inbound, outbound and transit shipments
- The application of a consistent risk management approach to address security threats
- The preferable use of non-intrusive detection equipment to effect customs examinations of high-risk containers and cargo
- The provision of benefits to businesses that meet minimum supply chain security standards and best practices

The intended outcomes of the SAFE Framework are the following.

- Establishment of standards that provide supply chain security and facilitation to goods being traded internationally.
- Enablement of integrated supply chain management for goods moving by all modes of transport.
- Enhancement of the capabilities of customs administrations to meet the challenges and opportunities of the 21st century.
- Strengthening networking arrangements between customs administrations to improve their capability to detect high-risk consignments.
- Promotion of co-operation between the customs and business communities.
- Facilitation the movement of goods through secure international trade supply chains.

The WCO Framework rests on the twin pillars of customs-to-customs network and customs-to-business partnership as delineated below.

a) **Customs-to-Customs network with eleven standards:**

i. **Integrated Supply Chain Management** - Customs administration should follow integrated customs control procedures as outlined in the WCO Customs Guidelines on Integrated Supply Chain Management (ISCM Guidelines).

ii. **Cargo Inspection Authority** – Customs administrations should have the authority to inspect cargo originating, exiting, transiting (including remaining on board), or being transhipped through a country.

iii. **Modern Technology in Inspection Equipment** – Non-intrusive inspection (NII) equipment and radiation detection equipment should be available and used for conducting inspections, where available and in accordance with risk assessment. This equipment is necessary to inspect high-risk containers or cargo quickly, without disrupting the flow of legitimate trade.

iv. **Risk-Management Systems** – Customs administrations should establish a risk-management system to identify potentially high-risk shipments and automate that system.

The system should include a mechanism for validating threat assessments and targeting decisions and identifying best practices.

v. **High-risk Cargo or Container identification** – High-risk cargo and container shipments are those for which there is inadequate information to deem shipments as low-risk, or which tactical intelligence indicates as high-risk, or which a risk-scoring assessment methodology based on security-related data elements identifies as high-risk.

vi. **Advance Electronic Information** – Customs administrations should require advance electronic information on cargo and container shipments in time for adequate risk assessment to take place.

vii. **Targeting and Communication** – Customs administrations should provide for joint targeting and screening, the use of standardised sets of targeting criteria, and compatible communication and/or information exchange mechanisms; these elements will assist in the future development of a system of mutual recognition of controls.

viii. **Performance Measures** – Customs administration should maintain statistical reports that contain performance measures including, but not limited to, the number of shipments reviewed, the subset of high-risk shipments, examinations of high-risk shipments conducted, examinations of high-risk shipments by NII technology, examinations of high-risk shipments by NII and physical means, examinations of high-risk shipments by physical means only, customs clearance time and positive and negative results.

ix. **Security Assessments** – Customs administrations should work with other competent authorities to conduct security assessments involving the movement of goods in the international supply chain and to commit to resolving identified gaps expeditiously.

x. **Employee Integrity** – Customs administrations and other competent authorities should be encouraged to conduct programmes to prevent lapses in employee integrity and to identify and combat breaches in integrity.

xi. **Outbound Security Inspections** – Customs administrations should conduct outbound security inspection of high-risk containers and cargo at the reasonable request of the importing country.

b) **Custom-to-Business partnerships consisting of six standards:**

i. **Partnership** – AEOs involved in the international trade supply chain will engage in a self-assessment process measured against pre-determined security standards and best practices to ensure that their internal policies and procedures provide adequate safeguards against the compromise of their shipments and containers until they are released from customs control at destination.

ii. **Security** – AEOs will incorporate pre-determined security best practices into their existing business practices.

iii. **Authorisation** – Customs administrations, together with representatives from the trading community, will design validation processes or quality accreditation procedures that offer incentives to businesses through their status as AEOs.

iv. **Technology** – All parties will maintain cargo and container integrity by facilitating the use of modern technology.

v. **Communication** – Customs administrations will regularly update customs-business partnership programmes to promote minimum security standards and supply chain security best practices.

vi. **Facilitation** – Customs administrations will work co-operatively with AEOs to maximise security and facilitation of the international trade supply chain originating in or moving through its customs territory.

Since India has signified it intention to implement the framework, and indeed has taken many steps in that direction, CBEC needs to undertake measures for implementation in a sound programme management framework.

VIII.4.k Authorised Economic Operator (AEO) Programme

One of the key elements of the customs to business partnership component of the SAFE Framework of Standards is the authorised economic operator (AEO) programme. At present, more than 50 countries, including India, have operational AEO programmes. Under the SAFE Framework, mutual recognition of AEOs is a broad concept whereby an authorisation granted by one customs administration is recognised and accepted by another customs administration. The objective of mutual recognition of AEOs is that one customs administration recognises the validation findings and AEO authorisations issued by another customs administration under its programme and agrees to provide substantial, comparable and – where possible – reciprocal benefits/facilitation to the mutually recognised AEOs.

The international trade supply chain has become extremely complicated and vulnerable to external terrorist threats in the post-9/11 scenario. It led to an urgent need to have a system that ensures end-to-end supply chain security while ensuring faster release of goods. With this objective in mind, the AEO Programme has been conceived by the WCO to standardise the procedure under the SAFE framework of standards and globally, many customs administrations, including India, have adopted it.

The Indian AEO Programme is available to all operators in the supply chain, such as importers, exporters, logistics service providers, customs brokers, warehouse owners, etc. Further, there is no monetary or any other threshold limit for eligibility under the programme, which enables any player in the global supply chain, including SMEs, to apply for certification. The pilot project was started in August 2011 and, after evaluation of the pilot, the programme was launched through the CBEC's circular F.No.450/179/2009-Cus. IV.(Pt) (Circular No. 28 of 2012) dated November 16, 2012. This circular spells out the benefits of the programme for different categories of AEOs and the respective eligibilities.

The AEO programme is an effective 'customs-to-business' partnership tool to achieve the common objective of securing the supply chain. Under the programme, approved economic operators are given preferential treatment in terms of faster clearance and less physical examination of goods along with many other benefits subject to their conforming to prescribed security standards and compliance with tax laws.

Once the AEO matures and is firmly in place, the next logical step is the mutual recognition agreement (MRA) with other customs administrations for mutual recognition of AEOs. Under the MRA, foreign customs administrations will believe the Indian AEO and vice-a-versa and allow hassle free clearance of goods without inspection. The AEO scheme is actually a step towards MRA and may finally lead to Globally Networked Customs (GNC), streamlining information exchanges between customs administrations and reducing transaction costs by dispensing with the need to submit the same information to multiple administrations and also considerably mitigating the risk of fraud.

However, the programme does not seem to have gained much traction. As of now, a total of nine companies are AEO certified, which includes importers, exporters, customs brokers, warehouse keepers, custodians and logistic service providers. It is reported that only one MRA has been entered into, which is with Hong Kong. This is in sharp contrast to the global trend. Europe is reported to have 14,000 AEOs, with half of them being in Germany and Netherlands. China is said to have over 2000 AEOs. A small nation such as Uruguay is reported to have 10 MRAs in place and seven more are to be launched soon. Uganda has 10 certified AEOs and 42 applications are in process.

It is clearly in the CBEC's interest to promote this programme which is a very important vehicle for promotion of voluntary compliance and enhanced sharing of risks and responsibilities with compliant business. The more is the number of AEOs the greater would be the contribution of the AEO programme to the improvement of overall security and compliance environment. At present it does not appear to be sufficiently invested in the programme. Currently, only an Additional Director General in the Directorate of Inspection is in charge of it and he does not have much support. Clearly the programme needs to be put on more robust foundations by assigning dedicated resources. As recommended earlier this is one of the key programmes that need to be implemented by the CBEC in the programme management mode.

There is also inadequate communication of the benefits of the programme among potential candidates that would be eligible for it. The level of awareness is fairly low. The CBEC needs to appreciate that it has to establish direct communication with such firms as programmes of this nature are often in conflict with the interests of agents who mediate between customs and importers/exporters. Of course, compliant agents themselves are also eligible for these benefits. More needs to be done by the CBEC to induce them to join the programme.

There is certainly a huge scope for expansion of the programme as can be seen from the data relating to just one, albeit the most important, segment of the players in the supply chain, namely

the importers. Table 8.7 shows the contribution of top importers to the total revenue collection of customs during the last three financial years.

Table 8.7: Distribution of importers on revenue basis

Commodities	Importer Category	No. of Importers in Financial Year		
		2011-2012	2012-2013	2013-2014
Non-POL Commodities	Top 25% Revenue Contributing Importers	64	58	53
	Top 50% Revenue Contributing Importers	394	337	333
	Top 90% Revenue Contributing Importers	10980	9958	9661
POL Commodities	Top 25% Revenue Contributing Importers	2	5	4
	Top 50% Revenue Contributing Importers	8	13	14
	Top 90% Revenue Contributing Importers	75	116	123

As can be seen, true to the Pareto principle, most of the revenue yield is from a small number of importers. The analysis can be further refined by adding other parameters like value of imports, number of consignments etc. The players in the SME sector also need to be identified as it is important to make the programme broad based. Based on such analysis, not only in respect of importers by also the other key players, the CBEC can identify the target population for the AEO programme and actively market it.

Considering the low participation, the bouquet of benefits under the programme clearly does not seem to have been attractive enough. The CBEC needs to carefully reassess the value of the facilitation it extends under the programme and it should do so in consultation with stakeholders

in trade and industry. The benefits do seem to be marginal and oriented largely towards procedural relaxations.

There is therefore a need for the CBEC to revisit the programme and reconfigure it in such a manner as to make it attractive to prospective applicants.

While doing so the following suggestions may be considered:

- It is time to weave the earlier ACP and the AEO programme into a common AEO programme. There seems little logic to run two separate programmes based on accreditation.
- Since the AEO programme has wider coverage over the supply chain participants, CBEC needs to carefully assess the different needs of the different participants and offer benefits that make the programme attractive to them
- The programme design does not need to adopt a binary approach. This is because a differentiated approach is necessary depending upon the different maturity levels of the supply chain participants based on an assessment of their capacity and commitment to compliance. There needs to be a regime that caters to such different situations and creates incentives for progress towards greater levels of maturity in compliance. The benefits available in a fully secure supply chain, in which all players are fully compliant AEOs have obviously to be different from the situations in which only a part of the chain is secure. The CBEC needs to think creatively to evolve such a regime, adopting what might be called a "stairway" approach, which provides enhancing facilitation benefits as clients climb the steps on the ladder of compliance. And it needs to generate internal capacity to effectively manage the programme.
- For successful implementation of the AEO programme, a critical requirement for the CBEC will be to rid itself of the disputatious attitude on the part of its officers where there are differences of perception or where there are unintentional errors. As was observed earlier, this has been mentioned to the TARC by many stakeholders as a major impediment against the success of the Accredited Clients Programme. The approach needs to be made more collaborative and partnership oriented, particularly towards clients in such programmes.
- Earlier in this report, the TARC has recommended that the CBEC, in a calibrated manner, make a fundamental shift in its control paradigm away from one rooted in the transactional approach and towards the global standards of delinking release from duty payment, return-based cargo accounting system and periodic duty payment etc. For the most compliant clients, the CBEC can consider fully automated release, based on risk assessment. The TARC believes that the AEO programme can provide a good anchor for starting the movement towards such capacity building and reform. It will prove a win-win situation for both the CBEC and industry and attract larger participation.

- In Chapter III of the TARC's first report, in relation to the large business segment, it has recommended the global best practice of adopting an account management type approach in the form of a relationship manager for each large client. This is the global trend among evolved customs administrations and needs to be adopted by the CBEC as well in the AEO programme. Each AEO should have an assigned relationship manager who, on the one hand, will be the CBEC's face towards the client and will carry, on the clients' behalf, the "voice of the customer" to the CBEC.
- The CBEC is also needs to build capacity, with third party partnerships if necessary, to assess and monitor the continuing compliance of the AEOs with the specified standards. It needs, as stated earlier, to adopt a programme management approach and conduct periodical evaluations of the programme on an ongoing basis so that best results can be obtained.
- Far greater thrust needs to be given for entering into MRAs with other customs administration for it is the MRAs that will give strong impetus to the AEO programme.

VIII.4.l Harnessing ICT and other technologies

It would be stating the obvious to say that the CBEC cannot achieve the vision of transforming itself into an organisation that is comparable to "best in class" without effectively harnessing the potential of technology, for technology alone can enable the organisational and procedural shifts that are needed. The CBEC needs to build capacities in relation to this along two key tracks. The first is the application of technology to continuously improve its policy as well as operations in all dimensions. The second is to gain a deeper understanding of how evolving technologies are shaping the global social, economic, trade and business landscape, adopt strategies proactively to deal with the changes that affect its mandate and exploit opportunities that emerge.

In Chapter VII of its first report, the TARC has discussed in detail the application of ICT in customs and has given a number of recommendations. As noted there, while the CBEC has been among the leaders in the country in ICT applications, it still has a long road ahead to traverse. As the TARC recommended in Chapter VII, the transformation that is desired cannot happen unless ICT permeates the core of the organisation and the CBEC shifts completely to the digital platform. The shift away from a predominantly transaction control paradigm, the strategic use of risk management and data and information based control (as opposed to the physical control) require a far deeper integration of technology with not only the CBEC's operations but also with its thinking. As already observed, technology has to get into the DNA of the organisation.

While the workhorse of customs, the ICES and its associated systems, namely the RMS and ICEGATE, has stood the CBEC in good stead, the time has come to replace them with an integrated next generation system that can meet the future needs of the CBEC and help it move towards the "digital by default" status. Considering the long time the development of such a system will necessarily take, the work on its design must start now.

For developing future customs systems, global trends will have to be kept in mind and systems designed to ensure

- interoperability of customs and other agencies involved in border management
- a fully distributed, open, wireless and mobile operational environment, and
- solutions for structured and unstructured data

The solution must dramatically increase the ability of customs administrations and other entities to work together and facilitate seamless operations across organisational and other boundaries. It should enhance the customs' ability to gain access to transaction data across the whole value chain by mean such as data exchange with other tax or regulatory agencies as well as other customs administrations. In an environment of maximum pre-arrival risk assessment and clearance of goods, this will be essential for robust fraud control.

Interoperability will need to be achieved through the global adoption of standards for transaction data capture and control, the extensive use of service oriented architectures (SOAs) and new models of IT governance.

The other major technology trend that is rapidly emerging is the "internet of things" (IOT). Although it is early days yet to say how it will transform business and regulation, by virtue of the fact that its application is very prominent in the logistics industry, it has implications for customs control. In essence, the internet of things comprises a variety of devices and sensors exchanging data with each other. IOT depends on uniquely identifiable objects (packages, containers, officers, trucks, vessels). The objects represent themselves electronically to sensors (cameras, weigh-bridges, electronic gates, RFID readers, motion sensors, mobile and GPS recording devices, etc.,) and can be represented as data points for use in software applications.

Customs is moving gradually towards the management of the "integrated supply chain". This concept was developed in response to the demand for a comprehensive strategy on supply chain security and has been incorporated into practices followed by customs the world over. The control procedures incorporated by customs included advance electronic submission to customs of data from the exporter and by the carrier for security risk assessment purposes. Further, integrated customs control procedures were to involve cross-border co-operation between customs administrations on risk assessment and customs controls.

Simultaneously, business enterprises have invested in supply-chain visibility solutions that are largely about demand and inventory visibility and optimising actions in distribution and replenishment of merchandise with a view to achieving low inventory carrying costs. The private sector has invested in collaborative processes that span across a number of logistics and trade parties in the supply chain.

Location data in a customs information system is currently largely viewed or used as strings of text or codes which appear on computer screens. Location information such as country, region,

country sub-division, facility/location and address of parties are potentially used as risk indicators in risk management systems.

Owing to the development of standards by ISO Technical Committee 211 on geospatial standards and subsequent availability of technical tools, a large part of which is available as open source software, it is now possible to visualise and use location information on interactive maps. Without making any change to the data requirements from trade, each existing piece of information on location in customs IT systems can be supplemented with their geospatial equivalents through a set of processes on a one-time basis. This process enables the following applications:

a) Tracking consignments in transit through tracking devices that run on geo-positioning systems (GPS). In-transit trucks that deviate from their normal route and schedule can be actioned for control purposes. A number of pilots and operational systems are already using this methodology.

b) Enhanced surveillance and interception capability by linking auto-identifying and GPS-enabled data of cargo and conveyances that is viewed together with 'fusing' data coming from different sources. There are examples of existing practical applications of this solution in customs and border management.

Additional possibilities include visualising goods declaration and manifest data not as 'text on screen' but as interactive maps. It is also possible for risk management systems to improve the evaluation of risk profiles when such systems are provided with numeric information (latitude/longitude) that supplement the currently used text or codes for risk indicators related to locations. Geospatial enablement could be an important vehicle for enhancing customs capabilities to manage information and to improve 'end-to-end' controls in the international trade supply chain.

There is need to apply such track and trace technologies directly in control over inland movements of goods as well. One of the challenges before a customs administration is to effectively monitor cargo allowed movement without collection of customs duties for various purposes. In India, the following types of cargo movement take place from the customs station of import without payment of duty:

- Port to CFS
- Port to ICDs
- Port to SEZs
- Port to bonded warehouses
- International Transit (to Nepal, Bhutan etc.)

The present system of reconciliation of cargo movement is based on a document being forwarded from the customs station of import to the receiving station and it being returned with an endorsement regarding the receipt of the cargo. It is dilatory, costly and unreliable. It is also not

trade facilitative since trade has to wait long for the cancellation and return of bonds/guarantees executed by them.

Deployment of an electronic tracking system is a possible solution not only to enhance customs control over the movement of such cargo but also to ease procedural/documentation requirements, eliminating a lot of paperwork and promoting the movement towards a paperless environment.

The electronic tracking system involves usage of technology (GPS, GPRS, e-seals etc.) to (i) track the truck/prime mover carrying the cargo at any point of time giving, inter alia, indication of the route being followed and deviations, stoppages, etc., and (ii) indicate any breach in container security.

The use of such a system would

- improve predictability of cargo and vehicle movement
- enable live tracking of cargo/vehicle movement by customs and plan for immediate intervention in case of any breach
- facilitate cross-border transit/transport by simplified formalities and procedures at border points, which is expected to lead to removal of congestion, and
- ensure efficient fleet management for transport operators and container deployment for shipping lines

Such systems have been conceptualised by the UNESCAP as the Secure Cross Border Transport Model (SCBTM) and are being applied in Thailand, PR China-Hong Kong border, Jordan, Kenya, etc., enabling live tracking of cargo vehicles and checking the integrity of the container seal.

The deployment of this technology in India will aid in enhancing customs control over the significant volumes of cargo being transported without payment of customs duties and will also help in facilitating legitimate trade.

Currently, the customs systems are not designed to take feeds from such sources. Evidently, the design of future systems will have to take account of such developments and ensure its integration with all relevant systems such as the RMS and with the global supply chain.

Considering the large variety and complexity of technologies, customs will need capacity to conduct experiments and run pilots before making final technology choices. This necessitates both high order of technology skills and required degree of functional and financial autonomy so that an environment in which innovation and creativity can be fostered, as recommended in Chapter III of the TARC report.

The TARC noted in Chapter VII of the first report that the Directorate of Systems of the CBEC, as it is positioned, lacks the capacity to meet this formidable challenge and needs to be strengthened. It needs to be prepared to assume the responsibility to provide thought leadership to the CBEC in this area. In the customs context, this thought leadership is needed not merely for

ICT but also other technologies such as non-intrusive detection systems that need to be integrated with ICT. The TARC had also recommended an SPV for delivery of ICT services and suggested a broad road map to attain the "digital by default" status. These recommendations need to be taken forward to position the CBEC as a modern 21st century customs organisation.

VIII.4.m Non-intrusive inspection systems (NIIs)

Customs have existing and planned major investments in non-intrusive detection systems. The most important among these are container scanners, some of which have already been installed while others are at different stages of the procurement process.

Two container scanners – one mobile gamma ray scanner and one fixed 9 MeV X-ray scanner – were installed at *Nhava Sheva* in 2004 and 2005 respectively on a pilot basis. Subsequently, mobile container scanners have also been commissioned at Tuticorin and Chennai in 2014. Another mobile container scanner is under installation in Kandla and four fixed container scanners at Tuticorin, Chennai, Kandla and Mumbai are under construction and are likely to be commissioned by March 2015. The contracts are being executed by two public sectors undertakings namely, Electronics Corporation of India Ltd (ECIL) for mobile scanners and Bharat Electronics Ltd (BEL) for fixed scanners.

These acquisitions involved delays owing to a number of reasons. The mobile scanners should have been commissioned by February 2013. However, scanners could be installed at Tuticorin and Chennai only recently and the one in Kandla is yet to be commissioned. Similarly, the four fixed X-ray scanners at Chennai, Tuticorin, Mumbai and Kandla ports were to be commissioned in different phases by September 2013. However, it is gathered that one reason these projects have been delayed is the desire of original equipment manufacturers (OEMs) to revisit certain clauses of the contract with M/s BEL.

In the meanwhile, technology has moved ahead and some countries have installed drive-through container scanners, which can scan about 100 containers per hour (as against a maximum of 20 containers for the existing fixed scanners). These scanners do not require the driver of the vehicle to get down and scanning takes place while the vehicle is in motion. Drive-through container scanners are available for scanning rail and road mounted containers and it is learnt that the CBEC has obtained in principle approval of the Atomic Energy Regulatory Board (AERB) for installation of both varieties of drive-through scanners, according to requirement at *Nhava Sheva*, Cochin and Mundra. Tenders for drive-through container scanners (road) were floated in July 2014, while tenders for the rail version are being developed. It is gathered that the process of installation of drive-through container scanners at remaining major ports in a phased manner, where substantial volumes of containers are handled, has been initiated by the CBEC.

It is reported that a major factor contributing to the delay has been lack of experience and domain knowledge on the part of PSUs, who have been awarded contracts to install the scanners. They have been completely dependent upon their original equipment manufacturers, who are reported

to have had some contractual issues, including cash flow issues, with the PSUs, resulting in inadequate deployment of manpower, machinery and material and hence delay.

The availability of land in the port areas and payment of lease charges has been another issue affecting the installation of scanners. This was pending for long and although it was finally decided by a Committee of Secretaries in 2009, lease agreements could only be signed in 2011. The Land Policy for Major Ports, 2014, provides for allotment of land on nomination basis to government departments and security agencies like state police, CISF, coast guard, etc., at concessional lease rent up to 75 per cent of actual lease rentals.

Container scanners not only assist the detection of mis-declaration of goods having revenue implications but are also useful in the detection of other contraband including arms and ammunition. Ports authorities are responsible for ensuring the security of their premises and hence, they are required to take appropriate measures in this regard. Under the ISPS Code implemented through Chapter XI-2 to enhance maritime security in the International Convention for the Safety of Life at Sea (SOLAS), the responsibility for ensuring safety and security has been cast upon port authorities too. Under these circumstances, it would be appropriate that land for the installation of container scanners and other such equipment in port areas be given free of cost.

The CBEC needs to give a thrust to efforts to install efficient and faster container scanners at gateway ports, including private and non- major ports. This will strengthen its ability to manage risks more effectively at the border itself and the need to have scanning facilities at hinterland ICDs and CFSs can be avoided.

Other than container scanners, CBEC has deployed 164 X-ray based inspection systems (XBIS) at various ports/airports and four high energy cargo pallet scanners at Salamabad and Chakan-da-bagh along the LOC. Field formations have also been provided binoculars, metal door detectors, hand-held detectors, HF and VHF sets. The CBEC has also provided firearms of different bores along with ammunition.

The deployment of a non-intrusive inspection system in the field was found to be inadequate. It is also learnt, based on inputs received from field formations that the requirement of anti-smuggling equipment has been compiled by the Directorate of Logistics and an action plan for procurement of equipment in three phases has reportedly been approved by the Board in early 2014. The process to procure 76 X-ray baggage inspection systems (XBIS), 32 high energy pallet scanners, installation of CCTV security and surveillance system at some LCS along the Indo-Nepal border, undercarriage inspection system at ICP Atari, 130 personal radiation detectors and 26 radionuclide investigation detectors, 18 carat meters, video scope and mail scanners have been initiated. However, the success of the procurement would depend upon the availability of funds for these anti-smuggling equipment in the near future and the finalisation of contracts.

Sniffer dogs have been found to be an effective means of detecting narcotics, explosives and, lately, fake Indian currency. The department had around 8 sniffer dogs in 2012 and these were found to be inadequate to meet requirements. Twenty-one Labrador dogs have been purchased and

deployed at 9 airports (Amritsar, Delhi, Mumbai, Pune, Ahmadabad, Cochin, Kolkata, Trivandrum and Tiruchirappalli) in the last two years after their training along with the handlers at National Training Centre for Dogs (NTCD), a BSF facility, Tekanpur, Gwalior. Considering the geopolitical location of the country and the efficacy of sniffer dogs in detecting narcotics and explosives, there is a clear need for the CBEC to strengthen its canine programme.

VIII.4.n Marine and Telecommunications Wings

From 2009 onwards, customs has procured 109 state-of-art patrol boats of three different configurations and deployed them at 42 locations along the coast. A separate cadre was created to operate these boats. At present, about 50 per cent of the sanctioned posts, mostly in the Group B grades, are lying vacant, resulting in gross underutilisation of the boats. The recruitment process could not be completed, since the cadre restructuring proposal is pending for approval in the Ministry since July 2013. It is learnt that the finalization of rules was held up because of bureaucratic delays which were largely beyond CBEC's control. Urgent action needs to be taken to finalize the process as it is of utmost importance that the fleet is made operational as soon as possible.

Customs had a dedicated telecommunication network comprising of HF and VHF sets for anti-smuggling activities. A separate cadre was created to maintain and operate the telecommunication network. The staff inspection unit under the Department of Expenditure had suggested winding up this network in view of increased and widespread availability of wireless services by other service providers. Customs, however, did not agree and perceived a need to retain it to meet anti-smuggling needs. In 2010, a Committee of Secretaries had directed that the manpower requirement based on functional needs be reworked. Accordingly, a cadre restructuring proposal was prepared on the basis of functional needs and is at present pending in the Department of Expenditure. Modernisation of the telecommunication set up cannot be undertaken until the restructuring is cleared. The recent trends of increased gold smuggling along the southern coast and the vulnerability of the long Indian coastline to smuggling of contraband, including narcotics, necessitate that the proposal must be processed expeditiously, as the customs have clearly established the business case.

The CBEC needs to expedite the infusion of technology in its operations to enhance its ability to secure customs borders while at the same time ensuring speedier cross border movement of legitimate trade and people. Hence, all these ongoing and planned procurements and installations need to be fast tracked.

A review of the procurement so far clearly shows that a large part of the delays were beyond the CBEC's control and were due to external consultations and approvals. Hence, action to mitigate delays lies beyond the CBEC. The TARC, in its first report, has highlighted the need for greater functional and financial autonomy to the CBEC as well as the CBDT. If those recommendations are implemented, a part of the problem would be resolved.

Going forward, the CBEC needs to strengthen the Directorate of Logistics and build the necessary technical capacity, and procurement and contract management skills in the directorate. Both in ICT and NII technologies, the procurement should be driven by product life cycles and obsolete equipment should be replaced on a regular basis. Besides, officers should be scanning the relevant technology fields for emerging technologies and exploring their potential for application in the CBEC. They should be closely engaged with industry, technical research institutions, the relevant wings of WCO and other international bodies to update their knowledge about emerging developments.

This means that a specialised skill set, of the required quality and in adequate numbers, must be sustained in these two directorates. Besides, the users – the officers in the field – also need to be trained in the use of different technologies.

Such large scale procurements also necessitate the ability to plan and execute large capital expenditure. This is difficult in the current set up which the required financial autonomy and independence as well as high quality financial management skills are missing. To enable CBEC to undertake such projects effectively and efficiently, it would be necessary for the government to grant it the necessary independence autonomy and create structures as recommended in the TARC's first report.

VIII.4.o Enforcement and Anti-smuggling operations

The prevention of commercial frauds and combating smuggling continues to be a key area of the CBEC's functions, which is vitally important for building and sustaining a culture of compliance. This function is primarily looked after by the DRI and preventive formations in the field.

Swift detection and deterrent action against wrong doers serves a dual purpose. First, it is a stern message to the non-compliant elements in society. Secondly, it prevents the demotivation of elements that are inclined towards compliance, who are likely to be discouraged if a pervasive atmosphere of non-compliance is allowed to exist.

In Chapters III and VI of its first report, the TARC has given certain recommendations in this area. The creation of a functional vertical under an officer of Principal Chief Commissioner and bringing the preventive and intelligence wings of the field commissionerates under DG, DRI has been recommended. This will bring about greater coherence and improve coordination and direction of enforcement efforts.

With the growing sophistication of financial crimes, there is an urgent need to upgrade the technological support for intelligence and investigation. Apart from new technology tools, there is also need to deepen the analytical abilities in this vertical to make extensive use of data analytics for identifying potential economic crimes. Capacities need to be built in ICT related areas such as computer forensics.

There is also an urgent need to significantly improve the investigative skills among officers. For enforcement to be effective, a sharper focus on the quality of investigation is essential. A clear

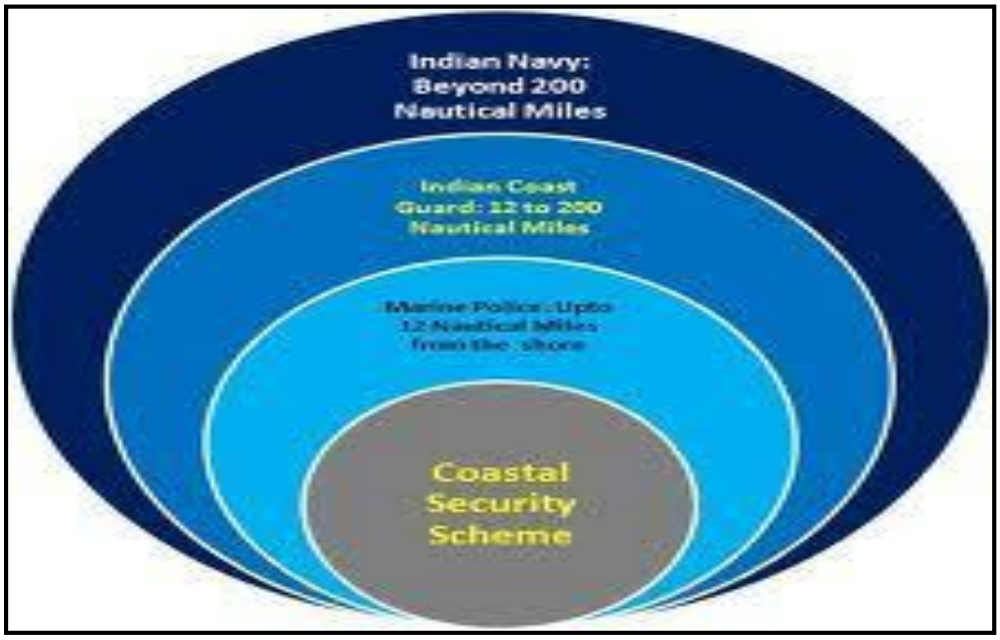
distinction needs to be made between cases which involve deliberate fraud and those that involve a difference of opinion or interpretation. The latter would usually involve technical issues in which there could be more than one opinion and need to be handled differently. Normally, the dispute resolution mechanism should be adequate to take care of such cases. The former on the other hand need detailed painstaking investigation that uncovers evidence that is sufficient to sustain the case in prosecution; for prosecution is the strongest deterrent to such malfeasance.

Experience shows that while customs regularly prosecute offenders in cases of smuggling, the performance in relation to commercial fraud has been not been very satisfactory. There is a need to improve on this score. It was for this reason that the TARC has recommended the creation of a Directorate of Prosecution in Chapters III and VI of its first report.

India has a long border and an extensive coastline and customs formations are deployed along them. On land, with the fencing of the western border, the risk of smuggling has considerably declined. The Indo-Nepal border and Indo-Bangladesh border, however, continue to be porous.

On the coast there is a well-organised coastal security plan involving the Navy, Coast Guard Marine Police and Customs. There is close co-ordination among these agencies and a layered approach to security, in which customs occupy the innermost layer as depicted in Diagram 8.5.

Diagram 8.5: Layered approach to coastal security



Unlike other agencies in the coastal security scheme, the role of customs extends from land to sea and they have certain advantages over other agencies. Customs personnel have their ears to the ground, a traditional informer base and network, and the location of preventive formations along the coast line, enabling them to tap information from local people and fishermen. Customs are, therefore, in a better position to develop more comprehensive intelligence on activities along the coast.

There are operational difficulties that they face. As noted above, although they have acquired a modern fleet, much of it is non-operational because of the difficulties in manning the boats. Consequently, these valuable assets remain underutilised. There is also a large human dimension to the problem. First, there is little encouragement to develop specialisation in the anti-smuggling area since the transfer policies adopted by the department involves the regular rotation of officers. This often leads to unsuitable and unwilling officers getting posted to such check posts and considering the often inhospitable locations of many such postings, there is a quick loss of motivation telling on the effectiveness of customs formations. Anti-smuggling operations and intelligence work requires not only special skills but also a particular bent of mind. Those who have these aptitudes and get posted to such areas are also moved out after short tenures because of the transfer policy.

In the south, a peculiar problem was mentioned repeatedly by officers as having a substantial impact on anti-smuggling activities. This arises from the fact that among the candidates sponsored by the Staff Selection Commission, there were a large number of candidates from other regions and very few with knowledge of local languages and familiarity with local culture. The difficulties this creates are particularly acute in anti-smuggling operations, which involve posting in remote areas where such officers stand out and are easily identified as customs officers. This makes it virtually impossible to maintain secrecy in their movements, an essential operational requirement. Further, intelligence gathering requires customs officer to mix freely and easily with the local population, which again is difficult because of the language barrier and cultural differences.

There appears to be no easy solution to this problem as it is inherent in the competitive examinations through which the SSC effects recruitment. However, this is a real problem that needs a solution.

