सत्यमेव जयते

NASSCOM®

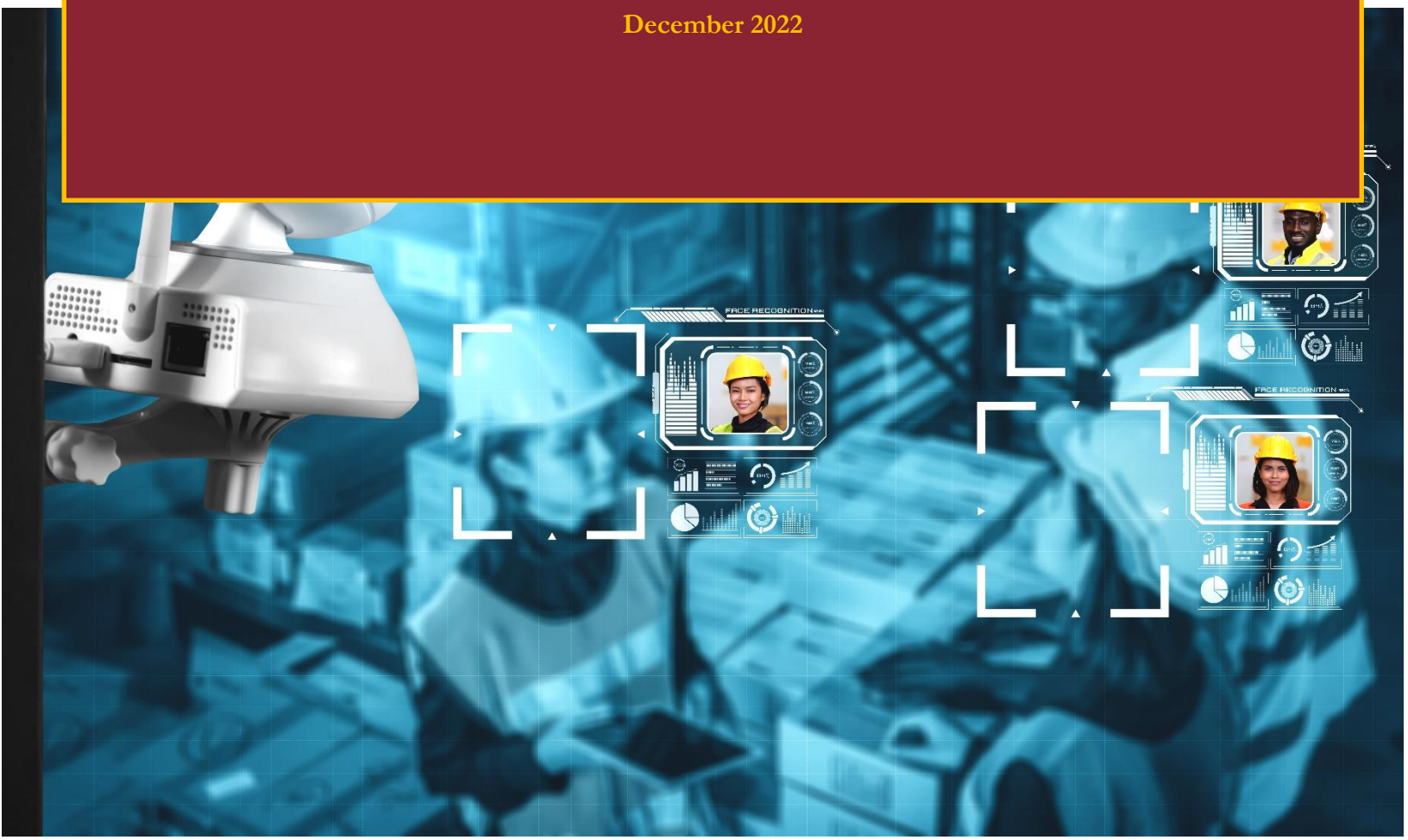
Elements of an Effective

Internal Compliance Programme

For Export/Transfer of Dual-Use Items

Version 1.0

December 2022



सत्यमेव जयते

NASSCOM

Table of Contents

Acknowledgments

This document has been prepared with contributions from various experts in the field of export controls/strategic trade controls. NASSCOM thanks the contributors for their valuable feedback and suggestions.

We extend our sincere appreciation to the Directorate General of Foreign Trade (**DGFT**) of the Ministry of Commerce and Industry, Electronics Research and Development Group of the Ministry of Electronics and Information Technology, Disarmament and International Security Affairs Division of the Ministry of External Affairs, Central Board of Indirect Taxes and Customs of the Ministry of Finance, other Government of India organisations and relevant stakeholders for offering their inputs in this document.

