INTERNAL COMPLIANCE PROGRAM

VOLUME 2

DEPARTMENT OF TRADE & INDUSTRY PHILIPPINES

WHAT IS AN INTERNAL COMPLIANCE PROGRAM (ICP)?

An Internal Compliance Program (ICP) refers to an effective, appropriate, and proportionate means and procedures, including the development, implementation, and adherence to standardized operational compliance policies, procedures, standards or conduct, and safeguards, developed by exporters to ensure compliance with the provisions and with the terms and conditions of authorizations set out in the STMA.

Simply put, an ICP is a system intended to prevent transfers of strategic goods to prohibited end-user/s, whether intentional or otherwise. It is an accumulation of policies and procedures designed to assist an entity or organization to comply with the STMA and its IRR.

WHEN IS AN ICP NECESSARY?

An ICP is necessary for applicants and holders of global authorization.

To comply with the STMA and its IRR, applicants and holders of global authorization must comply with the elements of an ICP listed down in this manual.

Moreover, companies may have different levels of commitment in implementing the STMA. The company's size, nature of business, financial resources, trading partners, concern for human security, consciousness for company reputation, company policy, existence of appropriate laws and government intervention are just some of the main factors that can influence a company's effort and involvement in promoting the legitimate trade of strategic goods.

WHAT ARE THE ELEMENTS OF AN ICP?

1. Management Commitment
2. ICP Structure and Responsibility
3. Screening Procedures
4. Shipment Control
5. ICP Training
6. Internal Audit
7. Standard Operating Procedures Manual
8. Recordkeeping
9. Reporting and Corrective Action
10. Technology Control Plan, if applicable

MANAGEMENT COMMITMENT

Management Commitment refers to the commitment and support given by the company's management to comply with the STMA and its IRR.

Effective strategic trade management requires the company's commitment to properly abide by the provisions of the STMA and its IRR. Responsibility in implementing the company's ICP comes from the top officials down to the lowest ranking employees.

Establishment of an ICP must be supported by the company's top executives since it entails additional tasks which could be both administrative and technical. Conducting awareness and functional trainings, incorporating screening processes and risk assessments to business transactions, record keeping, reporting, among others, will require not only human and financial resources but more importantly, a firm mandate from the company.

For companies that will be establishing ICPs for the first time, including those under the category of Micro, Small and Medium enterprises (MSME), it is imperative that their management or owner understands this responsibility.

The commitment to comply with the STMA should be declared through a document signed by a senior representative, such as the Chief Executive Officer (CEO), or someone holding a similar position. In this document, said officer must state that the company is aware of the STMA, its rules and regulations and that all officers and employees in the organization are aware thereof.

MANAGEMENT COMMITMENT

A copy of this document shall be furnished to all concerned employees.

It should be posted in a conspicuous place inside the company premises along with other business permits and licenses. Another copy should be included in the company's ICP Manual.

Contractors and agents who represent the company must likewise be informed of this responsibility and must make the same commitment as a prerequisite to engaging business with the company. Other entities and persons whose duties are subject or related to strategic trade management such as consultants, freight forwarders, distributors, sales representatives, and joint venture partners must likewise be made to uphold the same commitment.

Companies may draft or adjust the contents of the document based on their own set-up. For micro, small, and medium enterprises (MSMEs), the owner or manager should be the one to sign the Statement of Awareness and Commitment.

MANAGEMENT COMMITMENT

Below is an example of a draft statement of awareness and management commitment:

(Company Letterhead)

DATE :
TO : All Employees & Contractors
FROM : Name, President/CEO/Chairman
SUBJECT : Strategic Trade Management Policy Statement

(*Company*) is aware of the Strategic Trade Management Act (STMA) and is committed to comply with all its requirements.

As such, all employees are hereby ordered to abide by the STMA and its Implementing Rules and Regulations (IRR).

