Government of India
Ministry of Commerce and Industry
Department of Commerce
Directorate General of Foreign Trade

Dated: 14th July 2025
Vanijya Bhawan, New Delhi

Trade Notice No. 08/2025-26

To,

1. Industry and Relevant Stakeholders
2. Export Promotion Councils

Subject: Inputs on Draft Internal Compliance Programme Document for adoption by Industry for export of dual use(SCOMET) items –reg

Reference is drawn towards the mandatory requirement of Industry to comply with export control regulations. To ensure necessary compliance, the Industry is expected to establish a set of internal policies and procedures, also known as an Internal Compliance Programme (ICP).

General Authorization Policies under Chapter 10 of the Handbook of Procedures (HBP) 2023, outlines provisions for submission of Internal Compliance Programme Document(signed and stamped by compliance manager of the company) under which the exporter is required to submit an ICP Checklist. In order to further standardize the elements of effective ICP, a draft document has been prepared in consultation with Bureau of Indian Standards (BIS).

2. In line with Para 1.07A of FTP 2023, which provides for consultation with stakeholders during the formulation or amendment of Foreign Trade Policy, Draft Management System Requirements for Internal Compliance Programme (ICP) for Dual-use items have been formulated and are enclosed as an Annexure to this Trade Notice. This Directorate invites views, suggestions, comments, and feedback from relevant stakeholders, including exporters, industry associations, and experts on the proposed amendments.

3. Stakeholders are requested to submit proposals, recommendations, or inputs to this Directorate for examination within 10 days from the issuance of this Trade Notice. Submissions may be made via email to scomet-dgft@gov.in.

4. This Trade Notice is issued with the approval of the competent authority in accordance with the provisions of Para 1.07A of FTP 2023.

(B Kruti)
Deputy Director General of Foreign Trade

(Issued from F.No.01/77/171/059/AM24/EC(S)

Annexure: Draft Public Notice for notifying the Internal compliance Programme Document by Industry for export of SCOMET Items.

Management System Requirements for Internal Compliance Programme (ICP) for Dual-use items

Table of Contents

0.0 Introduction

0.1 General

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 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. Export of SCOMET items is either prohibited for export, or restricted, or exempted from such authorisation for export to certain destinations with certain port-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.

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.

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 organizations/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.

0.2 ICP and its need

The purpose of an Internal Compliance Programme (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.

ICP is pre-requisite for obtaining the Global Authorisation for Inter-Company Transfers (GAICT) scheme of the Directorate General of Foreign Trade (DGFT) and Open General Export License (OGEL) schemes of the DDP. GAICT schemes 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.

1.0 Scope

This document establishes a comprehensive framework to guide organizations in developing, implementing, maintaining, and continually improving effective ICPs. Its primary purpose is 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. It is relevant for all organisations that deals in the export/transfer of dual-use items.

2.0 Normative References

• India's Foreign Trade Policy (FTP), 2023

• Foreign Trade (Development & Regulation) Act, 1992

• DGFT’s SCOMET Policy Guidelines

• Wassenaar Arrangement Best Practice Guidelines (2011)

• Missile Technology Control Regime (MTCR) Guidelines

• ISO 37301:2021 – Compliance management systems

• ISO 31000:2018 – Risk management – Guidelines

• ISO 27001:2022 – Information security management systems

3.0 Terms and Definitions

This section provides commonly used terms in the Internal Compliance Programme (ICP), explained in plain language. These definitions are derived from internationally accepted standards, such as ISO 37301 (Compliance Management Systems), ISO 31000 (Risk Management), and ISO 27000 (Information Security), and adapted for the Indian export control context. For the purposes of this document, the following terms and definitions apply. ISO and IEC maintain terminology databases for use in standardization at the following addresses:

7. ISO Online browsing platform: available at https://www.iso.org/obp
8. IEC Electropedia: available at https://www.electropedia.org/

3.1 Objective

An objective is a specific result an organisation aims to achieve.

