SAFERWORLD
PREVENTING VIOLENT CONFLICT. BUILDING SAFER LIVES

CENTER FOR POLICY RESEARCH
UNIVERSITY AT ALBANY

AITEC 商务部国际贸易经济合作研究院
Chinese Academy of International Trade and Economic Cooperation

Strategic trade control outreach and industry compliance

Tools and resources

SAFERWORLD
PREVENTING VIOLENT CONFLICT. BUILDING SAFER LIVES

CENTER FOR POLICY RESEARCH
UNIVERSITY AT ALBANY

CAITEC 商务部国际贸易经济合作研究院
Chinese Academy of International Trade and Economic Cooperation

Strategic trade control outreach and industry compliance

Tools and resources

Acknowledgements

This manual was developed by Elizabeth Kirkham, under the overall guidance of Bernardo Mariani and with support from Saferworld's Arms Unit and China team, as well as research staff from the Center for Policy Research at the University at Albany, and the Institute of Trade and Investment Security of the Chinese Academy of International Trade and Economic Cooperation. Preliminary drafts of this manual were discussed with government officials, policy experts, practitioners, and industry representatives from Asia, Europe, and the US during meetings held in 2018 in Beijing, London, and Vienna.

We acknowledge with great appreciation the input and feedback provided by members of the Expert Working Group associated with this project. For their time and expert contributions, special thanks go to: Muhammad Nadeem Ahmad, Dr Zafar Ali, Dr Malin Ardhammar, Peter Cheah Hee Keong, Dr Cheng Hui, Spencer Chilvers, Kevin J. Cuddy, Janine Green-Holmen, Dr Guo Xiaobing, Dr Han Lu, Han Shuang, Dr Patrick Edgar Holzer, Roy Isbister, Yi Jiang, Dr Jing Rui, Kyung-Lyung Lee, Datin Mega Marissa Abdul Malek, Armando Q. Mercado Jr., Jay Nash, Se-Hee Ryu, Brinley Salzmann, George Tan Swee Cheng, Tang Xiaomin, Tian Yilin, Wu Jinhuai, Xie Jiaoning and Dr Zhang Wei.

We are also grateful to the many people in Europe, Asia and the US who shared their comments, insights and expertise, including during meetings, seminars and roundtable discussions. For the critical role in bringing this project to print, we thank Saferworld's communications team along with copyeditor Jatinder Padda and designer Jane Stevenson.

The manual was developed based on independent expert discussions and does not reflect official government positions. Responsibility for the content and any opinions lie solely with the authors.

The production of this resource manual was made possible thanks to generous financial support from Canada's Department of Foreign Affairs, Trade and Development.

Contents

PART B
Elements of industry internal compliance programmes

List of acronyms

AEO	Authorised economic operator
EWG	Expert Working Group
IAEA	International Atomic Energy Agency
ICP	Internal compliance programme
ITT	Intangible technology transfer
MNC	Multinational corporation
RMC	Research management centres
SECDIV	Strategic Export Control Division (Pakistan)
SMEs	Small and medium-sized enterprises
STA	Strategic Trade Act (Malaysia)
STC	Strategic trade control
STMA	Strategic Trade Management Act (the Philippines)
STS	Strategic Trade Secretariat (Malaysia)
UK	United Kingdom
UN	United Nations
US	United States
WMD	Weapons of mass destruction

Preface

This manual is the product of research and discussions involving Asian, European and US experts from government, industry, international organisations, and the non-government sector – the Expert Working Group (EWG) – that have taken place for over a year. The project has been driven by growing international concern over the illicit proliferation of sensitive goods and technologies and the potential for this to contribute to the development of weapons of mass destruction and other destabilising military capabilities. To this end, Saferworld, the Center for Policy Research at the University at Albany, the Chinese Academy of International Trade and Economic Cooperation, and the EWG identified the need for targeted resources to support government outreach on strategic trade control (STC) and industry compliance initiatives.

Drawing on a huge wealth of knowledge and experience from government, industry, academia and civil society, the authors of this manual seek to provide assistance for those in government and elsewhere who are seeking to establish, develop or improve existing systems for STC outreach, and for those in industry seeking to establish or further develop systems for STC compliance. Although it has not been possible to include a detailed response to every possible situation that may be encountered in relation to STC outreach and compliance, it is hoped that the many examples and resources that are referenced and linked to in this manual may assist users in finding answers elsewhere.

This manual is divided into two parts. The first part addresses the subject of government-led outreach to industry and other relevant actors on STCs. In addition to suggestions for topics that should be covered, the manual includes a comprehensive range of strategies and methods that will facilitate effective STC outreach by government and other stakeholders, including online resources and person-to-person interactions.

The second part addresses the subject of internal STC compliance on the part of companies and institutes involved in the trade in strategic goods and technologies. This sets out the costs, benefits and challenges of internal compliance programmes (ICPs) and includes information on the types of systems and processes that are required, including details of screening processes, record-keeping and compliance audits.

PART A

Government outreach on strategic trade controls

1 Introduction

Strategic trade controls (STCs) are a vital part of national and international efforts to prevent the proliferation of sensitive technologies and their use in the development of weapons of mass destruction (WMD) programmes and military capabilities by illicit actors. Whereas the primary responsibility for the establishment and administration of STCs lies with national authorities, the vast global trade in strategic goods means that few, if any, governments are in a position to conduct physical checks on every consignment that is exported from their territory. In addition, there are a variety of different entities – including international brokers, transportation agents, and research and financial institutions – whose roles in this global trade, although much less visible, nevertheless require regulation and oversight. Governments therefore depend on the support of industry and other relevant actors[1] concerned with exporting and trading strategic goods and technologies in order to ensure compliance with export and international trade control laws; in this regard, companies are often referred to as 'the first line of defence' against proliferation of sensitive goods and technologies.

It is therefore in governments' interests **to raise awareness and understanding of STCs** among industry and other relevant actors and to provide information and advice that will enable them to fulfil their STC obligations. While the scope of government outreach on STC issues will depend on the size of the country concerned, the extent of its involvement in the international trade/transfer of strategic goods and the resources available, all governments should – at a minimum – make clear what is expected in terms of STC compliance, including required systems and procedures (for example, in relation to record-keeping).

Government STC outreach should also involve **promoting the adoption** – where feasible – **of STC internal compliance programmes (ICPs)** on the part of industry, and stressing the benefits of adopting such programmes and including recommended elements. However, it should be clearly recognised that, depending on the nature, complexity, and location of a company/institute's business, a fully-fledged ICP may take time to develop and refine. Given that awareness and understanding of STCs varies hugely among different industries and other relevant actors, it is also important to ensure that outreach is pitched at a level that is appropriate for the audience in question.

The principal targets of government STC outreach will depend on the nature of the issues that are to be addressed. In respect of general STC issues affecting manufacturers, traders, and those involved in the physical movement of strategic goods, technologies, and/or the provision of associated technical assistance, **special attention should be given to small and medium-sized enterprises (SMEs)**, given that such companies tend to have lower levels of awareness and understanding of STCs. However, when addressing the specialised issue of technology – in particular intangible technology transfer (ITT) – which may also include the provision of associated technical assistance, the focus should be expanded to include academic and research institutions.

There are **challenges** to the effective provision of information by governments to industry, enterprises, and institutes concerned with STCs. Some key challenges include:

- scarcity of resources in terms of funds, time, human resources, and expertise
- changing and competing priorities within government (e.g. a government may decide to focus less on STC outreach to industry and more on detecting and prosecuting STC violations)
- political will for systematic and effective outreach
- ensuring that the right information is transmitted to the right people
- assisting companies/institutes in understanding what their STC compliance requirements are and what systems or provisions are appropriate for their situation
- avoiding mixed messages being transmitted (e.g. through an overemphasis on trade promotion activities compared with the need for responsible STCs)

If government STC outreach efforts are to be successful in ensuring optimal levels of STC compliance, it is vital that these efforts also focus on the development of **a genuine partnership within and between government, industry, and other relevant actors** concerning STCs, the latest technological developments, and supply chain issues. Experience suggests that such partnerships, based on trust and mutual understanding, can encourage industry and other relevant actors to **report suspicious enquiries** and STC compliance problems and to **seek appropriate assistance** before a situation escalates. Accordingly, governments may wish to engage industry groups and other relevant actors in dialogue, with a view to gathering and sharing information and building a partnership that enhances the effectiveness of STCs, both in terms of their development and their implementation.

NOTES

1 For the purposes of this manual, 'industry and other relevant actors' is an umbrella term intended to capture all entities involved in the export and/or international trade in strategic goods and technologies. This includes, but is not limited to: manufacturers; distributors; brokering agents; transportation and shipping companies and agents; research, development, and production companies; universities and other research institutions; and financial actors, including banks and investment and insurance companies.

2 Identifying relevant actors

Industry and other non-government actors involved in the international trade in strategic goods and technologies and/or the provision of associated technical assistance have a responsibility to adhere to the STCs that apply in all jurisdictions where they are operating. This necessitates a full understanding of the nature and extent of STCs in each relevant context, including potentially complex issues such as the regulation of international brokering and financing, ITT, and catch-all controls. However, **not all relevant actors are aware of their STC responsibilities**, and in some contexts governments may place too great an emphasis on self-regulation.

Box 1: Examples of types of entities to which STCs may apply

- Manufacturers of strategic goods (both state-owned and private enterprises)
- Technical services companies
- Academic institutions (schools, colleges and universities)
- Research institutes
- International brokers and trading companies
- Promotional and sales agents and consultants
- E-commerce actors
- Air freight companies
- Road haulage companies
- Shipping companies
- Transportation agents
- Freight forwarding agents
- Private security companies
- Banks and financial institutions (including insurance companies and agents)
- Telecommunications companies
- IT companies and service providers (including data storage and cloud services)
- Free ports and other free-trade zone authorities, and companies located within such zones

While the majority of companies operating in the field of strategic exports will be known to government, it is quite possible that some entities – in particular SMEs – may be operating 'under the radar', unaware or ignorant of their STC obligations. Government authorities should therefore **take proactive steps** to reach out, as far as possible, to all entities that are impacted by STCs.

Box 2: Sources of information/methods that may help to locate relevant entities

- Company registration authorities
- Public business directories
- Regional, provincial, and local authorities
- Local chambers of commerce/business federations
- Trade associations
- Manufacturing sector associations
- Freight forwarders/logistic services providers
- International brokers and trading companies
- Enforcement agencies, in particular customs
- Intelligence agencies
- Banks and financial institutions
- Trade and investment companies and boards
- Trade conventions and other events
- Mass advertising campaigns (e.g. at airports and seaports)
- Internet searches using key words
- Other governments, including foreign intelligence
- Company tip-offs
- Customs authorities

Given the difficulty of identifying and reaching every enterprise and organisation that is impacted by STCs, government authorities could consider adopting certain **administrative measures**, including:

- Information on STCs and opportunities to engage with relevant government outreach efforts could be flagged as part of a company's registration process with national authorities.
- Information on relevant entities trading in strategic goods may be drawn from customs clearance information, specifically the Harmonized Commodity Description and Coding System (HS Code);[2] companies that have exported items using HS Codes that cover strategic goods can be identified and steps taken to ascertain whether the goods in question were subject to STCs and duly authorised, and whether controlled intangible technologies and technical services have also been exported.