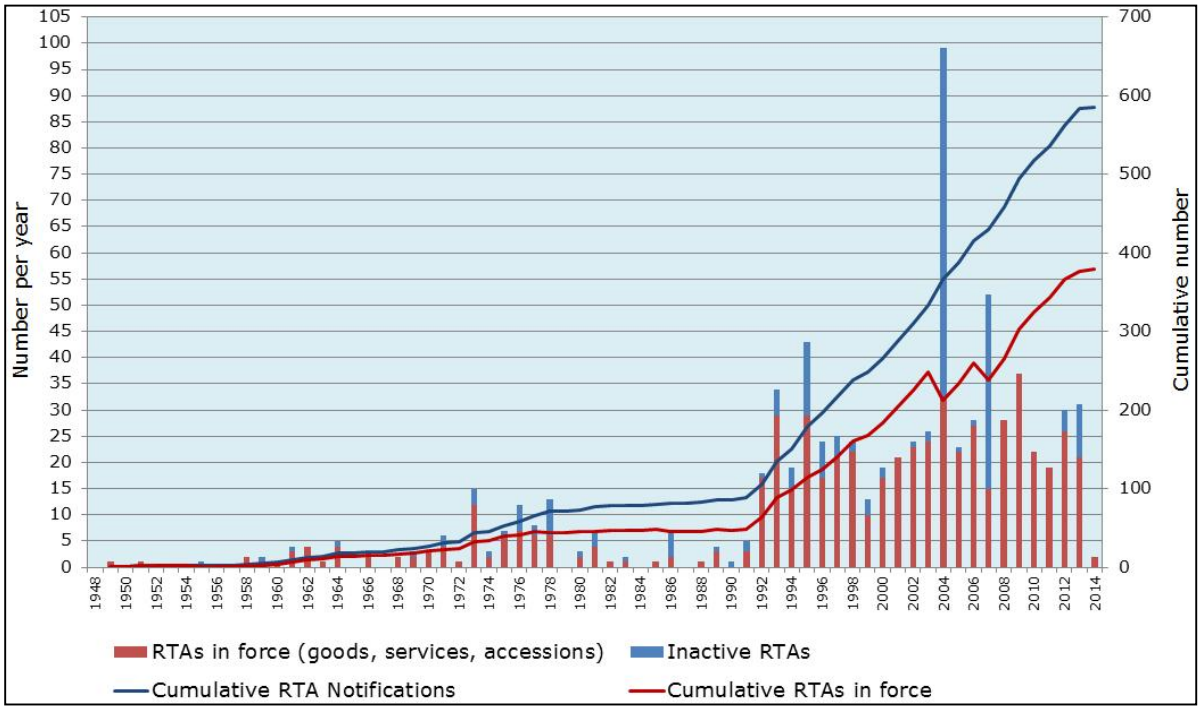
Considering the remote location and inhospitable terrain of many such postings, measures need to be taken to incentivise willing and able officers to elect for such posting and stay there for a sufficient length of time to contribute effectively to keeping vigil along sensitive coasts and borders to check smuggling and security risks. It would be desirable to make provision for facilities like special allowances, the retention of government accommodation in places where adequate medical and educational facilities are available, etc. The CBEC will have to develop a scheme for this purpose and secure government's approval.

There is also need for specialised training in anti-smuggling operations, which is tailored to specific requirements, including the peculiarity of local conditions in the diverse environment in which these operations have to be carried out.

VIII.4.p Regional Trade Agreements (RTAs)

As was noted earlier in this report, the failure of the Doha rounds of trade negotiation resulted in the proliferation of trade agreement between regional trading partners and trading blocs. Graph 8.2 shows the evolution of RTAs from 1948 to 2014.

Graph 8.2: Evolution of Regional Trade Agreements in the world, 1948-2014



Source: WTO database

The World Trade Organization (WTO) had received notifications for 585 RTAs up to June 15, 2014.[113] Of these, 412 notifications were made under Article XXIV of the GATT 1947 or GATT 1994, 39 under the Enabling Clause and 134 under Article V of the GATS. Of these 585 RTAs, 379 are currently in force. According to the Origin Database developed by the WCO, 96 per cent of the WCO Members are taking part in one or more RTAs, with an average of approximately 8 agreements per WCO member.

India is also an active user of FTAs and has signed FTAs which are under implementation with the following partners:, ASEAN (major users: Indonesia, Thailand, Malaysia, Singapore), Japan, Korea, SAPTA & SAFTA (SAARC countries), APTA (China, South Korea, Bangladesh, Sri Lanka, Laos), Singapore, Malaysia, Chile, Mercosur (Argentina, Brazil, Uruguay and Paraguay), Thailand, Afghanistan, Nepal, Bhutan and DFTP (Unilateral concession given to LDCs).

The FTAs under negotiation include those with the EU, EFTA, Israel, Canada and the Regional Comprehensive Economic Partnership Agreement (RCEP), which has 15 major trading partners from Asia including China. Thus, a significant portion of India's trade could potentially be eligible to be covered under an FTA within the next five years. Hence, there is an urgent need to strengthen institutional structures and build capacities for effective negotiation, implementation and review of FTAs and for managing the associated risks.

[113] On the basis of separate RTAs for goods, services and WTO accessions.

Rules of origin

Rules of Origin (RoO) are the set of rules that are used to identify the country of origin of an exported item and play a pivotal role in determining the eligibility for preferential treatment for imported goods. The rules of origin that determine the country of origin for a product, for purposes other than preferential treatment under RTAs, are usually referred to as the non- preferential or economic rules of origin. The rules of origin that determine the eligibility for preferential treatment are commonly referred to as the preferential rules of origin.

The WTO regime requires that equal tariff rates are applied on an MFN basis to all imports, regardless of their country of origin as long as the country is a WTO member. But the RTAs, because of their selective nature, reduce or eliminate tariffs only on specific items imported from specific countries. These RTAs, therefore, result in a veritable spaghetti bowl of tariff rates, which are otherwise meaningless under the multilateral trading regime.

Rules of origin are essentially mechanisms for establishing the economic nationality of a product.[114] Tariff benefits under free trade area (FTAs) are linked to certificates of origin issued under the respective Rules of Origin. A general review of the preferential rules of origin of the RTAs shows that, increasingly, not a single method, but a combination of methods for determining origin is used. According to the Kyoto Convention, if a product is "wholly obtained or produced completely" within a country, the product shall be deemed to have origin in that country. For a product that is produced in more than one country, it shall be deemed to have origin in the country where the last substantial transformation took place.

To determine substantial transformation, three rules, either singly or in combination, are applied:

- change of tariff classification
- value addition criteria, and
- technical or special processing rules – the specific transformation is described in terms of manufacturing transformation or process

The simplest rule of origin is where goods are "wholly obtained" or produced without any participation of materials from outside the exporting country. These are generally products that are grown, harvested or extracted from the ground in the territory of a single country, as well as goods produced from such materials. While there are areas of the definition of "wholly obtained" that can become contentious (such as fish taken from the sea outside any territorial sea), in the vast majority of cases, there is no controversy as to the application of this criterion.

A second set of rules of origin is based on substantial transformation criteria. It is defined in three ways: tariff-shift, value content and technical rules. These methods of defining originating goods can be used individually and/or in combination with each other. Tariff-shift rules require that a

[114] Robertson 2005, (reporting figure of 55 per cent) from, Anne van de HeetKamp & R. Tusveld, "Origin Management – Rules of Origin in Free Trade Agreements", Chapter 1, Pp 3, Springer-Verlag Berlin Heidelberg 2011

good (imported from a party outside the free trade agreement or a non-beneficiary to the preference scheme) that is incorporated into a product that is exported to a party must go through a specified change in tariff classification under the Harmonised Commodity Description and Coding System (Harmonised System or HS). The specified shift could be at the two-digit, four-digit, six-digit or more disaggregated level, the usual practice being to define it at the six-digit level. In some instances, tariff shift rules exclude the use of non-originating goods from specified subheadings, headings and chapters of the Harmonised System. Tariff shift rules have the benefit of being the simplest to apply. One has simply to examine the bill of materials and determine whether or not the imported materials meet the tariff shift criteria. The disadvantages of tariff shift rules stem from their limited transparency, their rigidity and in some circumstances, their arbitrariness, as well as from all the difficulties relating to classification. It is important to bear in mind that the Harmonised System was not designed with the rules of origin definition in mind, grouping products together in chapters, headings and subheadings based on criteria that have nothing to do with establishing the origin of goods.

Value content rules require that the prescribed minimum levels of value addition must be in the country of export. This type of rule makes it very difficult to prove origin as it assumes certain levels of accounting skills and record keeping that is often scarce within developed country customs authorities and SMEs. The most user-friendly alternative to minimum value added is maximum levels of foreign content (an input value always recorded by customs in the country of export) in the finished goods exported to a free trade agreement-trading partner. Despite these difficulties, value-content rules are generally regarded as the most transparent.

Technical rules are often associated with steel, textile and apparel goods. They specifically outline what process or input must be used in the making of an originating good. Although this substantial transformation criterion is easy to understand and verify, it usually is very restrictive in terms of alternate and/or flexible sourcing of inputs. These rules suffer from some of the same drawbacks as the tariff shift rules in that they are not transparent. Their inflexible nature complicates matters further. The rules for apparel products can also be tortuous, requiring not only that the fabric be cut, sewn and finished in a beneficiary country, but also that the fabric, yarn, sewing thread, as well as the fabric of visible linings and pocketing originates in the same place. The production cost implications of meeting these requirements, let alone the costs of proving compliance, can result in situations where it is simply uneconomical to use tariff preferences.

Origin Management

Origin Management is an all-inclusive approach towards the creation of a single, auditable, and global platform that enables companies and governments to successfully claim preferential origin, and to assist in sustaining, reviewing and auditing preferential claims. This approach further involves sharing and exchanging information and resources between various stakeholders and the supply chain, resulting in competitive advantages, synergies and a central point of wisdom for all origin associated issues. The strategies adopted in origin management may, *inter alia*, include analysis of the FTAs entered into by a country. This assists in analysing the use of a specific FTA by a country and the consequent implications on account of irregular origin certifications. Keeping

in view emergence of FTAs as a vehicle for trade enhancement, the CBEC needs to considerably augment its capacity in origin management.

Verifying rules of origin by customs

Looking at the complexity involved in determining rules of origin, customs administrations often have onerous responsibility in verifying preferential origin. Most customs administrations rely on the certificate of origin issued by competent authorities. Developing detailed case studies from their experience of origin verification, Korean customs came to realise that administrative costs and burden have emerged as key concerns for industry and, to minimise this administrative costs and burden, it was recommended that the following principles be adopted for origin verification:

- post-verification after the release of goods from customs
- document-based verification first
- on-site verification under exceptional circumstances and
- respect for procedures under the agreements

The proof of origin issued by exporters is also widely accepted. The utilisation of importer-based certification is very limited. Customs administrations conduct verification by utilising multiple methods. Among them, administrative co-operation is the most frequently utilised method. While many administrations conduct verifications after the release of goods (post-clearance), some carry out verification only before release. The major challenges faced by customs administrations are, among others, non-compliance to certification requirements, lack of standardised procedure for verification and lack of capacity.

The importance of verification is underlined by the fact that in several cases where the country of origin certificates were found to have been issued on the basis of misrepresentation. The verification process contemplated under the FTAs involves writing back to the issuing authority through the Government; this presupposes a very high level of intellectual rigour/integrity on the part of all concerned which has been lacking. Thus for instance the Indo-Thailand FTA has extended preferential tariff benefits to gold jewellery which have a value addition of 20 per cent; It may be pertinent to mention here that to sell plain gold jewellery costing 20 per cent higher than the value of primary gold is commercially not a viable preposition since the sourcing of gold is at the prevailing international prices -however there had been a surge of such imports all accompanied by certification making such imports eligible for the preferential benefit. The verification process led to strenuous confirmation of the certificates. Last year alone DRI booked cases related to import of cocoa, gold jewellery and LED televisions where crores of duty exemption was fraudulently claimed.

Strengthening co-operation with competent authorities of trading partner countries

A certificate of origin is the leading type of proof of origin. Declarations on commercial invoice are other proofs. Customs of the exporting country and exporters are the leading types of issuer of

certificates of origin. Categorising the issuers according to their characteristics can help in building co-operation and strengthening trade relationships. Building co-operation can lead to acceptance of exporter/producer self-certification.

It has been reported by the World Customs Organization (WCO) that customs administrations generally require the proof of origin in paper format; electronic certificates are accepted by very few customs administrations. Enhanced co-operation between these competent authorities would lead to trade facilitation enabling customs administrations to accept electronic certificates and they might not insist on a proof of origin for every single shipment. Mutually recognised documentation requirement can be prescribed and audit can be undertaken on the basis of a robust risk analysis and post-clearance verification.

Creation of a Directorate of Origin

Emerging trends and practices in the global context makes a compelling case for bringing increased focus on origin administration. Effective preparation for negotiation and implementation of FTAs requires continuous engagement with industry to gauge the impact of RoO and tariff concessions on domestic sectors and from the risk point of view. The current trend of negotiating the tariff concessions and RoO HS line wise would entail the development of capacity to track each HS line from the perspective of the capability of the trading partner to fulfil the relevant RoO, the state of domestic production or import dependency in India, the MFN rates and changes thereto etc. This should be based on industry consultations and data relating to domestic production and external trade of the merchandise.

At present, this crucial work that involves extensive research and consultation is dealt with by divisions in Department of Commerce and DoR (CBEC) along with their other allotted work, and hence, does not receive adequate focus. Considering India's engagement on FTAs and given the ambit and time required for doing this work meaningfully, it would be desirable to task this work exclusively to a directorate.

Many customs administrations such as those in EU, Japan, Korea Israel, Australia, New Zealand, USA, Canada, etc., have adequately staffed divisions that engage with their domestic industry and trade associations to sectorally analyse offensive and defensive interests and evolve product specific rules (PSRs) and tariff concessions that they should offer and can accept. They also lead the negotiations on rules of origin. Such an arrangement would offer several advantages in the Indian context also.

Officers of the CBEC have experience in not only negotiating the goods portion of the FTAs but also in implementing them. FTAs (the portion dealing with goods) primarily deal with subjects dealt with by the CBEC, namely, rules of origin, trade facilitation, verification system and customs co-operation, rates of duty and reductions thereto and HS line wise product specific rules of origin. The CBEC also has comprehensive data on manufacturers, exporters and importers, which gives it the capability to access vital information on goods manufactured/exported/imported, as well as, interact with domestic manufacturers to provide inputs for a negotiating strategy suited to India's

interests. The use of the ICES and ACES databases gives the CBEC the ability to access and tap information on producers, exporters and importers of each given commodity, conduct consultations with them, assess the impact of possible tariff concessions and ROOs and monitor the implementation impact.

The CBEC also has a strong presence overseas by way of officers with domain knowledge posted in Indian missions, who can be leveraged to provide inputs to FTA negotiations and review.

Considering the above and the structural change in foreign trade passing through the FTA trade lane, the functional specialisation and multi-disciplinary approach that is required on the subject, a separate Directorate of Origin should be created immediately in the CBEC. The officers of this directorate will have the responsibility to study origin determination rule(s) in various FTAs/PTAs, keep abreast of changing industrial processes that impact origin determination and play an active role in domestic consultation in formulating origin rules for various FTAs/PTAs. The officers in this directorate should also have a thorough understanding of international trade frameworks and associated forums/bodies such as WTO, UNCTAD, and UNESCAP. They should be tasked with undertaking intensive industry consultations sector wise to evolve the rules of origin that are in India's interest as also tariff concessions that can be given and obtained.

This directorate will also have the mandate to participate/assist in negotiation of harmonisation of non-preferential rules of origin in the WTO and formulate and implement non-preferential rules of origin for India as this plays a vital role in the accurate collection of anti-dumping, safeguard and countervailing duties. The current template of WTO harmonised non-preferential rules of origin can serve as the basis for India's non-preferential rules of origin.

These officers should also be equipped with knowledge of accounting, production processes, auditing, analytical and supervisory skills. The Origin Management Directorate should be entrusted with the following roles and responsibilities:

- Administration of origin regimes including addressing trade distortion and policy recommendation in relation to trade agreements, monitoring of utilisation of origin benefits and coming up with analytical papers on key trends, produce research papers, performing research and analytics to spot trends, distortions and support policy recommendations, and harmonising regulations relating to origin across various agreements so as to simplify usage by the industry. As a measure of trade facilitation, the directorate should aim to publish an origin benefit schedule that would link the benefits available under various FTAs with the Harmonised System and sensitise Indian industry to take full advantage under various FTAs.
- The Directorate of Origin would also be in-charge of the overall implementation of origin regimes that would entail co-ordinating with specialised agencies for issuance of origin certificates, acting as a grievance redressal forum on origin issues including co-ordination with various stakeholders on various aspects of grievances.
- Opportunities for mis-use of duty concessions often present themselves from sudden arbitrage opportunities arising from increases in MFN rates vis-à-vis the preferential rates. Thus, there

is need for constant vigil over these duty rates to undertake preventive enforcement/review. This directorate, therefore, should be responsible for ongoing risk analysis to identify emerging risks in a dynamic trade environment and protecting any possible loss to the exchequer on account of origin frauds by referring suspected cases for further investigation by revenue intelligence agencies and triggering verification of origin, including on-site verification under exceptional circumstances and co-ordinating with trade partners at the stage of on-site verification as well as with authorities in India issuing the certificate of origin.

- The Directorate of Origin in addition, should be tasked with studying the working of rules of origin under various FTAs/PTAs in order to pinpoint potential misuse and technical difficulties in their operation. For example, the value addition clause for certain product sectors is unrealistically high and creates difficulties in truthful declaration of origin. At present, the certification of origin for export goods is done by private agencies where record keeping and calculation of value addition norms might lack the requisite precision.
- In view of the increasing number of FTAs as well as the increasing volume of imports thereunder, it is critical, both as an enforcement measure and as a deterrent, to cause verification of origin in select cases. The criteria for verification could be based on risk parameters such as the quantum of duty being foregone, information available about the declared country of origin's capacity to produce and export a given commodity, nature of commodities that are prone to mis-declaration of origin, compliance record of the importer etc. The verification could also be undertaken on a random basis. Suitable criteria have to be devised for selection of import consignments for verification. The risk management system could select such cases and prompt the assessing officer to take up the cases for verification.
- The directorate should work closely with the RMD to suggest the risk criteria for selection for post-import verification. It is also necessary to provide external intelligence inputs such as production and export capacities of the FTA partners, extent of imports that feed into production, etc., to the RMS
- The directorate may also co-ordinate verification visits undertaken under the FTA provisions.
- Effective implementation of FTAs requires strong and institutionalised co-operation between customs administrations to detect and investigate origin frauds, for exchange of FTA utilisation data etc. However, our FTA partners have not been forthcoming in terms of sharing data with India. Given the serious threat of revenue frauds (under invoicing as well as origin frauds), the CBEC needs to leverage FTA concessions to demand bilateral exchange of information documents to verify description, valuation and country of origin as a pre-condition to extending preferential benefits. This can be positioned as a necessary condition for achieving bilateral and reciprocal interests of facilitation and enforcement.

VIII.4.q Trade Remedies

While current difficulties in multilateral negotiations have resulted in the proliferation of bilateral and multilateral trade agreements on the one hand, it has also led to the heightened use of trade remedy measures like anti-dumping, countervailing and safeguard measures on the other. Many

countries, both developed and developing, now rely heavily on anti-dumping measures. One difference between countervailing and anti-dumping measures (or, indeed, safeguards) is that they represent only one of two means of responding to a subsidy, because they target the conduct of a country rather than commercial actors. Whereas anti-dumping measures target the actions of commercial actors acting unfairly by pricing goods below normal value, countervailing measures target the conduct of a country by responding to the subsidy provided by such country. In contrast, safeguards measure do not address any unfair trade practice and merely act towards ameliorating the condition of an already ailing domestic industry by insulating such industry from international competition. All these measure are subject to review, which is generally done at the end of five years, also known as a sunset review. However, in certain cases, such a review may be conducted at the end of one year as well, and is called a mid-term review.

Safeguard measures provide carve out from WTO obligations, sometimes referred to as an "escape clause" or "economic emergency exception." It typically consists of a duty or other measure targeted at a particular imported product that is imposed on imports from all countries and all producers. A measure qualifies as a safeguard based on events in the country implementing it, in stark contrast to anti-dumping measures and countervailing duties the legality of which hinges on events in the exporting country (e.g., the price of a good in the exporting country or whether a subsidy exists). Safeguards look only to the importing country, because they are intended to provide a "safety valve" that allows WTO members to avoid their WTO obligations on a temporary basis in response to an economic shock of some sort. This is an important distinction between safeguards and the two other categories of trade remedies (anti-dumping and CVDs) because the implementation of a safeguard does not require any showing of undesirable or "unfair" conduct by another state. It is enough that conditions in the importing state satisfy the relevant requirements. In other words, the exporting state may be subject to a permissible safeguard measure, and that measure may cause injury to the exporting state, even if it did nothing "wrong" (other than being a successful exporter).

There are two types of safeguard inquiries: global and bilateral. In a global safeguard inquiry, the effects of goods imported from all sources on domestic producers are considered. In a bilateral safeguard inquiry, the effect on domestic producers of goods imported from one of the countries with which a country has entered into a bilateral free trade agreement is considered.

Indian context

Laws in India relating to trade remedies are based on the WTO agreements and hence, are compliant with it. The essential features of the trade remedy measures implemented by India are that the Directorate General of Anti-dumping and Allied Duties (DGAD) and Directorate General of Safeguards (DGSD) are the primary nodal/administrative bodies that recommend implementation of trade remedial measures like anti-dumping, countervailing and safeguard measures in terms of tariff and quantitative restrictions, as may be applicable. Anti-dumping and countervailing measures are administered by the Directorate General of Anti-dumping and Allied Duties (DGAD) of the Department of Commerce, which is headed by the "designated authority". The designated authority’s function, however, is limited to conduct anti-dumping/anti subsidy and

countervailing duty investigations and make recommendations to the government to impose anti-dumping or anti-subsidy measures. Such duty is finally imposed or levied through a notification by the Ministry of Finance. Thus, while the Department of Commerce recommends the anti-dumping duty, it is the Ministry of Finance, which levies such duty. Safeguard measures, on the other hand, are administered by another authority, namely the Director General (Safeguard), which functions under the Department of Revenue, Ministry of Finance. The Standing Board of Safeguards, chaired by the Commerce Secretary, considers the recommendations of the DG (Safeguards) and then recommends the imposition of a safeguard duty as it deems fit, to the Ministry of Finance, which then levies the duty.

India is one of the most active users of anti-dumping measures. It has imposed 702 anti-dumping measures since the inception of the WTO in 1995. The products involved are chemicals and products thereof, plastics and rubber and products thereof, base metals, and textiles and clothing etc. On the other hand, there have been relatively few safeguard actions, awareness in respect of which seems much lower than of anti-dumping duties.

In India, as described above, applications for imposition of anti-dumping and countervailing duties arising out of subsidies are processed by the designated authority in the Ministry of Commerce. The designated authority is a senior IAS officer of the rank of Joint Secretary or Additional Secretary and is assisted by 6 to 8 officers, largely drawn from the Indian Trade Service and some from the Indian Cost Accounts Service and Indian Statistical Service. Since customs are intimately involved in implementing anti-dumping duties, DGAD will gain from the involvement of customs officers in his team and this will ensure enhanced co-ordination.

Safeguard measures are taken by DG Safeguards working under the CBEC. He is assisted by a few officers working under the CBEC. The function of imposing safeguard measures needs to be more systemised by posting an adequate number of motivated officers. They should not only familiarise trade with the WTO Agreement on safeguards but also with the instruments of safeguard measures provided under various FTAs/PTAs and develop expertise in this area.

While the administrative agencies for trade remedies are required to analyse and recommend the occasions for imposition of trade remedy measures, the actual implementation of such measures is undertaken only at the customs borders. They should form an important element in customs risk management. Given this, in addition to the above steps, government should actively consider capacity building in customs administration from a trade remedy perspective. The need to ensure proper application of these remedies at the customs borders is clearly linked to the necessity to develop non-preferential rules of origin referred to in the previous section.

Customs could become the agency responsible for enhancing co-ordination between various stakeholders like the ministry of commerce, ministry of external affairs, industry and business, academic and research institutions, ministry of law and justice, etc., to become the nodal agency to protect the interests of domestic industry through safeguard measures. The agency should assist in bridging the gap between the government and small and medium enterprises (SMEs) and

unorganised sectors. They should be actively engaged in the publication of regular information, updates, and research material to increase awareness regarding trade remedy measures.

In particular, DG (Safeguards) should undertake intensive outreach programmes to sensitise and inform industry of the remedies available to them. Information desks in the customs and DGFT offices can also help spread awareness.

VIII.4.r Intellectual Property Rights (IPR)

The role of customs in the protection of IPR has gained salience since the entry into force of the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS Agreement) in 1994.

Not only do counterfeiting and piracy adversely affect the legitimate interests of the right holders, potentially dangerous counterfeit goods also threaten consumers' or user's health and safety. The World Health Organization (WHO) reports on several cases in which counterfeit drugs caused the death of a number of persons in developing countries and acknowledges that weak enforcement of IPR legislation with regard to fake pharmaceuticals is a crucial element in this regard. The other cause of concern is the involvement of organized crime networks in counterfeit trade in what appears to be assuming the dimensions of a parallel industry. An OCED study[115] estimates that up to USD 200 billion of internationally traded products could have been counterfeit or pirated in 2005. This amount is larger than the national GDPs of about 150 economies. The figure does not, however, include counterfeit and pirated products that are produced and consumed domestically, nor does it include non-tangible pirated digital products being distributed via the Internet. If these items were added, the total magnitude of counterfeiting and piracy worldwide could well be several hundred billion dollars more.

With the issue of Intellectual Property Rights (Import of Goods) Rule, 2007, the related notifications under the Customs Act, 1962 and circulars for implementation, the CBEC has created the legal and administrative framework for tackling IPR issues. It has also put in place an online system, the Automated Recordation and Targeting System (ARTS) for IPR protection.

However, in order to effectively tackle the issue of IPR violations, the CBEC needs to enhance the capacity of its officers through extensive training. It also needs to forge close coordination between the customs and the industry. Indian customs has in place the provisions to take action, however there still exists challenges in getting a quick definite response from the right holders, on the authenticity of the goods. Customs need to engage closely with industry and not shy away from taking them as partners in the fight against IPR violations.

VIII.4.s International Co-operation

Having regard to the potential benefits that India can harvest from enhanced international co-operation and by acquiring a higher international profile in the customs domain, the TARC in

[115] The economic impact of counterfeiting and piracy, OECD (2007) http://www.oecd.org/sti/38707619.pdf, accessed in September, 2014

Chapter III of its first report had recommended the creation of a separate directorate for international co-operation. Many advanced customs administrations have set up such dedicated wings. The reasons why the CBEC too needs to undertake capacity-building in this area are elucidated below.

Customs, by its nature, has an enormous international agenda. Globalisation has caused countries to enhance international co-operation for efficient movement of goods and people. There is pressure on customs administrations to facilitate and at the same time ensure security of the borders. The illicit economy and illegitimate trade has also become globalised.

Each customs administration is engaged in a modernisation process, adopting global best practices, facilitating legitimate trade, safeguarding revenue collection and securing the borders. Reflecting the aspirations of all customs administrations, the WCO has launched a number of initiatives including a framework for future customs – 'C21' (Customs in the 21st Century). As part of this roadmap, the WCO had dedicated the year 2012 to the promotion of "connectivity" with the slogan "Borders divide, Customs connects". The theme for 2014 is promoting communication under the slogan "Communication: sharing information for better co-operation."

Initiatives such as the SAFE Framework, mutual recognition, pre-arrival information, air cargo security, supply chain integrity and dematerialisation of documents are increasingly demanding international co-operation and exchange of information to meet their objectives. .

Customs co-operation at the international level aims to improve control of trade flows and enforcement of applicable laws and regulations through the exchange of information on customs aspects such as export and import declaration data, trader-related information, origin and valuation-related information. Bilateral intelligence co-operation with other customs administrations is mainly through customs mutual administrative agreements (CMAAs)/memoranda of understanding (MoU). Such co-operation assists customs administrations to improve security and facilitation. Customs co-operation also takes place at the international level through the World Customs Organization (WCO) by establishing international customs standards and harmonised procedures and by providing training and technical assistance to build the capacity of customs administrations to use these new instruments and tools.

Indian customs participates in a number of international forums, including the WCO, IBSA, BRICS, ASEM, WTO, SASEC, SAARC etc. Officers also participate in customs reform and modernisation capacity building activities organised by WCO and other multilateral international organisations. As a member of the international customs community, a number of events, training activities and hosting of senior delegations from other countries and the WCO is organised by the CBEC. Indian customs has been contributing to the capacity development of the developing and least developed administrations through the National Academy of Customs, Excise and Narcotics (NACEN) and through the Directorate of Valuation in the areas of environmental protection, drug law enforcement and use of valuation databases.

In the CBEC, the work pertaining to international customs is handled by the Joint Secretary (Customs) and Commissioner (Customs and Export Promotion). The JS (Customs) has two Additional Commissioner level officers to assist in the work relating to international customs – Director (Customs) and Additional Commissioner WCO Cell. The Director Customs is responsible for the implementation of the WCO Revised Kyoto Convention, AEO programme and MRAs (DGICCE carries out the work relating to AEO certification and the MRAs are negotiated by the policy section of Board) and the work relating to Harmonised Systems Committee of the WCO. The Additional Commissioner, WCO cell, handles work relating to multilateral international co-operation, namely WCO, WTO and ASEM. For WTO customs trade facilitation related work, there is close interaction with the Department of Commerce, which is the nodal department for WTO matters.

Further, the foreign travel budget of the CBEC is managed by the JS (Customs). However, the Director (ICD) and his section process the nominations for deputation of officers to attend meetings, trainings, seminars, workshops, etc., in foreign countries. The initial processing of files relating to nomination of officers by the Board to travel for WCO, WTO and ASEM events is done by the Additional Commissioner, WCO cell, and thereafter, the ICD section is responsible for other clearances and issues sanction orders, etc.

Commissioner (Customs and Export Promotion) is assisted by two Additional Commissioner/Joint Commissioner level officers – a Director (International Customs Division) and OSD (ICD). The work includes all matters relating to bi-lateral international work, agreements and MoUs for mutual administrative assistance in customs matters with other foreign governments, work relating to IBSA, BRICS, SAARC, SASEC and trade agreements with respect to FTA/PTA/CEPA/CECA. Work pertaining to land customs stations, which needs close coordination with the MEA and the Department of Commerce on issues relating to overland trade in South Asia, is also with the ICD division.

Apart from the above, the Tax Research Unit in the CBEC handles work relating to the tariff related work of international agreements as well as engagement with the OECD.

The current situation is such that matters of international engagement are handled in a fragmented and disorganised manner and there is an absence of continuity. There is considerable scope to streamline this. The international work of customs can be consolidated under a directorate and it should have different wings dealing with various areas of co-ordination, collaboration, communication and co-operation with key national and international departments, ministries, organisations and stakeholders. This would lead to improvement in international engagement and a consistency in approach on issues before bilateral and multilateral fora with respect to India's commitments. A substantial part of the time of the Director (ICD) is wasted in getting clearances for foreign travel, etc., which in a routine way could be handled by the protocol division within a Directorate of International Co-operation. This directorate could also have a separate fund created for capacity building activities for our officers and to provide technical assistance to other developing countries and LDCs in Indian customs' areas of expertise.

VIII.4.t International data exchange

Each customs administration is in some manner or other engaged in a modernisation process, adopting global best practices, facilitating legitimate trade, safeguarding revenue collection and securing the borders. Reflecting the aspirations of all customs administrations, the World Customs Organization (WCO) has launched a number of initiatives including a blue print for future customs in the form of 'Customs in 21st Century'.

The initiatives such as the SAFE Framework, mutual recognition, pre-arrival information, air cargo security, supply chain integrity, dematerialisation of documents are increasingly demanding international co-operation and exchange of information so as to meet the individual objectives of these initiatives. In this back drop, risk management has taken centre-stage and has become indispensable to enhance the effectiveness of customs administrations. Independently, the increase in trade volumes accompanied by just-in-time inventory systems of industry has necessitated greater attention to information exchange between different customs administrations as a tool to augment the efficiency of customs administrations. The greater attention has brought in greater focus on the need for standardisation of information exchange between customs administrations.

Many customs administrations, whether developed, developing or least developed, have entered into a number of international agreements with other customs administrations for information exchange to facilitate trade and ensure better enforcement. In fact, there has been significant proliferation in the number of international agreements in the last decade related to information exchange. Concomitantly, there is growing concern regarding the cost, time and effectiveness of implementing and operationalising the exchange of information.

Lack of standardisation in information exchange has adversely affected the efficacy and efficiency of international agreements. Globally Networked Customs possibly is a way to address this growing concern. Standardised exchange of information between customs administrations would act as a catalyst to take forward WCO initiatives.

However, standardisation of information exchange should recognise the complexity and diversity in the interests of countries. Exchange of information should be primarily driven by national interests and the standards should provide for diversity in engagements considering the varying interests and levels of IT maturity across customs administrations.

The dimensions of information sharing related to export and import at present are the following:

i) Business to business

ii) Business to customs in exporting country, and

iii) Business to customs in importing country

The fourth dimension, i.e., customs to customs sharing of information is equally crucial. The fourth dimension would complete the loop of information sharing, thereby ensuring the accuracy, security and validation of information that is held between all the partners in the quadrilateral loop – i.e.

the exporter, customs administration (export), importer and customs administration (import). It is pertinent to note that ensuring information integrity is as important as safeguarding supply chain integrity.

For standardisation in information exchange to succeed, it is critical that customs administrations should have complete freedom and flexibility in embracing standards for cross border exchange of information. Without the key features of autonomy and flexibility, the customs administrations may not volunteer to engage in information sharing. Moreover, the information exchange needs to be cost effective and beneficial and standardisation should promote usability, reliability and replicability, such that readiness to exchange information with one customs administration would automatically ensure readiness for exchange with all other customs administrations who are signatories to the standards. Further, the mutual concerns on privacy, confidentiality and security need to be fully addressed for information to be exchanged, using legal safeguards and IT expertise.

Given the foundations of e-connectivity, e-commerce, e-services and the level of IT maturity in the customs administrations as well as in international trade, there is a strong business case for standardised exchange of information between customs administrations. Information sharing has the potential to usher in a seamless, paperless and secure supply chain and thus can contribute to tangible benefits at minimal cost to both trade and customs.

From an Indian perspective, Indian customs has entered into more than 50 international agreements which envisage some form of exchange of information. The growing numbers, coupled with lack of standards had an adverse impact on the cost and time of implementation of electronic exchange of information. Despite the fact that Indian customs had been engaging with other customs administrations for the last 7 to 8 years to establish a system of sharing/exchange of information, the efforts are yet to bear fruit. The challenges in this endeavour are that export, transport and import procedures are not fully harmonised across various countries, and information captured on these procedures and processes is also not uniform. For instance, the trader status information including amendments, suspension, and revocation may vary from country to country. Similarly, the way valuation or origin information is captured and stored may vary from country to country. The international community is yet to arrive at common global standards and the legal framework that enables sharing of information.

From the experience so far, for international information exchanges to succeed in the Indian context, the following would appear to be the necessary conditions.

- Given the varying levels of interest and emphasis of countries on revenue, regulation, enforcement, facilitation, supply chain integrity, risk management, security, terrorism, drug trafficking, counterfeiting, health and environment in relation to their expectations from information sharing, there should be a clear understanding and articulation of the objectives of the information exchange vis-à-vis each country with which information exchange is proposed to be undertaken.