We also acknowledge the vital contribution of the members of the Information Technology (**IT**) industry in finalising this document.

NASSCOM

Preface

Export controls applicable to India's IT industry and transfer of technology are significant for the industry, the government and other stakeholders. As the representative of the Indian IT industry, NASSCOM has been playing a significant role in enhancing industry awareness and creating a dialogue between the industry and the government on matters related to export control.

Given the technological advancements and the complexity of supply chains today, effective export controls depend largely on the awareness of companies and organisations and their active efforts to comply with export control obligations. For this, they establish a set of internal policies and procedures, also known as an Internal Compliance Programme (**ICP**). Towards this, the document covering the elements of an effective ICP for export/transfer of dual-use items. Dual-use items include goods, software and technologies. The document provides a framework to help organisations identify and minimise risks associated with export/transfer of dual-use items, and to ensure compliance with the relevant national laws and regulations on export controls. This is especially relevant for the IT industry where exports of controlled items take place through an intangible medium.

This document aims to assist organisations in formulating their ICPs or bringing their existing ICPs in-line with the essential elements. Common approaches and practices on ICPs can contribute to a consistent application of export controls in India. This document also provides a checklist that can be answered by the organisations when applying for a general authorisation with the DGFT or Department of Defence Production (**DDP**). This is expected to assist the relevant authorities in easily navigating through the organisation's ICP.

We hope that this document will be useful in sensitising the industry and other stakeholders on the need for an ICP, compliance obligations under India's export control laws and regulations thereby ensuring effective compliance. This document is intended for a wide range of technology related companies and organisations, specifically, those who are involved with the export of controlled items from India.

Ashish

Ashish Aggarwal

Vice President and Head of Public Policy

NASSCOM

संतोष सारंगी, भा.प्र.से.
महानिदेशक
Santosh Sarangi, IAS
Director General

भारत सरकार
वाणिज्य एवम् उद्योग मंत्रालय
विदेश व्यापार महानिदेशालय
वाणिज्य भवन, नई दिल्ली-110011

Government of India
Ministry of Commerce & Industry
Directorate General of Foreign Trade
Vanijya Bhawan, New Delhi - 110011

FOREWORD

India's membership of export control regimes has opened new opportunities for "Made in India" high technology items to be transferred across the world. India is engaging with the world, with sensitivity and responsibility, in the trade of high technology dual-use items, in many sectors including technology and software. It is now more important than ever for companies operating within India to be cognizant of responsibilities and obligations and create robust internal processes and systems to play their part in helping in non- proliferation of goods and technology into the hands of non-state actors. I believe that adequate awareness and compliance with export control obligations by the industry is the key to prevent proliferation. Common approaches regarding internal compliance programmes can contribute to a uniform and consistent application of export controls throughout India.

This document on Elements of an Effective Internal Compliance Programme will play a key role in providing guidance to the industry to have robust compliance to ensure the export of dual-use items is done as per the existing rules and guidelines to secure their exports. Adopting the described elements will assist the industry including new exporters, start-ups and academic and research institutions in fulfillment of export control obligations, especially for export/transfers of intangible technology transfers. Following the checklist prescribed in the Annexure titled 'Indicative Checklist for Submission of ICP to Licensing Authority along with application for General Authorisation' will assist DGFT in better understanding and navigating through the ICPs of organisations, thereby potentially expediting the general authorisation process and helping in liberalising the SCOMET policy further.

1.12.2022

(Santosh Sarangi)

Muanpuii Saiawi
Joint Secretary (D&ISA)
Tel: 23014902

विदेश मंत्रालय, नई दिल्ली
MINISTRY OF EXTERNAL AFFAIRS
NEW DELHI

FOREWORD

Export controls of dual-use goods and technologies that play a key role in the non-proliferation architecture, is a challenging area to implement in the context of technology transfers, in view of its intangible nature and evolving technologies. Internal Compliance Program (ICP) is an important tool for implementation of export controls by organisations, especially from the perspective of intangible technology transfers. Towards this goal, I welcome the joint Government of India – Industry initiative on formulation of 'Elements of an Effective Internal Compliance Program for Export/Transfer of Dual-Use Goods and Technologies', which could facilitate the institution of ICPs in organisations, and a framework for the government to ensure compliance in export/transfer of dual-use goods and technologies, in particular for intangible technology transfers. This would further strengthen our established non-proliferation credentials in export/transfer of dual-use goods and technologies.