No transfer of item, software, or technology, by any individual operating on behalf of (*Company*) shall be made contrary to the provisions of the STMA and its IRR.

No activities in violation of the STMA shall be undertaken.

Failure to comply with these regulations may result in the imposition of administrative fines, including monetary and criminal penalties against individuals or employees aside from possible disciplinary action and/or termination.

Please contact the following personnel for any questions concerning the legitimacy of a transaction or potential violations:

Name of ICP Personnel and Title

Phone and E-Mail

[Name of Official] is responsible for disseminating this Statement throughout the organization through *[Company's]* Internal Compliance Program Manual updates, incorporation into training and presentations, and posting on the (*Company*) Intranet and Web site.

_____
President/CEO/Chairman

_____
Signature

_____
Date

ICP STRUCTURE AND RESPONSIBILITY

An ICP structure refers to the composition and arrangement of different personnel tasked in implementing the ICP.

Chief Strategic Trade Control Officer (CSTCO)

The CSTCO is the person primarily responsible for ICP implementation. The CSTCO must possess an authority to require compliance from employees and must have sufficient knowledge on ICP. For MSMEs, the CSTCO could be the owner or manager.

ICP STRUCTURE AND RESPONSIBILITY

The following are the responsibilities of a CSTCO:

1. He must ensure that all employees fully comply with the company policy on STMA.
2. He shall be responsible for establishing and implementing the ICP. This includes making the necessary revisions to the program, whenever there are new regulations or when the program is already obsolete.
3. He should also oversee the development of the Standard Operating Procedures of the company pursuant to the provisions of the STMA.
4. He must ensure correct product classification and identification, promoting strict end-use/r screening and risk management, and making the final judgment on whether or not the business transaction should proceed. This task involves directing and communicating with exporters, importers and other concerned parties to meet STMA requirements. The CSTCO shall also be primarily responsible for providing guidance to subsidiaries and affiliates in matters related to STMA.

   Business transactions of concern must be reported to the CSTCO. In case there is doubt on whether to continue with a business transaction, based on a belief that doing so may lead to STMA violation, the CSTCO must be informed so he can help in reaching the final decision.
5. He must assign a personnel who is in charge in conducting internal audits.
6. He must ensure the proper training of employees on the STMA and proper recordkeeping of all transactions within the period required by the STMA.

For MSMEs, one or two personnel may be sufficient to do all the tasks concerning ICP. For large companies, however, considering the size of the organization, the nature of the strategic goods being traded, and the volume and frequency of transactions, the CSTCO would need assistance of a unit to properly implement the ICP.