- The practical benefits in terms of additional advantage in receiving data from other customs administrations, with regards to improving the facilitation, risk management and enforcement functions of the CBEC, have to be qualitatively and quantitatively assessed. The projects of information exchange cannot progress unless there is clear and identifiable benefits that could be derived out of data exchange by the end users – RMD, DRI, DoV, and customs houses.
- The international information exchange project requires dedicated resources and manpower. The resources include software (i.e. customised applications for linking export data with import data and vice-versa and disseminating or making it available to end users and transmission of data to other countries as per mutual agreements), hardware to support the volumes of data that is received/transmitted and, equally importantly, committed human resources to implement these projects.
- There should be clear administrative responsibility with regards to who would be in-charge of facilitating the transmission, access and storage of data exchanged and utilising the data to meet the objectives of each end user.
- The CBEC has to adopt a policy framework for international data exchange, in conformity with international standards. The administrative responsibility related to policy formulation, legality, transmission and utilisation of data has to be clearly delineated. A standard process for handling such projects, including a cost-benefit analysis from the end-user's perspective, the respective roles and responsibilities of officers connected with data exchange and the manner of utilisation of data received from other customs administrations, need to be clearly specified.
- The Directorate of Systems and the end users, i.e., customs houses, RMD, DRI, DGoV, DGICCE and Board should co-ordinate and work in an integrated manner with international partners to expedite current projects.
- There should a concerted effort towards capacity building of end users in use and integration of cross border information flowing from other customs administrations into their day-to-day functional domain.

VIII.4.u HR and People development

Capacity development in the various areas we have dealt with above cannot happen unless there is a concerted and long-term action taken for the purpose. And this requires patient and well directed efforts. The CBEC will have to develop multi-year plans for building, sustaining and renewing these capacities in the context of the overall strategic plan and vision that we referred to in the beginning of this report.

In Chapter IV of the TARC's first report, we have dealt with the people function extensively, identifying current weaknesses, and outlining the course for improvement. If those recommendations are implemented a number of the issues will be addressed.

The CBEC needs to revisit its transfer policies that prevent specialisation, dilute accountability and affect its performance. It needs to address the issue of people development in a properly constructed competency framework. The National Training Policy, 2012, (DoPT) suggests a competency based approach for training. Competencies encompass knowledge, skills and behaviour, which are required in an individual for effectively performing the functions of a post. The fundamental principle of the competency framework is that each job should be performed by a person who has the required competencies for that job. The training plan needs to address the gap between existing and required competencies and provide opportunities to the employees to develop their competencies. A competency is measurable or observable knowledge, skill, and ability that contribute to successful job performance.

The competencies can be categorised as behavioural or technical. Behavioural competencies refer to values and behavioural skills that support successful performance for specific jobs throughout the organisation. These competencies generally refer to the way a person acts, thinks or feels and are products of personal motives, traits and self-image. Technical competencies refer to the technical knowledge, skills and abilities that are relevant to specific jobs across the organisation. Technical competencies are usually acquired through specific learning or work experience in applying the knowledge and skill.

In a competency-based approach to HR and training, the underlying principle is that organisational performance will result from having the right people in the right jobs with the right skills and abilities. As noted in the TARC's first report as well as in this chapter, there is a need for substantial competency building of all levels of the customs organisation in order to promote high levels of professionalism. NACEN will need to substantially upgrade its curricula and training methodology with greater infusion of technology and widening of its training coverage. It will also have to build capacity for delivery of training to all levels in emerging areas of customs administration. For this, it needs to build greater linkages with its counterpart in advanced customs administrations and also relevant institutes in India. It should also work towards accreditation and aspire to grow into a customs university of international standing. The CBEC will also need to back that vision and work towards that.

There is a huge skill gap at the operating level in customs because the capacity of the NACEN to deliver trainings to Groups B and C officials is woefully inadequate. As a result, officers and staff are assigned to jobs without any formal training to prepare them for discharging their responsibilities. This is a grave risk to the organisation both from the service delivery and enforcement perspectives. Therefore, substantial capacity building is required for the NACEN, putting adequate faculty and staff at regional training institutes. Arrangements needs to be made in collaboration with the armed forces or police institutes for providing arms training to officers and staff of these levels. Looking at the numbers to be trained, NACEN should embark on e-training, virtual classes, webinars, etc so that the training coverage is enlarged and delivered at the place of work. Adequate infrastructure and allocation of financial resources will be part of this capacity building.

There are frameworks for capacity building available specifically tailored to the customs context. One such programme is the WCO's Columbus programme that has been used by many customs administrations.

VIII.4.v WCO Columbus Programme

In view of the changed global trade environment, the WCO has initiated a number of capacity building programmes and activities. The most significant is the Columbus Programme, Aid for SAFE trade. The aim of the Columbus Programme is full implementation of the SAFE Framework of Standards, and other WCO conventions and instruments, as well as best practices in the area of customs administration.

The Columbus Programme is a three-phase programme to provide a comprehensive response to the capacity building needs of WCO members. It is intended to deliver a standardised approach to identifying customs capacity building needs and develop solutions tailored to a country's reality based on gap analysis. It incorporates linkage to WCO instruments, tools and best practices in different key areas which include the following:

- Organisational Development Package
- Customs Capacity Building Diagnostic Framework
- WCO Capacity Building Development Compendium
- Leadership and Management Development Programme
- Orientation Package for Decision Makers
- Guidelines for AEO Implementation
- Risk Management Compendium
- Integrity Programme

Phase I involves a comprehensive diagnostic "needs" assessment of the current situation in a customs administration. It uses the WCO's diagnostic framework tool that has been widely acknowledged. A diagnostic study is carried out by capacity building experts through interviews with all concerned parties, including the members of the trading community. The outcome is a diagnostic report covering the current situation, a gap analysis to full implementation and the suggested way forward through a number of recommendations.

Phase II is the planning and implementation phase and the WCO assistance includes

- support in preparation of an overall customs modernisation plan or specific project action plans
- support in the development of project proposal and business cases for submission to stakeholders and potential donors

- support in preparing and conducting pilot projects towards sustainable implementation of modernisation initiatives
- support to identify possible sources of financial support, where needed

Phase III is the monitoring and evaluation phase that looks at the progress achieved in the context of the individual administration, taking into consideration unique conditions and environment. Using a programme monitoring methodology developed by the Capacity Building Directorate of the WCO, Phase III seeks to achieve several specific objectives. These include

- evaluation of the implementation of Phase 1 recommendations
- evaluation of the overall progress achieved in terms of modernisation at a point in time
- evaluation of the results of the key actions taken to achieve this progress
- assessment of the manner in which the reform has been conducted and managed
- issue recommendations to improve the continued modernisation efforts, and
- identify lessons learned to apply to future implementation

It also evaluates the progress of the implementation of key WCO standards and recommendations, namely the SAFE Framework of Standards, Revised Kyoto Convention standards prioritised by the member, as well as other relevant conventions, instruments and standards.

It is reported that under the Columbus programme, WCO has completed 122 diagnostic missions under Phase I, supported over 110 members in Phase II and completed Phase III in respect of 5 members with more being planned.

It is learnt that the CBEC had participated in the programme and WCO had carried out a comprehensive Phase-I Diagnostic study of Indian customs sometime in the Year 2005-2006. Its fate is not known. Considering the clear need for capacity building, the CBEC would do well to pick up the thread and revisit the study then conducted, update it to meet contemporary conditions and proceed further in a systematic manner in its capacity building efforts.

VIII.5 Summing up

In the face of the increasingly globalized world, custom today face multidimensional challenges. One the one hand, globalization, while affording opportunities for economic growth also provides opportunities for trans-border crimes. Customs, being at the frontline of the border have to play an important role in the country's physical as well as economic security. At the same time, they have to facilitate legitimate trade so as not to impair the country's competitiveness and attractiveness as an investment destination. The steady growth of international trade leading higher volumes and the emerging trends such as increase in regional trading arrangements etc., e-commerce, changing supply chain dynamics etc. are adding to the challenges faced by customs. These trends necessitate creation of new capacities in diverse areas without necessarily increasing the human resources. The demand on customs, therefore, is to do more with less.

To face this challenge, Indian customs would need to move away from their traditional administrative approach towards a more proactive and wholesome compliance management approach. They would need to transform their governance, change their control paradigm and become a highly technology driven organization with a robust and reliable risk management based approach to governance. They will have to move away from excessive revenue orientation to be able to fulfil their mandate in relation to areas such as supply chain security, effective implementation of their responsibilities in trade related areas, IPRs, OGA requirements etc. and play a much more proactive and prominent role in trade facilitation. Hence their compliance philosophy needs to be oriented towards promotion of voluntary compliance based on a trust based approach towards the compliant trade coupled with very effective enforcement against non-compliance.

This will require large investments in capacity building in human capital as well as physical and technological infrastructure. Trade facilitation in particular will need capacity building not only in customs but also in other regulatory agencies. By virtue of their strong background in cargo processing and high international alignment of customs processes, customs need to be given a lead role to achieve inter agency harmonisation and coordination in this area.

To enable the transformative changes that are required, the government needs to empower and enable customs by according the CBEC functional and financial autonomy as recommended in the TARC's first report, subject, of course, to the restructuring and accountability as also recommended in that report.

VIII.6 Recommendations

The TARC recommends:

i) Governance

a) The CBEC should immediately commence work on the development of a customs vision and strategic plan, setting out the strategic goals and the implementation strategy that will ensure its place among "best in class" customs administrations. The strategy must enhance customer focus and proactively promote voluntary compliance and should include measures like customer guidance in the form of self-assessment check-lists, manuals containing standard operating procedures and fully updated, user friendly and reliable website. Active guidance should be provided to importers through lucid and detailed publications furnishing detailed guidance about the valuation regime. (Section VIII.4.a)

b) The implementation will have to be backed by a robust performance management framework to enable the CBEC to measure the progress and benchmark itself with best international practices in the spirit of continuous improvement. (Section VIII.4.a)

c) The CBEC should aim at developing systems, structures and processes that ensure a consistent and uniform response across the organisation whether in the area of customer services or enforcement. The strategy should reflect the changing role of customs beyond exclusive

revenue orientation and focus on capacity building in emerging areas of importance. (Section VIII.4.a)

d) The control paradigm must shift from high levels of pre-clearance interdictions to intelligence-led, risk-based interventions by exception, supply chain management and post-clearance audit. (Section VIII.4.a)

e) The CBEC needs to develop an enterprise wide risk management framework in the context of which tools like the RMS need to be operated. The spirit of the compliance management philosophy that underlies the principle of self-assessment needs to be internalised in the organisation. (Section VIII.4.a)

f) The Risk Management Division should be strengthened. The risk management module for container selection needs to be integrated with the CBEC's other operational systems. The CBEC should progressively move away from a local approach in risk management to a strong national approach and move towards setting up a national targeting facility such as the ones set up in the US, Australia and New Zealand. (Section VIII.4.d)

g) In critical areas, identified on the basis of analysis and other evidence, the CBEC needs to undertake compliance improvement plans, implement them effectively, measure and evaluate results as feedback and continue the process in a cyclical manner. (Section VIII.4.a)

h) The CBEC needs to build capacity for more meaningful contribution to trade policy, based on credible research and analysis. (Section VIII.4.c)

ii) Customs core clearance processes

i) The CBEC should revamp its core clearance process and aim at aligning with the best international practices to ensure that cargo moves seamlessly through Indian ports and airports and build substantial capacities in the area of post-clearance audit. It should abandon the "gate-keeper" approach underlying the current control mechanism as it is ineffective and promotes rent seeking. (Section VIII.4.a)

j) The CBEC should move to a model of centralised assessment for compliance verification, adopting the centres of excellence concept. There needs to be a thrust on full digitisation of the processes, dematerialisation of the documents and documents management system. (Section VIII.4.c)

k) The regime of advance filing needs to be effectively implemented ensuring high data quality. (Section VIII.4.c)

l) Greater capacity in the form of adequate skilled and expert resources needs to be developed for the post-clearance audit. The results of audit need to be fed back into the risk management. Audit should also pay attention to data quality. (Section VIII.4.c)

m) Related party transactions should be handled as part of post-clearance audit and the Directorate of Valuation should be strengthened to become a centre of excellence in this area by building strong expertise. (Section VIII.4.c)

n) The automation of international express cargo and international post-offices should be expedited. (Section VIII.4.e)

o) Development of advanced passenger information system (APIS) incorporating modern identity management and entity analytics solutions should be fast-tracked. (Section VIII.4.f)

p) Capacity building through extensive training and close engagement with the industry is also needed in the area of IPR. (Section VIII.4.r)

iii) Enforcement and anti-smuggling

q) Greater capacity needs to be built in customs to counter trade based money laundering by greater use of analytics and strong co-ordination among the DRI, RMD, FIU and Directorate of Enforcement. (Section VIII.4.c)

r) To motivate officers in anti-smuggling operations in remote areas, a package of special facilities should be developed. (Section VIII.4.o)

s) Specialised training facilities for anti-smuggling operations, tailored to specific requirements, should be created. (Section VIII.4.o)

t) There is need for greater infusion technological and analytical capacities in enforcement functions. Stronger focus is required on prosecutions in cases of commercial frauds. (Section VIII.4.o)

iv) Technology and logistics

u) The CBEC should commence work on building a new generation system to replace the current ICT systems. There should be extensive reliance on service oriented architecture in designing the new system and it should ensure interoperability of customs and other agencies involved in border management, a fully distributed, open, wireless and mobile operational environment and solutions for structured and unstructured data. The system must enhance the ability of customs and other entities to work together. (Section VIII.4.l)

v) Customs should leverage the adoption of the emerging "internet of things" by the logistics industry to real-time tracking of movement of goods across the supply chain, including to CFSs, ICDs, SEZs etc. and eliminate dilatory, costly and unreliable paper based processes. (Section VIII.4.l)

w) The process of induction of non-intrusive inspection technologies such as container scanners, X-Ray scanners, etc., needs to be expedited. (Section VIII.4.l)

x) A strong capacity for an innovative adoption of latest technologies through experimentation and pilots needs to be created. (Section VIII.4.l)

y) Recruitment of crew for the recent acquisition of 109 modern patrol craft needs to be expedited. Similarly, expedited action should be taken for operationalising the telecommunications set up. (Section VIII.4.l)

z) The Directorate of Logistics needs to be strengthened and the required expertise in technology, procurement and contract management needs to be created and sustained in the directorate. It should regularly engage with industry and technical institutions to keep its knowledge current. (Section VIII.4.l)

v) SAFE framework and trade facilitation

aa) There should be clear ownership on the part of the CBEC of the facilitation programmes undertaken by it. It should undertake immediate steps to achieve the facilitation targets set out in its own circular dated September 2, 2011. (Section VIII.4.j)

bb) The CBEC needs to take a robust and pragmatic view in relation to the denial of ACP status to clients on account of show-cause notices and should not deny such status to other wise compliant clients where there is no wilful fraud or evasion. (Section VIII.4.k)

cc) The CBEC should follow best international practice by regularly undertaking and publishing time release studies. (Section VIII.4.g)

dd) The CBEC should be enabled, through appropriate administrative and legal empowerment, to play a leadership role among the various border agencies to ensure proper co-ordination at the border. ensure trade facilitation, allow greater participation of all agencies in a common risk management framework and enable the development and implementation of a single window (Section VIII.4.h)

ee) The SAFE and AEO programme need greater visible commitment from the CBEC and there needs to be much greater communication of the benefits of the programme among stakeholders to induce them to join the programme. (Section VIII.4.j)

ff) The CBEC needs to revisit the AEO programme to align it better with different needs of different players in the supply chain and create better incentives for improving compliance. (Section VIII.4.k)

gg) The CBEC needs to create institutional mechanism for direct engagement with senior management in trade and industry. (Section VIII.4.g)

hh) The CBEC needs to undertake review of key business processes in the spirit of continuous improvement to simplify and streamline them. (Section VIII.4.c)

vi) RTAs and trade remedies

ii) A Directorate of Origin should be set up in the CBEC to handle RTA related issues. It should develop specialised expertise on rules of origin and related areas. (Section VIII.4.p)

jj) Posting of customs officers in the Directorate General of Anti-dumping will ensure enhanced co-ordination and better management of anti-dumping measures. (Section VIII.4.q)

kk) The Directorate of Safeguard needs to be strengthened and should be enabled to play a more proactive role in the propagation of safeguard measures in industry, particularly among SMEs. (Section VIII.4.q)

ll) There is need to develop non-preferential rules of origin to ensure proper application of anti-dumping and safeguard measures. (Section VIII.4.q)

vii) International co-operation

mm) Directorate of International Co-operation should be created and adequately staffed in view of the high importance of international co-operation in customs functioning. A clear framework needs to be created for international data exchange and dedicated resources assigned. (Sections VIII.4.s and VIII.4.t)

nn) In consultation with the relevant ministries, the CBEC should initiate a programme for cross-border co-operation with India's neighbours, which can lead to joint border control as envisaged in the Revised Kyoto Convention. This can begin with an institutionalised arrangement for regular border meetings between designated customs officials to deal with day-to-day operational issues that create difficulties for trade. (Section VIII.4.i)

viii) Capacity building

oo) The CBEC needs to revisit its transfer policies that presently prevents specialisation, dilutes accountability and affects its performance. It needs to address the issue of people development in a properly constructed competency framework. (Section VIII.4.u)

pp) Urgent steps are required for bridging the skill gap of Groups B and C officials through effective training and competency building. (Section VIII.4.u)

qq) NACEN needs to substantially upgrade its curricula and training methodology with greater infusion of technology and widening of its training coverage. It will also have to build capacity for delivery of training to all levels in emerging areas of customs administration. (Section VIII.4.u)

rr) NACEN should embark on e-training, virtual classes, webinars, etc so that the training coverage is enlarged and delivered at the place of work. Adequate infrastructure and allocation of financial resources will be part of this capacity building. (Section VIII.4.u)

ss) The CBEC should consider undertaking capacity building by joining the WCO's Columbus programme, which is specifically tailored for customs capacity building. (Section VIII.4.v)

Chapter IX

Information Exchange

IX.1 Need for Information Exchange

Tax administrations are data and information centric.[116] Data and information generation is proliferating at an unprecedented pace and volume. The adoption of information and communications technology (ICT) by tax administrations has helped in the collection, analysis and management of large volumes of data and information, providing a big opportunity for the tax administration to improve tax compliance and ensure better enforcement. This opportunity, however, has also presented the tax administration with challenges as data is being generated incessantly and in increasing volumes by different agencies, often disconnected and scattered. Data and information are never static in terms of sources, complexity and frequency. This is because the different agencies generating data or information do so for different purposes and uses. A key objective for any tax administration, therefore, is to identify data sources, collect data and make meaningful use of it for its own work such as increasing revenue collection, optimising operational capability, managing new risks and enforcing compliance.

Despite the flood of data, tax administrations find it daunting to identify the source and use what they require. Data are often unreliable as they may not be accurately sourced, complete, relevant or integrated. Consequently, tax administrations face challenges in making timely, information-driven information and in achieving compliance. The quality of data and its maintenance underpin their relevance. It is, therefore, of utmost importance to institute a robust mechanism by encouraging inter-agency partnerships and co-ordination to assure data quality, which would ensure their relevance. Processes and technology need to be designed to bridge the gap between disconnected agencies, so that they leverage existing management and governance structures.

The success of data-driven tax administrations is thus contingent upon their ability to adopt an approach that would enable them to leverage sourcing of data from different agencies, transcending organisational boundaries. Such an approach would not only require co-ordination and standardisation for data exchanges within the same agency but also across different agencies. Working across structural and functional boundaries of different agencies is possible only when these agencies agree on not only what is important, but also share a common vision and commitment to its achievement. This requires adherence to the whole-of-government approach. This approach would help all agencies to work in sync with each other and respond to changes more effectively. A disjointed approach, on the other hand, is more expensive and results in loss of time in collecting data that another agency has already collected

[116] Data is a value or set of values representing specific parameters. Data becomes information when analysed and can provide meaning and context when combined with other data. Information thus results from adding value to data.

and from which it can easily be sourced. This will also ensure the authenticity, accuracy and credibility of the data as the data will be collected in the normal course of business by an agency, and not necessarily by the tax administration itself. It also benefits taxpayers, who have to file information just once rather than having to provide the same information several times to different agencies.

The seamless flow of information across agencies in a structured manner, therefore, is required for exchange of data and information. Countries have adopted various collaborative mechanisms for such inter-agency exchange of data and information. These exchanges are mandated by law in the form of statutes in some countries. Various inter-agency partnership agreements, memoranda of understanding (MoUs), statements of practice, standard protocols, etc., supplement laws to ensure exchange of data or information. The flow of information depends upon the nature of information requested or required, purpose of requests, agency requesting information and the agency which holds the data or information. Tax administrations have benefited from these organised data and information exchanges through a significant reduction in the cost and time involved in collecting the data afresh. The exchange ensures data accuracy, which results in increased compliance by the taxpayers and ultimately improves voluntary compliance.

IX.2 Current status

Both the CBDT and CBEC collect enormous amounts of data on a daily and regular basis in respect of different tax entities – individuals, business firms, companies in the course of their normal business. Data collected by them is transaction data as well as accounts data. Apart from that, they also receive third party information on certain transactions.

The CBDT collects information mainly through the annual information return (AIR), the Central Information Branch (CIB) and under the automatic and spontaneous exchange of information from foreign jurisdictions. Information is also collected under special and pilot projects by the Directorate of Intelligence and Criminal Investigation (DI&CI). Other sources of information are the Suspicious Transaction Reports (STRs) received from the Financial Intelligence Unit (FIU) and Tax Evasion Petitions (TEP) from individual agencies, etc. Such specific information is verified with the CIB and AIR information received or by comparing them with information collected from other sources. Verification is done according to the relevant CBDT instructions.

The Customs EDI System (ICES), operational at 116 locations, and the Automation of Central Excise & Service Tax (ACES) at all locations form the backbone of the entire automated network for the CBEC. ICES handles nearly 98 per cent of India's international trade in terms of import and export consignments. ICES interacts with trade, transport, banks and other regulatory agencies through online, real-time electronic interface for customs clearance of import and export cargo through ICEGATE, the e-commerce gateway for customs.

Data collection for excise duty and service tax has been automated through ACES. But, it is not connected to any other related agency by way of data/information sharing, except with designated banks through which duties and taxes are collected by the department via the

electronic payment system of CBEC, called the Electronic Accounting System in Excise and Service Tax (EASIEST).

Mechanisms of data collection by the two Boards, the CBDT and CBEC, along with other entities in the Finance Ministry and by outside agencies are summarised below.

IX.2.a Central Board of Direct Taxes (CBDT)

The Income Tax (I-T) Department uses several ways and means to collect, collate and disseminate data from different sources, both domestic and international. Domestic sources, such as the taxpayer, local authorities, registrar of companies, registrar for properties registration, stock exchange, Reserve Bank of India (RBI) and various depositories are obligated under Section 285BA of the I-T Act, 1961, to furnish AIR to the I-T Department on specified financial transactions.[117] Under this legal obligation, these agencies are required to submit information in respect of specified financial transactions within a stipulated time, in a manner prescribed by Rules 114B to 114D of the I-T Rules. The CBDT has notified the National Securities Depository Limited (NSDL) as the prescribed agency to receive AIR from the specified persons. At present, seven categories of persons are required to compulsorily file AIR, namely, banks accepting cash deposit of Rs. 10 lakh or more in a year from any person, bank or company issuing credit cards where payment against bills exceeds Rs. 2 lakh in a year for any person, mutual funds collecting Rs. 2 lakh or more for sale of units by any person, a company receiving Rs. 5 lakh or more against issue of shares, a company receiving Rs. 5 lakh or more against issue of bonds/debentures, registrar/sub-registrars in respect of sale/purchase of immovable property exceeding Rs. 30 lakh and the RBI for issue of bonds exceeding Rs. 5 lakh.

The filing of AIR is monitored through the ITD system and notices are issued to non-filers/late filers and to filers who file defective AIRs for filing rectified supplementary AIRs. In the case of non-filers, penalty is also initiated under Section 271FA of the I-T Act. During FY 2012-13, notices were issued in 1,467 cases for defective AIRs and in 3,878 cases for non-filing of AIRs. Penalties were imposed in 225 cases. In cases where PAN data is not available, CBDT issues query letters to the transacting parties and populates PAN in the AIR data. In case the transacting parties do not have PAN and they declare so in prescribed Forms 60 and 61, this information is digitised for further analysis and used for widening the taxpayer base. During FY 2012-13, CBDT issued 2.49 lakh query letters and based on the response from it, PAN in 35.5 per cent cases were populated. In more than one lakh cases, letters were issued to field functionaries for verification of AIR data not having PAN.

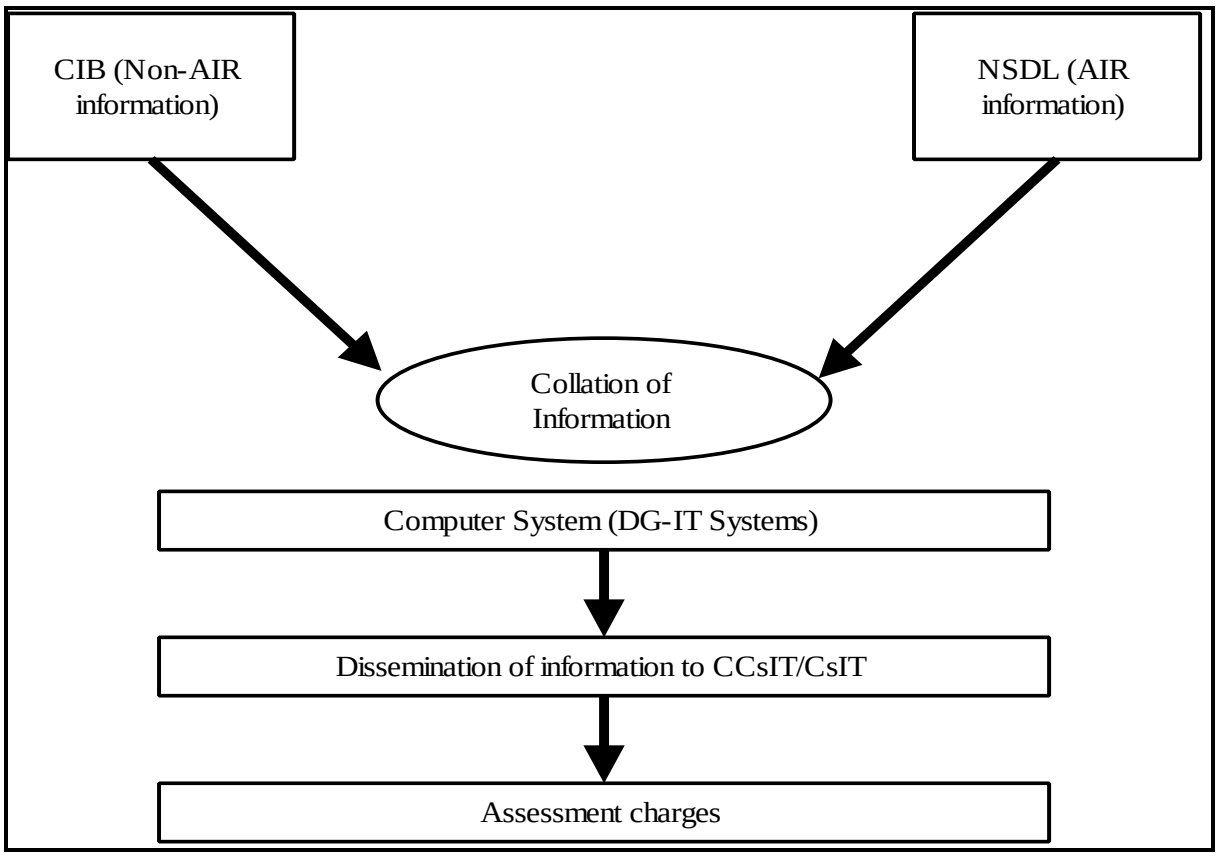
Third party information from internal as well as external sources, in addition to the AIR mechanism, is collected through the CIB by the I-T Department. The legal force for collection of information by CIB is through instruction no.1759 dated June 11, 1987, revised vide

[117] CBDT circular no.7/2005, dated August 29, 2005, prescribes that AIR is to be filed in terms of Rule 114E by the "specified persons" in respect of those 'specified transactions' which are registered or recorded by them during a financial year.

instruction no. 1874 dated January 7, 1991. CIB collects information from 40 internal and external source codes of which 12 are compulsory. This information is on financial transactions like investment, expenses, payment of taxes, etc., and details of persons involved in these transactions. CBDT has made PAN quotation compulsory under Rule 114B of the I-T Rules for these transactions. During FY 2012-13, CIB collected 20.07 crore pieces of information pertaining to CIB codes from different organisations. CIB data is analysed through the Enforcement Information System (EFS) of the present ITD system. This has been explained further in Appendix IX.1.

Diagram 9.1 schematically shows the flow of AIR and CIB information into the ITD system of the I-T Department. DG (Intelligence & Criminal Investigation) in CBDT is in charge of collecting, collating, cleaning, and disseminating AIR and CIB information to field functionaries.

Diagram 9.1: Flow of AIR and CIB information into the ITD system



The FIU is the nodal agency responsible for receiving, processing, analysing and disseminating information on suspicious financial transactions (STRs). These STRs are also passed on to the CBDT. The CBDT is reportedly the largest recipient of STR reports. Such reports also include cash transaction reports (CTRs). Until October 20, 2012, these STRs were being received from the FIU in physical/paper form; after October 20, 2012, the information dissemination to the CBDT is online through FINnet, a network between reporting agencies and the FIU for exchange of information and submission.

Apart from the above mentioned means of regular data collection under the specified codes of AIR/CIB, field functionaries in the CBDT also collect information under statutory provisions.[118]Special projects have also been taken up for collection of such information. In these special projects, data is gathered and analysed by the Directorates of Investigation of CBDT and actionable cases are identified and then shared with field authorities to initiate statutory action on them.

Specific information, regularly collected by the assessing officers under Section 133(6) of the I-T Act, on specified transactions from third parties, related or unrelated persons, in a prescribed format is not placed in the computer system for verification; consequently, vital information is often not systematically used. This also holds true for investigation directorates, who often collect information in large volumes but due to the lack of an institutional mechanism, this information is used only for the limited purpose at hand rather than being systematically shared for larger departmental work.

The CBDT also collects information online on a regular basis on TDS data and this has cast a legal obligation on tax deductors to submit quarterly data in Form 26QAA. This data is received by the CPC-TDS at Ghaziabad and is matched online with tax collection statements received from banks. The CBDT has also facilitated online submission of Form 15CA/CB in the case of foreign remittances. These data are seen, and often scrutinised, by the international taxation divisions for verification of tax payments on those remittances.

To handle taxation issues arising from cross-border transactions and transfer pricing, the Competent Authority under Article 26 and 27 of the Double Tax Avoidance Agreements (DTAAs) receives and sends information to foreign tax jurisdictions. Separate Tax Information Exchange Agreements (TIEAs) have also been entered into by India lately with nine low/no tax jurisdictions and another thirty-seven are at various stages of negotiation. The information received under the TIEAs can be disclosed to other authorities with the written consent of the Competent Authority of the other country. A dedicated Exchange of Information Cell has also been created within the CBDT to facilitate exchange of information in a faster and more meaningful manner. The basic legal framework for exchange of information under TIEAs is provided for in Article 5, *Exchange of Information upon Request*, of the TIEAs, which obliges the Competent Authority to provide information relevant to tax administration. India thus receives information from foreign tax jurisdictions under automatic/spontaneous exchange of information. Automatic exchange of information is periodic transmission of bulk taxpayers' information for fees for technical services, dividends, interest, royalties, salaries, pensions, etc., and spontaneous exchange of information is done on request-and-offer basis. A short note on the methods of international exchange of information is given in Appendix IX.2.

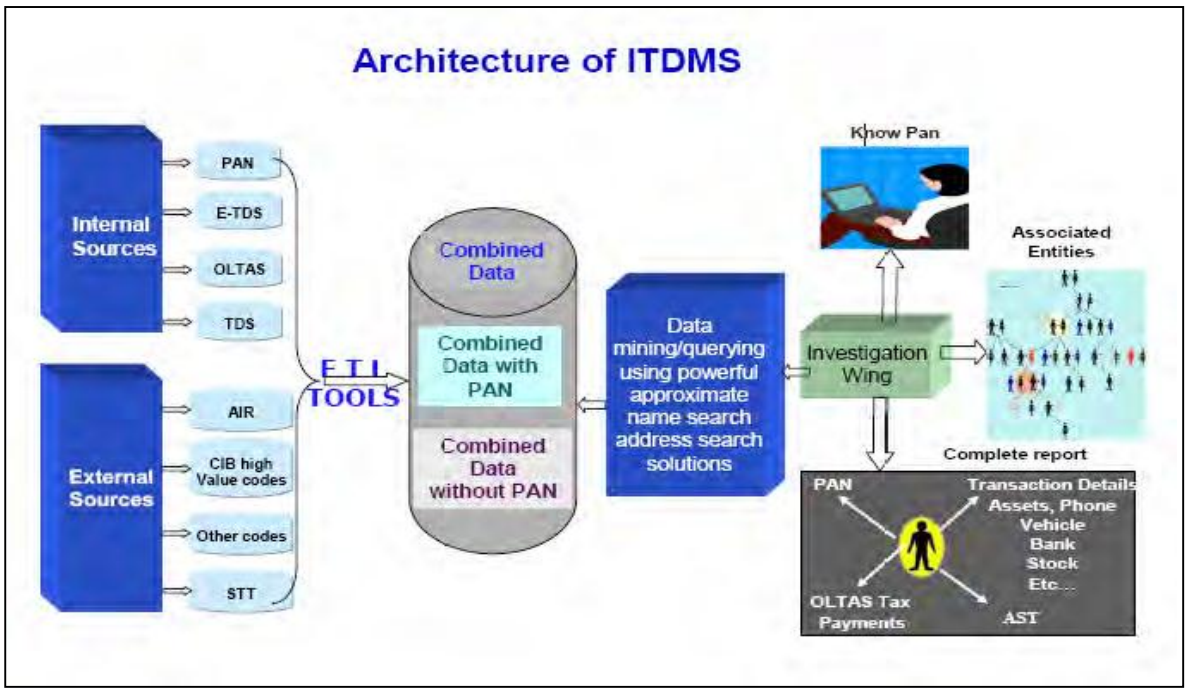
Integrated Taxpayer Data Management System

In 2009, the investigation wing of the I-T Department developed a data mining method – Integrated Taxpayer Data Management System (ITD-MS). This was intended to centrally

[118] Section 133B and Section 133(6) of the I-T Act in specific cases from banks

manage data collected from internal and external sources. Prior to this, data collected were at different platforms, which did not allow the investigation wing of the I-T department to effectively work out its enforcement objective. The lack of a standard format for storing names and addresses in multiple large databases with a large volume of records – 20-50 million – did not allow a single parameter that would enable search activities. Since internal data was not being utilised fully, the investigation wing of the I-T Department was dependent upon informers, tax evasion petitions from the public, etc. But these practices were invasive, and often open to misuse. The challenge was to convert such large amounts of information into actionable intelligence and correlate the huge volume of information on financial affairs with returned incomes/tax payments. A solution was thus developed through which a search tool could handle variations in parameters such as name, address and date of birth while dealing with large data volumes and rank these results so that the best results could be arrived at. It was also important that the response time was in milliseconds for it to be efficient. A schematic diagram for such a solution, called ITD-MS, is given in Diagram 9.2 below.

Diagram 9.2: Schematic diagram of Integrated Taxpayer Data Management System



Source: Department of Administrative Reform, Government of India.