(Muanpuii Saiawi)

गौरव मसलदान
संयुक्त सचिव (सीमा शुल्क)
Gaurav Masaldan
Joint Secretary (Customs)

भारत सरकार
वित्त मंत्रालय/राजस्व विभाग
केन्द्रीय अप्रत्यक्ष कर एवं सीमा शुल्क बोर्ड
कमरा न. 156-B,
नॉर्थ ब्लाक, नई दिल्ली - 110001
Government of India
Ministry of Finance / Department of Revenue
Central Board of Indirect Taxes & Customs
Room No. 156-B, North Block, New Delhi-110001
Phone : +91-11-23092978
Fax : 011-23093475
E-mail : masaldan.gaurav@nic.in

FOREWORD

Indian Customs has been encouraging voluntary compliance by various stakeholders to complement the efforts towards enforcement of border controls and protecting India's frontiers. The AEO Programme which was initiated in 2011 is one such programme aimed at setting standards for ensuring safety and security of the supply chain. This is based on the World Customs Organisation's SAFE Framework. The programme presently has nearly 5,000 AEO certified entities and is instrumental in propelling India' image as a serious player in terms of seamless movement of goods across frontiers while ensuring supply chain security.

In this context, I appreciate the Government of India – Industry initiative on development of 'Elements of an Effective Internal Compliance Program for Export/Transfer of Dual-Use Goods and Technologies'. This would supplement our existing efforts on voluntary compliance and facilitate the process we have initiated towards further streamlining the AEO programme.

Gaurav Masaldan

(Gaurav Masaldan)

Introduction to Export Control Compliance

India's Foreign Trade Policy (**FTP**) governs the export and import of goods and services. Under the FTP, a list of items have been identified whose export is to be controlled. This is because of the dual-use character of these items. Dual-use refers to the nature of an item, allowing it to be used in military applications or in weapons of mass destruction (**WMD**), as well as in civilian/industrial applications. The list of these dual-use items is called the Special Chemicals, Organisms, Materials, Equipment and Technologies (**SCOMET**) List. The SCOMET list is notified under Appendix 3 to Schedule 2 (Export Policy) of the Indian Trade Clarification (**ITC**). Export of SCOMET items is either prohibited for export, or restricted (thus requiring prior export authorisation), or exempted from such authorisation (subject to issue of a general authorisation) for export to certain destinations with certain post-reporting and recordkeeping requirements etc.

India is a member of three multilateral export control regimes: the Wassenaar Arrangement, Missile Technology Control Regime, and Australia Group, which have contributed to the goals of non-proliferation by issuing guidelines for export controls and lists of specific items whose exports are to be regulated. India's SCOMET List is harmonised with the control lists prescribed under these regimes, as well as that of the Nuclear Suppliers Group and the Chemical Weapons Convention.

As per our national laws and regulations, export of technology related to items specified under the SCOMET list is also controlled and requires an authorisation from the licensing authority. Technology means information (including information embodied in software) other than information in the public domain, that is capable of being used: in the development, production or use of any goods or software; in the development of, or the carrying out of, an industrial or commercial activity or the provision of a service of any kind in relation to an item specified under India's SCOMET list. This information may take the form of technical data (blueprints, plans, diagrams, models, formulae, algorithms, tables, engineering designs and specifications, manuals, instructions, etc., written or recorded on other media or devices) or technical assistance (instruction, skills, training, working knowledge, consulting services).

Companies and other organisations dealing with dual-use items are mandated to comply with export control regulations. Effective control of exports to prevent proliferation of dual-use items is possible only if all the stakeholders, including manufacturers of dual-use items, exporters and other organisations/stakeholders with the technical expertise or knowledge on these items, recognise the need for such controls and support their compliance with all the resources available to them. A trust-based partnership between industry, other organisations/stakeholders and the government is vital to achieve this shared objective of non-proliferation of dual-use items. An industry or organisation's expertise, including the knowledge of the technical characteristics of the items and knowledge of the end-users outside India, plays a key role in implementation of export controls.

ICP and its need

Given the scientific and technological developments, complexity of supply chains and the intangibility of technology exports, effective export controls depend extensively on the awareness and efforts by companies and other organisations to comply with export control regulations. To this end, organisations usually put in place a set of internal policies and procedures, also known as an ICP, to ensure compliance with export control regulations. The purpose of an ICP is to create a system that help organisations operate their export activities in accordance with Indian laws and regulations on export controls. Having an effective ICP helps organisations integrate requirements from export controls with their business operations. This helps in the early detection and prevention of attempts to procure WMD, minimises risks of violating regulations and streamlines export operations.