Creating an ICP Team

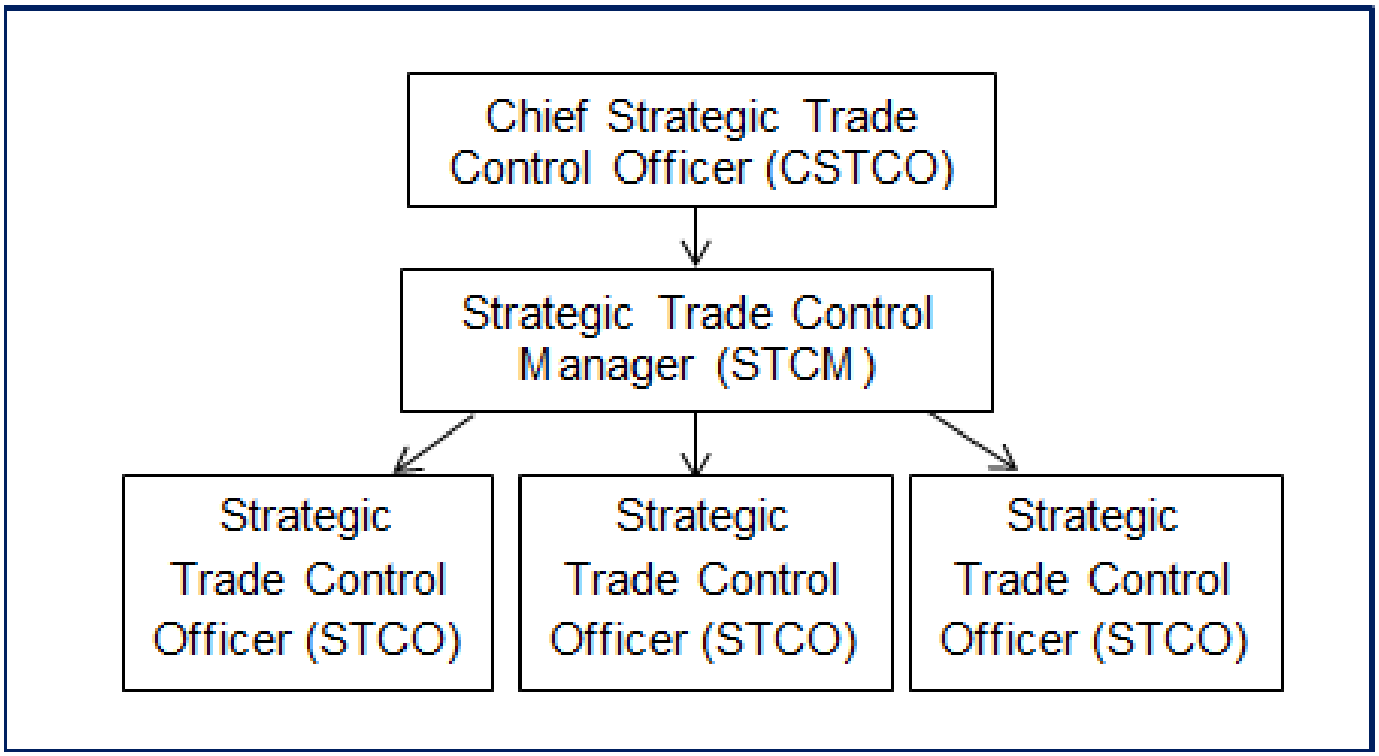
The CSTCO shall determine who will form part of the company's ICP Team and what their respective duties and responsibilities will be in the unit.

One option is to create a new unit for the sole purpose of ICP. Another is to assign the respective tasks to personnel from different units as an additional tasks, as the company deems fit.

It is important for an ICP team to be independent from the sales department. This will avoid business decisions that may favor sales rather than trade security, especially in transactions where there is high risk of diversion.

An organizational chart showing the internal structures and responsibilities for STMA must be distributed to all employees so the persons responsible under the ICP could be easily identified and reached for queries or for any matter that needs their attention.

Example of an ICP Structure for Large Companies



ICP STRUCTURE AND RESPONSIBILITY

Large companies that are engaged in voluminous transactions of strategic goods may also appoint a Strategic Trade Control Manager (STCM) and create a Strategic Trade Control Unit (STCU).

The STCM shall supervise the STCU and will carry out the strategic trade control operations under the directions of the CSTCO.

Further, a large company composed of numerous units or departments having STMA-related functions may choose to appoint a Strategic Trade Control Officer (STCO) in each unit, i.e. sales, marketing, production, research and development, logistics, et al. Each STCO shall be responsible for creating awareness on the instructions and requirements of the STCM in his own unit. The STCO will also ensure staff training and uphold STMA operating procedures.

There is no “one size fits all” rule in ICP. The number of staff that should comprise the ICP structure within a company depends primarily on the volume and/ or nature of strategic goods or technology being traded and on the size of the company. Hence, ICP structure should be suitable to the company’s organizational framework.

Identifying how much of the company’s workforce have access or tasks related to controlled commodities, technology or information is important in determining how many staff should compose the ICP team.