The ITD-MS generated a 360-degree profile of an entity by compiling information on a dynamic basis from all data sources to track tax payments. This system created a family tree of the person in the case of an individual taxpayer and linked the information to any entities in which the taxpayer had a financial interest. The ITD-MS proved beneficial in tracking tax evasion by high net worth individuals. Since this large data mining system was developed by the investigation wing, it was used only by the Directorates General of Income Tax (Investigation) and not by other field formations despite this database being in operation for three years.

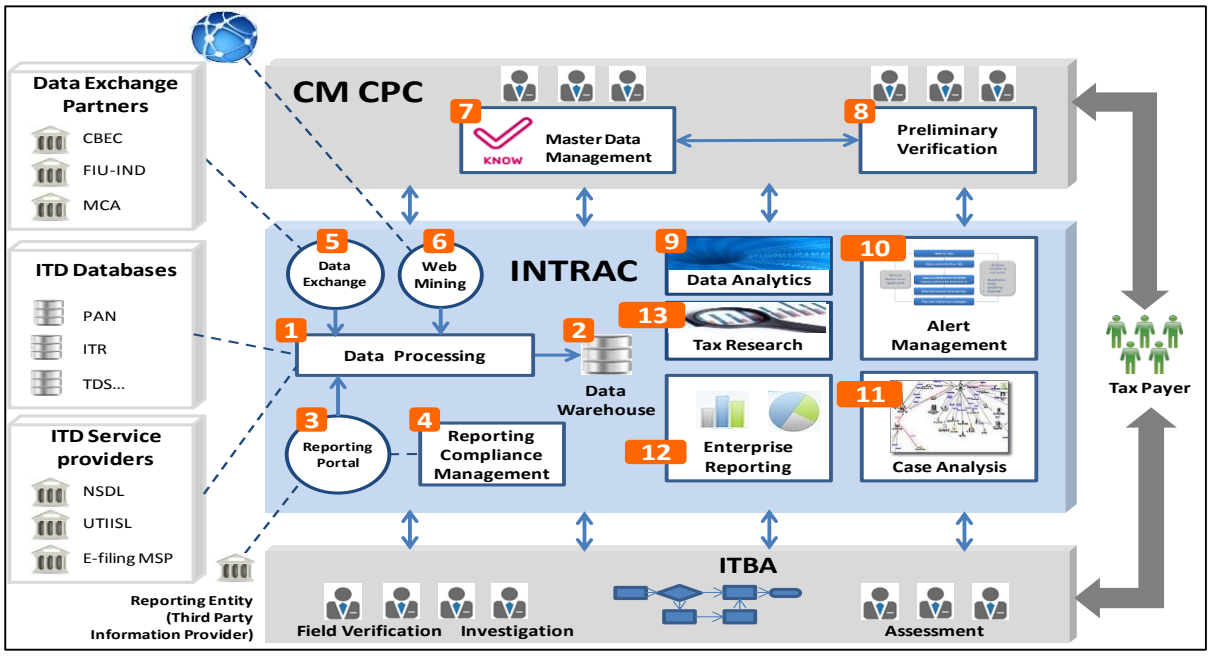
Data warehouse and Business intelligence (DW& BI)

The I-T department has initiated a project on DW & BI to strengthen the non-intrusive information driven approach to improve compliance and effectively utilise information in all areas of tax administration. The objectives of the project are:

- Widening the tax base
- Deepening the tax base
- Improving compliance with tax laws
- Detect fraud and leakage of revenue
- Supporting investigation
- Increasing effectiveness of tax collection
- Enhancing co-operation with exchange partners
- Generating enterprise wide reports
- Monitoring high risk scenarios
- Providing inputs for policy making

A schematic diagram of the proposed DW & BI is given in Diagram 9.3 below.

Diagram 9.3: Schematic diagram of DW & BI



Source: DGIT (Systems), CBDT

The project aims to integrate enterprise data warehouse,[119] data-mining, web-mining, predictive modelling, data-exchange, master data management, centralised processing, compliance risk management and case analysis capabilities. A Compliance Management

[119] Data warehouse is also referred to as data mart.

Centralised Processing Centre (CMCPC) is also being set up under the project to handle resource-intensive, repetitive tasks and ensure optimum resource mobilisation within the I-T department for high skill work. The project also envisages meeting requirements relating to Foreign Account Tax Compliance Act (FATCA), Common Reporting Standard (CRS) and Automatic Exchange of Information. The project is expected to be rolled out in 2015 and will be operational by 2017.

IX.2.b Central Board of Excise and Customs (CBEC)

The CBEC generates large volumes of data on various transactions. The CBEC has not been procuring data from any outside agency, unlike the CBDT, which has been procuring data under AIR and CIB on a regular basis, as discussed above. The budget for FY 2014-15 provided for Section 15A in the Central Excise Act, 1944, which empowers the CBEC to collect information from specified agencies (on the same lines as under the present I-T Act) for specified periods. Appendix IX.3 gives the data collection mechanism of the CBEC in detail.

The ICES exchanges/transacts customs clearance related information electronically using Electronic Data Interchange (EDI) through message exchanges in prescribed formats. A large number of documents that trade, transport and regulatory agencies (collectively called trading partners) are required to submit/receive in the process of customs clearance are now being processed online. The CBEC also collects information on organised smuggling, money laundering and commercial fraud on customs duty evasion through the Customs Overseas Intelligence Network (COIN).

The Automation of Central Excise and Service Tax (ACES)[120]is the e-governance initiative by the CBEC. It is a software application that aims to improve taxpayer services. Its objective is to strike an optimal balance between trade facilitation and enforcement and to promote a culture of voluntary compliance.

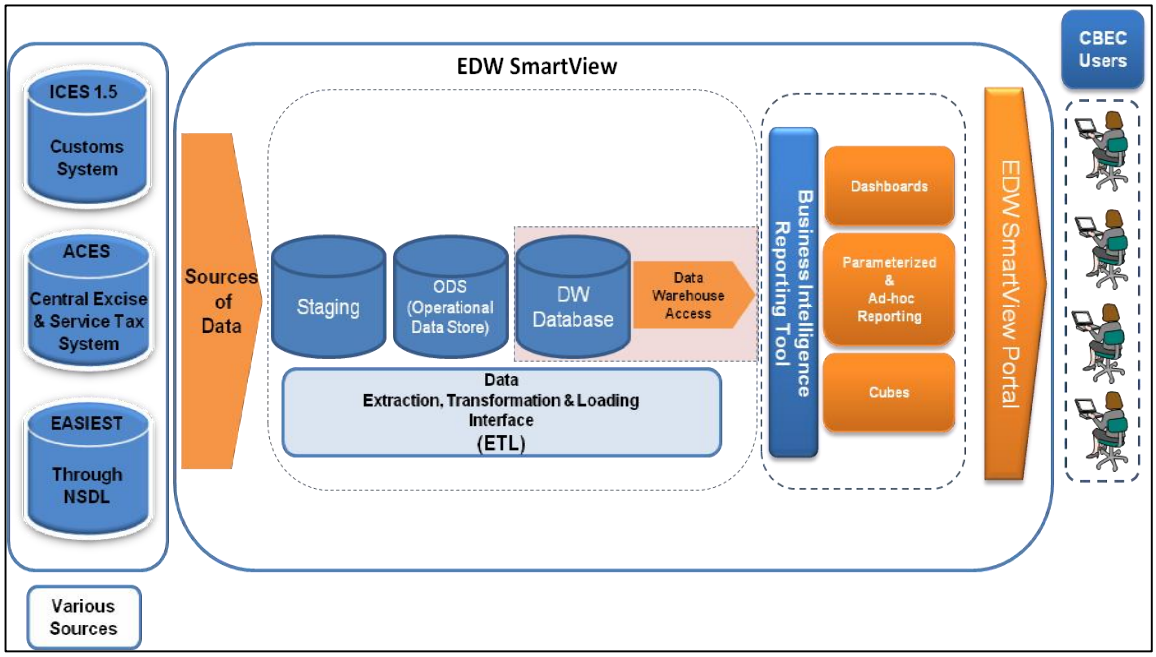
The Directorate General of Central Excise Intelligence (DGCEI), an intelligence organisation under the CBEC, develops intelligence in new areas of tax evasion through its intelligence network across the country and disseminates information in this respect to apprise field formations of the latest trends in duty evasion. The Directorate of Revenue Intelligence (DRI) also functions under the CBEC and is entrusted with the responsibility of collecting intelligence, its analysis, collation, interpretation and dissemination on matters relating to violations of customs laws, and to some extent, anti-narcotics law. It also maintains a close liaison for exchange of information with the World Customs Organization, the Regional Intelligence Liaison Office at Tokyo, INTERPOL and foreign customs administrations.

[120] ICES and ACES have been discussed in detail in Chapter VII of the first report of TARC.

Enterprise data warehouse (EDW)[121]

The Directorate of Systems of the CBEC has implemented CBEC's data warehouse, a web based analytical decision support system that is specifically designed for prompt responses to queries and sophisticated analytical capabilities, using the latest data warehousing technologies. The enterprise data warehouse (EDW) is a centralised repository of the nation-wide data on customs, central excise and service tax. The objective of setting up the EDW was to provide access to a single data repository on customs, central excise and service tax to empower the CBEC's internal and external users to pose queries and report according to their business needs. A schematic overview of EDW is given in Diagram 9.4.

Diagram 9.4: Schematic diagram of EDW of CBEC



Source: DG (Systems), CBEC

The current source systems from which the data is extracted into the EDW are ICES 1.5, which is the online workflow application for clearance of imports and exports in India, for customs data, ACES, which captures the assessees' registration and returns details, for central excise and service tax data, and the EASIEST application that makes available accurate tax payment data. EASIEST data is received in the data warehouse through the NSDL gateway. The customs and EASIEST data is refreshed on a daily basis whereas the central excise and service tax data is refreshed on a monthly basis in the data warehouse.

Departmental users have been provided EDW licences for reporting and analysis purposes. The statistical capabilities of the data warehouse tools serves the statistical and multi-dimensional analytical and reporting requirements of agencies like the Tax Research Unit (TRU), Directorate of Revenue Intelligence (DRI), etc., for the purposes of policy formulation,

[121] The scope of the data warehouse for the CBEC has also been discussed in Chapter VII of the first report of the TARC.

intelligence, risk management, enforcement and monitoring of revenue collection. There is a profusion of data requests from the CBEC and field formations and other ministries, RTI, CAG and Parliament.

Exchange of data between CBDT and CBEC

In January 2014, the CBDT and CBEC had exchanged with each other bulk data on a pilot basis to identify actionable cases and potential cases of data mismatches. This exchange of bulk data was carried out under two pilot projects, namely, CBEC-CBDT Data Exchange for Service Tax (ST-3/ITR) and the Data Exchange (Tax 360). As part of this exercise, the CBEC shared service tax returns data (ST3) on identified fields for FY 2012-13 for two sets of taxpayers – those who had filed their tax returns and those who had not filed their tax returns but had registered themselves for service tax. The bulk matching of these datasets resulted in the generation of additional revenue of approximately Rs.151 crore in service tax and identification of 1.06 lakh cases for further investigation under direct taxes.

The pilot project, Data Exchange (Tax 360), was an initiative to profile a taxpayer across key direct and indirect tax systems and identify potential cases of non-registration and generation of additional revenue through data comparisons across tax systems. As part of the pilot project carried out jointly by the CBDT, CBEC and the Maharashtra sales tax department, CBDT shared 13.65 lakh PAN records pertaining to companies, firms, Hindu Undivided Family (HUF), trusts and proprietors registered in Maharashtra for doing business, tax returns data (ITRs 4,5 & 6) and payments data (OLTAS and TDS) for them for FYs 2008-09 and 2009-10.The authorities in the Maharashtra sales tax department, however, maintain that the quality of data was not up to the mark as the data shared was not consistent and had a number of gaps; hence, the outcome of the pilot project was not as desired.

IX.2.c Other key agencies in the Ministry of Finance

i) Central Economic Intelligence Bureau (CEIB)

CEIB, under the Ministry of Finance, is the nodal agency for economic intelligence and is responsible for co-ordinating and strengthening economic intelligence and enforcement activities of agencies under the Ministry of Finance. According to revisions in its mandate introduced in 2003, CEIB, *inter alia*, is to act as a think tank on issues relating to economic offences and to examine trends on intelligence and the changing dynamics of economic offences, the nexus between anti-national elements, money launderers, drug traffickers, etc., including new *modus operandi* for such offences, and suggest measures to deal with them effectively.[122]The CEIB is also required to ensure real-time monitoring of and effective interaction and co-ordination among various agencies on economic offences. It functions as the clearing house of all economic intelligence and provides a platform for exchange of such intelligence between various agencies with the Department of Revenue and other intelligence

[122] CEIB mandate of 2003 is at Appendix IX.4.

and enforcement agencies, including IB, RAW, CBI, etc. CEIB also houses the COFEPOSA Unit,[123] which deals with preventive detention and related activities.

To achieve the mandated objective of the CEIB, institutional structures and mechanisms have been set up for co-ordination, intelligence sharing and investigation among various law enforcement agencies at the national as well as regional levels. The existing co-ordination mechanism in the CEIB at the national level is brought about by the Economic Intelligence Council (EIC) under the Chairmanship of the Finance Minister,[124] the Working Group on Intelligence Apparatus pertaining to EIC chaired by the Revenue Secretary and by the Group on Economic Intelligence (GEI). At the regional level, the Regional Economic Intelligence Committees (REICs) co-ordinate, as nodal agencies, actions of various intelligence/enforcement agencies of both the central and state governments dealing with economic offences.

The EIC, an apex forum for co-ordination and exchange of information/intelligence on important economic offences, is mandated to consider various aspects of intelligence related to economic security and evolve strategies for effective collection and collation of such intelligence and its dissemination to identified user agencies. It is primarily responsible for facilitating the exchange of strategic information on a real time basis between intelligence and investigative agencies, and regulators.[125] The major issues on which the EIC focuses include the circulation and smuggling of counterfeit currency, tax evasion, illicit drug trafficking, terrorism and organised crime. Besides sharing intelligence, the EIC also reviews measures to combat economic offences and formulate a co-ordinated strategy of action by various enforcement agencies. Apart from these, it advises on amendments in laws and procedures for plugging loopholes to take effective action against economic offenders and reviews measures to combat the generation and laundering of black money. It also approves the strategy for dealing with black money operators and tax evaders. The CEIB acts as the secretariat of the EIC.

At the regional level, CEIB operates through REICs.[126] There are 22 REICs functioning in different parts of the country. REICs are headed by the Director General Income-Tax (Investigation) or the Chief Commissioner of Customs and Central Excise. All investigative and intelligence agencies including the central and state revenue departments and the economic intelligence wing of state police are represented. To make REICs broad-based, heads of RBI, SEBI, registrar of companies, state sales tax department and head of the office of DGFT, wherever posted in the state, have also been included as members in REICs. REICs are mandated to meet once every two months. Information is exchanged either directly between

[123] Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974 (COFEPOSA) provides for preventive detention in certain cases for the purposes of conservation and augmentation of foreign exchange and prevention of smuggling activities and for matters connected therewith.

[124] Other members being Governor RBI, Finance Secretary, Revenue Secretary, Secretary (Corporate Affairs), Secretary (Banking), Chairman SEBI, Chairperson CBDT, Chairperson CBEC, DG, CEIB, Directors of the CBI and IB, and DGFT.

[125] EIC mandate of 2003 is available at Appendix IX.5.

[126] REICs were constituted in 1996.

member agencies or through the REIC forum. REICs also undertake co-ordinating role for joint action by different investigating agencies on specific issues that are likely to have significant ramifications. Member agencies can also make specific requests to share information and documents.

Although mandated to meet once every two months, REICs do not meet that often. The number of meetings in a fiscal year is between 2 and4, seldom touching 5 or 6 in an FY for any zone. Of late, however, regular meetings of REICs have been reported. The outcome of these meetings is that the I-T department sponsored a total of 91 cases in REICs during FY 2012-13 and out of that, 43 were picked for further action. Revenue realised in these cases, attributable to the sharing of information, was estimated at Rs. 21.30 crore.

Group on Economic Intelligence (GEI)

The GEI, started in December 2005, exchanges raw intelligence on a real-time basis with intelligence and investigative agencies dealing with economic intelligence and ensures effective interaction and co-ordination among agencies regarding economic offences. While the EIC and the Working Group are inter-ministerial groups to keep an oversight on the emerging scenario of economic offences to evaluate and approve suitable co-ordinated policy responses, the GEI is focused on matters relating to intelligence sharing. Besides central intelligence/enforcement agencies, regulators like RBI and SEBI are also members of GEI. However, the reluctance on the part of member agencies to share data and information has rendered this forum ineffective.

Two exchange networks – Secured Information Exchange Network and National Economic Intelligence Network – maintained by the CEIB, are discussed below.

a) Secured Information Exchange Network (SIEN)

SIEN has been envisaged to fulfil the need to have a secured platform for online exchange of intelligence. Member agencies for SIEN include CEIB, DRI, DGCEI, CBDT, CBI, BSF, IB, RAW, ED, NCB and FIU.[127] SIEN's central server has been set up in the CEIB and a database server is connected to client machines. Besides exchange of information through a secured network, SIEN also enables agencies to share details of cases booked by them and helps in building dossiers on significant economic offenders. The data warehouse maintained in the CEIB is also accessible to member agencies through authorised channels. The National investigation Agency (NIA) is likely to be included in this network.

b) National Economic Intelligence Network (NEIN)

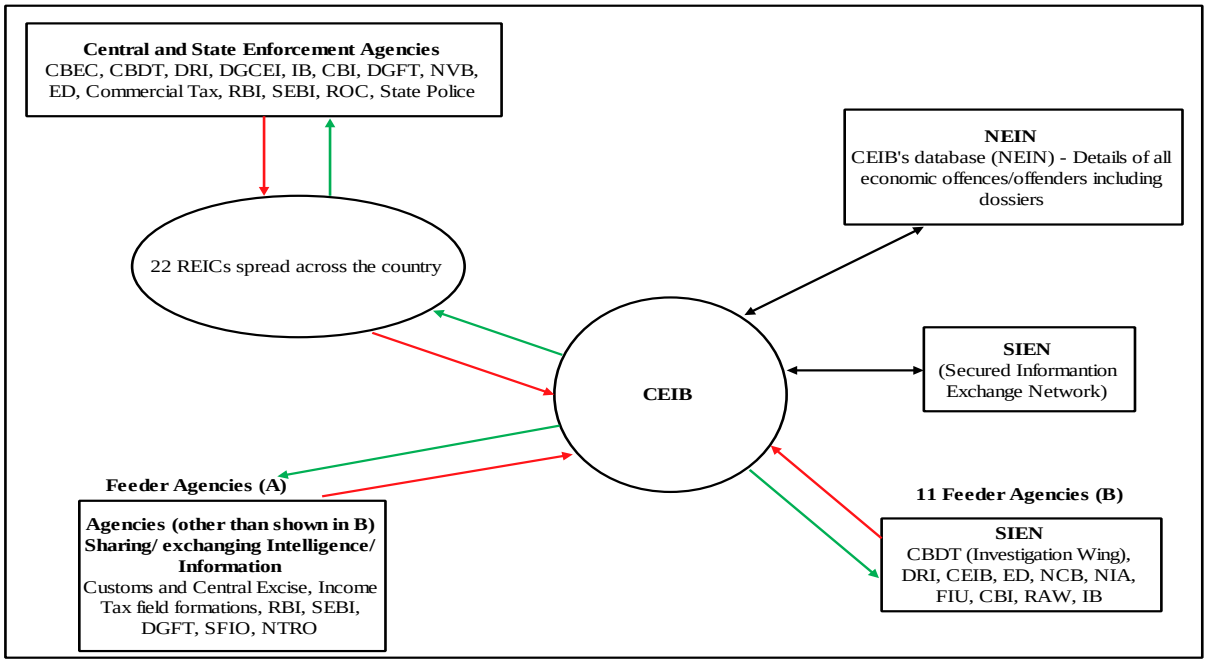
NEIN provides a database on economic offenders. Details of cases booked by different agencies are entered into this database in a defined format. These details are then collated and used for building dossiers on economic offenders. The CBEC, CBDT, BSF, CBI and other intelligence agencies and state police authorities contribute to this database. This database, maintained by the CEIB, is used to share details of economic offenders between different agencies. Dossier

[127] CBI: Central Bureau of Investigation, BSF: Border Security Force, IB: Intelligence Bureau

details are cross-referenced with FIU for further linkages. CEIB has also developed a separate database to maintain case particulars/information shared in REICs. Restricted access to the NEIN database is provided to member agencies of SIEN to ensure faster access to information. CEIB also develops strategic intelligence in the areas of customs, central excise, service tax, income tax, frauds, *hawala*, drugs, fake Indian currency notes, etc., and identifies other cases having inter-agency ramifications, for joint and/or co-ordinated action and provides a co-ordination platform for sharing intelligence between member agencies. Inputs shared through this platform help in pooling resources for co-ordinated action to combat economic offences.

Diagram 9.5 explains the network of data exchange by CEIB.

Diagram 9.5: CEIB data or information exchange network



Source: CEIB

Examples of work of CEIB

The role of the CEIB, thus, is to provide a platform for sharing information and disseminating information to different state and central government agencies on the *modus operandi* for tax evasion. One example of this is when the CEIB, as per its mandate, shared information received from the sales tax department, Mumbai, with the I-T department regarding bogus sales bills. This information was based on a data-mismatch between the VAT credit being claimed on purchases and VAT payments being shown on sales. Based on this information, the I-T department at Mumbai detected bogus purchases worth Rs. 8,100 crore and undisclosed income of Rs. 1,995 crore. The encouraging outcome of the success in detecting evasion prompted the CEIB to urge all state governments to carry out such matches of the data on VAT credit claimed and VAT payments made.

Another example of CEIB's working was the implementation of the report of the Malegaon Committee on urban co-operative banks. The Malegaon committee report had pointed out

deficiencies in the working of urban co-operative banks, which were found to be used as conduits for unaccounted income. The CEIB, the secretariat of the EIC, was mandated by the Finance Minister to monitor implementation of the above report along with the RBI, thereby fulfilling a co-ordinating role for policy dimension information sharing.

ii) Financial Intelligence Unit (FIU)

The FIU, set up in 2004, is the central agency that receives, processes, analyses and disseminates information on suspect financial transactions to enforcement agencies and foreign FIUs. It co-ordinates and strengthens collection and sharing of financial intelligence through an effective national, regional and global network to combat money laundering and related crimes. It receives suspicious transaction reports (STRs), cash transaction reports (CTRs) and other prescribed reports, analyses these reports and, in appropriate cases, sends them for action to relevant intelligence/law enforcement agencies and regulatory authorities. It also disseminates information to any domestic agency, authorised or notified by the central government to receive information under the Prevention of Money Laundering Act, 2002 (PMLA). The FIU also assists law enforcement agencies by providing information relating to financial transactions based on requests received from these agencies. It may be noted that it is not mandated to investigate any case. The FIU reports directly to the Department of Revenue. A short note on FIU is available in Appendix IX.6.

The FIU received 594 requests for information in the year 2013-14 from intelligence and law enforcement agencies and was able to provide information in 507 cases. Apart from this, it collected 5.6 million CTRs, 61,953STRs and 301,804 Counterfeit Currency Reports (CCRs). Out of 61,953 STRs received, 35,953 were processed and 15,288 were disseminated.

The FIU shares its data with various agencies. Among them, the CBDT is the largest recipient of STRs and information on CTRs. Until January 2013, the CBDT had received more than 30,000 STRs. Table 9.1 gives a snap-shot of the sharing of data by the FIU with different tax agencies, including state government tax departments.

Table 9.1: Sharing of data by FIU with the tax agencies

Agency	No. of cases referred	No. of cases for which matches found	No. of bank accounts shared
CBDT			
Corporate Non-filers	4.31 lakh	20,484	38,763
Arrear Demand cases	11, 468	5,456	40,000

Agency	No. of cases referred	No. of cases for which matches found	No. of bank accounts shared
DRI			
Arrear Demand Cases	200	71	384
DGCEI			
Service tax stop filers and non-filers	66,093	19,593	1,30,471
Maharashtra Sales Tax			
Arrear demand cases	288	--	242

Source: FIU

As a result of the FIU sharing STRs, different investigating agencies have detected unaccounted income and have seized assets (these are summarised in Table 9.2 for the period January 2013 to July 2014).

Table 9.2: Financial outcomes of STRs

(In Rs. crore)

Agency	Unaccounted income detected/tax evaded	Value of seized assets
CBDT	7,078	163
DRI	750	17
DGCEI	6.83	-
ED	19.45	15.34

Source: FIU

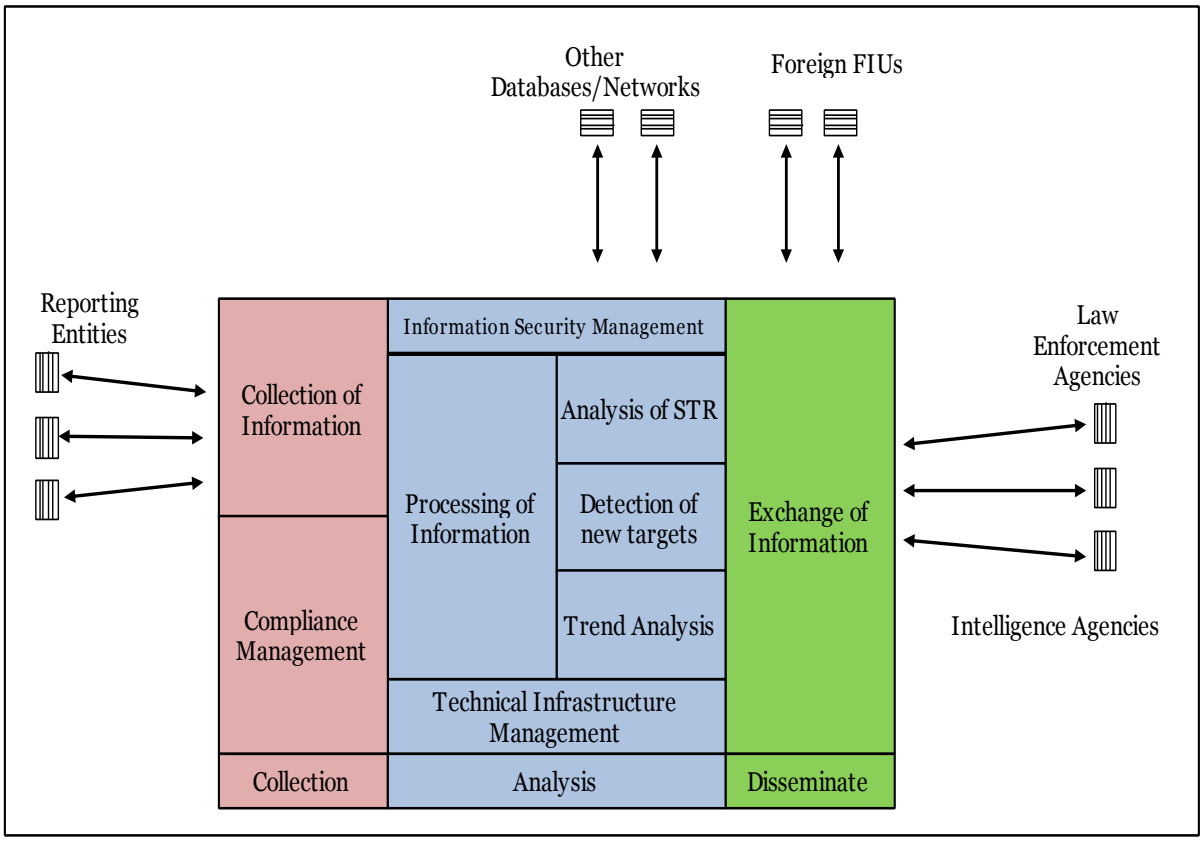
The FIU has set up the Financial Intelligence Network (FINnet) to collect, analyse and disseminate valuable financial information to combat money laundering and related crimes. The network has three segments:

- **FINgate:** For uploading reports and other exchanges with reporting entities. XML format. Internet-based, secure portal.

- **FINcore:** For analysis of reports and generation of various intelligence products by FIU analysts. High-end technology for identity and relationship resolution. No internet exposure.
- **FINex:** For exchange of information with law enforcement agencies (LEAs) – collection of feedback –LEA requests and references. Internet-based, secure portal.

An overview of the FINnet can be seen in Diagram 9.6.

Diagram 9.6: Schematic diagram of Financial Intelligence Network



Source: FIU

iii) Directorate of Enforcement(ED)

The Directorate of Enforcement, established in 1956, has been responsible since 1999for administration of the Foreign Exchange Management Act, 1999 (FEMA) and certain provisions under the Prevention of Money Laundering Act, 2002 (PMLA). ED has been entrusted with investigation and prosecution of cases under PMLA. It also collects, collates and develops intelligence and carries out investigation into suspected cases of money laundering, *hawala* foreign exchange racketeering, non-realisation of export proceeds, non-repatriation of foreign exchange, and attachment/confiscation of assets acquired from the proceeds of crime under PMLA. ED transmits its data on foreign exchange remittances relating to money laundering, *hawala* and foreign exchange violations to the DRI under the CBEC. The data are then disseminated to field formations through DRI alerts.

iv) Reserve Bank of India (RBI)

The Reserve Bank of India (RBI) is responsible for the overall supervision of the financial sector comprising commercial banks, financial institutions and non-banking finance companies. The functions of the RBI include regulation and supervision of banking and non-banking financial institutions, including credit information of companies and regulation of money, forex and government securities markets as well as certain financial derivatives. RBI also acts as the banker to banks and to the central and state governments. The RBI is responsible for the oversight of the payment and settlement systems, currency management and research and statistics. Both the CBDT and the CBEC exchange data or information with the RBI and other banks on a regular basis. For example, data on all foreign remittances are routed electronically through the RBI to the I-T department for verification of TDS payment (if leviable) on such transactions. Similarly, data on foreign remittances or export proceeds are transmitted from the RBI to the customs department in the form of bank realisation certificates.

v) Securities and Exchange Board of India (SEBI)

The Securities and Exchange Board of India (SEBI) is a statutory body constituted under the SEBI Act, 1992, and is the registering, supervisory and regulatory body for the securities sector. The primary functions of the SEBI consist of protecting the interests of investors in securities, promoting the development of the sector; and regulating the securities market for matters connected therewith. SEBI is also the regulator for related intermediaries, stock exchanges, depositories, credit rating agencies, foreign institutional investors (FIIs) and collective investment schemes, such as mutual funds. SEBI, being a regulator, exchanges data or information with investigating agencies on a needs basis.

IX.2.d Key agencies in the other ministries

The CBDT and CBEC also collect data or information from agencies in other ministries of the Government of India. These agencies are the Narcotics Control Bureau, Serious Fraud Investigation Office and National Investigation Agency.

i) Narcotics Control Bureau (NCB)

The NCB, established in 1986 under the Ministry of Finance, now functions under the Ministry of Home Affairs. It is responsible for co-ordinating actions by various offices, state governments and other authorities under the Narcotic Drugs and Psychotropic Substances Act, 1985, Customs Act, 1962, Drugs and Cosmetics Act, 1940and implements obligations in respect of counter measures against illicit traffic under various international conventions and protocols that are in force. It is also responsible for facilitating the co-ordination and universal action for prevention and suppression of illicit traffic in drugs and matters relating to drug abuse. NCB shares its information on narcotic drugs and psychotropic substances with the CBEC, through the CEIB platform for data or information exchange.

ii) Serious Fraud Investigation Office (SFIO)

SFIO functions under the Ministry of Corporate Affairs and it usually takes up investigation of only those cases concerning serious violations of the Companies Act,2013,characterised by complexity and having inter-departmental and multi-disciplinary ramifications, substantial involvement of public interest to be judged by size, either in terms of monetary misappropriation or in terms of persons affected and the possibility of investigation leading to or contributing towards a clear improvement in systems, laws or procedures. SFIO exchanges its findings with the investigation wings of the CBDT and with CEIB on a regular basis. Exchange with other agencies such as the CBEC, CBI, RBI and SEBI is done on a needs basis if investigations show violations of a serious nature. SFIO so far has developed tools to analyse existing data and is in the process of setting up its own data warehouse.

iii) National Investigation Agency (NIA)

Under the National Investigation Agency Act, 2002, the central government has set up the NIA –a federal, specialised and dedicated investigating agency to investigate and prosecute scheduled offences, in particular offences under the Unlawful Activities (Prevention) Act, 1967, including terror financing. The NIA has concurrent jurisdiction with individual states, and this empowers the central government to probe terror attacks in any part of the country. Officers of the NIA have all the powers, privileges and liabilities that police officers possess. The NIA Act empowers the central government to order NIA to take over the investigation of any scheduled offence anywhere in the country. The NIA Act also provides for the setting up of special courts. The NIA exchanges its data or information with the investigating agencies of the Finance Ministry as and when the need arises.

IX.3 Global Best Practices

Countries around the world, at differing stages of development of their tax policies and procedures, are increasingly accessing more data and information from various agencies domestically as well as internationally by entering into international agreements. As the regulatory environment and corporate governance grow stronger in many countries, tax administrations seek to leverage filings and reporting, such as public financial statements and customs or trade regulators' data that can prove valuable for their work. Increased data from a variety of sources and the increased use of filing returns electronically – facilitated by technology advancements – support tax administrations' ability to perform data analysis and information matching to assess risks. Today, tax administrations face challenges in understanding the complexities of new business structures and transactions because of the expanding global footprint of people and businesses. All these have necessitated the exchange of data or information and this has given rise to related challenges, like setting up common standards and taxonomy, instituting secured protocols for data and information storage, access and disposal, and networks for exchange which are secure and cannot be breached.

While countries have different frameworks for exchange of data or information, there is a general pattern on the data and information to be collected and exchanged. Legislations often provide basic frameworks for data and information exchange by requiring that an agency shares

certain types of data or information in specified circumstances, or by placing restrictions on the ability of agencies to share data or information. These legislations can take the form of statutes such as the Internal Revenue Code for the US IRS or a code of practice such as the Canadian CRA's Code of Ethics and Conduct. Within such legal frameworks, agencies usually enter into bilateral agreements in the form of memoranda of understanding (MoUs), service level agreements (SLAs), written collaborative arrangements, etc., with other agencies to facilitate data or information sharing.[128] The agreements usually contain details of the types of data or information that can be shared, the circumstances under which such sharing can take place, restrictions upon sharing information, etc. The statutes that authorise disclosure of information also prescribe specific conditions under which data or information can be disclosed. Between tax jurisdictions/countries, data or information exchange is based on Tax Information Exchange Agreements (TIEAs). These TIEAs are usually based on the 2002 Model Agreement framed by the OECD. This has been discussed further in Appendix IX.2.

While legal frameworks supplemented by partnership agreements serve as the foundation for data or information exchange, elements such as common standards and taxonomy, metadata, storage, access and disposal, lifecycle management, audits and safeguard reviews, clearly defined roles and responsibilities of personnel handling data or information and agency usage are integral to the overall functioning of the exchange mechanism.