Infringements of export control regulations carry legal consequences, such as, fines, suspension/cancellation of importer exporter code under the FTP or imprisonment under the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act 2005, Customs Act 1962, etc. Moreover, the media may highlight actual or alleged non-compliance stories or incidents. This can impact the organisation's reputation and the industry or sector's credibility. Further, non-compliance has implications for the country's track-record in export control related compliance. An ICP can help organisations in avoiding the consequences of non-compliance.

Moreover, an ICP is a pre-requisite for obtaining the Global Authorisation for Inter-Company Transfers (**GAICT**) scheme of the DGFT and Open General Export License (**OGEL**) schemes of the DDP. GAICT scheme offers significant practical benefits to compliant exporters. It authorises the exporter to export a range of items to the exporter's affiliated companies in several countries. Due to its scope, applicants must fulfil certain requirements to establish their credentials in export control compliance. The GAICT scheme requires the applicant to implement an ICP capable of ensuring that the global export licence is utilised responsibly. It is expected that the general authorisations that may be formulated by Government of India in the future may also have an ICP document as one of the mandatory requirements for obtaining these authorisations.

Elements of Internal Compliance Programme

This section identifies the following elements as critical for an effective ICP for export/transfer of dual-use items subject to export control regulations. These elements provide a foundation for the basic structure of an organisation's ICP. The manner in which these elements may be implemented depends on the size of the organisation, nature of its operations, geographic location of the organisation, its subsidiaries and customers, nature of the dual-use items that the organisation deals in, the potential end-use and end-users of these dual-use items, etc.

Therefore, prior to the implementation or review of the ICP, a risk assessment should be done to determine the specific dual-use trade risk profile of the organisation. Such assessments help organisations in identifying which parts of its business need to be covered by the ICP. The assessment can also identify the effectiveness of already implemented export control measures and to determine which areas may require adjustments.

The development of this ICP guidance document for trade in dual-use items takes into consideration and builds on the existing approaches towards export control compliance, in particular the:

- Wassenaar Arrangement Best Practice Guidelines on Internal Compliance Programmes for Dual-Use Goods and Technologies (2011)
- Wassenaar Arrangement Best Practices for Implementing Intangible Transfer of Technology Controls (2006)
- Export Compliance Guidelines, Bureau of Industry and Security, United States Department of Commerce
- Commission Recommendation number 2019/1318 on Internal Compliance Programmes for Dual-use Trade Controls under Council Regulation (EC) No 428/2009, European Commission
- Authorised Economic Operator (**AEO**) Programme of Indian Customs, CBIC Circular 33/2016 – Customs, as amended

The elements are:

1. Management Commitment
2. Organisation structure, responsibilities, and resources
3. Screening procedures
4. Performance Review and Internal Audit
5. Training and Awareness
6. Record Keeping
7. Reporting and corrective action
8. Physical and Technical security

Element 1: Management Commitment

Management commitment aims to build a corporate/organisational compliance culture for export controls and promotes the organisation's awareness on their internal compliance procedures. It results in allocation of adequate organisational, human, and technical resources for the organisation's commitment to compliance. The objective is to communicate to all employees the importance of export compliance, the commitment to adhere to the export control regulations and support to the internal compliance procedures of the organisation. The management commitment entails a formal statement on the organisation's letterhead, dated and signed by the senior management of an organisation. This statement should be reviewed and disseminated annually for the information of all the employees in the organisation. It should also be included in the organisation's ICP document and made available to all the employees. Refer to Annex A for a sample management commitment statement.

Steps involved:

a. Develop the statement stating that the organisation complies with the national export control laws and regulations. This statement should contain the following:
    - That there would not be any exports or transfers of controlled, dual-use items made in violation of the applicable national laws and regulations on export controls.
    - Information on action taken in case of non-compliance within the organisation. For example, appropriate actions taken within the organisation, voluntary self-disclosure, or intimation to the relevant government authorities, etc.
    - Information of the Chief Export Control Officer or other equivalent designation, or any other nominated persons from the export control or relevant department, in case of export control compliance questions by employees.

b. Define the management's specific compliance expectations and convey the importance of export control compliance procedures.

c. Clearly and regularly communicate the corporate commitment statement to all the employees.

Element 2: Organisation Structure, Responsibilities, and Resources

Adequate organisational, human, and technical resources need to be allocated for the effective development and implementation of the internal compliance procedures. Clear organisation structure along with well-defined responsibilities needs to be created, without which it is likely that the ICP will not be implemented and enforced properly.