Example of ICP Structure for MSMEs

Under Republic Act No. 9501, otherwise known as the Magna Carta for Micro, Small, and Medium Enterprises, below is the classification of organizations according to assets, including the projected number of employees, based on the establishment category used by the Senate Economic Planning Office in 2012:

Table 1: MSME Classification Enterprise Category[1]

Classification	By Asset Size	By Number of Employees (*estimate only*)
Micro	Up to P3,000,000	1 - 9 employees
Small	P3,000,001 - P15,000,000	10 - 99 employees
Medium	P15,000,001- P100,000,000	100-199 employees

It should be noted, however, that companies with employees or assets greater than the medium classification can be considered as large companies.

The ICP Team for MSMEs could be constituted as follows:

Class	Composition of ICP Team
Micro (1 to 10 employees)	May have only one (1) personnel, i.e. CSTCO only.
Small (10 to 99 employees)	Considering the volume of transactions and sensitivity of goods, the ICP team may be composed of one (1) to three (3) personnel. However, additional personnel can be added to make sure that all aspects of STM are covered.
Medium to Large (100/ more employees)	Taking into consideration the volume of transactions, sensitivity of goods, etc., ICP team could be composed of three (3) or more members.

The table above estimates how many personnel can be assigned to internal compliance given the size of an organization. Companies can use this as a guide in establishing an ICP team.

Notwithstanding estimates given above, each organization must create a compliance structure based on what is most suitable to the nature and demand of its business.

SCREENING PROCEDURES

Screening procedures include four (4) elements: product classification, end-use screening, end-user screening, and risk assessment.

Screening procedures must be documented and form part of the ICP Manual.

Product Classification

Product classification is the process of determining if the item, software, or technology to be transferred is controlled and requires an authorization from the STMO.

A product is controlled if it meets the specifications in the NSGL. Technical experts on the commodity should be asked to assign the correct NSGL codes. Consultations can be made with competent authorities such as:

a. Manufacturers of the items (for externally sourced items); and,

b. Educational institutions or government agencies that specialize on the study of the subject goods.

However, items not listed in the NSGL may still be subject to STMO's authorization if the same falls under the catch-all provision under Section 11 of the STMA.

SCREENING PROCEDURES

The table below shows a list of possible experts who may be consulted when classifying a commodity:

Party	Persons who can make initial determination if product is strategic
Manufacturer exporting own commodity	The technical product design unit and CSTCO or STCM should coordinate in classifying items pursuant to the specifications in the NSGL.
Distributors or dealers and other intermediate parties	The original supplier or manufacturer should provide technical specifications of the items and must be able to give an assessment as to the classification of the items under the NSGL.

End-Use Screening

End-Use screening is the process of determining the reason why the strategic good is being exported or the purpose for its utilization by the end-user.

The company must verify that the items will not be used in violation of the STMA or for purposes other than the declared end-use in the End-User Certificate (EUC) provided by the end-user.

The importer/ buyer/ stated end-user will provide information on the end-use of the commodity after verifying that the business of the ultimate end-user is in line with the end-use of the commodity.
Likewise, the company must be cautious of the end-use/r of a non-listed dual-use item, especially if it is for a military end-use and is destined to a country subject to an arms embargo or UN sanctions list as provided under Section 11 of the STMA.

SCREENING PROCEDURES

End-user screening is the process of identifying the ultimate end-user of the commodity and ensuring that said end-user is not included, or connected to a person/ entity, in the denied party/ persons list/ sanctions list.

It includes conducting a background check on present and previous ties or affiliations of the customer/end-user. If the end-user is a juridical person, the check may also extend to its trade partners, board members, and other company officials. Information gathered from online resources can be useful in screening third parties.

End-users must execute an End-User Statement (EUS) which must contain the following information: (a) that the end-user has undertaken to import the goods with specific value and amount; (b) the purpose of the use of the goods; and (c) that the end-user shall not re-export or re-assign the goods without prior written authorization.

All EUS executed by end-users must be archived for audit purposes.