Information regarding companies that are concerned with strategic goods or technologies can also be sought from relevant **industry associations**. Alternatively, investment companies and banks that are involved with high-tech enterprises in particular may also be able to provide information on relevant actors.

Once relevant entities are identified, government authorities should write to company directors with information on STC compliance and invite them to attend relevant STC training/outreach events (see 'Strategies and mechanisms for government outreach on STCs' on page 29). Companies may be encouraged to attend if such events are conveniently located and free of charge.

NOTES

2 UN Trade Statistics (2017), 'Harmonized Commodity Description and Coding Systems (HS)' (https://unstats.un.org/unsd/tradekb/Knowledgebase/50018/Harmonized-Commodity-Description-and-Coding-Systems-HS)

3

Information provided as part of government outreach on STCs

Laws, regulations, and administrative procedures

The first task of any government STC programme on outreach to industry and other relevant actors is to provide **information on STC-related laws** that exist within their jurisdiction and on how these laws are implemented through regulations, policies, and administrative mechanisms (such as an STC licensing system, customs codes, procedures and declarations, and/or government compliance audits).

In order for STC laws to work effectively and to be easily understood, they must be based on firm foundations and be clear and unambiguous. Such laws should not require a lot of additional explanation and legal commentary in order to be understood – too much information will reduce the likelihood of them being read. Every effort should be made to ensure that the information provided is useful and accessible to those who require it.

Governments may also consider including some information or references relating to **STCs that operate in other jurisdictions**, and in particular in countries that are key trading partners; for example, companies or institutes should be made aware of countries that apply STCs extra-territorially, such as the US which subjects any product with US-manufactured components to US export control regulations. Representatives of foreign governments could be enlisted to provide training and outreach on their STC systems.

The international context for STCs

Government outreach on STCs should include information on the **origins and provenance of certain laws and regulations** – for example, where they flow from international obligations or multilateral commitments. Companies and relevant institutes should be made aware of existing **United Nations (UN) and other relevant multilateral sanctions**, the implications for strategic trade, and the need to ensure compliance with such restrictions. In addition, background information could also be provided in respect of relevant **international non-proliferation regime(s)**, including their role in the establishment of international export control standards and applicable control lists.

Government outreach should also, as far as possible, include an explanation of the types of problems that the national laws and regulations are designed to address (see 'Proliferation concerns' on page 12). In addition, the **benefits of effective national and international controls** on the trade in strategic goods should be highlighted, including how the establishment of a stable regulatory environment can increase the likelihood of attracting high-tech inward investment. Governments should explain, as appropriate, the nature of their particular engagement with relevant international agreements and regimes and how these have helped shape their national STCs.

Box 3: Relevant international non-proliferation regimes

1. Legally binding agreements[3]

- Nuclear Non-Proliferation Treaty
  https://www.iaea.org/publications/documents/treaties/npt
- Chemical Weapons Convention
  https://www.opcw.org/chemical-weapons-convention
- Biological and Toxin Weapons Convention
  https://www.un.org/disarmament/wmd/bio/
- Arms Trade Treaty
  https://thearmstradetreaty.org/
- UN Security Council Resolution 1540[4]
  https://www.un.org/en/sc/1540/resolutions-committee-reports-and-SC-briefings/security-council-resolutions.shtml

Box 3 continued

2. Other arrangements

The four major multilateral export control regimes listed below have played an active role in creating control lists and guidelines that represent a multilateral consensus on the types of goods and transactions that should be subject to regulatory controls. The regime control lists and their guidelines are available on their respective websites.

- Australia Group (chemical and biological-related items)
  https://australiagroup.net/en/
- Missile Technology Control Regime
  http://mtcr.info/
- Nuclear Suppliers Group
  http://www.nuclearsuppliersgroup.org/en/
- Wassenaar Arrangement (munitions and conventional dual-use items)
  https://www.wassenaar.org/

Control lists

Governments should provide information on where to find **relevant control lists that are applicable within a particular jurisdiction** along with relevant explanatory notes or best practice guidelines. Ideally these lists and guidelines will be provided in both the local language and other languages, including English, to enhance the prospects of relevant overseas entities being able to understand and comply with national STCs. Where national lists of controlled goods and technologies are based on lists adopted by international non-proliferation regimes, an explanation should be given of **the process that is followed in the development and updating of those lists**; any differences between national lists and those propagated by non-proliferation regimes should also be highlighted and explained.

Governments may also provide information on how to identify the control classification of strategic goods and technologies, and should **enlist the help of engineers** and other technical experts in this task.

Box 4: Examples of STC control lists from around the world

- Australia Defence and Strategic Goods List
  https://www.legislation.gov.au/Details/F2018C00287
- Canada Export Control List
  https://laws-lois.justice.gc.ca/eng/regulations/sor-89-202/FullText.html
- China Catalogue of Administration on Import and Export Licences for Dual-Use Items and Technologies
  http://www.mofcom.gov.cn/article/b/c/201812/20181202821810.shtml
- European Union List of Dual-Use Items
  http://trade.ec.europa.eu/doclib/docs/2018/october/tradoc_157453.pdf

  Common Military List
  https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018XG0315(01)&from=EN
- Hong Kong Strategic Commodities Control List
  https://www.stc.tid.gov.hk/english/checkprod/sc_control.html
- India Special Chemicals, Organisms, Materials, Equipment and Technology List
  http://dgft.gov.in/sites/default/files/SCOMEThelp04092018.pdf
- Japan Ministry of Economy, Trade and Industry Control List
  http://www.meti.go.jp/policy/anpo/matrix_intro.html
- Korea Strategic Trade Control List
  https://www.yestrade.go.kr/user/main.do?method=main
- Malaysia Strategic Items List
  http://www.federalgazette.agc.gov.my/outputp/pua_20181015_PUA263.pdf
- New Zealand Strategic Goods List
  https://www.mfat.govt.nz/assets/Strategic-goods-forms/2018-NZ-Strategic-Goods-List-August-2018-with-Table-of-Contents-reviewed.docx
- Singapore Dual-Use List
  https://www.customs.gov.sg/businesses/strategic-goods-control/strategic-goods-control-list/list-of-dual-use-goods

  Military List
  https://www.customs.gov.sg/businesses/strategic-goods-control/strategic-goods-control-list/list-of-millitary-goods
- Pakistan Control List
  http://www.secdiv.gov.pk/uploads/Control_Lists_4th-f55d.pdf
- United Kingdom (UK) Strategic Control List
  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/740156/controllist20180914.pdf
- U.S Commerce Control List
  https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl

  Munitions List
  https://www.ecfr.gov/cgi-bin/text-idx?node=pt22.1.121#se22.1.121_11

Proliferation concerns

Government outreach on STCs may also highlight **why certain strategic goods and technologies may be of interest to illicit networks** that are involved in proliferating WMD or sensitive military items.

This could include case study examples of illicit trafficking of strategic goods and associated proliferation activities and/or the human costs of the illicit trade in strategic goods and technologies.

Box 5: Examples of proliferation-sensitive goods and why they may be sought

- Certain general purpose integrated circuits – nuclear and military applications
- Heat exchangers and condensers – chemical weapons production
- Spraying or fogging systems and their components – biological weapon delivery
- Triggered spark gaps – nuclear weapon detonation
- Guidance sets – missile guidance
- Frequency changers – gas centrifuge component
- Carbon fibre (fibrous or filamentary materials) – missile bodies, nuclear centrifuges
- Triethanolamine – chemical weapons production
- Freeze dryers – biological weapon production
- Computer Numerical Control machine tools – nuclear centrifuge, missile and general military production
- High-end encryption – conventional military communications
- Corrosion-resistant pumps and valves – chemical weapons production
- Drilling and mining equipment – nuclear material production
- Vibration tables and other testing equipment – missile testing
- Image intensifiers and focal plane arrays – conventional military production
- Biological agents – biological weapons
- Toxic gas monitors and monitoring systems – chemical weapons production and testing
- Certain graphite – nuclear material production
- Powdered metals – missile fuel
- Fuses – conventional ordnance detonation

Countries of concern

Identifying country **destinations that raise concerns for reasons of proliferation, conflict, or international security** will enable industry and other relevant actors to be alert to the risks associated with the export and international transfer of strategic goods, technologies, and/or the provision of technical assistance, and will ensure they are better placed to make informed decisions in relation to proposed contracts. Information should be shared in relation to sanctions that have been instituted on a national basis as well as those agreed internationally.

Box 6: Mandatory UN arms embargoes[5]

- Central African Republic
- Democratic Republic of the Congo
- Iran
- Iraq (non-government forces since 2004)
- ISIL, Al-Qaeda and associated individuals and entities
- Lebanon (non-government forces)
- Libya
- Democratic People's Republic of Korea
- Somalia
- South Sudan
- Sudan (Darfur region)
- Taliban
- Yemen (non-government forces)

Box 6 continued

UN sanctions[6]

The UN has imposed broader sanctions on a number of the above states and against some non-state actors, and has established committees to oversee implementation of these sanctions, including in relation to:

- Central African Republic
- Democratic Republic of the Congo
- Democratic People's Republic of Korea
- Guinea-Bissau
- ISIL, Al-Qaeda and associated individuals and entities
- Iraq
- Libya
- Mali
- Sudan
- Yemen

Entity watch lists

SMEs in particular tend to lack the information, resources, and experience required to identify suspicious actors. It is vitally important for governments to provide **information on entities that are known to have been involved in the illicit trade in strategic goods** and technologies or, at least, to be able to point enquirers towards external sources of relevant information, so that they may undertake effective due diligence. This will assist industry and other relevant actors in assessing the advisability of entering into particular contracts or arrangements. In addition, the inclusion of information relating to historical cases of diversion and illicit trafficking would enhance understanding of how industry and other relevant actors can assist government in identifying and meeting such challenges in the future.

Some governments provide lists of 'denied' or sanctioned entities and associated tools that could be publicised as part of STC outreach efforts.

Box 7: Entity watch lists

- Consolidated UN Security Council Sanctions List
  https://www.un.org/sc/suborg/en/sanctions/un-sc-consolidated-list
- Japan Foreign End-User List
  http://www.meti.go.jp/press/2018/05/20180502001/20180502001-1.pdf
- EU Consolidated List of Sanctions
  https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions
- EU Restrictive Measures (Sanctions) in Force
  http://eeas.europa.eu/archives/docs/cfsp/sanctions/docs/measures_en.pdf
- EU Sanctions Map
  https://sanctionsmap.eu/#/main
- Australia Consolidated List
  https://dfat.gov.au/international-relations/security/sanctions/Pages/consolidated-list.aspx
- UK's Sanctions and Embargoes Lists
  https://www.gov.uk/business-and-industry/embargoes-and-sanctions and
  https://www.gov.uk/guidance/current-arms-embargoes-and-other-restrictions
- U.S Department of Treasury's Consolidated Sanctions List and Specially-Designated Nationals and Blocked Persons List
  https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/consolidated.aspx
- U.S Consolidated Screening List Search Tool
  https://www.export.gov/csl-search

Specialised STC issues

It is important to share information on especially **complex or anomalous STC issues** that require particularly detailed explanation, such as ITT, technical assistance, international brokering, and catch-all controls (see 'Awareness and consideration of specialised STC provisions' on page 70), in order to increase levels of compliance with such provisions. It will be difficult for government to take action against companies and institutes that do not adhere to such controls if there is limited awareness or understanding of them. In such areas, where there are particular challenges to STC enforcement, the focus of government outreach efforts should be firmly on:

- **Raising awareness of the controls that exist.** In the area of ITT – in addition to explaining the basis of applicable controls – information shared may include the implications of cloud storage solutions where information is stored on servers located at home or abroad, and any mitigation measures that might be taken (e.g. data encryption).
- **Clarifying what is expected of companies in adhering to controls within a particular jurisdiction.** In terms of catch-all controls, this should include the responsibilities of a company/institute to conduct necessary checks prior to entering into arrangements for the export or international transfer of listed and/or unlisted goods, technologies, and technical assistance, and any requirement to inform government of any concerns about their end-user or end-use.