ISO 37301:2021 – Clause 3.6

3.2 Organisation

An organisation refers to a company, institution, or any group of people that work together toward shared goals and have defined roles and responsibilities.

ISO 37301:2021 – Clause 3.1

3.3 Responsibility

Responsibility means being assigned to carry out tasks and make decisions to meet compliance goals. It includes taking necessary action within the role assigned.

3.4 Accountability

Accountability is the obligation to answer for completing a responsibility, including explaining how it was fulfilled and accepting any consequences for failures.

ISO 37000:2021 – Clause 3.2.2

3.5 Process

A process is a set of connected activities that use inputs (like data, materials) to produce outputs (like services or products).

ISO 9000:2015 – Clause 3.4.1

3.6 Documented Information

Documented information includes all written or digital records that an organisation keeps to run its compliance systems—like manuals, procedures, logs, licenses, and audit reports.

ISO 9001:2015 – Clause 7.5

3.7 Monitoring

Monitoring means regularly checking the progress or condition of a process, system, or activity to ensure compliance.

3.8 Continual Improvement

Continual improvement involves making ongoing efforts to enhance compliance procedures and overall performance.

ISO 9001:2015 – Clause 10.3

3.9 Performance

Performance refers to how well a task or process is carried out, usually measured using data or quality indicators.

3.10 Regulation

A regulation is a rule made and enforced by a government authority that organisations must follow.

3.11 Review

A review is the process of evaluating compliance systems or documents to determine if they are current or need changes.

3.12 Risk

Risk is the effect of uncertainty on objectives. It can be a threat or an opportunity. In ICP, this means identifying and managing compliance-related risks.

ISO 31000:2018 – Clause 3.1

3.13 Top Management

Top management refers to the senior leadership of an organisation responsible for strategic decisions and oversight of compliance obligations.

3.14 Key Performance Indicator (KPI)

A KPI is a measurable value that shows how well an organisation is achieving its compliance goals. Examples: number of non-compliance incidents, or percentage of trained staff.

3.15 Value Chain

A value chain is the full set of activities and parties (like suppliers and partners) that contribute to producing a good or service.

4.0 Context of the Organisation

4.1 Understanding the organization and its context

The factors that affects the organisation’s ICP are:

7. Size and complexity: Consider the size and organizational structure, including subsidiaries, partnerships, and outsourcing arrangements.
8. Nature of operations: Understand activity types, operational complexity, and risk landscape to shape an effective ICP.
9. Geographical Location: Specific regulatory requirements and enforcement activities may vary depending on the organization’s geographic locations and operations.
10. Subsidiaries and customers: The compliance risk and complexity can increase with subsidiaries in various jurisdictions and diverse customer profiles.
11. Nature of dual-use items: Analyse the types of dual-use items involved, their applications, and associated risks.

4.2 Understanding the needs of interested parties

The main interested party in ICP are the regulatory bodies, which are often government entities, which have several key needs. They require organizations to establish and implement controls that ensure compliance with laws and regulations. This includes the development of internal policies and procedures that align with regulatory standards. Regulatory bodies also need to monitor how organizations are complying with these laws and regulations. This involves assessing the effectiveness of an organization's compliance program and its adherence to regulatory requirements. When non-compliance is identified, regulatory bodies focus on remediation, which includes identifying areas of non-compliance, taking corrective actions, and preventing recurrence. Reporting is another crucial need of regulatory bodies. They provide mechanisms for organizations to report on their compliance status, which helps in transparency and accountability.