SCREENING PROCEDURES

Companies may refer to the different EUS formats provided by the STMO. Below is a sample EUS:

END-USER CERTIFICATE

I/ We,	
End-user details	
Company Name:	
Company Address:	
Telephone Number:	
Fax number	
Website:	
Email Address:	
Type or Nature of Business:	
have requested	
Exporter details	
Company Name:	
Company Address:	
to export	

Product details *(attach separate sheet/s if necessary)*

Product description	NSGL Code	HS or CN Code	Brand and Model	Quantity	Currency and value

which is intended for

End-use details

	Consumption	in* _____	for**	_____
	Production	in* _____	for**	_____
	Distribution	in* _____	for**	_____
	Repair	in* _____	for**	_____
	Other *(please specify)*	in* _____	for**	_____

* Country of final destination

**Provide specific detailed end use of the goods/technology identifying the specific operations to be performed by the goods in support of the end-user's business activity

END-USER CERTIFICATE
I/ We declare that the strategic or unlisted goods listed above:
1. shall be used exclusively for the stated end-use;
2. shall not be used in the development, production, handling, usage, maintenance, storage, inventory, or proliferation of weapons of mass destruction and its delivery systems;
3. shall not be sold/ transferred to an individual or entity who is involved directly or indirectly, or is known or suspected to be involved in the development, production, handling, usage, maintenance, storage, inventory, or proliferation of weapons of mass destruction and its delivery systems;
4. shall not be sold/ transferred to an individual or entity who is sanctioned or restricted under applicable United Nations Security Council Resolutions; and
5. shall be re-exported or sold to a third party in accordance with the originating/ supplying and receiving countries' export control laws, as applicable.

CERTIFICATION BY THE END-USER		
I/ We hereby certify that all facts stated herein are true and correct based on my/our own personal knowledge and nothing contained herein is inconsistent with my/ our declaration. We shall promptly update the exporter should I/ We know of any facts or intentions set forth in this statement which may occur after the execution of this certificate.		
AUTHORIZED SIGNATURE	COMPANY STAMP	NAME OF AUTHORIZED PERSONNEL
		TITLE/ POSITION
		DATE *(dd-mm-yy)*
		VALID FOR THE DURATION OF THE LICENSE

Risk Assessment

Risk assessment is the process of identifying and evaluating risks that are present in a transaction after going through product classification, end-use and end-user screening. It is the final step before a company decides whether to push through with the transaction or not.

Evaluating the level of risk present in a given transaction requires scrutiny of all available information such as:

a. Whether the end-user is included in the denials/ sanctions list, or has links/ affiliations with known terrorist groups, individuals or countries of concern.
b. Whether the technical specifications and amount of the goods match the stated end-use.
c. Whether the country of destination is subject to UN sanctions or other applicable sanctions, arms embargo, or is known to be engaging in illicit or underground programs to develop WMD.
d. Whether the purchaser is willing to buy the dual-use goods even at a high price or at quantities inconsistent with the stated purpose.
e. Whether there is potential risk of diversion.

SCREENING PROCEDURES

Companies should be vigilant in identifying red flags when vetting their customers which may include the following factors:

a. The customer is reluctant to offer information about the end-use of the items.

b. The customer asks that the goods be transferred to a forwarding address.

c. The customer is reluctant to provide clear answers to commercial or technical questions which are normal in routine negotiations.

d. An unconvincing explanation is given as to why the items are required, in view of the customer's normal business or the technical sophistication of the items.

e. Routine installation, training, or maintenance services are declined.

f. Requests for excessive spare parts or lack of interest in any other spare parts.

g. Unusually favorable payment terms such as higher price and/ or lump sum cash payment are offered.

h. Unusual shipping, packaging, or labelling arrangements are requested.

i. Unusual (high) security around installation site in view of the type of equipment being installed.