Depending on a country's industrial, technological and trade profile, governments may decide to provide outreach that is focused on addressing specialised STC issues, such as ITT, technical assistance, and catch-all controls. This could include **specific guidance documents, workshops and training seminars, potentially alongside government 'help desks' with personnel capable of answering questions related to specialised STC issues**. In addition, by providing information in local and foreign languages, governments can help to increase understanding of, and compliance with, their controls on the part of foreign-based companies and institutes whose strategic trade activities take place within their jurisdiction.

Box 8: Malaysia–Internal Compliance Programme Guidance for Intangible Technology Transfer pursuant to the 2010 Strategic Trade Act (excerpt)[7]

The implementation of ITT in the institutions/entities will be based on the five elements of ICP.

1. Management Commitment

- Research Management Centres (RMC) for universities or any equivalent divisions in other institutions/entities may be appointed as the focal point for matters under the 2010 Strategic Trade Act (STA).
- Institutions/entities are expected to establish a policy statement which states its commitment to the obligations under STA.

Box 8 continued

2. ITT Application Form

- Institutions/entities are expected to embed the requirement of STA clause in:

  1. Letter of Award
  2. Non-Disclosure Agreement
  3. Contract
  4. Ethics Research Form
  5. Research Collaboration and Consultation Agreement

3. Screening

- Institutions/entities are expected to utilise the existing compliance committee/peer review committee to identify research activities related to strategic technology.
- RMC/focal point should be able to identify courses/materials which are considered as strategic under STA.

4. Training

- The Strategic Trade Secretariat (STS) may provide the outreach or training on STA to institutions/entities based on RMC's/focal point's coordination. RMC/focal point may conduct own training programmes utilising other local or international experts in ITT, based on STA's requirements.

5. Audit

- STS and its partner agencies may conduct an evaluation exercise for the permit holders in the institutions/entities to check their obligations under STA, including record-keeping of relevant documents.
- STS and its partner agencies may conduct an evaluation exercise for institutions/entities to assess the overall commitments under STA, based on their ICP.
- Elements of the audit include system, process, and documentation audit.
- The statutory requirements for record-keeping for the documentation audit is six years, including end-use statement, export permit, letter of invitation, list of participants, and presentation slides.

Box 9: New Zealand Foreign Affairs and Trade Department Guidance on Catch-All Controls (excerpt)[8]

Catch-all provisions

The export of goods, software, and technologies which are **not** listed in the New Zealand Strategic Goods List, but which may be intended for use relating (directly or indirectly) to any or all of the following are prohibited:

- the development, production, or deployment of nuclear, chemical, or biological weapons or their means of delivery in any country
- a military end-use in a country subject to a UN Security Council arms embargo
- use as parts or components of military items listed in the New Zealand Strategic Goods List (categories ML1–ML22) which have been unlawfully exported from New Zealand

Exporters have a statutory obligation to inform the Secretary of Foreign Affairs and Trade if they are aware or should reasonably be aware that an export is intended for or may have any of the prohibited uses described above.

What is 'Military end-use'?

Military end-use means:

a) incorporation into military items that fall within categories ML1–ML22 of the New Zealand Strategic Goods List

b) use of production or testing of analytical equipment and components in relation to the development or production referred to in a) or maintenance of military items

c) use of any unfinished products in a plant for the production of military items referred to in a)

NOTES

3 Legally binding agreements are binding on states that are party to the relevant Treaty/Convention.

4 Website of the 1540 Committee: http://www.un.org/en/sc/1540/

5 Stockholm International Peace Research Institute (SIPRI), 'Arms embargoes database' (https://www.sipri.org/databases/embargoes)

6 United Nations Security Council, 'Sanctions' (https://www.un.org/securitycouncil/sanctions/information)

7 Malaysia Ministry of International Trade and Industry (2016), 'Strategic Trade Act 2010: Intangible Technology Transfer (ITT) Guideline' (https://www.miti.gov.my/miti/resources/ITT_Guidelines_2016-Final.pdf). These guidelines are currently under revision, to be completed in 2019.

8 New Zealand Ministry of Foreign Affairs and Trade, 'Which goods are controlled?' (https://www.mfat.govt.nz/en/trade/trading-weapons-and-controlled-chemicals/which-goods-are-controlled/)

4

Methods to promote industry compliance

ICP requirements and guidance for industry and other relevant actors

Government expectations regarding industry ICPs vary. In some countries – for example, Germany (see page 23) – establishment of an ICP is mandatory; in others, guidance is provided, such as the guidelines issued by the Chinese Ministry of Commerce[9] and by the Malaysian Ministry of International Trade and Industry.[10] Other governments (including Switzerland)[11] provide indications of best practice in this field, while the UK has a Compliance Code of Practice.[12] Explicit guidelines set by government can help promote the adoption of ICPs by industry and other relevant actors and provide a standard against which the adequacy of industry programmes can be assessed. Some governments require companies and institutes to implement programmes to the required standard before they are eligible to apply for individual and/or bulk export licences.

Box 10: Examples of selected requirements for industry ICPs

In the **Philippines**[13] there are nine ICP elements recommended by the Strategic Trade Management Office:

1. Management commitment (a document signed by a senior officer of a company and provided to all relevant employees, stating the company's commitment to comply with the Strategic Trade Management Act – STMA).
2. ICP structure and responsibility (an internal organisational structure responsible for creating awareness of and developing systems and overseeing proper implementation for compliance must be established).
3. Screening procedures (product classification/identification, end-use and end-user screening, risk assessment).
4. Shipment control or technology control plan (verification and final check of documents, licences, and other requirements before shipment is made to prevent the diversion of strategic goods while in transit).
5. ICP training (all relevant employees must be trained on the STMA prior to having access to strategic items, software and technology, or prior to being involved in transactions related to the STMA).
6. Internal audit (audit conducted annually by the company to detect possible weaknesses in the company's ICP that lead or tend to lead to violations of the STMA).
7. ICP standard operating procedure (comprehensive, clear, and implementable manual that sets out the company's standard operating procedure for following the STMA).
8. Record-keeping (all persons engaged in any business involving STMA are required to keep secure records – both hard copy and electronic copy – for a period of ten years from the date of completion of the transactions).
9. Reports and corrective action (a mechanism for reporting violations of the STMA must be created by the company along with preventive measures and corrective actions to prevent recurrence).

Box 10 continued

In **Germany**[14] the 'Principles of the Federal Government for Evaluating the Reliability of Exporters of War Weapons and Arms-related Goods of 25 July 2001' require exporters to put in place adequate organisational and workflow structures to ensure compliance with STCs, including licensing requirements and record-keeping. A senior company representative must be designated Chief Export Control Officer and is personally responsible for transfers and exports, including signature of licence applications. The Officer plays an important role in organising export control within the company, is personally responsible for ensuring compliance with the legislation, and must make a declaration concerning the establishment of an ICP. Fulfilling these arrangements is key to the establishment of a company's reliability and its eligibility to apply for export/transfer licences; an on-site audit of the company's ICP provisions is undertaken before it can apply for bulk authorisations.

Box 11: ICPs for academic and research institutes: a summary of Pakistan's approach[15]

There is a growing need for export control professionals to be employed at universities and research institutes. This is due to increasing partnerships between institutions at home and abroad, the growing numbers of foreign students, advances in different kinds of technologies, the development of online courses and more. The growth in advanced technology and associated research involving dual-use goods applicable across different sectors – from IT to bio-technology and speciality materials – carries with it a stewardship responsibility. However, export compliance departments cannot eliminate all risks: all staff and students need to understand their strategic trade control obligations.

Box 11 continued

Best practice guidelines for research/academic institutions include:

- Assigning designated officials for export control matters, as well as a designated faculty member(s) as a research/foreign visitors' coordinator(s)
- Widely disseminated institutional compliance policies and procedures
- Setting up exclusive areas, with access control for research areas that fall under export controls
- Access control – securing computers/gadgets and documents containing sensitive information/data
- Training in export control matters
- Close liaison and coordination with the export control authority for guidance updates
- Compliance with proprietary rights and non-disclosure requirements
- Factoring in national export compliance requirements as part of contractual obligations for joint ventures/projects involving foreign nationals
- A requirement to not export any items or materials without consulting the institution's compliance officer, even at the request of a government sponsor
- Taking adequate precaution against 'deemed exports' (i.e. release of controlled technology or information to a foreign national located in Pakistan)
- Never agreeing to contract language that requires provision of indemnification for violations of the export regulations
- Seeking guidance before travelling to or undertaking research/projects in sanctioned/embargoed countries with denied persons
- Conducting periodic risk assessments
- Investing in the institution's website as a useful tool with contact details for questions/inquiries

Incentivising compliance and ICPs

Companies and institutes that take a positive approach to compliance and conduct due diligence in discharging their STC obligations are, in effect, assisting the government authorities by helping to reduce the burden of STC administration. In some countries, reliable industry entities are given particular 'trusted' status and can benefit from some or all of the following:

- access to licence or authorisation exemptions
- general/global/bulk licences or authorisations
- faster licence/authorisation processing times
- some documentary exemptions

Box 12: Examples of incentives for effective ICPs

In the **Republic of Korea**, under Article 25 of the Foreign Trade Act, the Minister of Trade, Industry and Energy may designate traders who have the capabilities prescribed by Presidential Decree – including the ability to identify strategic items and to assess the bona fides of importers and end-users – as 'self-compliance traders'. This provides an incentive for enterprises or research institutes to improve their capacity for self-regulation and to manage strategic items.

Article 7 of **China**'s 'Measures on the Administration of General Licensing for Export of Dual-Use Items and Technologies', issued by the Ministry of Commerce, stipulates the conditions to be met by the general licensing operators for the export of dual-use items and technologies. These conditions include the establishment by such operators of an internal export control mechanism for dual-use items and technologies. Article 10 of the regulations also provides that a general licence shall not be applicable if an enterprise has established a complete internal export control mechanism but cannot confirm its effective implementation. China's general licence system serves both as a trade facilitation mechanism and a means of encouraging enterprises to adopt a comprehensive and effective ICP.

Box 12 continued

In the **UK**, Her Majesty's Revenue and Customs uses the Authorized Economic Operator (AEO)[16] system – an internationally recognised quality mark indicating that a company's role in the international supply chain is secure, and that their customs controls and procedures are efficient and compliant. It is not mandatory, but it gives quicker access to certain simplified customs procedures and in some cases the right to 'fast track' shipments through some customs and safety and security procedures. While there is an export control compliance element to AEO, the focus is primarily on customs controls and procedures.