4.3 Determining the Scope of the Compliance Management System

The purpose of the scope of Compliance Management System (CMS) is to establish and maintain an effective ICP for the responsible export of dual-use items, ensuring compliance with applicable national and international regulations. The scope should include:

7. Adherence to laws and regulations relevant to export controls
8. Identify and assess potential compliance risk and implementing controls to mitigate them
9. Develop and documenting clear policies and procedures for employees to follow

10. Reviewing and updating policies and procedures
11. Providing training to employees on the organization’s compliance program and its importance
12. Establishing a process for reporting suspected compliance violations

4.4 Compliance Management System

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

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

5.0 Leadership

5.1 Management Commitment

The top management should build a corporate/organisational compliance culture for export control. 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. It should also be included in the organisation’s ICP document and made available to all the employees.

The management commitment statement should contain the following:

7. 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.

8. 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.
9. 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.

5.2 Service Quality Policy

This is a documented and endorsed policy serves as a compass for ethical conduct within the organization. The service quality policy includes the following:

7. Statement of commitment that states the organization’s commitment to compliance and responsible export practices.
8. Primary objective of achieving and maintaining full compliance with relevant export control regulations.
9. Approach to identifying, assessing, and mitigating risks associated with export/transfer activities.
10. Channels for effectively communication the policy to all employees.
11. Consequences of non-compliance and emphasize individual accountability for upholding the policy principles.

5.3 Roles, Responsibilities, and Authorities

The organization is advised to establish a written organizational structure designating individuals with overall responsibility for the implementation of internal compliance procedures. Ideally, this role should be fulfilled by a senior management member. The organization must ensure the presence of skilled employees covering all aspects of the business related to dual-use exports or transfers. It is recommended that at least one person within the organization should be assigned an export control function, with consideration given to establishing a reporting line to top management. This approach fosters a comprehensive and efficient internal compliance framework. The steps to be taken by the organisation:

7. Appoint and empower the position of a Chief Export Control Officer, or any other equivalent designation, and clearly define the responsibility of this role, these responsibilities may include the following:

8. Development and revision of the ICP, operational procedures, etc.
9. Having expertise and staying updated with the current information on export control laws and regulations.
10. Represent the organisation in matters related to export regulations such as licensing requirements, items classification, disclosures, etc.
11. Classification/Identification, screening, and approval of export controlled and related business transactions.
12. Providing guidance to the employees and organisation’s affiliated entities.
13. 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.
14. 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.

5.4 Communication

There should be comprehensive training programs educate all personnel on the Service Quality Policy, ICP procedures, and individual roles and responsibilities. Open communication channels, including hotlines and forums, foster a collaborative environment where ethical conduct thrives. Stakeholder engagement expands the message of compliance beyond the organization's walls, showcasing commitment to responsible practices and building trust within the broader ecosystem.

6.0 Planning the Service Delivery

6.1 Actions to address Risks

The organizations should identify potential risks related to the delivery of services. 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 port-licensing controls.

7. Establish a process to evaluate whether a transaction involving

dual-use items is subject to applicable national export control laws and regulations.

8. 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.
9. Transaction risk assessment:
    7. 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 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.
    8. Screening the end user and 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.
    9. Screening the risk of diversion of items from authorised end-user to unauthorised end-users.
    10. 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.
10. Screening for red flags or warning signs, these are:
    7. The customer is being opaque or unclear about the end-use or end-user of dual use items.
    8. The stated end-use or the product’s capabilities is inconsistent or do not fir with the customer/buyer’s line of business, level of technical sophistication, etc.
    9. Receiving unsolicited communication from any person or entity requesting assistance with modifying existing technology or software requesting training/guidance in modifying technology or software for a potential military/WMD purpose.
    10. The customer is willing to pay cash or an expensive item when

the terms of sale would normally involve financing.

11. A freight forwarding firm, agent or trader is listed as the product's final consignee or end user.
12. The shipping route is abnormal for the product and destination.

11. 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.
12. 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.

6.2 Service Quality Objectives and planning to achieve them

The organizations are advised to outline their service quality objectives. These objectives are specific, measurable, achievable, relevant, and time-bound (SMART). The organisation should:

7. Aim to achieve zero incidents of unauthorized access/transfer of dual-use items during export/transfer.
8. Develop a specific action plan for implementing physical and technical security measures with measurable milestones and timelines.
9. Allocate resources and personnel for the implementation and maintenance of these measures.