Unusual requirements for excessive confidentiality about final destinations, customers, or specifications of items

a. Unusual characteristics of the order, e.g., the quantity or performance capabilities of the goods ordered significantly exceed, without satisfactory explanation, the amount or performance normally required for the stated end-use.

SCREENING PROCEDURES

Risk assessment can be considered as a catch-all check.

Exercising due diligence may require a person to ask questions such as “does everything in this transaction add up?” or “is what I’m seeing now the whole picture of this transaction?” The answers to these questions can help detect inconsistencies or any missing information and aid in evaluating existing threats.

The procedure on risk assessment must not only be able to guide the company to identify and assess the risks but also provide the appropriate subsequent steps that will address and reduce the threats, or if possible, eliminate them completely. A weak or incomplete risk assessment procedure could allow lapses that may result into transfers that constitute a violation of the STMA.

The level of identified risk should serve as a basis for deciding whether the transaction should proceed

SHIPMENT CONTROL

Shipment control is a system that prevents diversion of strategic goods as they are transferred from one country to another.

As commodities are shipped from the company's premises en route to the end-user, security checks should be done before, during, and after shipment, which include the following:

Checking if the classification/ identification and transaction screenings are completed.

Checking if the goods and technologies and their quantities correspond to the descriptions set out in the export/ import instruction documents and/or STMO authorizations.

Confirming that all the necessary documents such as Product Manuals, Technical Specifications, Authorizations/ Licenses, Certificates, Permits, and other descriptive documents that must accompany the commodity are readily available during the entire shipment.

Ensuring the trustworthiness of the shipper, freight forwarders, warehouses, and all other persons who will be safekeeping and transporting the goods through proper screening.

SHIPMENT CONTROL

Risk assessment can be considered as a catch-all check.

Exercising due diligence may require a person to ask questions such as “does everything in this transaction add up?” or “is what I’m seeing now the whole picture of this transaction?” The answers to these questions can help detect inconsistencies or any missing information and aid in evaluating existing threats.

The procedure on risk assessment must not only be able to guide the company to identify and assess the risks but also provide the appropriate subsequent steps that will address and reduce the threats, or if possible, eliminate them completely. A weak or incomplete risk assessment procedure could allow lapses that may result into transfers that constitute a violation of the STMA.

The level of identified risk should serve as a basis for deciding whether the transaction should proceed

Checking the packaging, labels, containers, and storage of the goods to avoid damage, spoilage or being lost during transit.

Ensuring that the goods will be received by the end-user. This could be checked through a Delivery Verification Certificate or other similar documents showing proof of delivery.

All possibilities during the transportation of items must be considered. Countries/ territories that are reported to be diversion hubs must be verified by exporters to ascertain the veracity of these reports and if possible, avoid these routes.

ICP TRAINING

ICP training is the process where an employee undergoes skill and/ or knowledge development in preparation for tasks concerning STMA.

To ensure that employees can carry out their duties properly, the company must see to it that its employees have received proper ICP training prior to engaging in any task related to the STMA. They must be trained before having any access to strategic items, software, information, or technology.

Employees whose duties are related to strategic trade management, i.e. those handling strategic goods, software, and technology, those who have access to controlled goods and information, those who are assigned in sales and export related units, and those who are involved in technology transfer, must be aware of the STMA, its IRR, and the relevant guidelines on STMA implementation.

Training topics may include STMA overview, ICP objectives, screening procedures including risk assessment, company's Technology Control Plan (TCP) for intangible transfers, principles/procedures on shipment control, reporting and corrective action, record keeping, and internal audit. Functional trainings focus on specific tasks the employee performs in relation to the ICP.

On the other hand, employees whose duties are not directly related to strategic trade management must undergo awareness training so that they will be informed about the STMA and their company's programs and policies regarding strategic trade management. The topics should include export and other STMA covered transactions, company's product line, violations and penalties, mechanism for incident reporting, especially those that potentially violate the STMA, etc.