Information on enforcement of STCs

The potential consequences for industry and other relevant actors of failing to adhere to national and international laws and regulations relating to STCs, and the associated risks of reputational harm, should be fully explained. As part of this effort, governments may wish to share information on how STCs are enforced. At the basic level such information should include which agencies are responsible for enforcement of STCs and what their specific roles are. Other topics that could be addressed include:

- different types of non-compliance (e.g. technical/inadvertent breaches vs. deliberate violations)
- penalties that can apply to companies or institutes that are found guilty of non-compliance
- investigation and prosecution procedures (e.g. government writes to a company/institute notifying it of specific compliance concerns, and requests remedial action and/or invites them to attend an outreach event)
- case study examples of non-compliance

Governments should also share information on processes for voluntary disclosures, to encourage companies and institutes to inform relevant authorities at the earliest possible opportunity in cases where there appears to be a risk of STC violations and/or in cases where violations may have been committed. It may also be useful to highlight the different types of consequences that follow disclosure of non-compliance compared with situations where failures are instead discovered by government authorities.

Equally, the implications of a company having taken remedial action versus no action may also be of interest to company executives.

Box 13: Examples of STC enforcement awareness raising by government agencies

- Singapore Customs STC 'Enforcement' information
  https://www.customs.gov.sg/businesses/strategic-goods-control/overview/enforcement
- Hong Kong (Special Administrative Region) Trade and Industry Department STC 'Prosecutions' summary
  http://www.stc.tid.gov.hk/english/hksarsys/files/prosecution_statistics.pdf
- UK Department for International Trade/Export Control Joint Unit's 'Notice to Exporters' regarding an enforcement case
  https://www.gov.uk/government/publications/notice-to-exporters-201810-hmrc-prosecutes-company-for-unlicensed-exports/notice-to-exporters-201810-hmrc-prosecutes-company-for-unlicensed-exports
- U.S Department of Commerce, Bureau of Industry and Security, 'Don't Let This Happen to You' publication
  https://www.bis.doc.gov/index.php/documents/enforcement/1005-don-t-let-this-happen-to-you-1/file

NOTES

9 China Ministry of Commerce (MOFCOM) Announcement No. 69 of 2007 on directive guidance for establishing ICP by enterprises dealing with dual-use items and technologies (http://aqygzj.mofcom.gov.cn/article/zcgz/200709/20070905071676.shtml)

10 Malaysia Ministry of Trade and Industry ICP guidelines can be found via the Strategic Trade Act 2010 webpage: https://www.miti.gov.my/index.php/pages/view/sta2010?mid=105 → Resources → Guidelines.

11 Switzerland State Secretariat for Economic Affairs, 'Aide-mémoires et formulaires' (available in French, German and Italian) (https://www.seco.admin.ch/seco/fr/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/industrieprodukte--dual-use--und-besondere-militaerische-gueter/formulare-und-merkblaetter.html#accordion1551354757981)

12 UK Department for Business Innovation and Skills (2010), 'Export Control Organisation, Compliance Code of Practice', March (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/341998/10-668-codepractice-compliance.pdf)

13 Sacedon-Dimayacyac J (2017), 'Updates on the Philippines Strategic Trade Management Act', Philippines Strategic Trade Management Office, Department of Trade and Industry, presentation delivered at the 25th Asian Export Control Seminar, Tokyo, Japan (https://supportoffice.jp/outreach/2017/asian_ec/pdf/25AttyJaniceDimayacyacPhilippines.pdf)

14 German Federal Office for Economic Affairs and Export Control (BAFA) (2018), 'Internal Compliance Programmes – ICP, Company-internal export control systems' (http://www.bafa.de/SharedDocs/Downloads/DE/Aussenwirtschaft/afk_merkblatt_icp_en.pdf?__blob=publicationFile&v=3)

15 Pakistan Ministry of Foreign Affairs Strategic Export Control Division (SECDIV) (2014), 'Internal Compliance Programme (ICP) Guidelines', December (http://www.secdiv.gov.pk/uploads/ICP-Guidelines-db7d.pdf)

16 For further information on the World Customs Organization AEO scheme and its application, see World Customs Organization, 'Compendium of Authorized Economic Operator Programmes: 2018 edition' (http://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/aeo-compendium.aspx)

5

Strategies and mechanisms for government outreach on STCs

Governments need to **ensure that STC laws, regulations and procedures are 'visible'** to those who must comply with them, and that industry and other relevant actors have enough information on STCs so that they can avoid over-compliance – for example by applying for an export or other type of licence when it is unnecessary. Information on STCs should therefore be provided in simple and straightforward terms so that industry and other relevant actors can be helped to comply with the law in practical ways.

A starting point for governments is to **provide comprehensive, accessible and easily navigable online information** and support, including details of and updates to legislation, regulations, administrative procedures, and international sanctions. Governments should also establish an online system of licence or authorisation applications along with clear guidance, including for the use of individual and open licences, with conditions of use and relevant documentary, record-keeping and reporting requirements.

In addition to online resources, governments should seek to **undertake a range of practical outreach activities** to deliver in-person STC education and training to industry and other relevant actors involved in the international trade in strategic goods and technologies and/or the provision of technical assistance. Governments may choose to undertake these outreach activities directly – either from the central authority or via provincial offices or authorities. Possibilities to partner with industry groups, trade associations, and local chambers of commerce in the dissemination of information may also be explored, as could the possibility

of outsourcing some aspects of STC training to organisations and businesses with relevant expertise.

Governments need to ensure that they have allocated sufficient resources to cope with the demands of the licensing process as well as for conducting adequate outreach; governments should also be accessible and open with their clients – the exporters. Ideally, governments will employ a range of methods to ensure that relevant STC laws, regulations, and administrative procedures are readily accessible and understood by all concerned stakeholders.

Online resources

Governments should provide comprehensive and easily navigable online information and support as the starting point for outreach to industry on STCs. Ideally this should be designed with the needs of SMEs in mind and should take the form of a **'one-stop-shop' or 'single window'** through which all necessary resources and information can be accessed – from legislation, product classification and customer screening to customs and enforcement information. Given that such online provision can be relatively cost-effective and can have potentially unlimited reach, every effort should be made to ensure online information on STCs is as comprehensive and easily accessible as possible. Providing information in several languages – including English – would help ensure the widest possible understanding internationally of any national STC information posted online. Any in-person education and training (see 'In-person education and outreach opportunities' on page 35) must be supported by online information resources, which should include:

- **Details of relevant laws**, regulations, administrative procedures and penalties for violations, along with explanatory notes (see for example information provided by the governments of Canada,[17] China,[18] Korea,[19] Malaysia,[20] the Philippines,[21] Singapore,[22] Switzerland,[23] the UK[24] and the US[25]). Governments may consider including some information or references relating to STCs that operate in other jurisdictions and, in particular, in countries that are key trading partners.
- **Details of relevant international agreements and standards** relating to STCs (see 'Information provided as part of government outreach on STCs' on page 9).

- **Regular email updates** to subscribers regarding new developments in applicable legislation, regulations, and international standards.
- **Control lists for strategic goods and technologies** – both military and dual-use – including guidance (see 'Control lists' on page 11), commodity classification tools, and published results of official classifications conducted by licensing agencies.

Box 14: Assistance for commodity classification

- Australian Online DSGL Tool
  https://dsgl.defence.gov.au/Pages/Home.aspx
- China provides export consulting services to enterprises that are unsure as to whether their items are subject to control; enquiries about these and other STC-related matters can be made through a facility on the Ministry of Commerce website
  https://gzlynew.mofcom.gov.cn/gzlynew/servlet/SearchServlet?OP=searchEgovText&siteid=egov&id=27
- Korea YesTrade 'Self-Classification' tool for goods and technology search by Harmonized System Korea
  https://yestrade.go.kr/common/common.do?jPath=/ja/jasj042C&judStep=01
- Malaysia Ministry of International Trade and Industry 'Strategic Items Finder'
  https://www.miti.gov.my/index.php/sti/sti_finder
- UK Goods Checker
  https://www.ecochecker.trade.gov.uk/spirefox5live/fox/spire/

- **Guidance as to special types of issues and controls** (e.g. the catch-all, intangible technology and technical assistance transfers, implications of cloud-based storage solutions, and encryption technology controls) (see 'Awareness and consideration of specialised STC provisions' on page 70).
- **An outline of the national export control system**, departmental competencies, and points of contact.
- **An online licensing/authorisation application process and tracking system** (including, for example, provision for registration of prospective exporters, guidance on how to fill out relevant forms such as licence applications, customs declarations including details of documentation requirements, and information on processing times).

Box 15: Online licence/authorisation application facilities

- Malaysia eSTA Permit Application site
  https://newsta.dagangnet.com.my/esta/login/login_notice.html
- Singapore Customs guidance on 'TradeNet Permit Applications'
  https://www.customs.gov.sg/-/media/cus/files/business/strategic-goods-control/tn4-1proceduresforstspermits.pdf
- China Ministry of Commerce (MOFCOM) guidance page on applying for dual-use export and import licences
  http://exctrl.mofcom.gov.cn/ (in simplified Chinese only)
- Australia Defence Export Controls 'Application to Export or Supply Controlled Goods or Technology'
  http://www.defence.gov.au/ExportControls/FormExport.asp

- **Details of types of licences/authorisations available** (including for export, import, transit/transhipment, trade/brokering and transportation of strategic goods and technologies).
- **Clear requirements for use of open licences, record-keeping, and reporting**.

Box 16: Provisions for reporting – UK Export Control Order 2008[26] (excerpt)

29.—(1) A person who—

(a) acts under the authority of a general licence granted by the Secretary of State; or

(b) acts under the authority of the Community General Export Authorisation whilst established in the United Kingdom

shall keep detailed registers or records.

Box 16 continued

(2) The registers or records shall contain sufficient detail as may be necessary to allow the following information, where appropriate, to be identified in relation to each act carried out under the authority referred to in paragraph (1)—

(a) a description of the act;

(b) a description of the goods, software or technology to which the act relates;

(c) the date of the act or the dates between which the act took place;

(d) the quantity of the goods (if any) to which the act relates;

(e) the name and address of the person referred to in paragraph (1);

(f) the name and address of any consignee of the goods to which the act relates or any recipient of the software or technology to which the act relates;

(g) in so far as it is known to the person referred to in paragraph (1), the name and address of the end-user of the goods, software or technology to which the act relates;

(h) if different from the person referred to in paragraph (1), the name and address of the supplier of the goods (if any) to which the act relates;

(i) any further information required by the licence or authorisation referred to in paragraph (1).

(3) The registers or records referred to in paragraph (1) shall be kept—

(a) in the case of a general licence authorising an activity that would otherwise be prohibited by Part 4 of this Order, for at least four years from the end of the calendar year in which the authorised act took place;

(b) in any other case, for at least three years from the end of the calendar year in which the authorised act took place

or for such longer period as may be specified in the licence or authorisation referred to in paragraph (1).