This entails the organisation having a written organisational structure that identifies and appoints persons with the overall responsibility of the implementation of the internal compliance procedures. It is recommended that this person is a member of the senior management of the organisation. The organisation should have employees with the required skills for all areas of the business related to dual-use exports or transfers. At least one person in the organisation (not necessarily exclusively) should be entrusted with an export control function. It can also be considered to provide this person a reporting line to the top management of the organisation. The employees should be protected from conflict of interest as much as possible, and they must have access to the applicable national laws and regulations on export control, including the SCOMET list and must understand these documents thoroughly.

Steps involved:

a. Appoint and empower the position of a Chief Export Control Officer, or any other equivalent designation, and clearly define the responsibilities of this role, such as:
    - Development and revision of the ICP, operational procedures, etc.
    - Having expertise and staying updated with the current information on export control laws and regulations.
    - Represent the organisation in matters related to export regulations such as licensing requirements, item classification, disclosures, etc.
    - Classification/Identification, screening, and approval of export controlled and related business transactions.
    - Providing guidance to the employees and organisation's affiliated entities.

b. Make available the contact details of the Chief Export Control Officer or any other equivalent designation and the team. If the duties of export control officer are being outsourced, then organise and make available the communication of the organisation with the outsourced persons.

c. Compile all the policies and procedures related to export controls and publish it in the format of a compliance manual. The compliance manual may also be regularly updated, based on the recent changes, if any.

d. Grant the Chief Export Control Officer or any other equivalent designation and the team access to all relevant laws and regulations; for example, national laws and regulations, UN Security Council sanction lists, SCOMET/dual use export control list, etc.

Element 3: Training and Awareness

This involves training and raising awareness among the organisation's employees on export controls. The training programmes should be designed as specifically as possible to help the employees to understand the internal compliance processes and their role in ensuring adherence to these processes.

A good training programme would provide up-to-date content on the applicable export control laws and regulations, organisation's internal compliance processes, job-specific knowledge for employees, communicate the responsibilities for each employee, and hold the employees accountable for export control training through assessments, where possible. Employees should receive different levels of export control training depending on the knowledge and skills needed to perform their job. The trainings can range from teaching the basics of export controls to detailed trainings on the organisation's export compliance processes, national export control laws and regulations and those of the countries that could impact the organisation's exports. Trainings could be in the form of seminars, subscription to information sessions offered by competent authorities, in-house training events, etc.

Steps involved:

a. Provide mandatory and continued trainings to all the employees associated with the relevant export control activities, including new staff, persons who work in sales and supply chain management, export related units, or are involved in technology transfer, international cooperation and training, etc.
b. Provide the trainings customised to the job/role of the employees and use the training material provided by the relevant authorities, if available.
c. Ensure by way of these trainings that all the concerned employees are aware of and understand the relevant export control laws and regulations, which include staying updated with the changes in them.
d. Incorporate the lessons learnt from performance reviews, audits, reporting and corrective actions in the trainings.
e. Providing an awareness session on export control related compliances for the new employees may be useful.
f. Undertaking an assessment/evaluation of the employees post training may also be useful.
g. Providing desk-based training using electronic media and other virtual methods may be useful to supplement and reinforce formal training sessions.
h. Archive the internal training records including participation of staff in external events pertaining to export control awareness, compliance, etc.

Element 4: Classification and Screening Procedures

This includes the organisation's internal measures to ensure that no transaction is made without the required license or in breach of any applicable national export control laws and regulations. The transaction screening procedures result in the proper classification of the dual-use item, determination of whether a license is required, risk assessment of the transaction, and post-licensing controls.

Steps involved:

a. Establishing a process to evaluate whether a transaction involving dual-use items is subject to applicable national export control laws and regulations.

b. Item classification: Determining whether the items are specified under the SCOMET list and other applicable national export restrictions. This is done by comparing the characteristics of the item with that in these lists. This would include a scrutiny of the description, specifications, end use, etc. of the materials, equipment, software, technology, parts, components, and other items.

c. Transaction risk assessment:

- Screening the end-use of the item being exported: verify that the items to be exported will not be used for purposes other than the declared use; ensure that any non-listed dual-use items are not being sent to a destination subject to United Nations Security Council (**UNSC**) arms embargo or proliferation-related UNSC sanctions; confirm that any non-listed dual-use items are not intended for military or WMD end-use.
- Screening the end user and all the parties involved in a transaction: verify whether the end user, buyer/intermediary/consignee, customer, other entities such as carrier/transporter, freight forwarder, agent, etc. are not specified on UNSC sanctions lists (or is not owned or controlled by a UNSC listed entity) or is not identified with red flags or other warning signs.
- Screening the risk of diversion of items from authorised end-users to unauthorised end-users.
- Establishing procedures to determine if there is information of concern about the stated end-use (catch-all controls for unlisted items). Pursuant to this, it should be ensured that the transaction does not happen without clarifying the points of concern and if necessary, to obtain proper authorisation from the relevant government authority.