Companies may coordinate with STMO on appropriate trainings on strategic trade management. Likewise, an archive of all training records should be maintained.

INTERNAL AUDIT

Internal audit is the process whereby a company assesses its own ICP.

The purpose of internal audit is to strengthen the company's ICP by detecting problems, threats, or gaps within the program which may lead or tend to lead to violations of the STMA.

Internal audit must be carried out regularly to determine if the ICP is carried out properly and in accordance with the company's ICP Manual.

For impartiality, the internal auditor/s should be independent from the company's ICP team to have a free and unbiased assessment.

The CSTCO may assign as internal auditor/s personnel from different units within the company, provided they have functional training on the STMA and ICP. Alternatively, an external compliance auditor may be considered, taking into account the structure, size, and financial resources of the company.

The results of the audit should be archived, and the issues identified resolved accordingly. Internal audits with resulting findings should be documented and must be carried out at least annually

STANDARD OPERATING PROCEDURES MANUAL

Implementing an ICP involves performance of tasks aimed to promote security from different threats. As such, employees should be properly guided by procedures on how their respective functions should be carried out.

The Standard Operating Procedure (SOP) on ICP contains detailed procedures that must be followed by employees to ensure compliance with ICP rules and policies. It serves as the best reference material that could provide consistency in the desired outcome regardless of the personnel assigned to perform a given task. Thus, it must be clear, understandable, and implementable.

It must cover each step involved in the performance of duties involving STM. Further, it must be attuned to the provisions of the STMA and assist in complying with the requirements and conditions of the Authorization. For this reason, the SOP must be constantly updated as needed to conform to the STMA and other guidelines issued by the STMO.

For companies that observe SOPs, the same can be revised by adding or integrating procedures relevant to internal compliance.

For example, in an SOP for conducting business transactions, additional documented procedures on product screening, end-use/r screening, risk assessment, authorization application, shipment control or TCP, record keeping and reporting (if needed) should be incorporated.

In principle, all employees must have a copy or access to the ICP Manual and abide by it.

RECORDKEEPING

Recordkeeping is a system by which a company maintains records of its transactions.

Archived records should be secure, organized, and traceable. Also, it must be readily available during audits as company records prove that the transactions undertaken are consistent with the STMA as well as the terms and conditions of the authorization.

Section 10 of the STMA provides the rules for recordkeeping. It states that "all persons engaged in the business involving strategic goods are required to keep at their principal place of business, in the manner prescribed by the IRR to be issued by the NSC-STMCom for a period often (10) years from the date of the completion of the transaction, all records of the transaction and/or books of accounts, business and computer systems and all commercial and technical data related to the transaction including:

a. The description of the strategic goods or related services;
b. The quantity and the value of the strategic goods or value of the related service provided;
c. The name and address of the parties in the transaction or activity;
d. The end-use and end-user of the strategic goods or related services; and
e. The date of the transaction or activity."

RECORDKEEPING

STMA-related transaction documents may also include the following:

a. export or import licenses issued by the concerned government authorities;
b. product classification/identification sheets;
c. end-use assurances;
d. commercial invoices;
e. delivery verification certificates;
f. contracts with buyers containing a common clause that items purchased will not be used for WMD or other illegal purposes;
g. email communications;
h. attendance and minutes of meetings;
i. records of electronic transfers;
j. shipping documents;
k. purchase orders;
l. invitation to bid;
m. request for quotations; and,
n. other documents that would contribute in ascertaining the circumstances surrounding the transfer of the strategic commodities.

Records must be kept both in hard and electronic copies. The procedures for archiving documents should be known by all relevant staff.

REPORTING AND CORRECTIVE ACTION

Reporting: Voluntary Self-Disclosure

Companies should report to the STMO any act that violates the STMA, its IRR or terms and conditions of the authorization.

A company must develop procedures for reporting violations of the STMA.