IX.3.a Information exchange framework

Most countries have a statute or an established legal framework for data and/or information exchange.[129] The obligation on a tax officer to disclose data or information is also provided in the statute. Tax administrations while collecting information from different taxpayers identify what type of information can be shared or restricted depending upon the nature and type of disclosure.[130] Most countries clearly specify the type of information covered under legal covenants allowing data exchange. Most of the data is covered by legal protection.[131]

In the UK, the Commissioners for Revenue and Customs Act (CRCA), 2005, (the Act which created HMRC) enshrines the methods for disclosure of information by HMRC. These legal provisions prescribe legal information gateways for sharing information with other government agencies. If there is no legal covenant, information can be disclosed by the HMRC only on fulfilment of certain conditions as set out in the CRCA. The procedure to disclose information through a legal gateway is normally outlined in a jointly agreed document. This document can

[128] A short discussion on MoUs, SLAs and written collaborative arrangements is given in Appendix IX.8 of this Chapter.

[129] Countries have either separate enactments or an umbrella legislation to access and share data or information. For example, HMRC has Commissioners for Revenue and Customs Act (CRCA), 2005, which specifically empowers HMRC for data access or sharing. Canada has an umbrella enactment, Access to Information Act, 2009, which is supplemented by a code in every organisation.

[130] US IRS defines Federal Tax Information (FTI) as any return or return information received by the IRS or secondary source, such as the Federal Office of Child Support Enforcement, Bureau of Fiscal Service, etc. FTI includes any information created by the recipient that is derived from return or return information.

[131] In UK, Data Protection Act, 1998, requires organisations that process personal data to meet certain legal obligations. These are contained within the eight Data Protection Principles.

take form of either an MoU or a protocol or a partnership agreement or statement of practice or code of practice. The UK recently enacted laws that provide for automatic exchange of information and has taken significant steps to access data in a manner that leads the way for Open Data.

HMRC collects data on its taxpayers through tax returns filed by taxpayers or other such means.[132] It also collects third party information and brings together data from different sources and cross-matches them to uncover hidden relationships between people, organisations and other previously unidentifiable data. The Connect System, one of its analytical tools, helps it do so. With this information, HMRC is able to produce target profiles and models to risk assess transactions and generate campaigns and cases for investigation or other taxpayer related activities, including developing strategies for development of client-related activities.

In the US IRS, information disclosure provisions are according to the spirit and intent of the Internal Revenue Code (IRC).The US IRS shares tax information with other governmental agencies by entering into agreements consistent with the provisions of the IRC. Comparable laws allow agencies to share their information with the US IRS. The information-sharing programme is available at all three levels, federal, state and local. Historically, the IRS shares data with state revenue agencies based on its needs.[133] To ensure the privacy of all taxpayer data, the disclosure programme overlooks and educates all employees and external partners, ensuring protection of taxpayer confidentiality rights.[134]

In the Australian Tax Office (ATO), the taxation law secrecy provisions in Division 355 of Schedule 1 to the Taxation Administration Act, 1953 (TAA) apply to protection of information. In order to disclose protected information, an ATO tax officer is required to comply with any MoU that applies to the proposed disclosure. An MoU, however, cannot authorise any disclosure of protected information that is inconsistent with the secrecy provisions under taxation law. But, it can stipulate agreed conditions for information disclosure, such as timeframes for responding to requests, or agency contacts to whom requests and disclosures are directed. Australian ATO procedures for sharing information are enshrined in an Act, the Data-Matching Program (Assistance and Tax) Act (DMA), 1990. Through this Act, ATO provides taxpayer data to other Australian government agencies for data-matching activities. The aim of the data-matching programme is to identify cases where there is a risk of either incorrect payment of personal financial assistance or tax evasion. The income information

---

[132] UK HMRC collects information from taxpayer data (i.e., self-assessment returns, disclosure facility data, data obtained through investigations and enquiries, and VAT and other returns such as excise), cross-government data (mostly 'cash seizure reports', which record instances where the amount of cash is over £1000 and unlawful conduct is suspected, and 'suspicious activity reports', which are reported to the National Crime Agency under the anti-money laundering legislation), other jurisdiction data, and third party data. (HMRC information notices, voluntary disclosures or information acquired by UK HMRC covered under the CRCA can be used by it in connection with any other function.)

[133] Governmental Liaison Data Exchange Programme (GLDEP) for exchange of information between the IRS and the states; Questionable Employment Tax Programme (QETP) for exchange of relevant employment data by IRS with state workforce agencies to verify whether people are employees or independent contractors; Abusive Tax Avoidance Transactions (ATAA) for exchange of information between IRS and the states on tax shelters.

[134] http://www.irs.gov/Government-Entities/Governmental-Liaisons/IRS-Information-Sharing-Programs, accessed in July, 2014

derived from tax returns are fed into the Centrelink Data Matching on a cyclical basis, up to nine cycles per year. The Data Transfer Facility (previously known as bulk data exchange) is a secure service hosted by the ATO.

The Canada Revenue Agency's (CRA) legal obligations to disclose information are specified in a number of legislations such as the Income Tax Act, Excise Tax Act, Excise Act, Privacy Act and the Access to Information Act. Exchange of information with various federal, provincial and territorial departments is done through written collaborative arrangements and MoUs so that an appropriate accountability framework for the protection and proper use of information is instituted, defined and documented. The information exchange framework has been discussed in further detail in Appendix IX.7.

In India, bilateral meetings between the CBDT and CBEC are held occasionally to develop a mechanism for exchange of data and information. Towards that, a standard operating procedure is being explored to actualise request based and spontaneous exchanges between the two Boards. The standard operating procedure comprises standard templates for making and receiving requests, standardised procedures, roles of nodal officers and authorising officials and a system to enable online access. For automatic exchange of data or information between the CBDT and CBEC, joint bulk matching exercises for service tax, and exports and imports are being planned for implementation.

IX.3.b Common Standards

Data or information collected is spread across different agencies that are often disconnected. The collaborating agencies exchanging the data or information apply a consistent approach with a common taxonomy, standards and agreed arrangements for data or information exchange. This is often preceded by elaborate activities on the part of these agencies, which often prepare themselves for such data or information exchange, identifying a common vision for such exchange. For example, the US Data Reference Model (DRM) provides a standard means by which data is described, categorised and shared.[135]The UK e-Government Interoperability Framework[136]also states that systems are expected to use agreed XML schemas and agreed data standards listed in the Government Data Standards Catalogue (GDSC), both of which are available on GovTalk. If suitable schemas or data standards are not available, or if those available are deemed inadequate in some way, the system purchaser/sponsor can invoke the Request for Proposals (RFP)/Request for Comments (RFC) processes immediately. The Australian government also sets out a common language, conceptual model and agreed upon technical standards that Australian government agencies can employ as a basis for interoperating to deliver the Australian government's policy and programme. For this, the Australian government has set up the Australian Government Technical Interoperability

[135] The DRM is one of the five reference models comprising the Federal Enterprise Architecture. The DRM provides a vehicle for establishing a common language within a community of interest. Additionally, it provides a forum for cross-agency consensus concerning governance, data architecture and information exchange architecture.

[136] UK e-Government Interoperability Framework: http://edina.ac.uk/projects/interoperability/e-gif-v6-0_.pdf, accessed in July, 2014

Framework, recognising that adopting common technical protocols and standards ensures government ICT systems interoperate in a trusted way with partners from industry and other governments.[137]

Such common taxonomy is reflected within each of the three areas – data description, data context and data sharing for standardisation. In the US, data description standardisation, as detailed in the Data Reference Model, provides a means to uniformly capture the semantic and syntactic structure of data. This enables comparison of metadata ("data about data")[138] for purposes of harmonisation, and supports the ability to respond to questions regarding what is available in terms of data descriptions (metadata). Australia has formulated formal Australian standards AS 4590 for data description. This standard is used for interchange of data or information. If these standards are considered unsuitable, then steps are taken to update the standard or establish a new one. A similar practice is prevalent in the UK, where e-Government Metadata Standards ensures the maximum consistency of metadata across public sector organisations in the UK.[139]

Data context standardisation establishes an approach to the categorisation of data assets using common taxonomies or common language, data models and other descriptive information. The Australian government has recognised this as the key to governance and hence, has created a framework, the Australian Government Technical Interoperability Framework, to provide a catalogue of standards applicable to data management and exchange. This framework is shared across government agencies and reflects the concerns of each agency for security, authentication, record keeping and data definition. Each agency, with a common vision, develops, maintains and complies with the standards. A similar framework is also available in the US, called the Federal Enterprise Architecture (FEA) reference model. Such common taxonomy enables discovery of data and provides linkages to other agencies.

The US National Information Exchange Model (NIEM)[140] enables data sharing by providing consistency in standards for sharing and governance. Data sharing is achieved in NIEM through the creation of Information Exchange Package Documentation (IEPDs). IEPDs map directly to the Data Reference Model's concept of an exchange package. While the NIEM model itself provides consistency in standards for sharing, it is the IEPD that provides the actual exchange package.

---

[137]http://www.finance.gov.au/publications/australian-government-technical-interoperability-framework/docs/AGTIF_V2_-_FINAL.pdf, accessed in July, 2014

[138] Metadata is data about data. It includes information describing aspects of actual data items, such as name, format, content and the control of or over data. Description of data used by a "community of interest" is a useful tool to identify elements included within data to establish appropriate data. This helps save invaluable time and enables quick responses to information requests. Metadata standards serve as an important part of information sharing. Internationally, ISO/IEC 1179 specifies the kind and quality of metadata necessary to describe data and even specifies its management and administration in Metadata Registries (MDR).

[139] http://www.nationalarchives.gov.uk/documents/information-management/egms-metadata-standard.pdf, accessed in July, 2014

[140] NIEM has been used by Federal agencies such as the Department of Justice and the Department of Homeland Security to operationalise the data sharing component of the DRM.

The CBDT and CBEC in India are setting up an exchange platform for request-based exchanges consisting of XML schema between the two departments. A uniform ICT-based system is being planned for tagging and transmission of useful cases for spontaneous exchange between the two departments.

IX.3.c Protection of data

As in the case of data standardisation, general laws govern the protection of data. Normally, these acts apply only to data which is held, or intended to be held, on computers or held in a 'relevant filing system'. Anonymised or aggregated data is not regulated by the act, provided anonymisation or aggregation has not been done in a reversible way. Certain provisions, however, are available that define the ambit of the information that can be disclosed. Various legal conditions are prescribed under which disclosure can be permitted. Normally, the information furnished by taxpayers to tax administrations is protected against unauthorised use, inspection, or disclosure. This ensures the credibility of the tax system and the faith of the taxpayer in the tax system. Unauthorised disclosures are punished by tax administrations. These punishments could be in the form of penal consequences, imprisonment, discharges, disciplinary actions, fines, etc. Such unauthorised access or disclosure becomes wilful when it is done voluntarily and intentionally with full knowledge that it is wrong.

US IRS continuously assesses disclosure practices and the safeguards used to protect confidential information. IRC 6103(a) considers all returns and return information as confidential. No current or former employee of the IRS, state or federal agency can access or disclose returns or return information unless specifically authorised under the provisions of the IRC. To ensure the privacy of all taxpayer data, the Disclosure Programme oversees and educates all employees and external partners regularly to ensure protection of taxpayer confidentiality rights. Generally, disclosures are made by the IRS in response to written requests signed by the head of the requesting agency or an authorised delegate. In the USIRS, disclosure provisions are contained in IRC 6103 to entities having a need-to-know. This disclosure of information is limited in extent.[141]

Sections 17, 18 and 20 of the CRCA define when the HMRC staff have lawful authority to disclose information. Section 19 of the CRCA makes it a criminal offence for HMRC officers to deliberately disclose HMRC information in an unlawful way. In addition to the department taking disciplinary action, the offence carries a maximum penalty of imprisonment for two years or an unlimited fine or both. Disclosing information to persons outside HMRC is permitted in certain limited circumstances. These conditions include activities undertaken by other government departments or disclosures made in public interest. It also covers situations created by another legislation making specific provisions for HMRC to disclose information to another government department, agency or public authority.[142]When HMRC uses a legal gateway to disclose information to another public body, it ensures that secured procedures are

[141] IRS Publication 1075: Tax Information Security Guidelines for Federal, State and Local Agencies Safeguards for Protecting Federal Tax Returns and Return Information.

[142] IDG 40120: http://www.hmrc.gov.uk/manuals/idgmanual/idg40120.htm, accessed in July, 2014

in place. The procedure cover the forms that must be completed on what information can be disclosed, who may disclose the information, who may receive the information, etc.[143]

The general rule followed by Canada's CRA is that all taxpayer information is protected. Depending upon the information, CRA takes special steps in handling it. CRA ensures that the information is shared only with the taxpayer concerned or with a third party after the taxpayer has given written consent, except where the disclosure is authorised by law. All personal or proprietary information of taxpayers that the CRA employees have access to is required to be protected and kept in strictest confidence. The staff is required to take an oath of secrecy, which mandates that they do not disclose any information that they become aware of. This includes information about policies, programmes, practices and procedures of the CRA to which the public does not have official access. Staff members in CRA are made aware of the requirements of confidentiality from time to time. Information security awareness is supported by CRA documents such as the Code of Ethics and Conduct, for which reminders are issued annually. Employees periodically receive training on the confidentiality of information and emails on the protection of documents.[144]

The Australian ATO defines protected information as information disclosed or obtained under or for the purposes of a taxation law (other than the Tax Agent Services Act, 2009), which relates to the affairs of an entity (including but not limited to the entity's tax affairs), and which identifies, or is reasonably capable of being used to identify, that entity.[145]ATO tax officers are required to follow certain procedures before disclosing protected information. The officer making the disclosure has to ensure that the exception under Division 355 of TAA applies before disclosing the information.

The protection protocol in the CBDT and CBEC are in terms of password management, single sign policy and audit trail of user login and log out timing.

IX.3.d Secure Storage and Access

IRS has categorised federal tax and privacy information as moderate risk. Minimum protection standards (MPS) must be used as an aid to determine the method of safeguarding taxpayer information. The US IRS provides that security can be provided for a document, an item or an area in a number of ways. These include, inter alia, locked containers of various types, vaults, locked rooms, locked rooms that have reinforced perimeters, locked buildings, guards, electronic security systems, fences, identification systems and control measures. The provision of the required security depends upon the physical facility (i.e., whether the floor or shelf, on which the data is stored has restricted access), the function of the activity, how the activity is organised and the type of equipment available.

---

[143]IDG 40320: http://www.hmrc.gov.uk/manuals/idgmanual/IDG40320.htm**,** accessed in July, 2014

[144] http://www.cra-arc.gc.ca/crrs/wrkng/cdthcscndct-eng.html#item3_d, accessed in July, 2014

[145] https://www.ato.gov.au/Tax-professionals/Legal-practitioners/In-detail/Privacy/Procedures-for-disclosing-protected-information/, accessed in July, 2014

Some tax administrations label tax data or information differently to distinguish data or information depending upon the degree of sensitivity or confidentiality involved. In the Canadian CRA, information received is stored according to MoU requirements and CRA policies. Various devices for storage are used such as locked filing cabinets, safes, portable USB keys, diskettes and encryption devices, if necessary. Information received is stored in designated, controlled storage rooms.[146] Some CRA forms and documents are marked Protected A or Protected B. These markings help CRA employees ensure that sensitive information is handled in a secure manner.

Personal information given to the ATO includes 'sensitive information', which is a particular category of personal information. While ATO recognises that maintaining the confidentiality of all personal information is important for gaining and maintaining trust, sensitive information is often afforded a higher level of protection in terms of access, security, etc.

Both the CBDT and CBEC have back-up data storage and data replication facilities.

IX.3.e Life cycle of data

The life cycle of data can be seen as a continuum of activities that facilitate integrated service delivery, give information on particular issues and support the management of joint areas of activity. In the US, the life cycle of data and information is governed by the Information Exchange Package Documentation (IEPD). IEPD determines the lifecycle of data to be in six phases – scenario planning, analysing requirements, mapping and modelling, building and validating,

Box 9.1: "Collect/create once, use many times"

The data which is already present are not easily traceable at the time when they are required and so the already available data have to be collected a second time around or extensive manual labour has to be employed for this data to allow re-use. The advent of XML schemas makes it possible to use metadata to provide some context to the document, to allow its (or any portions of the document) timely retrieval, as and when needed. Without metadata, documents tend to lose their context, becoming essentially useless, rendering its re-use impossible. This leads to wastage of valuable time, money and effort on the part of employees. Therefore, with the help of common data standards, taxonomy and metadata, the philosophy of "collect/create once, use many times" has to be embraced. Steps in this direction need to include:

- *Establish agreed authoritative sources of information.*
- *Explore how metadata can cross technical, spatial and temporal boundaries including translations between temporal boundaries, including translations between businesses, recordkeeping and archiving systems, across levels of aggregation, through time and across contextual boundaries.*
- *Develop metadata tools, for example, metadata registries, mapping tools, standardised data representations and communication protocols.*
- *Clearly defined accountability arrangements.*

[146]Memorandum of Understanding for the Provision of Protected Information by the CRA with the Canada Border Services Agency:http://www.cra-arc.gc.ca/gncy/ntrnl/2012/mmrndm-cbsa-asfc-eng.html, accessed in July, 2014

assembling and documenting, and publishing and implementing.[147]

Australia practices the '*collect/create once, use many times*' approach.[148] Agencies are deterred from thinking only of their immediate information requirements and are encouraged to think long-term so as to enable re-use of the information. Based on these operating principles, the information life cycle is divided into five stages – planning, creating and collecting, organising and storing, access and usage, and maintenance. Although these stages are carried out in sequence, but can also be undertaken simultaneously, iteratively, partially or in different orders.

The CBDT and CBEC have not embarked on life cycle management of data. However, steps in that direction are underway and these steps are being discussed with key stakeholders to understand data needs and alternatives available to ensure maximum benefit at minimum cost (time and effort), security and sustainability, preparation of reporting format (schema) keeping in view various aspects such as data availability, compliance cost, proposed utilisation, existing data structure, development of utility to assist preparation of data in prescribed formats, implementation of data collection and utilisation processes, and implementation of data backup policies.

IX.3.f Re-use of information

Where there is a repeated need for the same data across agencies, it is important to recognise and use authoritative sources of information so that credible and current data can be used a number of times. This re-use reduces the cost and burden of data collection and storage and improves the overall quality of data collection and sharing. Apart from this, it helps save precious time and helps avoid unnecessary duplication of work on the same task by two different agencies or twice by the same agency. Australia uses the Business Entry Portal transaction manager tool that allows data created once to be used many times. This allows management and completion of online transactions at all levels within the government via access to over 4,000 government forms. The transaction manager allows users to store their multiple personal and business details in profile. These profiles automatically pre-fill and complete online transaction forms as users access them.[149] For this to happen, different agencies agree as to which one holds the prime responsibility to act as custodian for that particular information. This agency is then entrusted with the responsibility to collect, store, manage and maintain information so that it can be used reliably by other agencies as well.

In the US, various agencies work on a common Enterprise Architecture (EA) with a centralised metadata repository to manage EA artefacts. These repositories support implementation of the data context standardisation area of the DRM. This centralised repository provides search and

[147] Report on the *Adoption and Use of the National Information Exchange Model (NIEM)* submitted by the Federal CIO Council on June 11, 2010.

[148] This concept has been further elaborated in Box 9.1 of this chapter.

[149] *Australian Government Information Interoperability Framework*, April 2006, Australian Government Information Management Office

discovery capabilities for potential re-use of enterprise architecture assets across that agency and within its component bureaus.

In India, the CBDT and CBEC hold meetings with other agencies and between themselves to understand mutual requirements and availability of data for re-use.

IX.3.g Disposal

Upon completion of use, it is important for agencies to destroy or archive or return the data or information. In the US, the information used by agencies which received the data from the IRS is destroyed or returned to the IRS according to the guidelines contained in Section 6103(p)(4)(F) of the IRC. Under the ATO Privacy Policy, when personal information collected by the ATO is no longer required, it is destroyed or deleted in a secured manner, in accordance with records authorities issued or agreed to by the National Archives.[150]

In Canada, the National Archives Act, 1987, along with the policy on the Management of Government Information Holdings requires that institutions schedule all their information holdings for retention and disposal. In addition to this, government institutions schedule personal information for retention and disposal in accordance with clearly defined principles. When personal information has surpassed its scheduled retention period and has been designated by the National Archivist as having archival or historical value, it is transferred to the control of the National Archives or otherwise destroyed in a manner consistent with its security classification.

IX.3.h Audits/Safeguard Reviews

The US IRS conducts regular on-site reviews of agency safeguards to determine the adequacy of safeguards as opposed to evaluating an agency's programmes. Several factors are considered to determine the need and frequency of reviews. Reviews are conducted by a separate, independent office. Safeguard reviews contain various requirements that cover aspects such as record keeping requirements, secure storage, access restrictions, reporting requirements, tax information disposal, computer system security, etc.

In Canada's CRA, MoUs entered into by parties include a clause requiring that internal audits should be conducted on the use and security of information provided. Apart from this, they also have subsequent review audits to assess the results on the finding of the previous audit. The objective is to provide assurance that CRA complies with conditions governing the use, communication, storage and finally destruction of information received.

Both the CBDT and CBEC follow ISO 27001 standards, along with standards prescribed by the Department of Electronics and Information Technology, Ministry of Communications & Information Technology. These safeguards are put in place at the time of project implementation itself. For audit, the two organisations employ the Standardisation Testing and

[150]https://www.ato.gov.au/About-ATO/Access,-accountability-and-reporting/In-detail/Privacy-notices/Short-Form-Privacy-Policy/, accessed in July, 2014

Quality Certification (STQC) Directorate, an attached office of the Department of Electronics and Information Technology, which also provides quality assurance for their projects.

IX.3.i Use of data

Data is used in tax examinations, collections and criminal investigations as well as by law enforcement agencies to conduct research in tax cases, tracing money laundering activities, investigative leads, and intelligence for tracking currency flows, corroborating information and probative evidence. The US IRS uses the data to improve tax administration by efficiently partnering with federal, state and local government agencies to increase compliance, enforcement and service to taxpayers. Data collected by the IRS is shared with state and local taxing agencies. This saves government resources by reducing duplication of effort. Together, they achieve mutually the beneficial goals of improving voluntary compliance, increasing the efficiency of tax administration and reducing taxpayer burden. UK HMRC accesses STRs (SARs in the UK) held by the FIU via a secure online facility – Moneyweb. Information obtained from the FIU is used by the tax administration to determine civil tax assessments and in tax crime investigations.

IX.3.j Managing Big Data[151]

Many advanced tax administrations are moving towards big data management for cost effective solutions. The US IRS's Research, Analysis and Statistics Division uses big data techniques to enable advanced analytics, such as econometric modelling, forecasting and compliance studies on massively large datasets. UK HMRC has also replaced its conventional debt processing systems with an innovative IT solution capable of mass customising debt collection interventions based on insights into customer behaviour – Analytics for Debtor Profiling and Targeting (ADEPT). ADEPT is a closed loop 13.5 terabyte big data analytics system, with a debt management system and a decision engine. It automatically combines data from 20 internal and external systems and monitors a wide variety of changes that affect up to a million debts each day. Debt information such as payments made or missed, records of notes from the field force, and letters returned as undeliverable are integrated with socio-demographic and other data. ADEPT transforms the data and creates a single source of business intelligence for debt management. By integrating ADEPT's big data approach with legacy batch-processing, HMRC achieves flexibility and speed while simultaneously maintaining the resilience of business critical systems that thousands of HMRC staff rely on to do their jobs.

The Australian Government Information Management Office (AGIMO) uses big data and its associated analytical tools to develop better policies and deliver better services without compromising the privacy rights of the public. The ATO has also started working on the new Data Analytics Centre of Excellence to use vast volumes of data captured by various

[151] The commonly accepted understanding of big data defines it as high-volume, high-velocity and/or high-variety information assets that demand cost-effective, innovative forms of information processing for enhanced insight, decision making, and process optimisation. Some analysts also discuss big data in terms of another two attributes, value (the economic or political worth of data) and veracity (uncertainty introduced through data quality issues).

government agencies. The Big Data Working Group is to work in conjunction with ATO's Data Analytics Centre of Excellence to deliver on a set of guidelines and initiatives to help government agencies take advantage of big data.

IX.3.k Chief Information Officer's Role

The Chief Information Officer's (CIO) role in data and information exchange is central as he provides an overarching, regulatory function to the tax administration. According to IRS Publication 1075, a senior information security officer is appointed with the mission and resources to co-ordinate, develop, implement and maintain an agency-wide information security programme. Other agencies in the US sometimes also refer to this official as the chief information security officer. The ATO also provides for a CIO who carries on the development and implementation of data and information exchange according to the Australian Government Technical Interoperability Framework. The CIO is required to rationalise processes to increase interoperability, to improve the quality of services and to reduce the cost of service provision. The CIO thus adopts the national framework as a guide to ensure its appropriate usage, oversees the quality and integrity of data and creates an environment for seamless data and information exchange with partner organisations. Apart from this, the CIO in the ATO also ensures that data and information is well-managed both within the agency and when transferred across agencies.

The position of DG (Systems), discussed in detail in Chapter III of the first report of the TARC, is akin to the CIOs in other tax administrations.

IX.3.l Financial Intelligence Unit (FIU)

Most countries have established FIUs that collect financial intelligence and analyse it. Countries have adopted different models for FIUs – as a unit of the police or public prosecutor's office, as an independent unit within the central bank, as a separate agency under the Ministry of Finance or as a separate agency under the Ministry of Justice (or equivalent).[152] Whatever be the structure, FIUs serve as a government-wide multisource financial intelligence and analysis network.

The FIU in the US is part of FinCEN, a bureau of the US Department of the Treasury that relies upon financial institutions to provide a stream of reported information to enable it to detect trends and patterns of potential illicit activity, which can be used as inputs to determine regulatory policies and to inform the financial industry of risks and vulnerabilities.[153] The mission of the FIU in the US is to safeguard the financial system from illicit use and to combat money laundering and promote national security through the collection, analysis and dissemination of financial intelligence and strategic use of financial authorities. The FIU also houses full-time liaison officers from other federal agencies. This facilitates exchange of

---

[152] OECD Report on *Effective Inter-Agency Cooperation in Fighting Tax Crime and Other Financial Crimes*, Second Edition, 2013

[153] It is considered that FinCEN has the same mandate as the CEIB. The Khan Committee (2011) pointed out this similarity.

information, typologies and trends with FIUs of other countries. FinCEN combines this data with other sources of information to produce analytic products supporting the needs of law enforcement, intelligence, regulatory and other financial intelligence unit customers.

Like the US FIU, the FIU in Canada is placed under the Ministry of Finance; it contributes to public safety and helps protect the integrity of Canada's financial system through the detection and deterrence of money laundering and terrorist activity financing. In the UK, on the other hand, the FIU is within the National Crime Agency, a law enforcement organisation and its role is to service UK police forces and other official agencies that have a legitimate need to access suspicious activity report (SAR) data.

Australia has positioned its FIU under the Attorney General's Department, Ministry of Justice, and its main role is to assist law enforcing agencies in investigating serious criminal activity and launching prosecution, including activities such as terrorism financing, organised crime and tax evasion. The role of the FIU also includes the integration of information with partner agencies and providing high-level on-site analytical support to these partner agencies.

IX.4 Gap

The TARC had pointed out in Section VII.1.c of its first report that "*ICT enablement by both these departments is completely isolated from each other with very limited application of technology for an integrated risk model or even seamless sharing of data……Both departments hold huge amounts of data in their systems which can be put together using the PAN to create a comprehensive profile of the taxpayer. There is huge potential to plug revenue leakage by doing so……..Both the Boards have undertaken data warehouse projects. While the CBEC's data warehouse is already in operation, the CBDT is in the process of setting up its project. However, one can well imagine the gains to the two administrations if, instead of being set up in two separate silos, a single data warehouse covering both direct and indirect taxes had been set up in a collaborative manner. Not only would it have resulted in considerable cost savings by providing economies of scale and avoiding duplication, the availability of comprehensive, cross tax data would have added significant muscle to their enforcement efforts."*

Section IX.2 also discusses this issue. At present, the two Boards, along with other agencies, maintain data only for their own use. It has been reported that even within the same department, different divisions/wings maintain different data and information and common access and usage is absent. Such silo working tends to develop patchy data that lack integration, uniformity and are far from being comprehensive. The basic intent is to address an immediate task rather than building a system which can deal with other usages as well. Different government agencies collect and hold information on individuals, corporations and transactions but they are largely directly relevant only to their present activities. This is opposed to the '*create once, use many times*' approach, often collecting the same data from the same person at different times.

Most advanced tax administrations recognise data and information as valuable assets. Keeping that in focus, they are moving towards a centralised governance framework for data and information collection. Towards this framework, they are putting valuable resources in

planning before any system is put in place for data collection or creation. All partner agencies are closely associated in this exercise. After the data are created or collected, considerable time and money is invested in organising and maintaining the data so that all partner agencies are able to access and use the data and information on a '*create once, use many times'* basis. At present, data and information management in India are scattered and disconnected. Each organisation, whether the CBDT or the CBEC, collects or creates a lot of data, but without a coherent framework. This approach needs to change to meet emerging realities, characterised by complex and voluminous transactions and inter-connectedness of data and information across many tax jurisdictions, which often leads to tax base erosion and tax evasion. Decentralised and disintegrated data and information collection also increases the cost incurred by the government and puts the overall effort at risk. Such a disjointed framework also often results in inconsistent data being maintained by organisations, leading to inaccurate analytical results. These affect tax collection too.

While the adoption and use of a common framework may not be sufficient to solve all the challenges facing data and information exchange by agencies in India at present, it will encourage agencies to develop a common, long-term vision for collection, use, storage, and disposal of data and information, thus getting rid of the silo structure and mentality that discourages exchange. It is also important to recognise that within government agencies, there are large volumes of data that can be leveraged usefully without incurring additional cost to collect the data afresh. The focus, therefore, should also be on organising the data within the inventory of the agencies or having a common database. It is not enough to address this by building the technology infrastructure alone, which is at present the focus in India for both the CBDT and CBEC; it is also necessary to address the question of whether a common data centre that would consolidate all the data within the two Boards as well as that of other partnering agencies could be considered to leverage the capabilities of all agencies.

IX.4.a Working of CEIB and FIU

The Government of India had set up a Committee in 2011 vide Department of Revenue Order No. 68 of 2011, dated March 29,2011, to review the role, functioning and structure of the CEIB. The Committee in its report pointed out that there is a need for a specialised central agency, which can take a perspective view of the entire arena of economic offences and should be designated as the nodal agency for receiving, processing, analysing and disseminating post action information and investigation reports on all specified types of cases of suspected serious economic offences and organised tax evasion noticed or investigated. The CEIB, according to this report, is to be the central repository for this purpose. The Committee also recommended that the CEIB should enter into MoUs with agencies outside the Ministry of Finance and with other regulatory bodies. It also recommended that there should be an agreed upon format for information sharing and this should be done in two stages – as incident report within 48 hours of the incident and as a summary of findings upon completion of investigation.

The data sharing arrangement between the FIU and CEIB continues to be patchy and often irregular. The FIU collects data from banks on a digital platform. On the basis of these, STRs and CTRs are generated. Despite the mandate to share data between FIU and CEIB, the present working is not very smooth.

The FIU in its deposition before the Committee stated that it disseminates intelligence after determining which investigating/law enforcement agency is the relevant agency to act upon the intelligence. It also stated that actionable intelligence is time critical and so should be shared only on a need-to-know basis. If there is no value addition and the CEIB only acts as a repository, data or information sharing with the CEIB, according to the FIU, would serve no useful purpose. The Committee disagreed with that view and recommended that full information on the STRs should be shared with the CEIB as the Committee considered the CEIB as the national data or information repository on economic offences. Despite such a clear view of the Committee as well as the specific mandate given in 2009 to the FIU to share STRs with the CEIB, it has been reported by the CEIB that data on STRs which come to it are incomplete and patchy, creating a handicap and making the data less than useful.

The Committee also pointed out that the CEIB has two networks for information exchange. While the SIEN is a secured network with eleven selected agencies, the NEIN is a stand-alone platform and is to be built as the national repository of data. But since there is minimal data flow in NEIN, the database "*has declined to negligible levels*" (Para 3.6.1 of the Committee report).

One major lacuna in the functioning of the FIU is that banks do not correctly deploy parameters while arriving at the finding of CTRs/STRs. These parameters are to identify connected suspicious bank transactions, high debit or credit transactions, high value transactions by non-profit organisations, transactions involving counterfeit or fake currency or high-value cross-border transfers and generate STRs and CTRs. The FIU is required to monitor whether the banks deploy the above parameters correctly so that the identification is complete and proper, but this is not being done on a regular basis.

A virtual office has also been set up by the FIU to monitor the feedback on the CTRs/STRs disseminated. The virtual office is supposed to be an inter-agency office, drawing one officer each from the CBDT, CBEC, CEIB and FIU. A Closed Under Group (CUG) has been created on the NIC portal for the officers to interact with one another and to send feedback to the FIU regularly.[154]

IX.4.b Policy and Legislative Framework

The National Data Sharing and Accessibility Policy, 2012 (NDSAP) addresses data exchange between government departments. It states in Para 3 that "*there is a general need to facilitate sharing and utilisation of the large amount of data generated and residing among the entities of the Government of India. This will call for a policy to leverage these data assets which are disparate. The current regime of data management does not enable open sharing of Government owned data with other arms of the government nor does it expect proactive disclosure of sharable data available with data owners.*"[155] The NSDAP enumerates the principles on which data sharing and accessibility can be based. The principles mentioned in

[154] Annual report of the Ministry of Finance (Budget Division), 2012-13

[155] Ministry of Science and Technology, Department of Science of Technology, Gazette Notification dated March 17, 2012

NDSAP are "*openness, flexibility, transparency, legal conformity, protection of intellectual property, formal responsibility, professionalism, standards, interoperability, quality, security, efficiency, accountability, sustainability and privacy*." But, it may be kept in mind that the above elements of NDSAP are for sharable data and not for data or information that are non-sharable and sensitive.[156] The data or information collected by the two Boards, the FIU, the CEIB and other investigation and intelligence agencies may fall in the category of non-sharable and sensitive as the data or information are often considered private and confidential, putting it beyond the scope of NDSAP.[157]

Whatever the policy position, the present working of the CBDT, the CBEC, the CEIB and the FIU have not paid attention to setting up a robust mechanism for data or information exchange between each other. There is so far no openness or transparency for setting up an interoperability framework for data or information exchange. The first report of the TARC in Section III.4.b had pointed out that, "*A common database between them will lead to great gains both in terms of enforcement and taxpayer services.* "The report also stated that, "*There is an almost complete absence of synergy between them whether in the matter of sharing data or resources or in the matter of doing things jointly to achieve greater efficiencies. Due to their silo functioning, each Board gets a fragmented view of the taxpayer. From the compliant taxpayer's perspective, therefore, enhanced integration between the CBEC and CBDT would result in a more harmonious and convenient taxpayer experience. At the same time, greater sharing of information between them would reduce opportunities for fraud."* While the two Boards hold bilateral meetings to understand mutual requirements and availability of data, the exercise falls short of creating "*one data and many users*". They have not yet moved towards life cycle management of data.