d. Screening for red flags or warning signs, such as:

- The customer is being opaque or unclear about the end-use or end-user of dual-use items.
- The stated end-use or the product's capabilities is inconsistent or do not fit with the customer/buyer's line of business, level of technical sophistication, etc.
- Receiving unsolicited communication from any person or entity requesting assistance with modifying existing technology or software or requesting training/guidance in modifying technology or software for a potential military/WMD purpose.

- Involved parties are located in a UNSC embargoed/sanctioned country.
- The customer has little or no business background.
- The customer is willing to pay cash for an expensive item when the terms of sale would normally involve financing.
- The customer is unfamiliar with the product's performance characteristics, but still wants the product.
- Installation, testing, training, or maintenance services are included in the sales price, but declined by the customer.
- Delivery dates or terms are vague or unexpectedly changed, or deliveries are planned for an out-of-the-way destination.
- A freight forwarding firm, agent or trader is listed as the product's final consignee or end user.
- Packaging is inconsistent with the stated method of shipment or destination.
- The shipping route is abnormal for the product and destination.
- When questioned, the buyer is evasive and unclear about whether the purchased product is for internal use, further transfer, export, or re-export, etc.

e. Determination of license requirements and licence application as appropriate, including the type of licence, the licencing authority, requirements of the application to be made, submitting the application, and required supporting documents, etc.

f. Post-licencing controls: checking that all the steps ensuring compliance were duly taken; if items are correctly classified; if any red flags have been identified and acted upon; if there is a valid licence for the shipment, whether items and their quantities correspond to those set out in the export license and other export related documents, whether all the conditions listed in the export license are observed, etc.

Organisations could carry-out these steps manually or with the support of automated tools, depending on the organisation's assessment.

Element 5: Performance Review and Audit

The ICP must be reviewed, tested and recalibrated periodically, to keep it effective and up to date. This entails internal performance reviews and audits to verify whether the ICP is being implemented effectively, i.e., consistent with the applicable export control laws and regulations. These reviews and audits are designed to detect inconsistencies, so that procedures can be revised in case they are resulting in non-compliance. Reviews or audits may also be outsourced to an external, third-party auditor. Such reviews and audits can provide an unbiased evaluation and validation of the organisations' internal compliance procedures and practices.

Steps involved:

a. Develop and perform audits to check the design, adequacy, and efficiency of the export control related procedures. These can be functional/unit level audits that look into specific areas of an export control process or programme level audits that look into the entire ICP.
b. Provide a mechanism for ad-hoc checks in the export control workflow, where required.
c. Establish procedures to govern the actions of employees when a suspected or known incident of non-compliance occurs.
d. Document the audit results.
e. Organisations may consider sharing the results of the review and audit process with the employees.

Element 6: Recordkeeping

Recordkeeping comprises procedures and guidelines for document storage, record management and traceability of export control related activities. Recordkeeping of some documents is required by law, e.g., all SCOMET or export control related application documents, including the correspondence documents with the buyer/intermediary/consignee/end-user/government, contracts, end-user certificates, financial records, shipping and trade related documents, etc. must be recorded for 5 years as per India's FTP. Additionally, it may be useful for organisations to keep records of other documents, e.g., documents describing the technical decision or assessment to classify an item under the SCOMET list, unit/employee who made that decision, end-user and end-use screening documentation, customs clearance and shipping/trade documents, records of technology transfers and relevant electronic communication, etc.

Keeping the records and documents in a systematic manner helps in efficient search and retrieval during the day-to-day export control activities, and also during the periodic audits. The period of retention of these documents should be at least as long as that required by applicable export control laws and regulations.

As the organisations are using electronic forms of communication, recordkeeping is also being done electronically. In this context, it is necessary that the employees understand how to navigate through the electronic recordkeeping system and retrieve the required documents efficiently.

Steps involved:

a. Verify the legal requirements for recordkeeping (period of safekeeping, scope of documents, etc.) in the applicable national export control laws and regulations.
b. Create an efficient filing and retrieval system for export control related documents and information. This can be done by categorisation of documents, using keywords, search functionalities, etc.