6.3 Planning of Changes

The organizations should plan for changes in its service delivery. Organizations are advised to have a process in place for communicating changes to relevant stakeholders. This process may include:

7. Identify the need for change. This could be due to non-compliance or potential non-compliance identified during reviewing and auditing.
8. Any known or suspected incidents of non-compliance with the applicable national export control laws and regulations or non-compliance with the organization's ICP should pe promptly reported.
9. The organisation should take prompt corrective action to eliminate

the cause of non-compliance and prevent its recurrence. This includes establishing appropriate actions within the organization for non-compliance.

10. If needed, the ICP should be revised after identifying potential vulnerabilities in it, to ensure that non-compliance does not recur. The revised ICP should be communicated to the employees.
11. The organization should communicate with the relevant government authority to discuss possible ways of strengthening the organization's ICP. The corrective measures taken by the organization for suspected or actual breaches should be documented.
12. The organization should review the effectiveness of the corrective actions to ensure that they have achieved their intended purpose. This is a crucial step in the continual improvement process.

6.4 Applicability to Sustainable Development Goals

The organization should recognize the potential connection between their export/transfer activities and the UN Sustainable Development Goals (SDG). Specifically, implementing robust ICPs contributes to:

7. SDG 3: Good Health and Well-being: By preventing the proliferation of weapons of mass destruction and dual-use items with harmful application, ICPs promote global peace and security, contributing to healthier lives.
8. SDG 16: Peace, Justice and Strong Institutions: Effective ICPs strengthen legal frameworks and institutions responsible for enforcing export control laws, fostering a just and secure environment.
9. SDG 17: Partnerships for the Goals: ICPs encourage international cooperation and information sharing on sensitive materials and technologies, advancing collaborative efforts towards achieving the SDGs.

7.0 Support

7.1 Resources

The organization should ensure that adequate resources are allocated for the effective development of and implementation of the internal compliance procedures. These resources include human, technological, and financial resources. Clear organisation structure along with competent employees and management should be employed.

7.2 Competence

A good training programme would provide up-to-date content on the applicable export control laws and regulations, organisation’s internal compliance processed and job specific knowledge for employees. 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 that could impact the organisation’s exports. The organisation should:

7. Provide mandatory and continued trainings to all the employees
8. Incorporate the lessons learnt from performance reviews, audits, reporting and corrective actions in the trainings.
9. Providing desk-based training using electronic media and other virtual methods may be useful to supplement and reinforce formal training sessions.

7.3 Awareness

The organization should promote awareness about the ICP among all levels of the organization and should ensure by way of the 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. An awareness session should also be provided the new employees on export control related compliance, the importance of ICP and its benefits, providing a comprehensive understanding from the beginning.

7.4 Communication

The organization should establish a process for internal and external communication relevant to the ICP. The contact details of Chief Export Control Officer or any other equivalent designation and the team can also be made available. If the duties of export control officer are being outsources, then organise and make available the communication of the organisation with the outsourced persons to ensure that all the relevant parties are kept informed about the ICP’s progress and any changes made.

7.5 Documented Information

7.5.1 General

The organization should establish a general framework for managing documented information related to the ICP. This framework should outline the processes for creating, updating, and controlling documented information.

7.5.2 Creating and updating documented information

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 certificated, financial records, shipping and trade related documents, etc. must be recorded for 5 years as per India's Foreign Trade Policy (FTP).

Additionally, it may be useful for organisations to keep records of 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 documentation, customs clearance and shipping/trade documents, records of technology transfers and relevant electronic communication, etc.

A compilation of all the policies and procedures related to export controls should also be made and published in the format of a compliance manual. The compliance manual may also be regularly updated, based on the recent changes, if any.

7.5.3 Control of documented information

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.