The existing Information Technology Act, 2000, deals with privacy or protection of data to some extent in three sections, namely Section 43A, 69 and 72A, but other elements as mentioned above in NDSAP have not been dealt with in the context of data or information exchange.[158] Under Section 43A, any organisation that possesses, deals with or handles any sensitive personal data or information and is negligent in implementing and maintaining reasonable security practices resulting in wrongful loss or wrongful gain to any person can be held liable to pay damages to the person so affected. Section 72A of the Information Technology Act provides for the terms of fine and punishment. But the overall governing framework is the contractual relationship between the two parties exchanging data. Section 69 provides an exception to the general rule of privacy and secrecy of data and states that where the government is satisfied that it is necessary in the interest of the sovereignty, security,

[156] Sharable data as per NDSAP are those which are not covered under the scope of the negative list and are non-sensitive in nature.

[157] NDSAP in Para 1.3 states that it is "*designed so as to apply to all sharable non-sensitive data available either in digital or analog forms but generated using public funds by various Ministries/Departments/Subordinate offices/organisations/agencies of Government of India. The NDSAP policy is designed to promote data sharing and enable access to Government of India owned data for national planning and development*."

[158] The Information Technology Act, 2000, provides legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternative to paper-based methods of communication and storage of information to facilitate electronic filing of documents with government agencies.

integrity or defence of the country, any agency can intercept, monitor or decrypt any data or information. As is evident, while the current provisions provide for data protection, they fail to address interoperability of exchange of data or information between organisations, which is what is required to address the needs of the tax administration.

While the Information Technology Act deals with privacy and protection of data, covering information only on the digital medium, traditional concerns of institutional lack of trust and misuse of data continue to remain unaddressed. Thus, there is an imminent need to fill this lacuna by instituting a robust framework which addresses data and information sharing. Any legislative framework governing inter-agency exchange of data or information needs to have elements such as provisions for the process of making request for data or information, time bound responses to such requests, consequences of not sharing and for unauthorised usage, developing common standards, layered authorisation, feedback mechanism on exchange of data or information and strengthening provisions for data privacy or confidentiality.

IX.5 Way Forward

From the above gap analysis, it can be seen that although the CBDT or CBEC collect or create huge volumes of data, there is no coherent framework for exchange of data and information. Many advanced tax administrations, as seen in Section IX.2 of this Chapter, have moved towards an organised method of data and information exchange. Some of these administrations have also moved towards a legal framework.[159] This casts a mandate upon agencies to share information with certainty and defined periodicity. Such a legal framework has also enabled them to move towards a common taxonomy, with the basic objective of fulfilling "*one data and many users*"[160] and facilitated re-using data with the intention of "*collect once, use many times"*, thereby reducing duplication of efforts as well as costs of collecting data and time expended in collecting the data. These frameworks for sharing information, however, may take different forms – direct access to information, automatic exchange of information, mandatory spontaneous sharing of information or request-based information sharing, depending on the needs of organisations, but the general objective remains uniform, as pointed out above.

> ***Box 9.2: "One data, many users"***
>
> *A concurrent data structure is a particular method of organising and storing data for access by multiple computing threads. This concurrent data structure can be constructed using:*
>
> - *Coarse-grained locking method that locks up all the data and allows it to be accessed only by authorised personnel*
> - *Fine-grained locking method where each fine-grained lock is responsible for protecting a region of the data.*
>
> *Further access from fine-grained locking is acquired by deploying special security protocols.*

The legal framework, with common taxonomy, has helped these countries in modernising tax administrations. Tax administrations have also instituted detailed protocols for sharing data and have increasingly

[159] Para 6.8.1 of the Khan Committee report

[160] This concept has been elaborated in Box 9.2 of this chapter.

trained their staff on this sensitive aspect, including clearly enumerating in the code of ethics and conduct what can be shared or what can be considered confidential. The tax administration in India also needs to adopt a similar approach to data collection and usage so that the pilot projects mentioned in Section IX.2 do not remain one-off activities with mixed results, but becomes part of the business rule of each stakeholder in this framework.

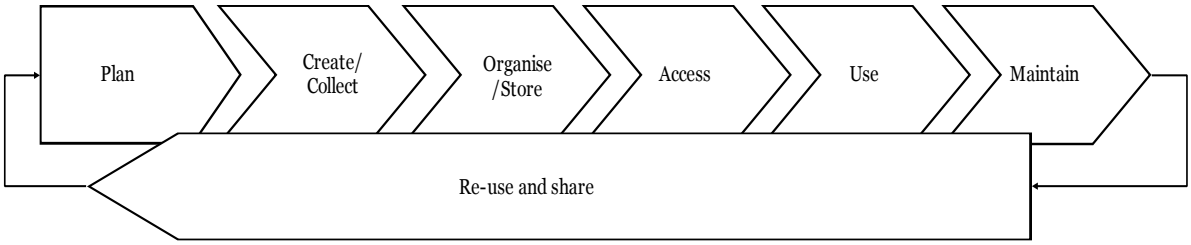
IX.5.a Mutual trust, openness and willingness to share

The CBDT and CBEC also need to create a mechanism for sharing data and information with each other to achieve the higher, common objective of reducing the tax gap. Although the two Boards have taken a few steps towards consolidating their database, there has so far been no comprehensive move towards creating a common database or providing a mechanism for exchange of data or information in a sure-footed manner. In addition, there has been no movement towards a common taxonomy or creating a common catalogue.[161] Such a catalogue would normally contain information on data, such as source of data, data structure, data definition, quality of data, frequency at which the data is updated, etc. This helps the party receiving the data or information to judge the relevance of data or information and whether it is readily available.

The building of this catalogue is contingent upon an attitude of mutual trust, openness and willingness to share data and information between the CBDT and CBEC. A legal framework, in the form of an enabling provision in the existing acts of different taxes or the enactment of an umbrella legislation dealing with data or information exchange that would cover all agencies supplemented by customised MoUs between agencies, or a standalone MoU or SLA between the two Boards can ensure such willingness and openness. Sometimes, MoUs/SLAs can also originate out of an act with supplementary provisions that enables such sharing of data or information. But many consider MoUs or SLAs between two government departments, in particular between the two tax departments, an anathema. What is thus required is to instil an atmosphere of mutual trust, openness and willingness to share, recognising the commonality in the goals of the two organisations, and thereafter to develop a common plan to build a database (may be separately, and not a common database to begin with), which can be used and re-used to improve the efficiency of the tax administration. One mechanism that would create such an environment would the setting up of a Joint Steering Committee comprising officials of both the CBDT and CBEC, and the Directorates of Systems of the two Boards. This committee will have the mandate to work out details of data life cycle – planning, collecting or creating, organising or storing, access, usage, maintenance, and re-use and sharing with a common vision and purpose. Diagram 9.7 brings out the sequence.

[161] It has been reported in the meetings with CBDT and CBEC officials that joint workshops were organised in the past for the System Directorates, but there were no significant outcomes from these meetings.

Diagram 9.7: Data life cycle[162]



It is important to point out that whatever the framework considered appropriate by the two organisations for data and information exchange – legal enactment or MoU/SLA – the basic framework for co-operation should contain the consequences of not sharing data or information, delayed sharing of data or information or sharing data or information wrongfully. Normally, punishment for unauthorised disclosures is part of such a framework misuse or unauthorised disclosure in any manner should not be tolerated. The absence of enforceability for not sharing data or information adversely affects the general environment of trust and openness. Many times, one instance of not sharing or delayed sharing of data or information leads to another, and finally the programme comes to a halt and there is no useful outcome. A stand-alone MoU/SLA without statutory backing renders its enforceability largely persuasive.

IX.5.b Common standards and taxonomy for data exchange

Common standards and taxonomy facilitates data exchange between different organisations and enables better reporting and analysis. Almost all countries reviewed, as discussed in Section IX.3 of this chapter, are moving to achieve a common standard and taxonomy. Such common standard and taxonomy is required to integrate disconnected data and information available with different agencies, many of whom do not have tax as their primary work. A consistent approach on data across agencies, such as, DGFT, SEBI, RBI, registrar of companies, banks, etc., will allow better collation of data and information, making its usage easy.

The key requirements for such common taxonomy, *de minimis*, are standardisation of data description, data context and data sharing. Sharing a catalogue, as discussed above, will be a step in that direction. This catalogue will enable comparison of metadata, which is the key to a common database formation.

IX.5.c Information from third parties

Legal, operational and organisational barriers prevent agencies from co-operating with each other for effective inter-agency information sharing. The absence of a robust legal framework restricts or prohibits other agencies as there is no clear mandate to ensure data or information sharing. Operational barriers, as also pointed out above, such as lack of awareness of

[162] Extracted from the Australian Government Interoperability Framework, April, 2006

availability of data or information or absence of common standards are also barriers to seeking information from third parties.

The I-T department, according to the CIB code, receives a large amount of third party information from a number of agencies. Often, these data have a large component of non-PAN data. Since PAN is the key taxpayer identification number, it becomes arduous and sometimes impossible to match data without it, defeating the very purpose of data collection from third parties.[163] A common framework of data or information is, therefore, important for exchange with third parties.

Many advanced tax administrations normally have MoUs with agencies supplying third party information. They establish common standards and taxonomy for such transactions, and also set up a mechanism that ensures that such information is exchanged on a regular basis. The CBDT has almost moved in that direction, relying largely on the legal provisions for third party data exchange.[164] Collection of data by the CIB, however, is through an instruction. The CAG, in its recent report on the performance of AIR and CIB data collection mechanism, pointed out a number of deficiencies.[165] Two of the notable deficiencies listed by the CAG are as follows:

- While extracting AIR data to the ITD system, NSDL should check whether PAN given in the data is valid. Merely checking data presence might not be enough.
- There is no time-limit to correct incorrect information.

The above observations point towards the requirement of a mechanism so that parties sharing/exchanging data have a common platform and standard. PAN as a Common Business Identification Number (CBIN) in the TARC's first report was recommended for that purpose. The report pointed out that a common identification "*help(s) (to) integrate the requirements of various government departments besides giving a certain identity to the business*."[166] Such a common identification number was intended to create a common platform and standard. This would also require a robust regulatory mechanism to oversee that data collection is coherent and relatively accurate. A periodic evaluation of the database should be carried out to see that the CBIN continues to provide a common standard and platform.

In the CBEC, the excise department does not have any mechanism for collection of third party information. The customs department, through ICES, collects information from other parties through a message exchange facility. The CAG audit review[167] had revealed major deficiencies in the system's design, leading to incomplete capture of data resulting in manual interventions, incorrect mapping of business rules, absence of appropriate input controls, absence of validation between 'customs tariff heading' and the serial number of the notification to ensure

[163]The I-T Department issues query letters for non-PAN cases received. On an average, less than one-third of these non-PAN cases get PAN-populated after the query letters are sent.

[164] AIR data is collected under Section 285BA of the Act while CIB collects data under a CBDT instruction.

[165] CAG performance Audit Report No. 4 of 2013

[166] Section VI.1.c of the first report of TARC

[167] CAG Performance Audit Report on ICES, No. 11 of 2014

correct availing of exemption notifications and absence of validation of licence and scheme code. Inadequate change management controls and wastage of resources have also been pointed out as the data available in the system is not being utilised and the manual process is resorted to instead. The CAG in its report has also pointed out the importance of a steering committee comprising various stakeholders to bring focus and direction to a strategic plan on data and information exchange.

Taking a cue from the CAG's observations, it is recommended that various stakeholders must be brought on a common platform to arrive at a common standard for data sharing/exchange. A steering committee could provide such a forum where all stakeholders can bring a catalogue of data, scoping of data, data availability, periodicity of data exchange, etc., so that a formal and dedicated channel of data exchange can be developed. It is also important to point out that exchange of data through a physical medium, i.e., through paper, compact disc, external drive, etc., should be avoided and any exchange of data or information should only be through a digital platform.

Data or information exchange should necessarily be done through a common utility, which can be tailored to the specific data availability or framework for data creation or collection by a particular organisation, so that data matching with existing CBDT and CBEC data is seamless and the error percentage is minimal. Over a period of time, this will also facilitate increasing data collection frequency. Organisational difficulties in data or information exchange through this utility can be discussed in a steering committee, comprising all the collaborating agencies, set up for the purpose. Each organisation will have to inform other stakeholders about its point of contact. Any request to that organisation can be directed towards this person. If a change occurs in the contact person, this will have to be informed on a real-time basis so that the stakeholders are not inconvenienced. One integral aspect of third party information exchange will be to maintain a common and mutually agreed upon framework on confidentiality of data exchanged. This is further discussed below.

IX.5.d Confidentiality framework

Stakeholders' confidence and trust in exchanging their data or information would rely heavily on protecting the data or information and its use for the purpose for which they were procured. While recognising the need to protect the confidentiality of data, many statutes prescribe situations in which data can be shared, if it is in public interest. The understanding of "public interest" has been circumscribed by the rulings of the higher judiciary. A recent amendment to the Information Technology Act, 2000, by inserting Section 43A, has cast responsibility on persons handling sensitive personal information.[168]

In the above background, it is important that adequate attention is given to the confidentiality aspect of data or information and this assumes even greater importance in the context of data

[168] The Constitution of India does not expressly confer any enabling provision towards right to privacy in India. The Supreme Court ruled in the case of Kharak *Singh v. State of UP*, (1964) 1 SCR 332, that the right to privacy is implicit under Article 21 of the Constitution. Section 43A of the Information Technology Act, 2000, defines 'Sensitive personal information' and requires all bodies corporate, which deal with personal information, to fulfil certain responsibilities. These rules have for the first time introduced an omnibus privacy and data protection law.

exchange with third parties. The agency receiving information and the agency providing information need to establish a process for evaluating the confidentiality and security related protocol of the data and information shared. This protocol would need to clearly articulate access rights and further sharing rights, and needs to be made available upfront to the other party. In addition, there should be additional checks for critical information in the form of layered authorisations. The receiving party should normally also share the extent of information security tools and processes established. Safeguards should be implemented to prevent unauthorised access and misuse. All these are trust and confidence building measures between the two parties.

IX.5.e Quality of data

The most critical aspect of establishing a data analytics infrastructure is to establish a mechanism to process and structure data so that it is ready for analysis. As a first step, an exercise will have to be undertaken to evaluate the quality of data available. Only with good quality data can one have meaningful analysis. General experience shows that often, there are significant quality issues in existing data. Such poor quality of data is also because transactional data such as arrear demand data has not been fully digitised and because, data or information continues to flow into the system through physical mediums as many collaborating agencies/departments do not have the means to upload data online.[169] It is thus important that collaborating agencies are considered key stakeholders in the exercise of collecting data and information.[170]

IX.5.f Layered authorisation

Layered authorisation is a normal management practice to deal with business activities wherein some people have authorisation to do a particular thing, while some have higher authorisation, depending on the nature of the work entrusted to them. Similar authorisation needs to be developed for data access. Data or information should not be open to everybody in an organisation; rather, it should be layered depending on the job role, responsibility and the nature of information. Layered authorisation also covers the process of granting permission to certain authorised personnel to access specific information and carry out specific actions. This also brings accountability to the authorised individual and layers defences and improves an organisation's security.

The tax administration can enforce effective access control so that authorised personnel are equipped with the least privilege needed to perform their official duties. These access controls could be set up in the data warehouses based on personnel clearances and accordingly personnel can be given restricted or general access.

[169] The I-T department continues to receive non-PAN data from organisations providing CIB information, like the land registry office, motor vehicle registry office, etc. These departments also do not have a terminal to verify online PAN.

[170] The I-T Department uses the AIR and CIB information as inputs for selection of scrutiny cases.

IX.5.g Data or information sharing

Information is required to be shared.[171] For such sharing of data or information, it is important that all participating departments need to categorise the data or information into what can be granted general accessibility and what can be considered for limited sharing or for somewhat spontaneous sharing. Spontaneous sharing of data or information may be with a maximum of one-level of authorisation. Sometimes, it may mean even multi-layered approval, depending on the sensitivity of the data or information. Normally, such sharing takes place only on the basis of a specific request and on a need-to-know basis. Sharing of the data catalogue by all the participating organisations will also promote re-use of data, once procured. This will help in being specific in the request. For smooth functioning of the system, such requests will have to be mutually respected. Effort should be made by each organisation to respect the request unless it cannot be shared due to a particular reason relating to sensitivity of the data. But all these must be known *a priori* to each of the participating organisations to build openness and demonstrate an attitude of willingness to share with each other.

IX.5.h Re-use of data

Information lifecycle management – planning, collecting or creating, organising or storing, access, usage, maintenance, and sharing will normally include re-use of data also. Such re-use can take place only if collaborating agencies share a common vision and purpose. For re-use of data to be part of lifecycle management, it is important to have an eye on future usage and not just on immediate requirements. This allows agencies to follow the *"collect once, use many times"* approach.

Thus, information should be collected and managed in a way that promotes its re-use either by the same agency or by some other agency, which legitimately requires this information. This practice saves valuable time and cost, which would otherwise be expended in collecting this same information for a second time by either the same agency or by some other agency. It also helps avoid duplication of effort with multiple agencies collecting the same data or information, as is the case now.

IX.5.i Safeguards

Effective safeguards are deployed to prevent unauthorised access and use. Agencies involved in information sharing – the agency receiving data and information and the agency providing data and information – can establish a process for evaluating the confidentiality and security related protocols of the data and information shared. This protocol will articulate the access rights and further sharing rights. In addition, for critical information, there is also need for sufficient checks and balance in the form of layered authorisation. The receiving party also needs to share and convince the organisation supplying data about the security of the data received and about the safeguard processes established.

[171] Section 138 of the I-T Act, 1961, for example, prescribes that only that data can be shared, after due authorisation by authorities, which can be considered to be in public interest. But a general understanding is that this provision deals with an individual request rather than an organisational, particularly a stakeholder, request.

IX.5.j Storage, Return and Disposal

Storage of data is an important aspect of data or information exchange. Many tax administrations specify in clear terms how a document or an area containing information can be secured. They also specify a case-by-case method for physically protecting data and systems along with non-electronic forms of data or information; there is usually a uniform policy to govern the entire framework. Many tax administrations either return the information (including any copies made) after its use or dispose of them by destroying them. A description of the procedures so implemented is part of the policy on storage, return or disposal.

In India, since there is no policy for storage of data or information, it is imperative that as part of the overall framework for data exchange, storage of data or information including return and disposal be given adequate importance and protocols be framed on the same lines as has been done by other tax administrations.

IX.5.k Personnel

There should be a dedicated, full-time team for sharing of data or information. Suitability of the personnel should be considered based on their ability, aptitude, competencies and past experience. Their skills should be continuously sharpened through training, seminars, and deputations to other collaborating agencies.

Training

Appropriate education and awareness in the form of training of personnel of collaborating agencies is an essential pre-condition to data or information sharing. The training would include disclosure training including conditions necessary for disclosure, obligations to disclose, along with prevention of unauthorised disclosure and basic confidentiality training to information system users on the usage, storage, destruction and finally, the disposal of confidential information. Apart from the above, role-based training to the assigned persons on their respective roles and responsibilities would be another set of training activities that will improve the delivery of the governance structure for data or information exchange. For this, training needs should be identified, training plans developed and all-out effort made to train the personnel. Thereafter, evaluation must also be made to find out whether the training helped hone the skills required for data or information sharing.

Specialised Personnel

The importance of specialised personnel to deal with data or information exchange cannot be undermined. Many advanced tax administrations have started employing data scientists to enable effortless and continuous data and information sharing.[172] Traditional data analysts look at data in a disconnected manner, whereas specialised data scientists explore and examine data

[172] For effective use of data or information, UK's HMRC has also hired personnel from the private sector. These people have extensive knowledge and experience of data mining, predictive analysis, operational analysis, expertise in developing and applying models for detection of fraud, customer segmentation, consumer behaviour, professional accounting skills, etc.

from multiple disparate sources by sifting through all incoming data to discover a previously hidden insight, which in turn can provide maximum use of all data in the environment effectively. A data scientist goes further than simply collecting and reporting on data and looks at it from many angles, determines what it means, then recommends different and unique ways to apply this data. In this way, data scientists enable effective inter-agency data or information sharing.

Although we do not at this point have any specialised personnel for data or information exchange, it is important that in this era of big data,[173] where data comes in from varied sources and analytical results out of those data are often required in a time-critical framework, the need for data scientists is not ignored. Such data scientists would fulfil the need to continuously track the evolution of ICT and security threats to be one step ahead with respect to security, scalability and efficiency. In addition, they can work on developing more and more sophisticated algorithms and software for analysis of data.

IX.5.l Audit and Accountability Policy

A robust audit and accountability policy addresses the purpose and scope of information sharing, roles and responsibilities of dedicated teams, layered authorisation for access to data, review the safeguards put in place by agency receiving information, and secure storage, disposal and confidentiality of the data and information. Apart from this, sound processes required to facilitate the implementation of this policy should be developed to address the controls associated with it. Such audits are required to be conducted by dedicated teams, who would report the findings to the DG (Systems) of the two Boards for course correction.

IX.6 Roadmap

In Chapter VII of the first report, the TARC had recommended establishing a Special Purpose Vehicle (SPV) to harness the combined potential of the data created or collected by the two Boards. The above recommendation was made keeping in view that data and information exchange would be more aligned if all the data of the two Boards is placed with one entity – the SPV. This will facilitate a single repository or storage of data with common taxonomy and standards. The SPV will receive all data and information from different entities, such as banks, financial institutions, the FIU, AIR and CIB and would place them on one platform so as to provide a common linkage between the relevant data. The recognition of PAN as CBIN, also recommended in Chapter VI of the first report of the TARC, will provide common identification of data and so storage, retrieval or use of data would be further eased. The SPV, therefore, becomes the lynchpin stakeholder organisation for data or information exchange.

Data usage by different organisations with whom data or information is being shared can be different, depending on the needs of the organisations. The strategic and regulatory role of the two Boards and DGs (Systems), elucidated clearly in the first report, would continue to facilitate such exchange of data and information. Since departments and investigating agencies of the CBDT and CBEC use data differently, the CEIB, FIU and SPV will be required to

[173] The TARC in its first report (Section VII.4) had emphasised harnessing the potential of big data.

develop separate MoUs/SLAs so that there is clear understanding about data exchange and their usage by the respective organisations. The above mechanism would promote '*create once, use many times*', facilitating the re-use of the data. This will also obviate the need for every organisation to create its own data warehouse. The interoperability framework governing the above framework to enable the transfer and use of data or information in an efficient and standardised manner is discussed later. This framework should transcend organisational boundaries so as to create an approach which would fulfil the needs of all collaborating organisations, thereby providing a means to arrive at a common framework.

IX.6.a Principles for a common framework

Data and information are strategic resources and they need to be treated as assets for storage, dissemination and usage. The focus, therefore, has to be on managing these valuable resources in a strategic manner so as to optimise their utilisation. A common framework would promote the practice of '*one data, many users*'. This will facilitate re-use of data and require the creation or collection of data each time it is required. This will also help in arriving at time-critical decisions in an expeditious manner and enable seamless flow of data between the participating organisations. Since data would be collected in a common framework with a common taxonomy, format and metadata, it would be ready to be used without loss of time, thereby reducing the time and cost of the data collection.

The basic principles of the common framework are as given below:

a) Collection of quality data or information
b) Storage of the data or information for quick retrieval
c) Use or re-use of data or information from one source
d) Institution of multi-layered authorisations
e) Promotion of a culture of mutual trust, openness and willingness to share between the collaborating organisations, with rights and responsibilities
f) Generation of information to support decision making

While NDSAP made some strides in the field of data and information sharing, it wasn't able to achieve sharing of sensitive data between the government agencies as the policy's mandate was restrictive in nature and only covered data that was sharable in nature. The exchange of data and information between different governmental agencies, in particular between the CBDT, CBEC, FIU, CEIB, RBI and SEBI needs to be the rule and not the exception.[174]

IX.6.b Act *versus* Policy

The question that needs to be addressed in the context of a common framework for exchange of data or information is whether a policy guiding the agencies and departments – CBDT,

[174] From our interaction with the agencies and departments, it is not very clear whether NDSAP made any impact in creating a common frame for data sharing. This may also be due to the fact that the agencies and departments consider their data to be sensitive, and hence non-sharable.

CBEC, FIU, CEIB, RBI and SEBI – is sufficient or whether there is need for a statute. While a policy is a document that normally outlines the intent and purpose and can also indicate an implementation plan and set long-term goals, it does not bring a binding mandate and an enforcement mechanism. A legal framework in the form of a statute would include all these. A statute would mandate all entities to exchange data in a timely and seamless manner, whether digitally or otherwise, and in case this does not happen, prescribe consequences, thus overriding numerous structural and functional differences or hurdles. If at all a policy were to be developed to give effect to a robust mechanism for inter-agency data or information exchange, amendments would be needed in statutes that govern these agencies which may be cumbersome and might not be feasible.[175]

Many advanced tax administrations have legislations to enable data sharing. These acts enumerate the general rules for data and information sharing in terms of its confidentiality, specifies the process of sharing and process for making requests, stipulates time bound responses to such requests, spells out the consequences of not sharing or unauthorised usage, specifies what constitutes authorised usage, safe storage, disposal, etc. Within these umbrella legislations, organisations normally customise partnership agreements, working collaborative arrangements or MoUs to share data or information. A similar practice can be adopted in India by enacting a specific legislation pertaining to inter-agency data and information sharing with the implicit understanding that while keeping the paramount considerations of confidentiality and security of such data and information intact, data and information can be shared across agencies.

IX.6.c SPV to actualise data or information exchange

The legal framework will also have to address access to data or information. As already stated, the modes of data or information exchange are direct access (automatic exchange), spontaneous exchange and exchange on request.[176] Since the TARC had recommended the creation of an SPV "*to harness the combined potential of the data created or collected*", an SPV would facilitate sharing and utilisation of data or information from one portal with common standards and taxonomy so that the present disparate data assets can be leveraged. All organisations – to begin with working those under the Finance Ministry – should be made part of the SPV. Thus, data for the CEIB and FIU will also be made available with the SPV and would be accessed from one common database. Since the FIU and CEIB data might involve a confidentiality aspect, it may not be accessible to everybody sourcing the data from the SPV; rather, such access to confidential data would be based on layered authorisations.

IX.6.d Data types and data formats

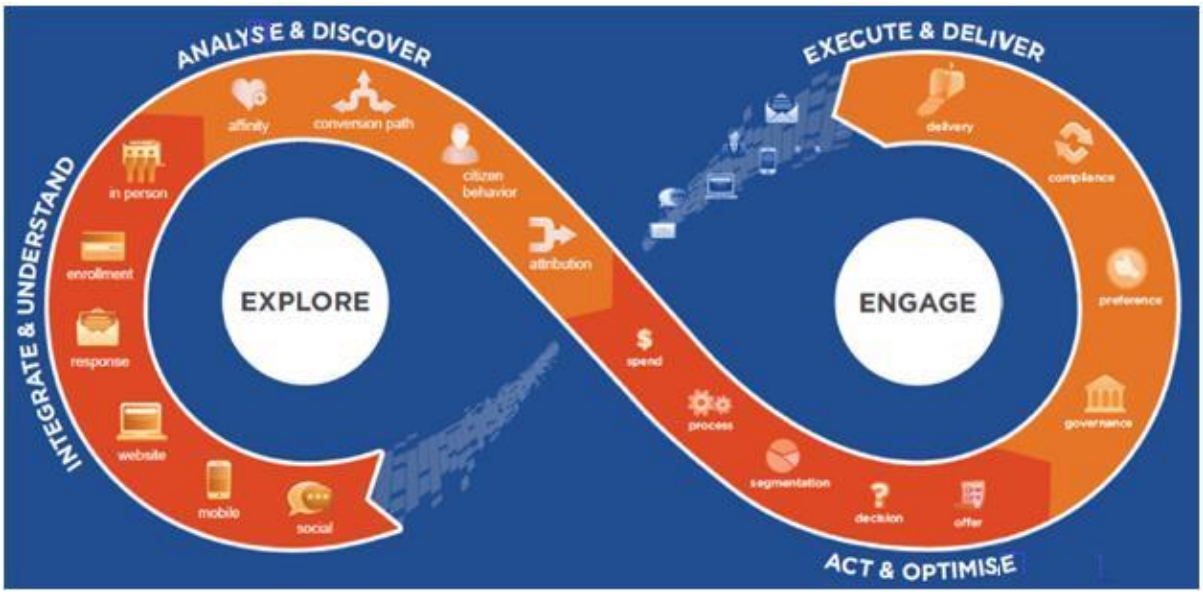
With technological advances, traditional definitions and understanding of terms of data and information are being increasingly challenged. "Data" and "information" are used

[175] While the I-T Act has provisions for sharing data, the indirect tax statutes do not have any such provision for data and information sharing. Apart from this, acts (such as PMLA) that empower other collaborating agencies (such as the FIU) would need amendments.

[176] Methods of information exchange have been elaborated in Appendix IX.7.

interchangeably and the two are increasingly difficult to tell apart. Given enough raw data, today's algorithms and powerful computers can reveal new insights that would previously have remained hidden. Data and information are being collected today from all areas of life. Data formats and types are fast becoming irrelevant as technology recognises different types of sources, using proper mining methods and technologies to find the treasure within each of these sources and then integrating and presenting new insights appropriately according to the unique goals of the organisation. This helps in making effective steering decisions. Since every answer will be different, it is important to recognise that there is no one-size-fits-all solution. Success lies, therefore, in developing algorithms, which can make sense of amorphous data and information. Diagram 9.8 demonstrates the data loop and cycle for optimal usage.

Diagram 9.8: Infinity loop for data and information



Source: Alan Webber, Asymmetric Insights, 2013

The diagram shows that irrespective of the source of data or information whether from social network profiles or computer and mobile device log files (also known as "internet of things"), it needs to be integrated and understood so that the same can be analysed. Continuous discovery from this plethora of data enables it to be acted upon so that its use is optimised, leading to smooth execution and delivery on the objectives and purposes of the exercise. This is a continuous and ever-going exercise, creating an infinity loop. This structure is general in its operation and the principles are universal.

IX.6.e Data or information access or exchange

Data or information can be shared directly by and with persons authorised to do so. In case a particular person is not authorised, access can be available on the basis of requests or through spontaneous sharing. The terms of usage of the SPV portal would govern aspects relating to disclosure and authorisation. The SPV portal would have a log of all such access and if the designated personnel to oversee the security see any breach of access rights, action should be taken on the basis of the recommended statute.

The SPV would also develop MoUs/SLAs for data or information exchange between different organisations. MoUs/SLAs would normally contain procedures for making requests, response time for such requests, reasons for refusing data or information access, mechanisms for audit to assess data or information usage, safeguard mechanisms for access rights, storage and disposal, archiving of data or information to enable their re-use, frequency of requests and special provisions for time-critical responses to requests that have imminent bearing on national security, public safety, etc. MoUs/SLAs would be triggered when further information or data are required, in addition to what is accessible on the portal. Such MoUs/SLAs must be consistent with the overall framework of the recommended statute for data or information exchange.

IX.6.f Key technologies and methods

An analytics programme is a widely available mission-critical technology, typically a platform designed to expand the use of data and significantly improve tax return processing or other key processes, resulting in better service to taxpayers. Key components of the solution will include service-oriented architecture to re-use processes and technology, thereby enforcing technology standards compliance. This architecture will protect investments made once and allow organisations to seamlessly "plug in" additional technologies to meet future business needs. Another component of the technology will be master data management that will provide a single source of reliable data to leverage across all business processes. The central repository of reliable, timely data will improve almost every aspect of the business processes of the tax departments. Third, business process management will allow organisations to rapidly build, test, deploy, and share workflows, as well as document and re-use across business processes, as appropriate.

IX.6.g Specialised personnel to use data or information

The importance of specialised personnel to deal with data or information exchange was discussed in detail in the previous section. These personnel would have requisite knowledge about handling data and information. They would find out the source in a continuous manner so as to fulfil the ever-increasing demand for data or information, work out common standards, develop common taxonomy, and develop sophisticated algorithms and software for analysis of the data. Such specialised personnel would be part of the DG (Systems)/CIO, given the strategic role of the DG (Systems)/CIO, as recommended in the first report of the TARC.

The TARC had also recommended in Chapter III the creation of a Knowledge, Analysis and Intelligence Centre (KAIC) to be the hub of data analytical activity for exploiting the value of the big data in the two Boards. In order to actualise the best outcome, the KAIC was envisaged "*as a shared service between the (two) Boards"*. In the context of the two – SPV and KAIC – the TARC had stated that "*the SPV can support the KAIC by providing it with the necessary platform, tools, technology and expertise*." The above recommendations point to the need to develop a complementary arrangement between the SPV and KAIC through an MoU/SLA.

The KAIC can employ data scientists to enable continuous data and information sharing, as is being done in many advanced tax administrations. These specialised data scientists will explore

and examine previously hidden insights from data or information from disparate sources. Drawing on a combination of computer science, statistics, and operations research, the analysis could help predict fraud and abuse, and help in arriving at smarter decisions by extracting actionable insights from the vast quantities of data within government agencies.[177] The data scientist will also be involved in real-time analysis to respond to queries on vast amounts of data immediately, as the data arrives, rather than waiting until sometime in the future when the data warehouse has batch-processed the data.

The role of data scientists in the era of big data, when tax departments capture trillions of bytes of data or information coming from millions of networked machines, embedded sensors and mobile phones would be able to capture, communicate, aggregate, store and perform analysis on these data.

Effective data visualisation will be another area of responsibility and work of data scientists. Data visualisation is an important tool in the decision making process, allowing decision makers to quickly examine large amounts of data, expose trends and issues efficiently, exchange ideas with key players, and influence decisions that will ultimately lead to desirable results.

IX.6.h Chief Information Officer's Role

In the first report, the TARC had recommended that the DG (Systems) be designated as the Chief Information Officer (CIO) for each Board.[178] Among the functions elucidated in the first report, the CIOs' role in data and information exchange is central as he provides an overarching, regulatory function. His main job is focused on the security aspects of data or information exchange, and towards that, he will co-ordinate, develop, implement, and maintain an agency-wide information security programme. Specialised personnel dealing with data or information exchange will work under the overall guidance and superintendence of the CIO to assess data or information requirements, work on developing common standards and taxonomy, consolidate data or information and develop algorithms and software for use of data or information. It will also be the responsibility of the CIO to rationalise the processes to improve overall interoperability, with improvement in the quality of data or information. The CIO, thus, will be in charge of developing "*thought-leadership*" so that data and information is well-managed both within the tax department and for inter-agency exchanges. The CIO will also be responsible for providing corporate leadership, vision, and direction for effective day-to-day provision of information technology services to the tax department and the continued development of the ICT portfolio to meet national and global requirements.

[177] The terms of reference of the TARC is also "*to review the existing mechanism and recommend measures to enhance predictive analysis to detect and prevent tax/economic offences*." This will be dealt with in a subsequent report.

[178] Chapter III, page 149 of the first report of the TARC

IX.6.i CEIB and FIU under the Governing Council

In the first report, the TARC recommended the abolition of the Department of Revenue and the distribution of the functions currently being carried out by the Department of Revenue between the two Boards. It has also recommended that the enforcement of FEMA and PMLA, which is the mandate of the FIU, should be looked after by the CBDT.[179] On the same lines, it is recommended that the FIU, while being placed under the CBDT, would report for strategic purposes to the Governing Council through the CBDT.