- **Information on how to assess the risks associated with a prospective international transfer of strategic goods**; for example, 'know your customer', 'red flags', proliferation risks, and how supply chains can contribute to WMD proliferation (see 'Understanding how to screen for proliferation risks' on page 62).
- **Details of online restricted party screening tools** – whether of government or private sector origin – which can help industry and other relevant actors to ensure there is a level of due diligence in their screening of all parties to a transaction (see 'Understanding how to screen for proliferation risks' on page 62). Such restricted party screening tools allow checking of, *inter alia*, suppliers, financial and transportation agents and customers against lists of proscribed actors that have been compiled by governments and international organisations.

Box 17: Examples of online restricted party screening tools (government origin)

- U.S Export Control and Related Border Security 'Restricted Party Screening Tool'
  http://www.restrictedpartiesscreeningtool.com/
- Korea Ministry of Trade, Industry and Energy 'Denial List'
  https://yestrade.go.kr/common/common.do?jPath=/ja/jaEa081C&MENUCD=ED&TOP_MENU_CODE=MENU0002&CURRENT_MENU_CODE=MENU0055&CURRENT_MENU_CODE=MENU0055&TOP_MENU_CODE=undefined
- 'Consolidated List of Financial Sanctions Targets in the UK'
  https://hmt-sanctions.s3.amazonaws.com/sanctionsconlist.htm
- Australia Department of Foreign Affairs and Trade 'Online Sanctions Administration System'
  https://dfat.gov.au/international-relations/security/sanctions/Pages/online-sanctions-administration-system.aspx

Examples of online restricted party screening tools (private sector origin)

- AEB Compliance Screening
  https://www.aeb.com/sg-en/products/compliance-screening.php
- Amber Road Restricted Party Screening
  https://www.amberroad.com/solutions/export-management/restricted-party-screening
- Dow Jones 'Risk and Compliance' Third Party Screening Tool
  https://www.dowjones.com/products/risk-compliance/

- **Information on relevant opportunities to receive education and training on STCs** – both web-based ('webinars') and in-person activities (see below).
- **Online magazines** outlining relevant political, industrial, and technological developments and their impact in relation to STCs.
- **Enforcement-related information**, including customs controls and penalties for non-compliance with STC laws, plus guidance on when and how to report a suspicious enquiry or potential STC violation.
- **Information on how to register with relevant authorities** as an entity concerned with the international trade in strategic goods/technologies, including **contact details** for relevant government ministries, departments and agencies.

In-person education and outreach opportunities

Person-to-person interactions are an important part of efforts to ensure that STCs are fully understood by and are relevant to the needs of industry and other relevant actors and, in particular, SMEs. In addition to providing direct education, these forms of interaction **allow people to address specific questions and help elicit useful feedback**, for example on the need for STC reform or on the utility of proposed new regulations.

Regular STC **outreach and compliance seminars and workshops** are an important tool. With a particular emphasis on reaching out to SMEs, such events would ideally be held at multiple locations during the course of a year and should focus on the full spectrum of STC issues. They should be **conducted by government (central and/or provincial) and non-government experts** to ensure maximum relevance and effectiveness. Key features may include:

- **pitching at different levels of knowledge/expertise** – from beginner (basic information) to more advanced (updates and latest developments)
- **targeting a range of relevant individuals**, including sales and marketing executives and engineers, as well as those who are involved in STC compliance
- **focusing on laws, regulations, and procedures** emanating from controls established at the national level, in multilateral organisations, and by the UN – governments may also consider including information relating to the STCs that operate in other jurisdictions and, in particular, in countries that are key trading partners

- **focusing on general STC principles and provisions** (e.g. control lists and commodity classification)
- **focusing on specialised issues and controls** (e.g. the catch-all, intangible technology and technical assistance transfers, implications of cloud-based storage solutions and encryption technology controls)
- **focusing on practical issues** (e.g. how to apply for export authorisation and access online resources)
- **focusing on assessing risks** associated with prospective international transfers of strategic goods (e.g. 'know your customer', 'red flags', proliferation risks, and how supply chains can contribute to WMD proliferation)
- **specific outreach to particular sectors** by experts in those particular industries and/or representatives of specific trade associations (e.g. aerospace, agriculture, chemicals, nuclear, oil and gas and pharmaceuticals) or to different types of actors (e.g. manufacturers, brokers, shipping companies, financial institutions, academia, and research institutes)
- **soliciting feedback** from industry and other related actors on the effectiveness or otherwise of export licensing systems and/or proposed legislative/regulatory changes
- **key messages** that will resonate with the audience, such as the patriotic value of adhering to national export controls, and the importance of early disclosure of potential compliance problems to enable prompt remedial action to be taken and to reduce the risk of severe penalties

Box 18: Examples of government-led education and training activities

Government/industry outreach, Philippines Strategic Trade Management Office 2017–2018[27]

Period Covered	Title	Venue
January 2017	Outreach Programme for HGST Philippines Corporation	Laguna Technopark
	Outreach Programme for Moog Controls Corporation	Baguio City
	Outreach Programme for Texas Instruments	Pampanga
February 2017	Outreach Programme for Toshiba Philippines	Laguna Technopark
	Outreach Programme for Ibiden Philippines and Philippine Economic Zone Authority (PEZA) Batangas Locators	Batangas
March 2017	Outreach Programme conducted during the Export Control Workshop in Cebu City	Cebu, Philippines
June 2017	Outreach Programme during the Strategic Trade Management Act Implementing Rules and Regulations Public Consultation	Malacañang, Manila
	Outreach Programme during the Philippine Semiconductor and Electronics Conference and Exhibit 2017	Pasay City
July 2017	Outreach Programme during the Philippine Export Competitiveness Programme	Makati City
	Outreach Programme for Amkor Technology	Parañaque City
	Outreach Programme during the Philippine Export Competitiveness Programme	Cebu City
August 2017	Outreach Programme for Maxim Integrated Philippines	Cavite
	Outreach Programme for Analog Devices	Cavite

Box 18 continued

Period Covered	Title	Venue
October 2017	Outreach Programme for the Philippine Economic Zone Authority (PEZA) Officers and Staff	Taguig City
	Outreach Programme for Infineon Technologies	Makati City
January 2018	Outreach Programme for STMicroelectronics Inc.	Laguna
May 2018	Outreach Programme during the Korean Industry Day in the Philippines	Shangri-La at the Fort
	Outreach Programme for Officials of the Department of Science and Technology	Manila
July 2018	Outreach Programme for the Agents of the Bureau of Customs	Port Area, Manila
August 2018	Strategic Trade Outreach Programme for Government Agencies	Diamond Hotel, Manila
	Outreach Programme during the Strategic Trade Industry Day	Diamond Hotel, Manila
September 2018	Outreach Programme during the 3rd Asian Defense, Security & Crisis Management Exhibition & Conference	World Trade Center Roxas Boulevard Manila
October 2018	Outreach Programme during the 2018 Global Logistics Conference	Manila
November 2018	Outreach Programme for the Department of Transportation	Manila
	Outreach Programme for PEZA locators in Cavite	Cavite

Box 18 continued

Period Covered	Title	Venue
December 2018	Outreach Programme for Samahan sa Pilipinas ng Industriya ng Kimika	Manila
	Outreach Programme for the Association of Semiconductor and Electronics Logistics Managers	Manila
	Outreach Programme during the National Export Congress	Pasay City
	Outreach Programme for PEZA locators in Baguio	Baguio City
	Outreach Programme for PEZA locators in Central Luzon Economic Zone	Cavite

Box 19: Examples of UK export control training events[28] (excerpt)

Beginners Workshop

Duration: Half-day
Pre-course Knowledge: None
Description: A general introduction to export controls if you are new to the subject.

Topics covered will include:

- Why have controls?
- What's controlled?
- What is meant by "technology" and how it may affect you
- Types of export licences
- Compliance and enforcement

After the workshop, you will be sent a short assessment module* to test your learning, before being awarded a certificate of achievement. The assessment module, delivered by Cranfield University, will be in the form of an online quiz with multiple-choice answers.

If this course is the first step in the Learning Path, it is recommended that attendees use their new knowledge to assess how Export Controls apply at their place of work before attending further training. This course can also be used to provide general awareness of Export Controls.

Box 19 continued

Licences Workshop

Duration: Half-day

Pre-course Knowledge: You will have some experience of making licence applications (if relevant) and undertaken prior training from the Learning Path.

Description: This Workshop aimed at improving the permissions exporters obtain to export, reducing the number of licences required and improving compliance.

With the wealth of Export Control Licences available to UK exporters, finding the right one to enable your company to export efficiently can be daunting. Based on course feedback, input from the SPIRE replacement program (LITE), and our Compliance Unit, this course is a development of our 'Making Better Licence Applications' workshop and aimed at guiding exporters through the licence types available; deciding which one is right for your export.

Attendees will first be taken through the core Standard and Individual Export Licence (SIEL) application screens to demonstrate how prior planning can reduce the number of 'Requests For Information' (RFIs), reduced work and quantity of licences required. The course will then turn to Open General Licences (OGLs and EU GEAs); covering what is available, online resources and how to read OGLs to improve compliance with the terms and conditions.

There will then be exercises to put the theory into practice. Please therefore feel free to put in your application an OGL you would like us to consider for review or prepare to discuss an issue you've had with Standard or Open Licences, and we will endeavour to use relevant examples.

Control list classification and using the checker tools

Duration: Full-day

Pre-course Knowledge: You will have some knowledge or experience of the classification (rating) process. We recommend the beginners workshop or intermediate seminar first.

Description: A course to provide guidance on identifying the control list entries that apply to your goods software and technology.

Workshops will concentrate on classifying military and dual-use goods.

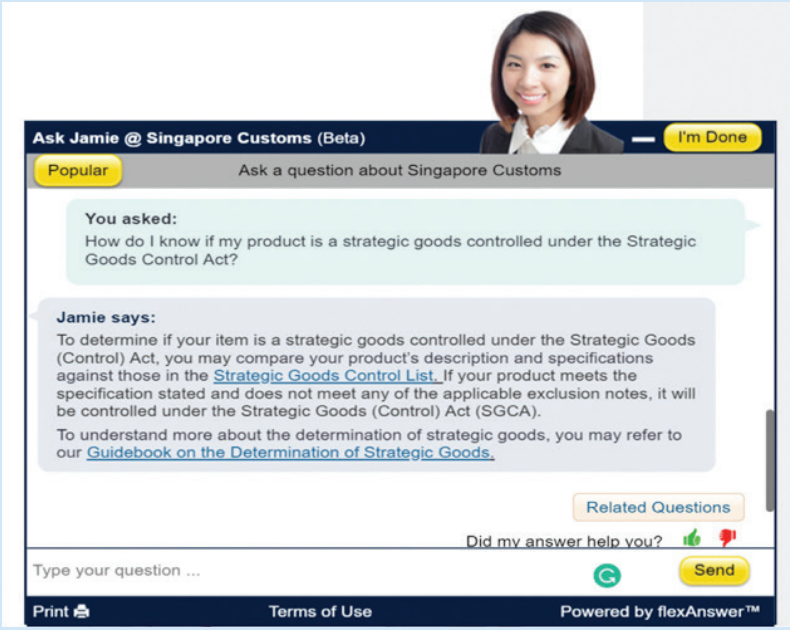
Outline:

- Export control lists – where they come from, including relevant legislation
- Military goods and dual-use goods – how to find them on the relevant list
- How to understand the terms and language used in control list entries
- Basic classification exercises – some general examples
- Software and technology controls
- Classification exercises using the Goods Checker tool
- Introduction to the OGEL (Open General Export Licence) Checker

Other person-to-person opportunities for government authorities to conduct STC training and outreach and provide direct assistance to exporters may include:

- **providing hands-on expert assistance with commodity classification** and other technical questions by personnel with detailed technical knowledge of particular industries
- **telephone and email 'helplines' and web-based interactive platforms** providing advice in response to specific STC questions

Box 20: Singapore customs 'Ask Jamie' online automated help-desk[29]



- **organising teleconferences** between licensing officers and industry representatives to address specific STC-related questions or issues
- **supporting town hall/chamber of commerce meetings** at different locations so that training and outreach can be provided to companies in different geographical locations
- sending delegations of STC licensing and enforcement officials to **conferences and trade events** to engage with participants and ensure that trade promotion activities are linked closely to STCs
- **one-to-one meetings and on-site training** of company personnel at their offices by licensing officials and technical experts

Central to the effectiveness of these approaches will be the **building of personal relationships** between individuals in relevant government agencies and those responsible for STC compliance in industry and other relevant actors. Government actors who invest in personal relationships and one-to-one interactions and who view outreach as a means of encouraging and supporting STC compliance are likely to find their audience to be more open and receptive to their messaging.