The organisation should create an efficient filing and retrieval system, that may be in electronic format, for export control related documents and information. This can be done by categorisation of documents, using keywords, search functionalities, etc.

8.0 Operation

8.1 Operation planning and control

The organization should establish, implement, control, and maintain the processes needed to meet compliance requirements. The organisation should:

7. Integrate physical and technical security measures into export/transfer procedures and checklists.
8. Securely log and track access to sensitive information and dual-use

items.

9. Implement secure protocols for communication with foreign collaborators and customers.
10. Monitor transportation routes and logistics for potential security risks.

8.2 Complaints/grievance handling

Complaints/grievance handling is an integral part of the ICP. The organization should establish a fair, transparent, and timely process for receiving, investigating, and resolving complaints or grievances related to compliance. The organisation should:

7. Establish a mechanism for reporting suspected security breaches or unauthorized access attempts.
8. Investigate reported incidents promptly and take appropriate corrective actions.
9. Communicate lessons learned from security incidents to prevent future occurrences.

9.0 Performance Evaluation

9.1 Performance Review

The ICP must be reviewed, tested and recalibrated periodically, to keep it effective and up to date. This entails 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 are designed to detect inconsistencies, so that procedures can be revised in case they are resulting in non-compliance.

9.2 Internal Audit

The organisation should conduct regular internal audits to assess the effectiveness or inconsistencies of ICP and ensure its alignment with the organization’s compliance objectives. Audits can 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.

The organisation should:

7. Develop and perform audits to check the design, adequacy, and efficiency of the export control related procedures.
8. Provide a mechanism for ad-hoc checks in the export control

workflow, where required.
9. Establish procedures to govern the actions of employees when a suspected or known incident of non-compliance occurs.
10. Document the audit results.
11. Consider sharing the results of the review and audit process with the employees.

The audit should be conducted by competent personnel and the results should be reported to the top management. Any non-compliances identified during the audit should be addressed promptly through corrective actions.

9.3 Management Review

9.3.1 General

The top management should periodically review the ICP to assess its effectiveness and ensure ongoing compliance with applicable export control regulations. This review should consider the results of monitoring, measurement, analysis, evaluation, and internal audits.

9.3.2 Management review inputs

The inputs to the management review should include information on:

7. Internal audit findings and recommendations
8. Performance monitoring and measurement data
9. Feedback from interested parties
10. Changes in external and internal context
11. Information on non-compliance and corrective actions

9.3.3 Management review results

The results of the management review should include decisions and actions related to the continual improvement of the ICP, changes to the ICP, and resource needs. These results should include:

7. Affirmation of commitment to export control compliance
8. Evaluation of ICP effectiveness and suitability
9. Identification of necessary improvements, such as:
10. Policy and procedure revisions
11. Training and awareness enhancements
12. Resource allocation adjustments
13. Risk assessment and mitigation strategy refinements
14. Communication and reporting channel improvements
15. Development of action plans for implementing identified improvements.

10.0 Improvement

10.1 Continual Improvement

The organization should strive for continual improvement in the effectiveness of the ICP. This involves using the results of monitoring, measurement, analysis, evaluation, internal audits, and management reviews to identify opportunities for improvement.

In case of any known or suspected incidents of non-compliance with the applicable national export control laws and regulations or non-compliance with the organisation's ICP, the incident should be promptly reported to the responsible person. 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.

10.2 Corrective actions

When non-compliance or potential non-compliance is identified, the organization should take prompt corrective action to eliminate the cause and prevent recurrence. The organization should:

7. Establish appropriate actions within the organisation for non-compliance, especially in case in intentional non-compliance.
8. 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.
9. 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.
10. Document the corrective measures taken by the organisation for suspected or actual breaches.