The CEIB, which was created on the basis of a government notification to co-ordinate intelligence gathering activities and enforce actions by various agencies, can work under the Governing Council, as recommended in the first report of the TARC. The CEIB, at present, does not get data or information in a regular manner. The CEIB, working under the Governing Council, will have an umbrella role. The CEIB, which is currently mandated to be a "think tank" on all issues relating to economic offences and maintain data on important subjects, examine trends on intelligence and the changing dynamics of economic offences, undertake analysis of economic activities and act as a nodal agency for receiving, analysing and dissemination to intelligence agencies and other competent authorities, can leverage its current working, with access to data and information, to graduate towards providing a strategic oversight advisory role to the Governing Council on data or information exchange. Such a role will provide inter-agency collaboration to improve business outcomes, minimise inefficiencies between collaborating agencies, co-ordinate associated interagency communication opportunities, work collaboratively to achieve compliance outcomes and provide strategic direction on ways to achieve interagency business outcomes while recognising risks to individual agency accountabilities. This change in the role of the CEIB will transform it into a centralised body to help the Governing Council in pooling data or information and making optimum use of resources of the different agencies.

Since, even under the present dispensation, the CEIB is the only agency carrying out such an oversight role, and there is no parallel agency functioning at the state level, the term "central" can be done away with as it is considered superfluous. The CEIB will then be known as the Economic Intelligence Bureau (EIB). The role of the EIB will be to act as the nodal agency collecting information and intelligence from all collaborating enforcement agencies, collate the information and thereafter disseminate actionable information to the relevant agencies. This way, the EIB will support enforcement agencies and contribute by being a multi-agency co-ordinator with a vision to be the national repository of information on economic offences.

IX.6.j Institutional mechanism to bring coherence

The TARC had recommended the creation of a Governing Council to oversee and approve broad activities to be adopted and make strategic decisions which have a bearing on all the organisations – the CBDT, CBEC, FIU and CEIB. An evaluation mechanism, Independent Evaluation Office, was also recommended to monitor the performance of the tax administration, promote accountability and evaluate policy activity. The Governing Council

[179] The CBDT is the largest recipient of STRs and CTRs from the FIU.

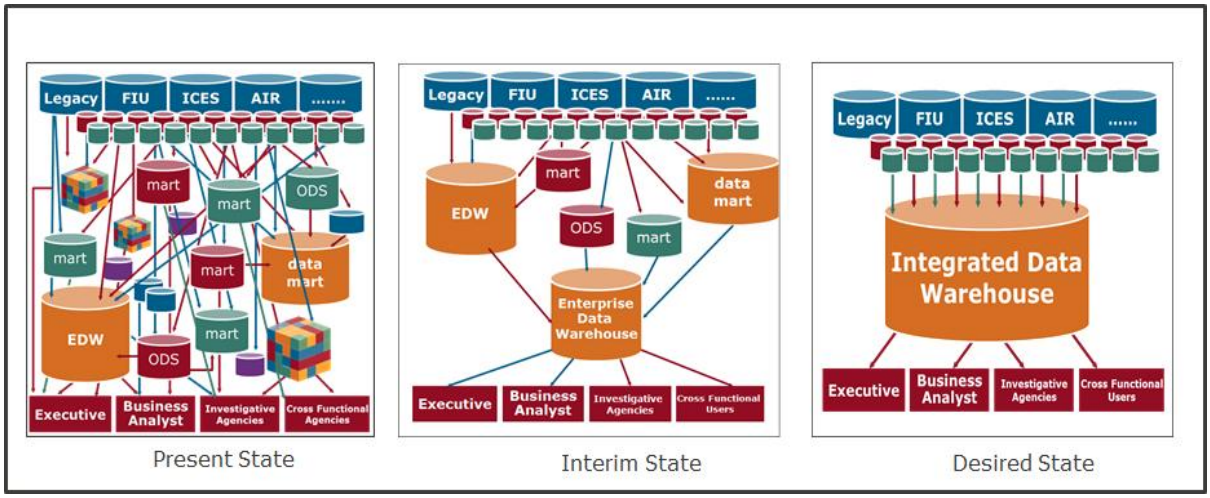
would thus play a key role in data and information exchange between the CBDT, CBEC, FIU, CEIB, SEBI, and banks and develop strategies to reduce the incidence of non-compliance and the tax gap. The Independent Evaluation Office will evaluate the performance of this activity and present its report and suggest course-correction, if it is so required, to the Governing Council to successfully implement data and information exchange by collaborating organisations.

IX.6.k Consolidation of multiple data warehouses

The consolidation of multiple data warehouses and other operational data stores will produce a single, consistent, integrated and accurate view of the data within an organisation. Creating an enterprise data warehouse, that consolidates and integrates multiple data and information, will be an optimal approach to provide a single view of the inflow and outflow of data or information. This will not only benefit the organisations by centralising their data in enterprise data warehouses and generating confidence in the accuracy of the information, it will also enable them to maximise the use of information with a comprehensive, standardised business intelligence platform. The standardisation of business intelligence tools will provide greater control over information and better alignment of ICT with users in collaborating departments. An integrated enterprise data warehouse will enable cross functional analysis as well.

At present, there are a number of disjointed and disconnected enterprise data warehouses, that are either in the process of being constructed (i.e., the CBDT) or are already working (e.g., the CBEC, FIU and CEIB). These data warehouses have been developed for organisation-specific goals and purposes. There does not seem to be a common understanding among them. Bilateral meetings between the CBEC and CBDT have been held to develop a streamlined mechanism for exchange of information. In these meetings, efforts have been made to arrive at standard operating procedures to streamline request-based exchange between the two departments, but there is no effort towards setting up an integrated data warehouse. It may also be pointed out that the first step towards an integrated warehouse would be to consolidate data and information as described above in the "infinity loop". Diagram 9.9 pictographically represents the stages involved in consolidation.

Diagram 9.9: Stages for setting up integrated data warehouse



IX.6.l Data security and usage

Usage and exchange of data or information often leads to challenges on security of data or information and its ethical use. The centralised architecture, with data or information being aggregated in one place and used by many people, needs a fine balance between creating safeguards for organisational data and ease of use, which impacts the user's ability to work efficiently. The most rudimentary security technique to secure data is to apply access controls to the data. Users should only be granted access to data on an as-needed basis. Having access to the wrong data not only means potential security vulnerabilities, it can also result in erroneous analysis and wasted time. Some of the key features around security, therefore, will be formulation of policies on user authentication, access and policy control. Integrity checks needs to be performed before and after use, transfer or backup of data. Data integrity can be verified through one-way cryptographic hash functions, digital signatures and cryptographic binding. Adopting and incorporating best practices around data security is imperative to maintain data integrity and privacy, prevent fraudulent use and ensure easy and efficient use of data and information.

IX.6.m Interim arrangement

While setting up the SPV may take time, it is imperative to outline an interim arrangement so that the eventual movement of data or information to the SPV is not stymied. To start with, it will be important for all the collaborating organisations to prepare a data catalogue which can be shared with other partner organisations. Each organisation will also have to classify what data or information can be shared and what cannot be shared. A common data management system encompassing systems and processes that ensure data integrity, data storage and security, including metadata, data security and access registers would also need to be developed by collaborating organisations. A common platform and scalable architecture with high availability should be developed, for which the CBDT and CBEC will have to take the lead to persuade other agencies to come on board. The CEIB will also play a key role in this effort.

The CBDT and CBEC, being the lead organisations, will have to provide technical know-how with respect to preparation of datasets, contribution of datasets, explanation of metadata and the entire workflow of data publishing, feedback management etc. They can impart training to their own officials as well as those of the collaborating organisations on roles and rules for access, disclosure guidelines and confidentiality framework with a view to ushering in transparency, openness and trust. Such training needs to bring about an overhaul in the environment to foster a culture of willingness to share.

Training on use of data could also be organised. Such training could be on visual analytical techniques to facilitate visual analysis of data across multiple domains, advanced pattern analysis, entity profiling, data mining, network analysis and simulation techniques to widen the tax base and identify revenue leakages/cases of tax evasion.

Institutionalisation of regular training to improve the competence of data users with tax tasks with specific focus on data analysis and interpretation for programme improvement and policy development are key to the success of data analytics. To ensure a properly skilled workforce,

sponsored programmes for education and outreach in data-driven initiatives and incentives to implement an interdisciplinary approach are needed. This could be further supported by focusing on developing and publishing best practices, information sharing, and sponsoring data related initiatives.

IX.7 Summing up

To remain effective and productive, all collaborating agencies will need to abandon the culture and practice of information hoarding and embrace exchange and sharing of data and information. Success will be based less on how strategically physical and financial resources are allocated, and more on how strategically intellectual capital is managed – from capturing, coding and disseminating information to acquiring new competencies through training and development, and to re-engineering business processes. In view of these trends and recognising that knowledge has great potential value and because there is a corresponding failure to fully exploit it, collaborating agencies will have to embark on comprehensive and integrated information exchange programmes.

Improved exchange across silos and inter-departmental exchanges will have to exploit technologies and processes in the data driven economy of the future. Diffusion of knowledge will not happen simply because of legislation, mandates or because new information technology hardware is available. ICT, while critical for enabling the spread of information cannot replace the human intervention required for capturing, storing and exchanging knowledge. Going further, capitalising on the opportunities offered by the variety, volume and speed of information generated will be critical. New and clever technology along with new age analytical techniques with greater inter-departmental and agency co-operation will allow the tax departments to identify non-compliance, willing and otherwise, fraudulent behaviour and patterns, and other unlawful activities. Tax evaders who thought they were beyond the reach of the law can be brought within its grasp and be subjected to accept their liabilities.

Effective organisational learning infrastructure will need to augment its workings. One of the key challenges of a data-based economy is the fostering of innovation. The only way to accomplish that goal will be to build an infrastructure that provides seamless dissemination of information and remain technologically relevant through continuous innovation.

IX.8 Recommendations

The TARC recommends the following:

i) Common framework

a) There is an imminent need to institute a robust framework which will address data and information exchange. This framework should have elements such as provisions for process or making requests for data or information, time-bound responses to such requests, consequences for not sharing and for unauthorised uses, developing common standards, layered authorisations, feedback mechanism on exchange of data or information and strengthening provisions for data privacy and confidentiality. (Section IX.4.b)

b) To enable inter-agency data and information sharing in a systemic manner, a specific legislation should be enacted, proving for general rules for exchange of data and information, with provisions for confidentiality, process of sharing, process of making requests, time bound responses to such requests, consequences for not sharing or unauthorised usage, authorised usage, safe storage, disposal, etc. (Section IX.6.b)

c) While the adoption and use of a common framework may not be sufficient to solve all the present challenges facing data and information exchange by agencies in India, it will encourage agencies to develop a common, long-term vision for collection, use, storage, and disposal of data and information, thus getting rid of the silo structure. (Section IX.4.a)

d) All collaborating organisations – the CBDT, CBEC, FIU, CEIB, RBI and SEBI – need to create a common catalogue of data or information. This will contain information on data, such as source of data, data structure, data definition, quality of data, frequency of update on the data, etc. (Section IX.5.a)

e) The focus of all collaborating organisations must be on organising the data within its own inventory and thereafter having a common database. (Section IX.4.a)

f) Openness and willingness to share must be made the cornerstone for building the catalogue. The catalogues will be shared between the collaborating organisations. A common framework would promote the practice of "*one data, many users*". (Section IX.6.a)

ii) **Common standards and taxonomy**

g) A consistent approach on data across agencies will allow better collation of data and information, making its use easy. A common taxonomy, based on such an approach, will standardise data description, data context and data sharing. Common standards and taxonomy facilitate data exchange between different organisations and enable better reporting and analysis. (Section IX.5.b)

h) Key requirements for common taxonomy must include *de minimis* standardisation of data description, data context and data sharing.(Section IX.5.b)

i) A common standard for data sharing/exchange with a third party is important. All stakeholders need to be brought on a common platform. A steering committee should be formed to provide the platform where all stakeholders bring their data catalogue, scoping of data, data availability, periodicity of data exchange, etc. (Section IX.5.b)

j) A common identification number (CBIN), as recommended in the first report of the TARC, will create a common platform and standard. A robust regulatory mechanism will be required to oversee that the data collection is coherent and relatively accurate. Further, a periodic evaluation of the database must be carried out to see that CBIN continues to provide a common standard and platform.(Section IX.5.c)

iii) **Third-party exchange**

k) All collaborating organisations must categorise the data or information into what can be granted general accessibility and what can be considered for limited sharing or for

somewhat spontaneous sharing. The categorisation must be known *a priori* to the other organisations. (Section IX.5.g)

l) This categorisation will help the organisations in being specific in their requests. These requests must be mutually respected. (Section IX.5.g)

m) The data or information exchange with third parties must be on a digital platform in a seamless manner and exchange of data or information through physical media, i.e., through paper, compact disc, external drive, etc., should be avoided. (Section IX.5.c)

n) SLAs/MoUs with third parties should be entered into to develop a common framework of data or information for exchange. (Section IX.5.c)

o) Data or information exchange must necessarily be done through a common utility, tailored to the specific data availability or framework for data creation or collection by a particular organisation, so that data matching with the CBDT's and CBEC's existing data is seamless and the error percentage is minimal. (Section IX.5.c)

p) For data or information exchange through SLAs/MoUs to be effective, each organisation will have to inform other stakeholders about its contact person. Any request to that organisation can be directed towards this person. If a change occurs in the contact person, this will have to be informed on a real-time basis so that stakeholders are not inconvenienced. (Section IX.5.c)

q) Organisational difficulties in data or information exchange through this utility can be discussed in a Steering Committee, set up for the purpose, comprising all collaborating agencies. (Section IX.5.c)

iv) **Data storage**

r) Algorithms must be developed to make sense of the amorphous data and information coming from various sources into structured data so as to execute and deliver the objectives and purpose of collecting the data. (Section IX.6.d)

s) Key components for developing analytics and algorithms will include service oriented architecture to re-use processes and technology, thereby enforcing technology standards compliance. This architecture must be such as to allow organisations to seamlessly "plug in" additional technologies to meet future business needs. Other components of the technology will be master data management to provide a single source of reliable data to leverage across all business processes and business process management to build, test, deploy, and share workflows, as well as document and re-use across business processes. (Section IX.6.f)

t) There will be portal of the SPV for access to data or information. Access to the SPV portal can be granted only to persons who are authorised and the portal will have a log of all such accesses. The terms of usage of the SPV portal will govern aspects relating to disclosure and authorisation. (Section IX.6.c)

u) The SPV will also develop SLAs/MoUs for data or information exchange between different collaborating organisations. These SLAs/MoUs will be triggered when further information or data are required, in addition to what is accessible on the portal. SLAs/MoUs will

normally contain procedures for making requests, response time for such requests, reasons for refusing data or information access, mechanisms for audit so as to assess data or information usage, safeguard mechanisms for access rights, storage and disposal, archiving of data or information to enable their re-use, frequency of requests and special provisions for time-critical responses to requests that have imminent bearing on national security, public safety, etc. (Section IX.6.e)

v) In line with the recommendations in the first report for the creation of an SPV, the SPV will facilitate sharing and utilisation of data or information from one portal with common standards and taxonomy so that the present disparate data assets can be leveraged. (Section IX.6.c)

w) The consolidation of multiple data warehouses and other operational data stores that consolidates and integrates multiple sets of data and information will be an optimal approach to provide a single view of the inflow and outflow of data or information. An integrated enterprise data warehouse will also enable cross functional analysis. (Section IX.6.k)

v) **Data usage**

x) The most critical aspect of establishing a data analytics infrastructure is to establish a mechanism to process and structure data so that it is ready for analysis. Therefore, it will be imperative for all collaborating agencies to evaluate the quality of data available for a meaningful analysis. (Section IX.5.e)

y) Information must be collected and managed in a way that promotes its re-use either by the same organisation or by some other organisation. This *'collect once, use many times'* approach helps save valuable time and cost and avoids duplication of efforts by multiple agencies. (Section IX.5.h)

z) For better re-use of data to be part of lifecycle management, all agencies must have an eye on the future use of data or information and not just on their immediate requirements. (Section IX.5.h)

aa) A joint Steering Committee, comprising officials of both the CBDT and CBEC and the Directorates of Systems of the two Boards, will have the mandate to work out details of the data life cycle – planning, collecting or creating, organising or storing, access, usage, maintenance, and re-use and sharing with a common vision and purpose. (Section IX.5.a)

vi) **Safeguard and security**

bb) Safeguards must be instituted to ensure confidentiality of data or information exchanged and prevent unauthorised access or use of data or information. The agency receiving information and the agency providing information need to establish safeguard processes for evaluating the confidentiality and security related protocol of the data and information shared. This safeguard protocol will need to clearly articulate access rights and further sharing rights and be made available upfront to the other party. (Sections IX.5.d and IX.5.i)

cc) Data or information should not be open to everybody in the organisation. Access to data or information should be layered depending on the job role, responsibility and the nature of information. (Section IX.5.f)

dd) The agencies can enforce effective access control so that authorised personnel are equipped with the least privilege needed to perform their official duties. These access controls could be set up in the data warehouses based on personnel clearances and accordingly personnel can be given restricted or general access. (Section IX.5.f)

ee) There should be additional checks in the form of layered authorisations. The receiving party must share the extent of information security tools and processes established. (Section IX.5.d)

ff) Key features for security of data will include policies on user authentication, access and policy control. Integrity checks needs to be performed before and after use, transfer or backup of data. Data integrity can be verified through one-way cryptographic hash functions, digital signatures and cryptographic binding. Adopting and incorporating best practices around data security is imperative to maintain data integrity and privacy, prevent fraudulent use and allow easy and efficient use of data and information. (Section IX.6.l)

vii) **Audit and accountability**

gg) A robust audit and accountability policy must be developed to address the purpose and scope of information sharing, roles and responsibilities of dedicated teams, authorisation layers access to data, review of the safeguards put in place by an agency receiving information and the secure storage, disposal and confidentiality of the data and information. Along with the policy, sound processes are required to facilitate the implementation of the policy. These audits must be conducted by dedicated teams who should report the findings of the audit to the DG (Systems) of the two Boards for course correction. (Section IX.5.l)

hh) The Independent Evaluation Office will evaluate the performance of this activity and present its report and suggest course-correction, if required, to the Governing Council for the successful implementation of data and information exchange by collaborating organisations. (Section IX.6.j)

viii) **Personnel management**

ii) Specialised personnel must be engaged to manage data or information exchange. Their job will entail finding sources of data or information in a continuous manner to fulfil the ever-increasing requirement for data or information, work out common standards, develop common taxonomy and develop sophisticated algorithms and software for analysis of the data. They will be part of the CIO/DG (Systems) in each Board. (Sections IX.5.k and IX.6.g)

jj) The CIO's role in data and information exchange will be central to provide an overarching, regulatory function and will focus on security aspects of data or information exchange. Towards that, he will co-ordinate, develop, implement, and maintain an agency-wide information security programme. The CIO thus will the overall in-charge for developing

"*thought-leadership*" so that data and information is well-managed both within the tax department and for interagency transfers. (Section IX.6.h)

kk) Specialised data scientists must be engaged to explore and examine previously hidden insights from data or information from disparate sources. They will also look at the data from many angles and help inter-agency data or information sharing. They will work in the Knowledge, Analysis and Intelligence Centre (KAIC), recommended for creation in the first TARC report. (Section IX.6.g)

ll) There should be a dedicated, full-time team for sharing data or information. The suitability of the personnel should be considered based on their ability, aptitude, competencies and past experience. Their skills should be continuously sharpened through training, seminars, and deputations to other collaborating agencies. (Section IX.5.k)

mm) The training needs of officials should be identified, training plans developed and an all-out effort made to train personnel. Thereafter, evaluations must be made to find out whether training helped in honing the skills required for data or information sharing. (Section IX.5.k)

nn) Training of officials of all collaborating organisations must be organised on roles and rules for access, disclosure guidelines, and confidentiality framework to usher in transparency, openness and trust. The CBDT and CBEC should take the lead in this effort and provide the technical know-how for the preparation of datasets, contribution of datasets, explanation of metadata and the entire workflow of data publishing, feedback management etc. Such training will help in fostering a culture of willingness to share. (Sections IX.5.k and IX.6.m)

oo) Training on the use of data, comprising visual analytical techniques to facilitate visual analysis of data across multiple domains, advanced pattern analysis, entity profiling, data mining, network analysis and simulation techniques is needed to widen the tax base and identify revenue leakages/cases of tax evasion. (Section IX.6.m)

ix) Revamping the FIU and CEIB

pp) The CEIB will work under the Governing Council, recommended in the first report, to play a strategic oversight advisory role to the Governing Council on data or information exchange. The Governing Council would thus play a key role in data and information exchange between the CBDT, CBEC, FIU, CEIB, SEBI and banks, and develop strategies to reduce the incidence of non-compliance and reduce the tax gap. (Section IX.6.i)

qq) Since the CEIB is the only agency carrying out such an oversight role even under the present dispensation and there is no parallel agency functioning at the state level, the term "Central" should be done away with as it is considered superfluous. CEIB will then be known as Economic Intelligence Bureau (EIB). The role of EIB will be to act as the nodal agency collecting, collating and disseminating information and intelligence to relevant agencies and to be the national repository of information on economic offences. (Section IX.6.i)

rr) On the same lines, the FIU, while being placed under the CBDT as recommended in the first report of the TARC, will report for strategic purposes to the Governing Council through the CBDT. (Section IX.6.i)

ss) A common platform and scalable architecture with high availability should be developed as a first step and for that, the CBDT and CBEC will have to take the lead and persuade other agencies to come aboard. The CEIB will play a key role in this effort. (Section IX.6.m)

Appendices

Chapter IX

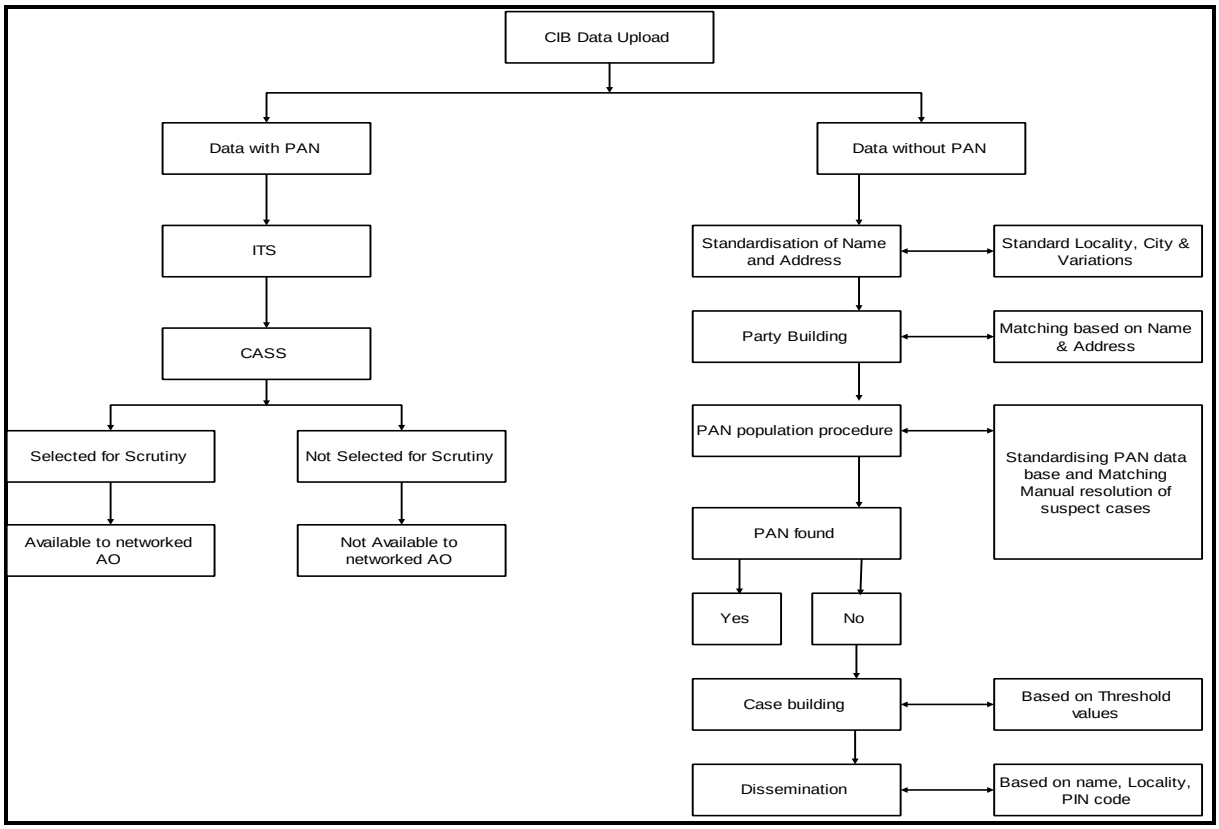
Information Exchange

Appendix IX.1

CIB module in the ITD System of the CBDT

The Enforcement Information System (EFS) of the ITD System of the CBDT contains the CIB module for sorting, collating, managing, organising and analysing information from various sources. The CIB uploads information in this module. The module assists in identifying the PAN of a transaction and allows updating of PAN information. The flow of CIB information (both PAN as well as non-PAN) through the ITD system is shown in Diagram 9A.1 below.

Diagram 9A.1: Flow of CIB information through the ITD system



Assistance to the AO at the time of scrutiny is provided in the form of Individual Transaction Statement (ITS) report, which brings together information from multiple sources against a PAN in a single report and gives a more comprehensive financial profile of the tax payer.

Appendix IX.2

Information exchange through DTAAs

Simultaneously and along with global efforts, effective steps have been taken in the last three years to create an appropriate legislative framework to receive and effectively utilise information received from foreign jurisdictions. These steps include renegotiating existing DTAAs to update the provisions on exchange of information to internationally agreed standards including enabling India to receive banking information (e.g., with Switzerland), entering into new DTAAs with provisions on exchange of information as per internationally agreed standards and entering into TIEAs with no tax or low tax jurisdictions (e.g., with Cayman Islands, British Virgin Islands etc.).

A number of legislative changes has also been carried out in the last two years including extending the time limit for completing assessments by one year if an enquiry is made from a foreign jurisdiction, extending the time limit for reopening cases to sixteen years where income that has escaped assessment is related to an asset located outside the territory of India,, putting in place a reporting mechanism for submission of details of foreign bank accounts, financial interests, immovable properties or other assets outside India, enabling provisions (Section 94A of the I-T Act) for notifying non-co-operative jurisdictions if the said jurisdiction does not effectively exchange information with India etc. Administrative measures, such as strengthening the Foreign Tax and Tax Research Division in the CBDT and creating a dedicated Exchange of Information Cell, have also been taken.

The basic legal framework for Exchange of Information under DTAAs is provided in "Article 26 - Exchange of Information", which obliges the Competent Authorities[180] of the two countries to exchange information to carry out the provisions of the DTAAs or to administer and enforce domestic laws concerning taxes. Article 26 of India's DTAAs are modelled on the OECD Model Tax Convention with some minor differences in individual DTAAs.[181]

India's TIEAs are based on the 2002 Model Agreement on Exchange of Information on Tax Matters developed by the OECD Global Forum Working Group on Effective Exchange of Information with certain variations.[182] The TIEAs only cover exchange of information on request, i.e., when the information requested relates to a particular examination, inquiry or investigation, and does not cover automatic or spontaneous exchange of information. The

---

[180] "Competent Authority" is defined in the DTAAs/TIEAs as the authorised representative of the Ministry of Finance.

[181] The number of the Article in different DTAAs can vary.

[182] Para 9 of the Commentary to Article 26 of OECD Model Tax Convention states that information can be exchanged in three ways – on request, on automatic basis and spontaneously. While most of India's treaty partners accept this view and exchange or are willing to exchange information on automatic basis and spontaneously, other treaty partners have reservations on exchanging information automatically. The government is making efforts both at the bilateral level and through global forums to make the exchange of information on automatic basis part of global standards.

requested party, however, is obliged to provide banking information and information without domestic interest. The information received under the TIEAs may be disclosed to other authorities with the written consent of the competent authority of the requested party. The TIEAs also have provisions for tax examination abroad.

Under DTAA/TIEA, information can only be provided to either carry out the provisions of the relevant agreement or to enforce or administer domestic laws concerning taxes covered by the agreement. In general, such information received under the DTAA/TIEA is to be disclosed and used by the persons concerned with the taxes as specified in the agreement. They may disclose it in public court proceedings or in judicial decisions. However, if such information is to be used for purposes other than taxation, then it can be done only in accordance with the specific provisions of the agreement.

There were no provisions in any of the DTAAs for sharing information for purposes other than taxation until the year 2009. The provisions of the Exchange of Information were revised by OECD in 2008 and it has been recommended that the same language be added in Article 26 itself according to the 2012 update to Article 26 of the OECD Model Tax Convention. Contracting States who wish to broaden the purposes for which they may use information exchanged under Article on Exchange of Information, can do so by including the revised text in their Article on Exchange of Information in their agreements.

India started revising its Article on Exchange of information in 2009 to bring it in line with international standards and has been negotiating with its treaty partners to include the paragraph referred above in all its existing articles on exchange of information. As on date, the paragraph enabling the Competent Authority to share information with other agencies, with the approval of the supplying state, is available in the agreements with Swiss Confederation, Norway, Nepal, Mozambique, Georgia, Estonia, Lithuania, Taiwan and Uzbekistan.[183]In addition, India has Tax Information Exchange Agreements (TIEA) currently in force with Liberia, Cayman Islands, Bermuda, Bahamas, British Virgin Islands, Isle of Man, Jersey, Guernsey and Macau.

[183] The revision of this paragraph with many other treaty partners are in different stages, viz., under negotiation, negotiations completed but awaiting signing of the agreement, signed but yet to be ratified by the other country etc.

Appendix IX.3

Data collection mechanisms of the CBEC

The Indian Customs Electronic Commerce/Electronic Data Interchange (EC/EDI) Gateway (ICEGATE) is a portal that provides e-filing services to trade and cargo carriers and other clients of the Customs Department (collectively called Trading Partners). At present, about 24000 users, who serve about 6.72 lakh importers/exporters, are registered with ICEGATE. ICEGATE links about 15 broad types of partners with the Customs EDI through message exchanges enabling faster customs clearance and facilitating export/import trade.

ICEGATE is an infrastructure project that fulfils the department's EC/EDI and data communication requirements. Through this facility, the department offers a host of services, including electronic filing of the bill of entry (import goods declaration), shipping bills (export goods declaration) and related electronic messages between customs and the trading partners using communication facilities (e-mail, web-upload & FTP) using the communication protocols commonly used on the internet. Airlines and shipping agents can file manifests through the internet using this facility, while custodians and cargo logistics operators interact with Customs EDI through ICEGATE for cargo and logistics and related information. Besides, data is also exchanged between Customs and the various regulatory and licensing agencies such as the DGFT, RBI, Ministry of Steel and DGCIS through ICEGATE. The National Import Database (NIDB) and Export Commodity Database (ECDB) for the Directorate of Valuation (DOV) are also being serviced through ICEGATE. All electronic documents/messages being handled by the ICEGATE are processed at the customs end by the Indian Customs EDI System (ICES), at 116 customs locations. The CBEC has embarked upon centralisation of its infrastructure and all customs locations have been shifted to the centralised infrastructure hosted at the data centre by linking them through MPLS based WAN.

In addition to e-filing, ICEGATE also provides a host of other services like e-payment through designated banks, on-line registration with Customs for IPR, online verification of DEPB/DES/EPCG licences and IE Code status through DGFT and links to various other important websites/information pertaining to the Customs core business process among other things.

The ICEGATE also provides a 24x7 helpdesk facility for its trading partners. To ensure secure filing, digital signatures need to be put on the bill of entry and other documents/messages to be handled through the gateway. Table 9A.1 gives a list of partners and the nature of information exchange in the ICEGATE.

Table 9A.1: EDI partners for data or information exchange

EDI trading partner	Nature of information exchanged through EDI	No. of messages in prescribed format (approx.)
Importers/Exporters/CHA	Bills of entry/shipping bills and related messages	13
Airlines/Shipping Agents/Shipping Line	Manifests and cargo logistics messages	26
Air Custodians	Cargo logistics messages	9
Sea Custodians	Cargo logistics messages	18
ICDs	Cargo logistics messages	6
Banks	Financial messages – duty drawback disbursal and customs duty payment	9
DGFT	Licence, shipping bills and IE Code data	13
RBI	Foreign exchange remittance data	1
DGCIS	Trade statistics	2
Directorate of Valuation	Valuation data	2

The ICES is running at 116 locations. The ICES has to automatically receive and process all incoming messages. It generates all outgoing messages automatically at the appropriate stage of the clearance process.

ICEGATE is the interface of ICES with the external world for customs clearance related messages and sharing of trade statistics/customs clearance data with licensing and regulatory agencies such as DGFT, DGCI&S, Ministry of Steel, RBI etc.

RMS (Risk Management System) is the 3rd component, which facilitates compliant trade segregation of the transactions requiring deeper scrutiny by customs officers.

Appendix IX.4

Mandate of the Central Economic Intelligence Bureau

F.No.A.11013/9/85/-AD-I
Government of India
Ministry of Finance
Department of Revenue

New Delhi, the 20th September, 1985

OFFICE MEMORANDUM

Subject - **Functions and powers of the Central Economic Intelligence Bureau**

The Central Economic Intelligence Bureau has been set up for coordinating and strengthening the intelligence gathering activities, the investigative efforts and enforcement action by various agencies concerned with Investigation into economic offences and enforcement of economic laws. The Bureau will be responsible for maintaining liaison with the concerned Departments and Directorates both at the Central and State Government level and in addition will be responsible for the overall direction and control of the investigative agencies within the Department of Revenue Itself.

Functions

2. The central Economic Intelligence Bureau will have the following functions:

i. Collection of intelligence and information regarding aspects of black economy which require close watch and investigations and also keeping in view the scene of economic offences. Bureau will collect information and provide periodical and special reports to the concerned authorities.

ii. To keep a watch on different aspects of economic offences and emergence of new type of such offences. It will be responsible for evolving the counter measures required for effectively dealing with the existing and new type of economic offences.

iii. To prepare and maintain dossiers on the organized gangs carrying on smuggling operations and other economic offence as also on individuals operating on a large scale. The Bureau alone will plan, coordinate and supervise the execution and the operation against such gangs and persons as well as the follow-up of investigation after such operations.

iv. To act as nodal agency for co-operation and coordination at the international level with other customs drugs, law enforcement and other international agencies in the area of economic offences.

v. Bureau in consultation with Central Board of Excise and Customs will be responsible for preparing the scheme of the nominated Central agency envisaged in Chapter 2 of

the Narcotics Drugs and Psychotropic Substances Act 1985. The Bureau will take all actions to obtain Government approval and for setting of this Central agency.

3. Director General, CEIB will also be designed as Additional Secretary (Economic Intelligence) in the Department of Revenue, Ministry of Finance. As Additional Secretary (EI) under the overall supervision to the Revenue Secretary, he will be responsible for division and undertaking programme of strengthening and modernizing the Intelligence agencies under the Department of Revenue. He will oversee, Inspect, and report in the performance from the technical angle in the various, heads of intelligence and enforcement agencies in the Department of Revenue. He will also have the authority issue such directions to these agencies as may be necessary for taken coordinating action and for following integrated system and procedures for the effective discharge of the intelligence and enforcement functions.