Element 7: Reporting and Corrective Action

This element involves promptly reporting known or suspected incidents of non-compliance with the applicable national export control laws and regulations or non-compliance with the organisation's ICP, to the responsible person. If the responsible person confirms the violation of the export control laws and regulations, it should be reported to the relevant government authority. Thereafter, necessary corrective actions to identify vulnerabilities in the ICP should be put in place to ensure that similar violations do not recur in the future.

Steps involved:

a. Creating internal and external reporting procedures for suspected non-compliance. Employees should be encouraged to report suspected non-compliance incidents and be made aware that the top-level management of the organisation views such reports as an integral part of the organisation's ICP and as a duty of each employee.
b. Create procedures to investigate, confirm non-compliance and correct the issue as needed. This should include: the criteria for when to conduct an investigation, the specific investigation procedures, investigative report documentation requirements, notification procedures if non-compliance is confirmed, documentation requirements of remedial actions taken, etc.
c. Establish appropriate actions within the organisation for non-compliance, especially in case of intentional non-compliance.
d. External reporting, i.e., voluntary self-disclosure or intimation to the government authorities should be done as soon as the confirmation of non-compliance is received. This should be substantiated by supporting documents, as may be prescribed under the relevant procedures/guidelines notified by the government authorities.
e. Revise the ICP if needed after identifying potential vulnerabilities in the ICP, to ensure that non-compliance does not recur, and communicate the same to the employees.
f. Communicate with the relevant government authority to discuss possible ways of strengthening the organisation's ICP. Document the corrective measures taken by the organisation for suspected or actual breaches.

Element 8: Physical and Technical Security

Having appropriate security measures in place for dual-use items enables minimising the risks of unauthorised export/transfer of or access to these items. One of the greatest risks of non-compliance with export control laws and regulations occurs during the export/transfer of technology including technical assistance (like transfer of technical data), technical exchanges with foreign nationals who are employees, contractors, visitors or customers or trainees through telephone, fax, e-mail, webinar/video conference, or in-person. Ensuring the secure handling of export controlled dual-use items requires the organisations to install physical security plans, information security measures, personnel screening procedures, etc. These processes ensure that the dual-use items do not get lost, pilfered, etc. or are not transferred without conducting the suitable export control compliance checks and if required, a valid export authorisation or license.

Steps involved:

a. Ensure that dual-use items are secured against unauthorised removal by employees or transfer to third parties, for example, by physically safeguarding the items, establishing and clearly defining restricted access areas, entry and exit controls, using secured storage devices, periodically checking the integrity of security systems, etc.
b. Ensure that the premises used in connection with dual-use items are capable of providing protection against unlawful entry/intrusion, and that appropriate access control measures are in place to prevent unauthorised access to restricted areas.
c. Establish appropriate measures for the handling of goods including protection against the introduction, exchange or loss of any material and tampering with goods.
d. Establish suitable measures relating to the conveyances used for the transportation of goods, so that they are capable of being effectively secured.
e. Conduct appropriate security screening of employees in security sensitive positions or having access to restricted access areas, including periodic checks.
f. Institute security procedures and safeguards for secured storage of and access to dual-use items in electronic form; for example, antivirus checks, file encryption, audit trails and logs, user access control, firewalls, protective measures for uploading/storing/transferring technology to the server or cloud, software to prohibit unauthorised access to system, restricted access to export controlled information, maintaining an immutable log of authorised user accounts that access export controlled data, documenting the transfer of files containing export controlled data (providing the date, time, identifiers and user who transferred the files), methods for internal reporting of unauthorised access attempts or breaches of export-controlled data, etc.

Annex A - Example of a Management Commitment Statement

Organisation's Letter Head

Date

To: All employees (especially associated with dual-use items)

[*Organisation name*] is committed to compliance with all applicable export control laws and regulations. It is [*organisation name*] policy that all employees, departments, divisions, and affiliates comply with applicable export control laws and regulations and under no circumstances shall transactions be conducted by, or on behalf of [*organisation name*] contrary to such laws and regulations.

Penalties for violations of export control laws and regulations may be imposed by law. [*Organisation name*] and its employees may be subject to civil or criminal penalties. Accordingly, [o*rganisation name*] will view the intentional failure of any employee to comply with its Internal Compliance Programme, as a serious violation of organisation policy and will be subject to appropriate actions.

Export control compliance is an important aspect of our corporate culture and is the responsibility of all [*organisation name*] personnel. Training will be provided for all the employees on a regular basis and will be tailored to fit specific departmental/unit requirements and individual responsibilities.