7. Review the effectiveness of the corrective actions to ensure that they have achieved their intended purpose.

Annexure A: Case Study — Implementing Internal Compliance Program in a Technology Manufacturing Company

This case study outlines the implementation of an Internal Compliance

Program (ICP) by a mid-sized Indian electronics and advanced materials manufacturer engaged in the export of dual-use items such as embedded semiconductor components and high-precision optical systems.

4.0 Context of the Organisation:

- The company operates across India, with customers in Europe, East Asia, and North America. It exports dual-use items controlled under Category 3 (Electronics) and Category 6 (Sensors and Lasers) of the SCOMET List.
- Interested parties include DGFT, Customs, DGCI&S, foreign clients, logistics partners, and industry regulators.
- Scope of the ICP includes all outbound shipments of controlled hardware, technical drawings, and associated software. It also covers intangible transfers to overseas clients and partners.

5.0 Leadership:

- A senior vice-president was appointed as the Designated Export Compliance Officer with direct reporting to the Managing Director.
- The company adopted a formal Export Control Compliance Policy signed by top management, committing to zero-tolerance for export violations and regular training.

6.0 Planning and Risk Mitigation:

- The company implemented item classification protocols aligned with Wassenaar Arrangement and BIS standards.
- All employees underwent ISO 37301:2021-based compliance training.
- A denied party screening solution was integrated with the ERP system for real-time vetting of clients and end-users.

7.0 Support:

- The company used ISO 31000:2018 to structure its export risk management framework, especially for high-risk transactions involving re-exports or third-country shipments.
- Staff were trained in ISO 19011:2018 audit practices to conduct quarterly internal audits of export records.

9.0 Performance Review:

- KPIs included: (a) percentage of SCOMET-screened transactions, (b) compliance training completion rate, (c) violations reported and closed.

- Lessons learned from audits led to updating ICP checklists and training content.
- The ICP implementation ensured timely SCOMET licensing, improved client trust, and facilitated faster customs clearance. The company was later granted a General SCOMET Authorisation under the GAICT framework by DGFT.

Relevant ISO References:

- ISO 37301:2021 – Compliance Management Systems – https://www.iso.org/standard/75080.html
- ISO 31000:2018 – Risk Management Guidelines – https://www.iso.org/standard/65694.html
- ISO 19011:2018 – Guidelines for Auditing Management Systems – https://www.iso.org/standard/70017.html

ETSL, a mid-sized Indian electronics manufacturer, exports semiconductor testing equipment that falls under the SCOMET list due to its potential dual-use in civilian and defence applications. ETSL implemented an Internal Compliance Program (ICP) aligned with the guidelines outlined in this document to meet export control obligations and to qualify for the Global Authorisation for Inter-Company Transfers (GAICT) scheme under DGFT.

1. Understanding Context:

ETSL operates in India with customers in Europe, the US, and East Asia. Given its exposure to multiple jurisdictions, it faces complex compliance risks. The ICP was designed to integrate export control considerations within daily operations, including R&D, logistics, and customer engagement.

2. Management Commitment:

The senior management issued a formal compliance policy, appointed a Designated Export Compliance Officer (DECO), and mandated quarterly compliance reports.

3. Risk Assessment:

All products were classified against the SCOMET list using technical specifications. A denied party screening system was adopted to evaluate customers and intermediaries.

4. Safeguards on Technology Transfers:

For technical drawings and test software shared with foreign partners, ETSL implemented data access controls, encrypted file transmission, and employee training on intangible transfer risks.

5. Documented Procedures:

ETSL created SOPs for export licence applications, recordkeeping (minimum five years), red flag reporting, and end-use verification protocols.

6. Performance Evaluation:

KPIs such as training completion rate, audit compliance score, and internal violation reports were tracked. An external audit was conducted biennially.

7. Results:

ETSL successfully obtained GAICT approval, reduced average export licensing delays by 40%, and avoided potential penalties by proactively identifying one end-use violation through internal reporting.

This case demonstrates how a private-sector company can adapt compliance systems to meet international best practices and national regulations while enhancing operational resilience and global trust.