4. Director General (CEIB) will be provided with administrative and other logistic support by the Director General Revenue Intelligence unit further orders and until the development of its own independent infrastructure.

Powers

5. It is envisaged that the intelligence agencies under the Department of Revenue will continue to the under the administrative control of CBEC and CBDT as the case may be. The authority of DG (CEIB) over these intelligence agencies will be confined to all actions required for attaining the objective and performing the functions outlined above. The Bureau will have the authority to direct the agencies under the Department of Revenue to collect and make available to the Bureau Intelligence and information required to discharge its responsibilities with the Functions of developing dossiers, enforcement capability against the big gangs and important economic offenders. Except for these areas the concerned agencies will continues to carry on their intelligence and enforcement actions as therefore under the administrative control of the two Boards. The Bureau would also not be concerned with routine administrative matters at these agencies. While DG (CEIB) is being authorized under the various Acts, it is expected that DG (CEIB) will limit the exercise of his powers of direction and control to the objective assigned to his organization and these alone. To provide authority, the DG (CEIB) will concurrently exercise the following powers:

1) That of a Collector of customs under the Customs Act, 1962 and of a Collector of Central Exercise under the Central Exercise Act, 1944.
2) Of the Director of Enforcement under the Foreign Exchange Regulation Act. 1972.
3) Of the detaining authority under, and the authority vested with powers for the purpose of Sections 9 of the Conservation of Foreign Exchange and Prevention of Smuggling Activities Act, 1974.
4) Of the Narcotics Commissioner under the Narcotics Drugs and Psychotropic Substances Act 1985
5) Of the Gold Control Administrator under the Gold Control Act, 1968.
6) Of the Commissioner of Income – tax under

i. The Income Tax Act, 1961

ii. The Wealth Tax Act, 1957.

iii. The Gift Tax Act, 1958.

iv. The Companies (Profits) Surtax Act, 1985.

v. The Estate Act, 1953

6. The receipt of this O.M. may please be acknowledged.

Sd/-
(J.M.TREHAN)
Under Secretary of the Govt. of India

To,

All Heads of Department
Under CBEC/CBDT and
Department of Revenue

Revised mandate of CEIB

F.No. 50/107/2003/Ad-I
Government of India
Ministry of Finance
Department of Revenue

New Delhi, the 12th December, 2003

Subject: **Revised Charter of Central Economic Intelligence Bureau (CEIB)**

Sir,

The Central Economic Intelligence Bureau (CEIB) was set up in 1985 for coordinating and strengthening the intelligence gathering activities, and enforcement action by various agencies concerned with investigation into economic offences and enforcement of economic law. The Bureau was made responsible for maintaining liaison with the concerned Departments and Directorates both at the Central and State Government level and in addition was made responsible for the overall direction and control of the regulatory agencies functioning under the administrative control of the Ministry of Finance.

2. In order to streamline and strengthen the functioning of the CEIB, the Group of Ministers (GoM) recommended that its Charter be revised to enable it to concentrate on its two roles, with one Wing functioning as the Secretariat for Economic Intelligence Council (EIC) and the other related to economic intelligence (ECOINT). The GoM further recommended that

besides the usual secretarial functions, the Secretariat Wing should pay special attention to keeping a close watch on the progress of implementation of all decisions taken by EIC and REICs and report the same to EIC. Its Intelligence Wing should receive intelligence reports from all sources of ECOINR, collate and analyse them and disseminate them among the users/consumers/decision makers.

3. Accordingly, it has been decided that the Charter of the CEIB shall be suitably revised.

Responsibilities

4. The CEIB will have the following responsibilities:

1) Act as a 'think tank' for the Department of Revenue, Ministry of Finance on all issues relating to economic offences and maintain data on important subjects and dossiers on important tax evaders, violators of economic laws, white collar operators, etc. Information for dossiers shall be sent to the CEIB within 30 days of finalization of investigations/issue of show cause notices.

2) Examine trends on intelligence and changing dynamics of economic offences, and the nexus among anti-national elements, money launderers, drug traffickers, etc., including new modus operandi for such offences; and suggest measures for dealing effectively against economic offenders.

3) Undertake analysis of economic activities at the macro level after interaction with academic and research institutions, if need be;

4) Act as nodal agency for receiving, analysing and dissemination to the intelligence agencies and competent authorities, disclosure of financial information concerning suspected proceeds of crime or as required by national legislation (in order to counter money laundering) relating to economic offences.

In addition, CEIB shall also monitor the action taken by relevant agency generation the intelligence input.

i. Act as nodal agency for co-operation and coordination at the international level with other international agencies in the areas of economic offences in addition to the existing international coordination in various fields by the respective intelligence agencies.
ii. Ensure suitable interaction with the National Security Council Secretariat on matters having a bearing on national and economic security.

Functions

5. The CEIB will have the following functions:

i) Act as the Secretariat for Economic Intelligence Council (EIC) by

- Providing all necessary support and assistance, including infrastructural support to the EIC in discharge of its functions.
- Organizing meetings at prescribed intervals
- Coordination of the progress on implementation of all decisions taken by the EIC

ii) Act as the nodal agency for ECOINT (Economic Intelligence) and ensure real time monitoring and effective interaction and coordination among the concerned regulatory agencies in the areas of economic offences. Intelligence having multi-agency ramifications shall be communicated to other concerned agencies through the CEIB. Coordination among various agencies in such cases shall thereafter be done by the CEIB

iii) To ensure prompt dissemination of intelligence having security implications among the NSCS, IB &RAW

iv) Coordination the functioning of Regional Economic Intelligence Councils (REICs).

v) Coordination with Multi Agency Centre (MCA)

vi) Organize meetings of the Working Group under the chairmanship of Revenue Secretary at prescribed intervals and submit a report to the Chairman of the EIC after every meeting.

Structure

6. The Office of the CEIB will be located at Delhi and will comprise four separate Units, each headed by an officer of the rank of a Joint Secretary, looking after specialized areas of Economic Intelligence (ECOINT), which will be as follows:

i. Financial Intelligence Unit (FIU) to combat money Laundering

ii. EIC Secretariat Unit acting as a Secretariat of the EIC and also coordinating the work of the REICs. This Unit will also handle Administration and Budget.\

iii. Economics Intelligence Coordination Unit looking after general coordination and work relating to economic offences including drug trafficking/narco terrorism, foreign exchange violations, supply of counterfeit currency, *hawala* transactions, financial frauds in stock markets, insurance, real estate, tax evasion, etc.

iv. COFEPOSA Unit, which is already in existence, relating to work under the COFEPOSA Act.

7. The receipt of this letter may kindly be acknowledged.

Yours faithfully,

(Prashant)
Director (Hqrs)

Appendix IX.5

Updated mandate of the Economic Intelligence Council

The Economic intelligence Council (EIC) was reconstituted in 1997 to improve co-ordination among various agencies and Departments under the Ministry of Finance (MoF) in view of linkages being developed in recent times between economic offences and threats to national security.

EIC has the following mandate:

i. Consider various aspects of intelligence relating to economic security and evolve a strategy to effectively collect and collate such intelligence and disseminate it to identified user agencies and departments.

ii. Review measures to combat economic offences and formulate a co-ordinated strategy of action by various enforcement agencies.

iii. Review important cases involving inter-agency co-ordination and approve modalities to improve such co-ordination.

iv. Consider and approve measure to strengthen the working of individual intelligence and enforcement agencies under the MoF.

v. Examine the changing dynamics of economic offences, including new *modus operandi* for such offences and approve measures for dealing with them effectively.

vi. Advise on amendments to laws and procedures to plug loopholes to ensure more effective action against economic offenders.

vii. Review measures to combat the generation and laundering of black money and approved strategy for dealing effectively with black money operators and tax evaders.

viii. Interact through its secretariat with the National Security Council Secretariat (NSCS) on matters having a bearing on national security and economic security.

ix. Consider and approve lists of annual tasks, including their periodic updating, for each of its agencies in consultation with all user departments and agencies, including the Intelligence Bureau (IB) and Research and Analysis Wing (RAW), and direct its secretariat to make available the task lists to the NSCS.

x. Consider and introduce a system of annual monitoring and evaluation (qualitative and quantitative) of the performance (in the field of intelligence collection, prompt dissemination, follow-up, etc.) of all agencies under its control.

xi. Consider and suggest appropriate budgeting of all agencies under its control.

EIC has the following constitution -

Finance Minister	-	Chairman
Minister of State (Revenue)	-	Vice Chairman

Members

Governor, Reserve Bank of India

Finance Secretary/Secretary, Department of Economic Affairs

Home Secretary

Secretary, Department of Company Affairs,

Secretary, Financial Sector, Department of Economic Affairs

Secretary, National Security Council Secretariat

Chairman, Securities & Exchange Board of India

Chairman, Central Board of Director Taxes (CBDT)

Chairman, Central Board of Excise & Customs, (CBEC)

Special Secretary-cum-Director General, Central Economic Intelligence Bureau (CEIB)

Director General, Narcotics Control Bureau (NCB)

Director General, Directorate General of Revenue Intelligence (DGCEI)

Additional Secretary, Department of Revenue Director, Directorate of Enforcement

Director General, Directorate General of Foreign Trade, Min. of Commerce

Director, Financial Intelligence Unit-India (FIU-IND)

Special Invitees

Secretary, Ministry of External Affairs

Secretary, RAW

Director, Intelligence Bureau

Director, Central Bureau of Investigation

Director General, Border Security Force

The EIC is serviced by the secretariat of the CEIB and the Director General, CEIB, acts as its Member-Secretary. It is required to meet once in six months, but may hold extraordinary meetings as and when considered necessary. It can also invite any other official or person whose views/participation is considered beneficial for the furtherance of its objectives.

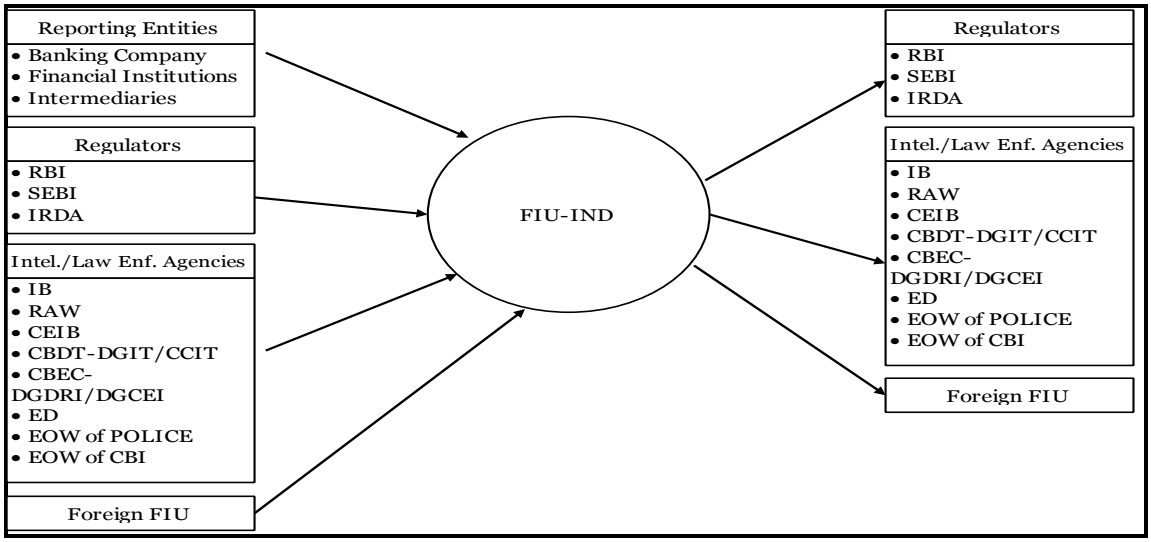
Financial Intelligence Unit

FIU-IND is a member of the Egmont Group, a group of 139 FIUs, which exchange information through a secured network. FIU-IND can seek information from its counterpart foreign FIUs based on specific requests made by law enforcement agencies in the prescribed form. The foreign FIUs respond on the basis of data available to them and in accordance with their domestic laws.

Section 12 of the Prevention of Money Laundering Act, 2002 (PMLA) lays down that every banking company, financial institution and intermediary shall maintain a record of all transactions (for a period of ten years), the nature and value of which may be prescribed. PMLA also prescribes that FIUs be informed about whether such transactions involve a single transaction or a series of transactions integrally connected to each other.

The FIU information comprises Suspicious Transaction Reports (STRs), Cash Transaction Reports (CTRs), Counterfeit Currency Reports (CCRs), and NPO Transaction Reports (NTRs).[184] A typical report contains information about related accounts, transactions, individuals, legal entities, and addresses in a structured manner with their relationships. The agencies reporting to the FIU are banking companies, financial institutions, intermediaries such as stock brokers, sub-brokers, underwriters, portfolio managers, and otherslikecasinos, registrar or sub-registrar of property transfers, real estate agents, dealers in precious metals, precious stones and other high value goods, and private locker operators upon notification by the central government. The framework for flow of FIU information is shown below in Diagram 9A.2.

Diagram 9A.2: Framework for flow of FIU information



[184] Cross-border wire transfer reports have been added to the list of reports to FIU from January 2013.

Three key areas identified for collaboration with the CBDT are effective use of CTR data for tax administration (*i.e.*, identification of high risk non-filers (I-T return) having PAN, identification of bank accounts in arrear demand cases, identification of bank accounts of persons involved in large cash handling, identification of persons with large cash transaction in specific high risk businesses and identification of CTRs in respect of persons already selected for scrutiny), effective use of STRs for tax administration (*i.e.*, review of dissemination and categorisation rule, use of FINnet for electronic delivery of reports, enabling linkage of STRs with CASS and 360-degree profile, enabling feed-back on cases, providing inputs for modifying RFIs); and use of FIU data for information relating to chronic tax evaders and for 360 degree profiling.

If during a routine investigation, the department comes across any gross violation of reporting of suspicious transactions and cash transactions or any violation of KYC norms, it may inform FIU-IND to take appropriate sanctions as part of its compliance function (especially in the case of co-operative banks, intermediaries of securities market and insurance companies where compliance to reporting obligations is rather poor).

The key outcomes of FINnet are as shown in Table 9A.2 below.

Table 9A.2: Key outcomes of FINnet

Function	Present	Under FINnet
Receipt of Reports	Data files	XML format and advanced utilities
	Submission of data files on CD	Online Gateway
	Offline data quality validation	Near real time data validation, compliance management
Analysis	Analysis of STRs using search and link analysis system	Automated identity and relationship resolution
	Basic CTR analysis	Alert generation (BI tools), Risk Management System
	Basic Trend Analysis	Data standardisation
Exchange of Information	Dissemination through letters	Secure role based access
	Request based exchange through letters	Secure information exchange protocol

Methods of information exchange

OECD report on effective inter-agency co-operation, 2013, provides for the following methods of data and information exchange:

i) Direct access to records and databases

An agency can grant direct access to its records and information stored on its databases to designated individuals within other authorities. This access can be for a wide range of purposes, or restricted to specific cases or circumstances. Direct access enables the agency requiring information to search for the information directly in a timely manner. Safeguards can be introduced to protect the confidentiality of sensitive information, such as restricting access to databases to a small number of nominated individuals, and maintaining records of what information was accessed and for what purpose.

ii) Mandatory spontaneous sharing of information

An agency collecting information can provide certain categories of information spontaneously, without requiring a request to be made. This is sometimes referred to as a "reporting obligation". This has the advantage that the information to be shared is identified by officials within the agency holding it, who are likely to have a greater understanding of the information in their records. However, in order for this to be effective, an agency must have clear rules and mechanisms in place to identify the information that must be shared. This is fairly straightforward where an obligation exists to provide all information of a certain class, for example, copies of all cash declaration forms, but is more complex where judgment needs to be exercised to identify information that would be relevant to an investigation.

Further, by itself, this method does not allow officials conducting an investigation to specify the information required. However, it can facilitate the detection of previously unknown criminal activity.

iii) Spontaneous sharing of information

An agency can have the ability to provide certain categories of information spontaneously, but is able to exercise its discretion in deciding whether or not to do so. Where this operates well, it can be as effective as the previous method.

Information is shared spontaneously, but officials in the agency holding the information are able to exercise their judgment to provide only that information which is of value and not all information of a particular class. This model is particularly effective when it is supported by close co-operative working arrangements and a good understanding by officials in each agency of the information requirements of the other agency. This means that, even in the absence of a specific obligation, information sharing between agencies can be very effective.

Models for information sharing that allow discretion to be exercised require clear rules on how this is to be done, For example, decisions as to whether or not relevant information is to be shared can be limited to individuals in certain positions or levels of management, with guidelines setting out the factors that need to be taken into account in making a decision. The effectiveness of this type of legal gateway is also dependent on the ability of officials to identify relevant information and their willingness to exercise discretion to provide information. Where there is no previous experience of inter-agency co-operation, the benefits to both agencies of sharing information must be made clear or there may be a danger that officials exercise their discretion and choose not to share valuable intelligence.

iv) Sharing information on request

An agency can provide information only when such information is specifically requested for. This can be seen as the simplest of the four methods for sharing information, as there is less need for rules or mechanisms to identify information for sharing or to provide access to records. It also has the advantage of allowing officials to specify precisely the information they require. In the context of an ongoing transaction where investigators have identified specific information that is required, this can be a valuable mechanism.

One disadvantage is that, in many cases, an agency might hold information that an investigator is unaware of. This can mean that the investigator is unable to request information, or is only able to do so at a later stage when the value of the information may be reduced.

Based on the above methods of information exchange, the OECD report also provides inter-agency information sharing in different countries in a tabular form, for view at a glance. Tables 9A.3 to 9A.7 give a snap shot of inter-agency information sharing in different countries.

Information sharing at a glance

Table 9A.3: Inter-agency information sharing in the United States

		Authority receiving information				
		Tax administration for civil tax assessments	**Agencies investigating tax offences**	**Customs administration**	**Police or public prosecutor investigating non-tax**	**Financial Intelligence Unit**
Authority providing information	Tax administration (IRS)		Direct access	On request	Reporting permitted	No sharing
	Customs administration	Reporting permitted	Reporting permitted		Reporting permitted	Reporting permitted
	Police or public prosecutor	On request	Direct access	Reporting permitted		On request
	Financial Intelligence Unit (FinCEN)	Direct access	Direct access	Reporting permitted	Direct access	
	Financial regulator	Reporting permitted	Reporting permitted	Reporting permitted	Reporting permitted	Reporting permitted

Table 9A.4: Inter-agency information sharing in the United Kingdom

		Authority receiving information				
		Tax administration for civil tax assessments	**Agencies investigating tax offences**	**Customs administration**	**Police or public prosecutor investigating non-tax offences**	**Financial Intelligence Unit**
Authority providing information	Tax administration (HMRC)		Direct access	Direct access	Reporting permitted	Reporting obligatory
	Customs administration (HMRC)	Direct access	Direct access		Reporting permitted	Reporting obligatory
	Police or public prosecutor	Reporting permitted	Reporting permitted	Reporting permitted		Reporting obligatory
	Financial Intelligence Unit	Direct access	Direct access	Direct access	Direct access	
	Financial regulator	Reporting permitted	Reporting permitted	Reporting permitted	Reporting permitted	Reporting obligatory

Table 9A.5: Inter-agency information sharing in Australia

		Authority receiving information				
		Tax administration for civil tax assessments	**Agencies investigating tax offences**	**Customs administration**	**Police or public prosecutor investigating non-tax offences**	**Financial Intelligence Unit**
Authority providing information	Tax administration (ATO)		Direct access	Reporting permitted	Reporting permitted	No sharing
	Customs administration	Reporting permitted	Reporting permitted		Reporting permitted	Reporting permitted
	Police or public prosecutor	Reporting permitted	Reporting permitted	Reporting permitted		Reporting permitted
	Financial Intelligence Unit	Direct access	Direct access	Reporting permitted	Direct access	
	Financial regulator	Reporting permitted	Reporting permitted	Reporting permitted	Reporting permitted	Reporting permitted

Table 9A.6: Inter-agency information sharing in Canada

		Authority receiving information				
		Tax administration for civil tax assessments	Agencies investigating tax offences	Customs administration	Police or public prosecutor investigating non-tax offences	Financial Intelligence Unit
Authority providing information	Tax administration (CRA)		Direct access	On request	Reporting permitted	Reporting permitted
	Customs administration	On request	Reporting permitted		Reporting permitted	Reporting obligatory
	Police or public prosecutor	Reporting permitted	Reporting permitted	Reporting permitted		Reporting permitted
	Financial Intelligence Unit	Reporting permitted	Reporting permitted	Reporting permitted	Reporting permitted	
	Financial regulator	On request	On request	No sharing	On request	Reporting permitted

Table 9A.7: Key of terms used in the Tables above and their meaning

Terms Used in Tables	Meaning
Direct access	Direct access to information
Reporting obligatory	Obligation to share information spontaneously
Reporting permitted	Ability to share information spontaneously
On request	Information shared on request only
No sharing	No sharing of information permitted

Appendix IX.8

Legal arrangements for inter-agency collaboration

In this Chapter, we have discussed various agreements for inter-agency collaboration for exchange of data or information. SLAs and MoUs are forms of service agreements, which are formal agreements between two or more parties (e.g., between departments, between a department and a common or shared service provider, or between various levels of government). These agreements articulate terms and conditions of a particular service relationship and enhance governance, accountability and service quality by clearly defining roles, responsibilities, processes and performance expectations. Thus, these agreements serve three primary functions:

- Articulating the expectations of the parties to the agreement
- Providing a mechanism for governance and issue resolution, and
- Acting as a means to assess and examine performance and results

It may be pointed out that though MoUs and SLAs have been referred to in the same breath, there are some differences between the two. While an MoU defines the broad parameters of a service relationship between the parties to the agreement, the service vision, and the exercise of decision-making authorities, an SLA establishes the operating parameters and performance expectations between the parties to the agreements. Normally, an SLA is established for each line of service or project. Table 9A.8 gives a comparison between basic elements for MoUs and SLAs for simple MoUs, MoUs and SLAs of medium complexity and for complex MoUs and SLAs.

Table 9A.8: Elements of service agreements

Element	Simple	Medium		Complex	
	MoU	MoU	SLA	MoU	SLA
Parties to the Agreement	Yes	Yes	Yes	Yes	Yes
Recitals ("Whereas" and "Therefore" Statements)	Yes	Yes	Yes	Yes	Yes
Definitions	Yes	No	Yes	No	Yes
Commencement date	Yes	Yes	Yes	Yes	Yes
Duration	Yes	Yes	Yes	Yes	Yes
Reference to supporting documents or related agreements	Yes	Yes	No	Yes	No
Maintenance of the agreement	No	No	Yes	No	Yes

Element	Simple	Medium		Complex	
	MoU	MoU	SLA	MoU	SLA
Notice period for termination or withdrawal	Yes	Yes	No	Yes	No
Designated officials	Yes	No	Yes	No	Yes
Signatories	Yes	Yes	Yes	Yes	Yes

While the normal practice is to frame MoUs and SLAs, written collaborative arrangements/agreements are also used for inter-agency data or information exchange. Collaborative agreements are required for specialised practices as it decides in advance the consequences of the collaboration failing, what happens when the objective or purpose is attained and decides the consequences of the outcome. Thus, collaborative agreements are usually entered into for future endeavours and primarily precede formal agreements. MoUs and SLAs, on the other hand, have a comparatively longer duration of collaboration. MoUs will normally precede SLAs.

Clarity of scope is pivotal to any service agreement. It is thus important to clearly articulate the scope in the service agreements so that the parties involved thoroughly understand their respective obligations, rights and duties. Table 9A.9 lists scope elements for MoUs and SLAs for different complexity levels. The complexity levels are contingent upon understanding, openness and the long-standing relationship existing prior to entering into the service agreements. The elements of the service agreements depend on the nature of its complexity. In some cases, even though the same element can be found in more than one agreement, the level of detail going into the element will differ depending on the nature of the complexity involved.

Table 9A.9: Scope elements service agreements

Element	Simple	Medium		Complex	
	MoU	MoU	SLA	MoU	SLA
Vision	Yes	Yes	No	Yes	No
Purpose or objectives	Yes	Yes	No	Yes	No
Key principles	Yes	Yes	No	No	No
Service scope	Yes	Yes	Yes	No	Yes
Service bundles/service inventory	Yes	No	Yes	No	Yes
Tiered service delivery/channels	No	No	Yes	No	Yes

Element	Simple	Medium		Complex	
	MoU	MoU	SLA	MoU	SLA
Relative roles and responsibilities	Yes	No	Yes	No	Yes
Key service assumptions	No	No	Yes	No	Yes

The governance framework in any service agreement oversees and guides service relationships. It outlines the specific roles and responsibilities of the agencies, the accountability framework, decision making processes, audit and monitoring and dispute resolution mechanism. It also establishes forms and structures for governance. Table 9A.10 compares elements for governance framework in MoUs and SLAs.

Table 9A.10: Elements for governance framework in service agreements

Element	Simple	Medium		Complex	
	MoU	MoU	SLA	MoU	SLA
Form and structure	Yes	Yes	No	Yes	No
Roles and responsibilities	Yes	Yes	No	Yes	No
Relationships with stakeholders	No	No	No	No	No
Accountability	Yes	Yes	No	Yes	No
Decision making processes	No	Yes	No	No	No
Dispute resolution	Yes	Yes	Yes	Yes	Yes
Amendment and termination	Yes	Yes	No	Yes	No
Audit and monitoring	No	No	No	No	No

While the governance framework in service agreements presents a framework for vision and objectives, the operation elements are essential to actualise and give effect to the overall governance structure. The security and privacy of data or information exchange, which is essential to any agreement, needs to be properly outlined and stated with a responsibility matrix to avoid any breakdown in operations. Table 9A.11 compares elements for operations in MoUs and SLAs.

Table 9A.11: Elements for operations in service agreements

Element	Simple	Medium		Complex	
	MoU	MoU	SLA	MoU	SLA
Policies and signing authorities	No	No	Yes	No	Yes
Infrastructure	No	No	No	No	Yes
Work sharing	No	No	No	No	Yes
Customer relationship management	No	Yes	No	No	No
Privacy	Yes	No	Yes	No	No
Security	Yes	No	Yes	No	No
Disclosure and use of information	No	No	Yes	No	Yes
Specific requirements	No	No	No	No	Yes
Service disruptions/business continuity planning	Yes	No	Yes	No	Yes

Any agreement needs to indicate performance targets. Service agreements also need to benchmark performance, and clearly specify specific service levels or other performance targets to be achieved and the nature and frequency of the performance reports related to those targets. The process through which service improvements to one or more services are tracked in response to performance deficiencies should also be described in the service agreements. Table 9A.12 compares performance elements in MoUs and SLAs.

Table 9A.12: Performance elements in service agreements

Element	Simple	Medium		Complex	
	MoU	MoU	SLA	MoU	SLA
Performance targets	Yes	No	Yes	No	Yes
Performance measurement and reporting	Yes	Yes	Yes	Yes	Yes
Link to performance management agreements	Yes	Yes	No	Yes	No
Monitoring responsibilities and processes	No	No	Yes	No	Yes
Evaluation and reporting frequency	Yes	No	Yes	No	Yes
Benchmarks	No	No	No	No	Yes

Element	Simple	Medium		Complex	
	MoU	MoU	SLA	MoU	SLA
Performance of the arrangement	No	No	No	No	No
Risk reporting	No	Yes	No	No	No
Continuous improvement	No	No	Yes	No	Yes
Consequences	No	Yes	No	No	No

Implementation elements identify the approach and timeframes for the phases and stages of the implementation, including detailed planning, service management, service delivery, and when the parties expect the service to be operational. The implementation elements in the service agreements should also identify when designated officials expect to review the effectiveness of the relationship, prior to continuing or including additional services. Table 9A.13 compares implementation elements in MoUs and SLAs.

Table 9A.13: Implementation elements in service agreements

Element	Simple	Medium		Complex	
	MoU	MoU	SLA	MoU	SLA
Transition activities	Yes	No	Yes	No	Yes
Transition roles and responsibilities	Yes	No	Yes	No	Yes
Milestones	Yes	No	Yes	No	Yes
Resource commitments	No	No	No	No	Yes
People and human resource considerations	No	No	No	No	Yes
Transition and training plans	No	No	No	No	Yes
Risk management	No	No	No	No	Yes

It may be also be stated that MoUs or SLAs should include training plans for people involved in implementing the agreements for data or information exchange. These tables have been drawn from the Guidelines on Service Agreements: Essential Elements of the Treasury Board of Canada.

Annexures

Annexure - I

TARC meetings with its stakeholders

Date	Name of the Stakeholder
12.06.2014	Meeting with CEIB
30.06.2014	Meeting of Focus Group on data or information exchange and customs capacity building with participation from CEIB
24.07.2014	Meeting with the officers from CEIB
04.08.2014	Interaction with Member (Customs), CBEC
05.08.2014	Meeting with officers from the Directorate General (Systems), CBEC
05.08.2014	Meeting with officers from the Directorate General (Systems), CBDT
08.08.2014	Visit to Integrated Check Post, Attari, Punjab for meeting stakeholders as well as customs officers
12.08.2014	Meeting with the officers of CEIB
14.08.2014	Visit to Land Customs Station, Petrapole, West Bengal for meeting stakeholders as well as customs officers
25.08.2014	Interaction with officers of FIU on data and information exchange
27.08.2014	Interaction with technology industry on customs capacity building
28.08.2014	Meeting with representatives from Federation of Freight Forwarders Association in India on customs capacity building
04.09.2014	Meeting with the officers of Chennai customs and industry representatives on customs capacity building
05.09.2014	Inspection of mobile container scanner at Chennai port
09.09.2014	Interaction with Sh. S. Mukhopadhyay, Ex-Member, CBEC on customs capacity building
19.09.2014	Inspection of customs facilities at the Gaya International Airport

Annexure – II

Composition of Focus groups

Sl. No.	Topic	Focus Group
1.	To review the existing mechanism and recommend measures for "Capacity building" in emerging areas of Customs administration relating to Border Control, National Security, International Data Exchange and securing of supply chains.	Mr. S. P. Sahu, WCO, Brussels, Ms. Kajal Singh, CE Mr. M. Satish K Reddy, ADB, New Delhi Mr. Bipin Sapra, E & Y Mr. Suresh Nair, E & Y Mr. Himanshu Tewari, BMR
2.	To review the existing mechanism and recommend measures for strengthening of Database and inter-agency information sharing, not only between Central Board of Direct Taxes (CBDT) and Central Board of Excise and Customs (CBEC) but also with the banking and financial sector, Central Economic Intelligence Bureau (CEIB), Financial Intelligence Unit (FIU), Enforcement Directorate etc. and use of tools for utilization of such information to ensure compliance.	Mr. Vivek Chaturvedi, CE Mr. Ravi Agarwal, I-T Mr. Sanjeev Singh, I-T Mr. Rajiva Ranjan Singh, ex I-T Dr. Sanjay Kagwade, CME, Mumbai Mr. Mukul Swaroop, BMR Mr. T. Koshy, E & Y

Note: I-T: Income Tax Department

CE: Custom & Central Excise Department

WCO: World Customs Organisation

ADB: Asian Development Bank

Annexure - III

TARC meetings

Date of the meetings
16th June, 2014
17th June, 2014
30th June, 2014
17th July, 2014
04th August, 2014
07th August, 2014
14th August, 2014
20th August, 2014
21st August, 2014
27th August, 2014
28th August, 2014
04th September, 2014
09th September, 2014
19th September, 2014
26th September, 2014

Annexure - IV

Gazette Notification constituting TARC

MINISTRY OF FINANCE
(Department of Revenue)
NOTIFICATION
New Delhi, the 21st August, 2013

F.No.A.50050/47/2013-Ad.I. –The Government in its Budget, 2013-14, had, inter-alia, announced the setting up of a Tax Administration Reform Commission (TARC) with a view to reviewing the application of Tax Policies and Tax Laws in the context of global best practices and recommend measures for reforms required in Tax Administration to enhance its effectiveness and efficiency. Accordingly, it has been decided to constitute the Tax Administration Reform Commission with the following composition:

i)	Dr. Parthasarathi Shome	Chairman
ii)	Shri Y. G. Parande	Full-time Members
iii)	Ms. Sunita Kaila	
iv)	Shri M. K. Zutshi	Part-time Members
v)	Shri S.S.N. Moorthy	
vi)	Shri M.R. Diwakar	
vii)	Shri S. Mahalingam	

2. The Commission will have a fixed tenure of 18 months from the date of its constitution and work as an advisory body to the Ministry of Finance. The Commission will give its first set of recommendations with six months of its constitution and thereafter submit periodic reports after every three months.

3. The Terms of Reference of the Commission will be as follows:-

a) To review the existing mechanism and recommend appropriate organizational structure for tax governance with special reference to deployment of workforce commensurate with functional requirements, capacity building, vigilance administration, responsibility of human resources, key performance indicators, assessment, grading and promotion systems, and structures to promote quality decision making at the highest policy levels.

b) To review the existing business processes of tax governance including the use of information and communication technology and recommend measures tax governance best suited to Indian context.

c) To review the existing mechanism of dispute resolution, covering time and compliance cost and recommend measures for strengthening the same. This includes domestic and international taxation.

d) To review the existing mechanism and recommend capacity building measures for preparing impact assessment statements on taxpayers compliance cost of new policy and administrative measures of the tax Departments.

e) To review the existing mechanism and recommend measures for deepening and widening of tax base and taxpayer base.

f) To review the existing mechanism and recommend a system to enforce better tax compliance – by size, segment and nature of taxes and taxpayers, that should cover methods to encourage voluntary tax compliance.

g) To review existing mechanism and recommend measures for improved taxpayer services and taxpayers education programme. This includes mechanism for grievance redressal, simplified and timely disbursal of duty drawback, export incentives, rectification procedures and refunds etc.

h) To review the existing mechanism and recommend measures for "Capacity building" in emerging areas of Customs administration relating to Border Control, National Security, International Data Exchange and securing of supply chains.

i) To review the existing mechanism and recommend measures for strengthening of Database and inter-agency information sharing, not only between Central Board of Direct Taxes (CBDT) and Central Board of Excise and Customs (CBEC) but also with the banking and financial sector, Central Economic Intelligence Bureau (CEIB), Financial Intelligence Unit (FIU), Enforcement Directorate etc. and use of tools for utilization of such information to ensure compliance.

j) To review the existing mechanism and recommend appropriate means including staff resources for forecasting, analysing and monitoring of revenue targets.

k) To review the existing policy and recommend measures for research inputs to tax governance.

l) To review the existing mechanism and recommend measures to enhance predictive analysis to detect and prevent tax/economic offences.

m) Any other issue which the government may specify during the tenure of the Commission.

4. The Commission will be supported by a Secretariat consisting of a Secretary at the level of Joint Secretary to the Government of India and other officials and support staff. They will be appointed on deputation/contract basis.

5. The Commission will be provided information and quantitative data of Central Board of Direct Taxes/Central Board of Excise and Customs to enable it to do statistical analysis for making recommendations.

6. The Headquarters of the Commission will be in Delhi.

M. L. MEENA
Joint Secretary