Collaborating on STC outreach with trade, industry, academic, private, public and international organisations

STC outreach workshops and seminars can be organised in **partnership with industry associations** that can help to publicise planned events, or with international organisations involved in non-proliferation activities. In addition, training can be **outsourced to strategic trade institutes and independent non-profit or consultancy organisations** with appropriate expertise.

Every effort should be made to ensure that **training is conducted in an interesting and engaging manner** with a balanced focus between incentives for compliance and penalties for violations. The ultimate aim should be for participants to understand how STCs affect their business and what steps they need to take to comply with regulations. Participants should also understand how STCs prevent illicit proliferation of WMD-related goods and technologies as well as conventional arms and other strategic goods and technologies – and that it is in their own interest to comply with STCs.

Box 21: Outreach by the Swedish Export Control Society[30]

The Swedish Export Control Society was established in 1994 on the initiative of industry. The purpose was to support company export control administrators/managers responsible for adherence to a variety of related laws and regulations (e.g. Swedish, EU and US export control legislation). Its members deal with export control issues in companies, organisations or authorities. The Society arranges in-depth training, with written exams leading to a qualification as a Certified Export Control Manager.

Since 2006 the Swedish Export Control Society has carried out both a broad and in-depth education programme on Swedish and international export control of strategic products, both in theory and practice. While aimed at industry, other interested parties – including specialist STC consultancies – also participate in this training. The education programme is developed in collaboration with the Inspectorate of Strategic Products. The programme consists of four modules covering a range of topics, including international sanctions and the catch-all. Each module is completed with a test. Anyone who achieves approved results on all four parts will achieve the status of a Certified Export Control Manager. Swedish government authorities are always present at the training and materials are updated each time. The Society also arranges an annual event, the Swedish Update – a two-day seminar where export control managers from all over Scandinavia meet.

Box 22: Joint government/International Atomic Energy Agency outreach on proliferation risks and trade controls[31]

The International Atomic Energy Agency (IAEA) has a mandate under the Nuclear Non-Proliferation Treaty to verify that nuclear material and activities are used only for peaceful purposes in non-nuclear weapon states. While this mandate is largely fulfilled through inspections and analysis of nuclear material and facilities declared by states, the IAEA also needs to collect and analyse information indicating undeclared nuclear material or activities that states might have omitted from their declarations. For more than a decade, the IAEA Procurement Outreach Programme has been collecting such indicators. It is a joint government/IAEA outreach to industry to raise awareness about proliferation risks and strategic trade controls, and to ask for voluntary information of relevance to the IAEA mandate, in the form of unfulfilled procurement requests for products that could be used in nuclear activities. All IAEA Member States are invited to cooperate and assist in this area.

The IAEA Procurement Outreach Programme is contingent on the voluntary involvement of member states. A broad range of nuclear-related products (single-use, dual-use, and catch-all-relevant) are identified that could be of interest to someone wishing to develop a covert nuclear programme. Efforts are then made – together with the cooperating government – to identify companies that could supply these products and which therefore might be approached by proliferators. During the joint outreach visits, the IAEA and national authorities inform the companies about the global and national non-proliferation systems, including the national export licence requirements and how to identify enquiries for products that might be intended for covert nuclear activities. Companies often feel encouraged and motivated when realising that they have something to contribute to global non-proliferation efforts.

Box 23: Examples of STC services provided by an external actor (Korean Security Agency of Trade and Industry):

- Support for enterprises during the export licensing process, including the development of accessible templates, guidance and documentation; providing consultation services during the licence application process; and review of licence applications prior to submission.
- Providing help with end-user checks, including sanctions, embargoes, denied persons, and watch list screening.
- Technical assistance for commodity classification, including using technical information to facilitate classification of goods and technologies, and providing advice on applicable STC licensing requirements.
- Support to enterprises seeking a compliance programme certificate (AEO status).
- Detailed technical information provided to enterprises in respect of the properties and uses of strategic goods and technologies, including via exhibitions, magazines, and training.
- Soliciting feedback from enterprises on the export licensing process and advising government on the review and amending of laws and regulations.
- Hosting STC seminars and conferences and providing newsletters and timely electronic distribution of STC updates – including information on developments specific to Korea and other countries.
- Providing information and training on compliance programme development, including guidance, seminars, workshops, consultations, and mentoring programmes.

Compliance visits

Governments can also support adherence to STCs among entities concerned with the export or transfer of strategic goods, technologies and services, by undertaking **company/institutional audits and compliance visits**. Such visits may take place within a set period of time after a company or institute has registered with STC authorities and/or applied for an export licence. They are usually conducted by government STC officials or licensing officers, but may also include officials from other relevant agencies or departments – such as customs or the defence ministry. Beyond ensuring that companies – including everyone from senior managers to engineering, sales, and finance officers – are fully cognisant of their STC responsibilities, such visits allow government to **check that relevant actors are complying with the terms of any licences** or authorisations they have received, are **fulfilling any obligations to keep records** relating to relevant export activities, and are not being taken advantage of by unscrupulous actors.

Industry is often cited as being 'the first line of defence' against illicit proliferation of sensitive goods and technologies. **Compliance visits and audits can help identify shortcomings in companies' ICPs** and enable solutions to be advanced so that they are more effective in identifying risky transactions. They can also yield information on the procurement activities of suspicious entities and can facilitate detection and prevention of potential violations before they happen. Typically such visits fall into two categories:

- **Proactive visits** – where no violations are suspected. These can involve routine visits, for example to check on a company's compliance with general or global licences; they could also take place at the invitation of a company/institution.
- **Reactive visits** – where violations or suspicious activities are suspected.

If a compliance visit uncovers issues of concern, recommendations may be made for the improvement of a company's ICP and a follow-up visit arranged for an appropriate interval thereafter; company/institute personnel can also be asked to attend future STC outreach events.

Compliance visits can be sensitive and, if not handled correctly, can produce poor results.

It is important that during such visits compliance officers take care to put people at ease and, where possible, treat each visit as a friendly, information-gathering exercise that aims to provide relevant assistance. This will help to build a constructive relationship and encourage honesty and **early disclosure of any compliance problems**. Such an approach is more likely to secure cooperation in identifying and responding to suspicious purchase requests; it can also provide useful information to government on new and emerging threats to STC and non-proliferation.

Box 24: Compliance assessment – some key features

- Company/institute transactions that have taken place over a specified time frame should be examined and an honest appraisal of compliance conducted.
- Self-reporting of potential problems on the part of the company/institute in question should be encouraged.
- When disclosing problems, companies/institutes should explain how they will amend their procedures to ensure that the reported non-compliance does not reoccur.
- The consequences of STC violations should be clear; if a violation is found, action should be taken against the company/institute and the violation should be publicised as this will have an important deterrent effect.
- Sanctions can take a number of forms but must be proportionate; some governments will give a written warning for administrative violations, while fines and custodial sentences are also possibilities for criminal acts.
- Companies/institutes that are found to have committed STC violations should be subject to increased scrutiny thereafter.
- Most company/institute non-compliance is not an intentional act to subvert controls but is the result of having insufficient compliance staff or failing to conduct an audit on a regular basis.

NOTES

17 Global Affairs Canada (2017), 'Export Controls Handbook', August (http://www.international.gc.ca/controls-controles/export-exportation/TOC-exp_ctr_handbook-manuel_ctr_exp.aspx?lang=eng)

18 The information portal of the Bureau of Industry, Security, Import and Export Control of the Ministry of Commerce of China, with information on the legal framework of STCs in China (http://aqygzj.mofcom.gov.cn/article/zcgz/)

19 Republic of Korea Ministry of Trade, Industry and Energy, 'Yestrade', online platform for management of strategic goods (https://www.yestrade.go.kr/user/main.do?method=main)

20 Malaysia Ministry of Trade and Industry, 'Strategic Trade Act 2010' (https://www.miti.gov.my/index.php/pages/view/sta2010?mid=105https://www.miti.gov.my/)

21 Philippines Department of Trade and Industry, 'Strategic Trade Management Act 2015' (http://www.officialgazette.gov.ph/2015/11/13/republic-act-no-10697/)

22 Singapore Customs, 'Legislation' (https://www.customs.gov.sg/businesses/strategic-goods-control/overview/legislation)

23 Swiss State Secretariat for Economic Affairs, 'Export controls of industrial products (dual-use) and specific military goods: Legal basis', unofficial English translation (https://www.seco.admin.ch/seco/en/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/industrieprodukte--dual-use--und-besondere-militaerische-gueter/rechtliche-grundlagen-und-gueterlisten--anhaenge-.html); Swiss legislation on arms export controls and related policies (weapons of war), French language (https://www.seco.admin.ch/seco/fr/home/Aussenwirtschaftspolitik_Wirtschaftliche_Zusammenarbeit/Wirtschaftsbeziehungen/exportkontrollen-und-sanktionen/ruestungskontrolle-und-ruestungskontrollpolitik--bwrp-/rechtliche-grundlagen.html)

24 UK Government legislation search engine: http://www.legislation.gov.uk/all?title=Export%20Control

25 U.S Department of Commerce, Bureau of Industry and Security → Regulations: https://www.bis.doc.gov/

26 UK Government legislation search engine → Export Control Act 2008: http://www.legislation.gov.uk/uksi/2008/3231/contents/made

27 Information reproduced with kind permission of the Philippines Strategic Trade Management Office.

28 UK Government Guidance, 'Export Control Training Bulletin' (https://www.gov.uk/government/publications/export-control-training-bulletin)

29 Singapore Customs website, interactive service 'Ask Jamie' on homepage: https://www.customs.gov.sg/

30 Swedish Export Control Society website: http://www.exportkontrollforeningen.se/this-is-the-swedish-export-control-society/

31 International Atomic Energy Agency website: https://www.iaea.org/ (For more information, contact outreach@iaea.org).

6

Ensuring internal government coordination on STC and industry outreach

Government outreach to industry and other relevant actors on STCs should be a partnership exercise involving central government departments and agencies and local authorities, as appropriate. Effective internal government coordination is therefore required. This should **ensure that all relevant departments/agencies have a clear understanding of laws and regulations** relating to STCs operating within their jurisdiction, as well as knowledge of how STCs relate to their own particular area of work. This may require internal government outreach initiatives on the part of the competent authority responsible for STCs. Such efforts will help **ensure a comprehensive and joined-up approach to industry outreach on STCs** and should also help avoid duplication of effort or conflicting messages; it may also provide a platform for combined interagency outreach involving, for example, export licensing and customs authorities.