To avoid false alarms, companies must consider a step-by-step process that starts when a vigilant employee suspects or gains knowledge that there has been a violation of the STMA, reports the same to the CSTCO or to an immediate supervisor. If reported to a supervisor, then he must report the same to the CSTCO after proper verification of the information received. The CSTCO, in turn, will report to the STMO.

Conversely, if a clear violation of the STMA is shown, companies must immediately report the same to the STMO or other appropriate government agencies such as the Bureau of Customs, Philippine National Police, or Philippine Coast Guard, most especially where immediate action is necessary to stop a shipment.

The STMO will provide a form for voluntary self-disclosure of violations. Voluntary self-disclosure of a violation inadvertently made could merit consideration on the imposable administrative penalty or fine.

Violations of the company's ICP need not be reported to the STMO but should be reported to the CSTCO.

Corrective Action

The company must implement preventive measures and corrective actions as maybe necessary so that violations will not recur. This may include issuing warning letters reminding erring employees to follow the company's SOP or requiring them to undergo re-training on ICP rules and implementation. On the other hand, disciplinary actions should be taken against staff members who are responsible for confirmed violations of the STMA and its IRR.

Immediate action must be taken once a problem is detected, as when a controlled item has been exported without a license as a result of wrong commodity classification. Thus, in this case a proper corrective action that may be included in the SOP is to consult with technical experts or seek advice from the STMO.

Reports of violations along with the corresponding corrective actions taken should all be recorded and made available for audit.

Reporting of Suspicious Request from Potential Customers

The industry is the first line of defense as proliferators usually seek to acquire strategic goods and technology by going through the normal process of purchasing from legitimate sources. Companies must be cautious of these attempts by carefully conducting screening procedures and promptly informing the STMO about any suspicious orders or requests received specially from new or unknown customers.

TECHNOLOGY CONTROL PLAN (TCP), IF APPLICABLE

Transfers under the STMA do not only cover actual shipment of strategic goods (tangible) but also the transmission of software and technology (intangible) either by electronic media, i.e. fax, telephone, electronic mail or any other electronic means or through non-electronic means, i.e. face-to-face communication or personal demonstration.

A Technology Control Plan (TCP) is a system designed to prevent unauthorized access, transmission or sharing of sensitive and controlled items, materials, information, software or technology.

One aspect of a TCP is determining the personnel who will be authorized to have access to the controlled items, materials, and technology. These personnel should be properly screened and a non-disclosure agreement/ clause must be included in their employment contracts or services. This requirement is to ensure that there will be no unauthorized sharing of sensitive information acquired during such engagement. The selected employees should undergo training which should cover topics including information, data or technology handling and security.

Another aspect is physical security plan which refers to security measures that should be taken to prevent unauthorized personnel from observing or having access to the premises wherein the research, development, production or storage of controlled goods are being made. Secured doors accessible only by access badges or biometric sensors, secured computers, locked cabinets or desks, among others may be utilized to ensure physical security against unauthorized access.

TECHNOLOGY CONTROL PLAN (TCP), IF APPLICABLE

For controlled electronic software or technology, an information security plan is imperative. This includes having User IDs, password control, or using encryption technology. Database access can be managed by a Virtual Private Network (VPN) to allow authorized persons to safely access and transmit data over the internet.

To avoid data loss or data theft, a network security plan must also be developed by companies with intangible software transmissions. Firewalls may be used to maintain security from outside intruders. Diagnostic tools can be utilized to identify specific security weaknesses.

For companies that employ or engage the services of a foreign individual, by reason of which controlled information or technology is being accessed by said foreign person, an authorization from the STMO may be required as such is considered as an export even if the transfer is made within the Philippines.

Where sensitive technology or information is to be discussed or shared in an event or meeting, e.g., via power point presentation that contains such controlled information, security control can be made by pre-checking the attendees and participants to said event. The CSTCO or his alter ego may decide whether to allow, limit or prohibit such presentation or information sharing.