If you have any questions concerning the legitimacy of a transaction or potential violations, please contact:

Name:

Title: Chief Export Control Officer (or other equivalent designation)

Phone:

E-Mail:

Note: This Statement of Management's Commitment to Export Control Compliance will be issued on an annual basis or if necessitated by personnel changes, changes in management, or regulatory changes.

[Signature]

[Name]

[Designation – President/CEO/Chairman/other equivalent designation]

Annex B – Indicative Checklist for Submission of ICP to Licensing Authority along with the application for a General Authorisation

Note: This is an optional checklist that may be submitted to the DGFT/DDP (as the case maybe) along with a copy of the ICP while applying for obtaining a general authorisation, to assist the relevant authorities in navigating through an organisation's ICP.

Question	Answer (Along with a reference to the organisation's ICP)
Has the top-level management signed a statement committing to internal compliance procedures in the organisation?	
How is the risk analysis for transaction of export controlled items being performed? Which risks are identified and how are they assessed?	
Which department/unit in the organisation is the anchor of export controls and how is this department/unit connected to other organisational units (organisational chart)?	
Do employees have direct access to the CECO or any other equivalent designation?	
What rules are in place for the absence of export control staff in cases of sickness, vacation etc.?	
How is the responsibility for classification of items under the SCOMET list handled?	
What procedures are in place to ensure that the classification of products/items under the SCOMET list is kept up to date, and how is this documented?	
Who can release a shipment that has been stopped due to concerns of non-compliance with export control laws and regulations?	
Does the organisation have an IT system for managing exports? If yes, what are the main features of this system in relation to export control compliance?	
Do the export control compliance-related employees in the organisation have access to the text of the applicable export control laws and regulations and the SCOMET list?	

How are the organisational, process-related and work instructions in the export control context made accessible to all the employees?	
How does the organisation take into account the UNSC arms embargo or proliferation related UNSC sanctions?	
How is the end-use by the consignee/end-user and its reliability assessed?	
How does the organisation handle red flags associated with export of dual-use items?	
How does the organisation ensure that controlled items are not exported without a license?	
How does the organisation ensure compliance with the Intangible Transfer of Technology (**ITT**) requirements (for example, e-mail and access to the Intranet from abroad, cloud computing)? Has the organisation issued clear and written instructions in relation to ITT compliance?	
What internal procedures are in place to ensure a final check before export that all the required measures have been undertaken?	
What internal procedures have been set in place to ensure compliance with the conditions of the export authorisation or license?	
Are the export control-relevant documents stored in accordance with the legal provisions?	
What system/procedures are in place to retrieve relevant recorded documents when needed?	
What trainings are conducted for employees associated with export control transactions, how frequently do they take place and how are they documented?	
How and for whom is awareness raised for risks associated with export of dual-use items?	
How frequently do audits of the organisation's ICP take place and who performs such audits?	
How are discovered errors handled?	
Do employees have access to a clear and written procedure for reporting potential or actual non-compliance?	
What procedures are in place to investigate a reported incident of non-compliance?	

What actions are taken as a response to the confirmed non-compliance?	
How does the organisation ensure physical security of the dual-use items? What are the suitable premises-related and access control measures in place for providing protection of dual-use items against unlawful entry/intrusion and to prevent unauthorised access to restricted areas?	
What are the appropriate measures in place for effective security relating to the handling of goods and the conveyances used for the transportation of goods?	
How does the organisation conduct appropriate security screening of employees/personnel in security sensitive positions or having access to restricted access areas?	
How are the organisation's IT or information security procedures and safeguards in relation to the secured storage/protection of and access to dual-use items?	

Contact Us

For any queries related to this report, kindly contact Garima Prakash (garima@nasscom.in) and Ashish Aggarwal (asaggarwal@nasscom.in) with a copy to policy@nasscom.in.

About NASSCOM

The National Association of Software and Services Companies (**NASSCOM**) is the premier trade body and chamber of commerce of the Tech industry in India and comprises over 3000 member companies including both Indian and multinational organisations that have a presence in India. Established in 1988, NASSCOM helps the technology products and services industry in India to be trustworthy and innovative across the globe. Our membership spans across the entire spectrum of the industry from start-ups to multinationals and from products to services, Global Service Centres to Engineering firms. Guided by India's vision to become a leading digital economy globally, NASSCOM focuses on accelerating the pace of transformation of the industry to emerge as the preferred enablers for global digital transformation. For more details, please visit www.nasscom.in.

Disclaimer

Contact us

E-mail: policy@nasscom.in

Twitter: @nasscompolicy @nasscom

Website: nasscom.in