Effective coordination should include:

- clear lines of responsibility and accountability
- coordination between departments/agencies responsible for the implementation of STCs and those responsible for outreach (if different)
- a shared strategic plan for outreach efforts
- possibilities for combined interagency outreach

Box 25: Examples of government coordination initiatives on STCs

U.S Export Enforcement Coordination Center (E2C2)[32]

E2C2 serves as a conduit between federal law enforcement agencies and the intelligence community, and it is the primary point of contact for enforcement authorities and agencies engaged in export licensing, public outreach, and government-wide statistical tracking. Through these efforts, E2C2 promotes a more robust whole-of-government approach to enforcement that ensures interagency coordination, promotes multi-agency collaboration, minimises the duplication of efforts, and strengthens the links between law enforcement, the intelligence community, and export licensing entities.

Pakistan's intra-government coordination on STCs

In Pakistan the export control administration – the Strategic Export Control Division (SECDIV) – is the hub for STC coordination between central government and provincial authorities. SECDIV also acts as a focal point for outreach and capacity building on STCs. The current approach to synergising outreach and capacity-building includes:

- joint visits with the National Authority, the Chemical Weapons Convention agency, the Pakistan Nuclear Regulatory Authority, and customs
- outreach sessions for industry in chambers of commerce and industry and associations
- joint awareness-raising seminars with the National Authority, the Chemical Weapons Convention agency, the Ministry of Defence Procurement, think tanks, and the Higher Education Commission
- joint publications with think tanks for awareness raising on Pakistan's strategic exports
- control system
- a SECDIV information desk established at the product display hall of the Defence Export Promotion Organization for awareness raising

All government departments and agencies concerned with STC have their own point of contact in order to ensure consistency of coordination efforts.

32 Export Enforcement Coordination Center (E2C2) website: https://2016.export.gov/e2c2/index.asp

PART B

Elements of industry internal compliance programmes

1 Introduction

Promoting and encouraging compliance with Strategic Trade Controls (STCs) on the part of industry and other relevant actors[33] is a key challenge for international efforts to prevent the proliferation of sensitive military and dual-use technologies to countries and entities of concern. As the **'first line of defence'** against the illicit trade in strategic goods, an understanding of proliferation risks among industry and other relevant actors, and a willingness to report suspicious activity, is vital.

In some countries it is mandatory for industry and other relevant actors concerned with the export or international trade in strategic goods and technologies to have a functioning internal compliance programme (ICP) – a system that helps companies to comply with applicable STC laws and which institutionalises the commitment to do so. Even in countries where an ICP is not a mandatory requirement, it is not uncommon for industry and other relevant actors to develop and maintain an ICP.

If a company/institute that exports strategic goods and/or technologies does not have an ICP, it could be at greater risk of violating STCs and possibly international sanctions; contributing to the proliferation of weapons of mass destruction (WMD), conventional arms and other strategic goods and technologies; and potentially facing civil or even criminal penalties. Accordingly, governments may focus more attention and resources on identifying and reaching out to such companies/institutes and raising awareness of STC obligations and how they should be fulfilled.

The establishment and maintenance of an **ICP should serve as a mechanism that fosters cooperation between the public and private sectors** and furthers mutual goals of complying with export control regulations, improving the quality of such compliance, and reducing the risk of STC violations among 'trusted traders'. In addition, companies/institutes that adopt STC compliance measures can be

incentivised by the knowledge that they are helping to strengthen efforts to prevent the illicit proliferation of sensitive goods and technologies and thereby contributing to national and international security.[34]

It is intended that while this part of the manual can be useful to all entities whose activities are impacted by STCs – including the manufacturing industry, international brokers and transportation agents, and academic and research institutes (for a more comprehensive list see 'Identifying relevant actors' on page 5) – it is likely to have greatest relevance for small and medium-sized enterprises (SMEs) that require support in the establishment or development of STC compliance systems. It is, nevertheless, possible that the smallest enterprises may struggle to establish and maintain a fully-fledged ICP, and so the emphasis should be on companies and institutes developing systems and processes that are commensurate with their particular circumstances. At the most basic level it is vital that senior officials within relevant organisations are fully cognisant of their STC obligations and how to fulfil them and that they ensure that screening procedures are undertaken effectively and comprehensive records are kept (see 'Key elements of an ICP' on page 61).

NOTES

33 For the purposes of this manual, 'industry and other relevant actors' is an umbrella term intended to capture all entities involved in the export and/or international trade in strategic goods and technologies. This includes, but is not limited to: manufacturers; distributers; brokering agents; transportation and shipping companies and agents; research, development and production companies; universities and other academic research institutions; and financial actors including banks, investment and insurance companies.

34 A number of international organisations, national governments, and non-governmental organisations have prepared and published information and resources to help those that need to comply with STCs in one or more jurisdictions and to provide assistance in the development of ICPs. Two such resources are:

- The U.S. Export Control and Related Border Security (EXBS) Program's 'Internal Compliance Program Guide' website (http://icpguidelines.com/), which contains a very robust set of ICP informational materials and ICP implementation tools, including ICP preparation templates, freely available product classification and party screening tools, and detailed explanations of each ICP element.
- Stockholm International Peace Research Institute's (SIPRI) publications on internal compliance, which can be accessed via the SIPRI website's publications page (https://www.sipri.org/publications). SIPRI's publications include specialised ICP guidance for different industry sectors, including defence and aerospace, IT and communications, nuclear, transport, and research and academia.

2

Why have an ICP?

Industry and other relevant actors involved in the international trade in strategic goods and technologies should be aware of their **responsibilities in relation to STCs** and how they should be fulfilled, including in respect of:

- goods and technologies that require export/transfer authorisation
- how to identify potential proliferation risks
- how to apply for export or transfer authorisation
- how to fulfil the necessary documentary requirements
- the maintenance of adequate records

In order to comply with their STC obligations, larger companies should establish an **ICP as the most efficient and effective way of systematising export control compliance**. For multinational corporations (MNCs) that operate across multiple jurisdictions, an ICP should facilitate STC compliance in each national context from or through which they are exporting or transferring strategic goods, technologies, and/or technical assistance. Given the risks of reputational damage, innate proliferation risks, and the potential negative impact on trade that can arise from STC violations in multiple jurisdictions, the development of an ICP is an essential element of many MNCs' business strategies and a justified case for investment.

Among SMEs the adoption of an ICP is less common. The reasons for this include:

- lack of awareness that the goods, technologies, and/or services they export/transfer are subject to STCs
- lack of understanding of or regard for the essential need for STCs in general and/or in the jurisdiction in which they operate

- lack of awareness of the potential implications of goods, technologies, and/or services entering into the possession of undesirable customers
- lack of support/advice from relevant governments to assist the uptake of an ICP
- lack of resources to allocate to the development and maintenance of an ICP
- belief that the costs of developing and maintaining an ICP would outweigh the benefits

While there is no universal system that can apply to all companies and institutions in all situations, there are certain **key elements that can provide the basis for STC compliance**. At a minimum, these elements include:

- senior management commitment to, and accountability for, STC compliance
- organisational structure and responsibilities for STC
- organisational policies and procedures relating to STC
- transaction screening processes
- training of all relevant staff in STC compliance
- adequate systems for record-keeping so that compliance can be demonstrated to the relevant authorities
- auditing and internal review
- reporting and corrective action

In addition, if a company/institute wishes to enter into **business partnerships abroad**, they will need to ensure that they understand and can comply with the STCs that apply in other contexts.

Box 26: Examples of costs and benefits of an ICP

Costs/implementation requirements of an ICP

- Requires investment in establishing systems and training
- Necessitates commitment from senior management
- Requires continual investment (time and resources) to ensure that systems and training are kept up to date
- Moves some of the burden of STC implementation from government to industry
- Does not guarantee that STC violations will not occur
- Reliance on self-regulation with increased administrative burden if using bulk permits

Benefits of an ICP

- Enhances understanding of and compliance with STCs
- Helps address weaknesses in company practices, reducing the likelihood of inadvertent or negligent STC violations – saving time and money
- Facilitates partnership on STCs between industry/other relevant actors and government by increasing industry awareness and reporting of suspicious requests from potential customers
- Can be a precondition for or can enhance possibilities of obtaining bulk permits, and can allow for fast-track licence review or enable expedited customs clearance in some jurisdictions
- Can facilitate the establishment of internal accounting and record-keeping processes that are necessary if using bulk licences/authorisations
- Safeguards company/institute personnel against the consequences of STC violation
- Being seen as a responsible company/institute that self-regulates and works in the national interest can be good for business

In some jurisdictions, companies cannot use general licences[35] or apply for bulk licences/authorisations unless they have an adequate and fully functioning ICP. Even where an ICP is not a prerequisite for obtaining bulk licences/authorisations, companies/institutes obtaining such permits will usually be required to **maintain records** – for example, of relevant shipments – and to **submit to regular audits** of their export activities to ensure compliance with the terms and conditions of the permits received. This may necessitate the establishment of the types of systems and processes that are, in effect, the foundation of an ICP.

NOTES

35 General licences or authorisations allow multiple shipments of less sensitive technology, often to a range of different end-users, where certain specified conditions are met. Entities are usually required to register with the competent national authority before using such licences.

3 Culture of compliance and due diligence

If a company/institute is to adhere to its STC obligations, it must develop and foster a culture of compliance. This is **an organisation-wide ethos** that begins with the most senior management, encompassing all employees at all levels and in all departments, and is based on a shared understanding of the importance of complying with STCs in all jurisdictions and contexts. A culture of STC compliance within an organisation will, in most cases, be matched by a similar ethos in respect of compliance with laws and regulations in other areas – for example, taxation.

Progress towards prioritising STC compliance and embedding a culture of compliance throughout a company will require *inter alia*:

- the identification of one or more individuals who have **special operational responsibility for STC compliance**, including engagement with licensing and enforcement authorities, potentially within a dedicated unit
- oversight of, and accountability for, the ICP to be given to **at least one senior company executive**
- hiring a sufficient number of **capable and reliable staff** with responsibility for STC compliance and ensuring adequate IT and technical support for this function
- staff concerned with activities that include product development, production, sales, human resources and accounting to **receive an appropriate level of training** and mentoring in STC compliance on a regular, if not ongoing, basis; many companies also provide **training for new employees** to familiarise them with the ICP and the importance of maintaining compliance with applicable STC laws and regulations

- the development of **clear and comprehensive company policies and practices** relating to the fulfilment of relevant STC obligations and raising awareness of these among all employees – including, where relevant, the existence of a compliance unit
- encouragement and facilitation of **open reporting** by staff who uncover compliance problems

Box 27: International Standards Organisation (ISO) – Guidelines on Compliance Management Systems[36] (excerpts)

Compliance is an outcome of an organisation meeting its obligations, and is made sustainable by embedding it in the culture of the organisation and in the behaviour and attitude of people working for it. While maintaining its independence, it is preferable if compliance management is integrated with the organisation's financial, risk, quality, environmental, and health and safety management processes and its operational requirements and procedures.

An effective, organisation-wide compliance management system enables an organisation to demonstrate its commitment to compliance with relevant laws, including legislative requirements, industry codes, and organisational standards, as well as standards of good corporate governance, best practices, ethics, and community expectations.

An organisation's approach to compliance is ideally shaped by the leadership applying core values and generally accepted corporate governance, ethical, and community standards. Embedding compliance in the behaviour of the people working for an organisation depends above all on leadership at all levels and the clear values of an organisation, as well as an acknowledgement and implementation of measures to promote compliant behaviour.

In developing and implementing an ICP, organisations are expected to undertake effective **'due diligence'**. This means that all reasonable steps should be taken to identify the risks associated with a proposed export or transfer of controlled goods, technologies or services, to make sure that the transaction is **within the boundaries of the law**, and to ensure that the customer is trustworthy and will only use the goods for legitimate purposes. All of this should be undertaken before a contract is signed. Due diligence requirements also necessitate procedures for regular internal audits of compliance with STCs (see 'Regular audits of STC compliance and responding to non-compliance' on page 78) and for reporting both on suspicious activities and mistakes that may have been made.

NOTES

36 A preview of ISO19600 can be found at the International Organization for Standardization, 'Online Browsing Platform (OBP)' (https://www.iso.org/obp/ui/#iso:std:iso:19600:ed-1:v1:en). Access to the full Standard can be obtained via https://www.iso.org/standard/62342.html

4 Key elements of an ICP

While ICPs will vary from company to company, there are certain elements that should be common to all. These include:

A clear ICP structure including effective internal systems and processes

The aims and scope of any given ICP will vary according to the size and reach of the company/institute in question. However, all ICPs should be underpinned by standard operating procedures including specific **company/institute policies and processes that clearly set out how STC compliance will be achieved** as a priority. These procedures include:

- a step-by-step **screening process** relating to products, recipients, destinations, end-use, shipping, and financial actors (see next page)
- provisions for **documentation and record-keeping** in relation to:
  - current and historical transactions
  - licences applied for, received, and denied
  - a database of information emerging from screening processes
  - checklists and sign-off procedures to ensure consistency and accountability
- provisions for an **internal audit of STC compliance**, including objectives, targets, processes, key actors, and responsibilities
- complementary **training of staff**, relevant to their role in the company/institute
- a periodic **review** of the overall ICP

Once an ICP is established, it should not simply be maintained; rather it should be continually developed and improved. At the very least, an ICP must adapt and evolve to account for emerging proliferation risks and any changes that occur to the laws, regulations, or control lists in a particular jurisdiction or to relevant international obligations.

Most ICPs are underpinned by a desire to ensure compliance with STCs in all relevant contexts. For an SME, this may be the limit of their ICP ambition. For an MNC that manufactures a broad range of strategic goods and technologies and has subsidiaries in multiple jurisdictions, there may also be a desire to build an international reputation as an entity that strictly adheres to STCs in all operational contexts, plays a role in educating subsidiaries and supply-chain partners, and which is seen as a global leader in STC compliance. Just as failing to live up to STC obligations can bring scandal and disrepute, being seen to be diligent and responsible can contribute to a positive public profile and be good for business.

Understanding how to screen for proliferation risks

An ICP is centred upon an understanding of how and why STCs are necessary and how to screen for, and identify, proliferation risks associated with the export/international transfer of strategic goods, technologies, and/or technical assistance. In addition to staff training (see 'Training' on page 79), the ICP must incorporate relevant documents, resources, and manuals that address the substantive elements of STC compliance; this should include **'suspicious enquiry guidance'**, which incorporates information on how to conduct screening (see below). At the most basic level, those involved in STC compliance should undertake due diligence in the screening process, be alert to anything unusual in relation to a transaction, and understand that if something seems too good to be true, then it probably is.

a) Product screening (commodity classification)

It is not uncommon for enterprises to be unaware of the strategic nature of the goods, technologies, and/or services that they export or transfer internationally, with the nature and extent of controls on dual-use technologies a particularly problematic area. Before an enterprise considers the export of specific goods and technologies, they must ensure that they know **whether or not their goods, technologies, and/or services require export, transit, or import authorisation** in all of the

jurisdictions that the goods are to pass from, through or into. Similarly, companies that are involved in brokering the transfer of strategic goods or who are involved in shipping them should also be aware of their responsibilities to check that the necessary authorisations accompany any international transfer of strategic goods and technologies.

Most governments have a published control list (see 'Control lists' on page 11) which should be consulted. If it is not immediately clear that a particular item does/does not require an export licence or other type of authorisation, specialist help should be sought. Some governments can provide help with **commodity classification**[37] (see 'Online resources' on page 30) but if this is not available, specialist assistance may need to be sourced from the private sector. For SMEs that trade in a limited number of products, it should be relatively easy and inexpensive to establish the classification of items for export.

It is also important for any prospective exporter of goods to be fully aware of the **capabilities and uses of the goods, technologies, and/or services** in question. This will assist the subsequent assessments of the end-user, destination and end-use, and help guard against inadvertent or negligent STC violations.

b) Destination screening

In addition to screening the product, **checks should be made on the situation of the country** where the recipient/consignee and end-user are located. If the final destination of the goods/technologies is different from that of the recipient, this could represent a red flag for a **possible diversion risk**; in the absence of any clear explanation for this situation, it should be reported to relevant authorities. In addition the exporter should check that the destination for the items is not:

- a country of proliferation concern – for example, a country that is known to be engaging in illicit/underground programmes to develop WMD
- a country that is subject to relevant UN or other relevant sanctions (see 'Countries of concern' on page 14)
- a country that is subject to a UN arms embargo or other relevant arms embargo (see 'Countries of concern' on page 14)

Should any of these circumstances apply, **careful consideration should be given as to the advisability of proceeding with the proposed transfer**. Detailed investigation should also be carried out into the end-use of the goods, technologies, and/or services in question. Again, due to the potential for circumstances to change in the interval between the placing of an order and its completion, **destination screening should be undertaken twice** – prior to acceptance of an order and prior to the processing of a shipment. This should help prevent the unwitting export of strategic goods, technologies, and/or services to a destination that is newly proscribed.

c) Recipient and/or end-user screening

If it is established that items for export require a licence or other form of authorisation and the declared destination is not a country of concern, the next step in the screening process is to **scrutinise the prospective recipient**. Industry and other relevant actors involved in the export or international transfer of strategic goods, technologies, and/or the provision of technical assistance should be aware that **the trade in certain items/services with particular end-users is not permitted**. Care needs to be taken to ensure that all parties involved in the export/transfer – including any intermediaries/consignees and the ultimate end-user – are all reliable and of good standing, and that the companies involved and their owners do not feature on any relevant national or international sanctions lists. For SMEs that require assistance with restricted party screening, some commercial enterprises have developed software that can link into a company's own business management systems to automatically flag up known risks in relation to specific individuals and enterprises (see 'Online resources' on page 30).

If any party to the transfer is not well known to the exporter as a trusted partner, full enquiries should be made regarding the nature of the organisation, its activities, its ownership and key staff, and its places of operation.

Box 28: Information required in relation to potential new customers[38]

Critical background information

- Company name, address, contact information, type of business
- Name, address, contact information of subsidiaries, affiliates or branches
- Company owners/partners, percentage of ownership, nationality
- Company directors/senior officers, nationalities, employment, and education background
- Description of the nature of the organisation's business and details of company accounts

Other useful information

- Links to any government or political party on the part of company owners/partners/senior officers
- Criminal charges faced by the organisation, its owners, directors, or senior employees
- Debarments/suspension from business involvement on the part of the organisation, its owners, directors, or senior employees
- Key organisation employees who are leading on the proposed contract
- Individuals who will provide services in support of the proposed contract
- Any other organisation or individuals with an interest in the proposed contract
- Three references from banks, business organisations or similar

In particular it should be investigated whether the prospective recipient is involved in activities that could be **a gateway for conventional arms or WMD proliferation activities**. Checks could be undertaken through a variety of means, including:

- **direct questions** put to the recipient and end-user and verified via checks on open source information
- examining **publicly available organisation records**, audit information, and published accounts
- using publicly available information (including reputable news outlets and social media) to **check, as far as possible, on the bona fides of the organisation** and its executive management teams, directors and beneficial owners, their business partners, and associate companies
- **visiting the premises of the prospective recipient or end-user** organisation if possible – or using online mapping sites to ascertain whether their business is situated as claimed
- **consulting relevant authorities** (national and local) in the exporting and importing country and verifying the information provided, for example, through internet news searches
- checking against **red-flag indicators** (see page 69)
- checking **sanctions listings and watch lists**, such as the US Denied Persons List of individuals and entities that have been denied export privileges, and the US Entity List of foreign parties prohibited from receiving some/all items subject to US Export Administration Regulations (see 'Entity watch lists' on page 15)
- using **online party screening tools** provided by governments (see 'Online resources' on page 30) or by private enterprises – some of which can be linked into an organisation's systems so that any problems in relation to particular transactions are automatically flagged

Due to the potential for circumstances to change in the interval between the placing of an order and its completion, **recipient screening should be undertaken twice** – prior to acceptance of an order and prior to the processing of a shipment. This should help prevent the unwitting export or transfer of strategic goods, technologies, and/or services to an entity that is newly proscribed.

d) End-use screening

Any company involved in the export or international transfer of strategic goods, technologies, and/or technical assistance should undertake effective end-use screening as a matter of course. For companies exporting military equipment it is generally easier to verify end-use because the end-user is usually the armed forces, security, and/or police forces in a country, or their appointed purchasing agents. The effectiveness of end-use screening also depends on whether the company sells directly to customers or relies on a network of agents and distributors. **If using a third party recipient/ consignee, the risks of diversion from the declared end-user are much greater**.

Checks should be made as to whether:

- the customer has a **credible and legitimate end-use** for the product and that it is not for military application in a destination subject to an arms embargo, nor for use in chemical, nuclear, or biological weapons proliferation
- the consignee is **known to be reliable** and is transferring the product to a verifiably legitimate end-user
- the consignee and/or customer **do not have a known history of diverting strategic goods and technologies** to unauthorised entities

If, after checks are complete, any concerns remain or new issues arise, then these issues should be raised with relevant STC authorities prior to shipment, and the exporter should work with them to resolve any areas of concern. These issues could include:

- the customer declining routine installation, training, or maintenance services associated with the items for export
- delivery dates that are vague or shipping routes that are unusual
- a freight forwarder that is listed as the final destination/end-user
- the consignee/end-user requesting that they pay for the items in cash
- the consignee/end-user having a known history of diverting controlled goods/technologies to unauthorised end-users (e.g. for WMD programmes)

e) Shipping screening

Prior to arranging or approving the shipment of any controlled goods and technologies, exporting companies should undertake checks to **establish the bona fides of any unfamiliar actors involved in the shipping process**, including road haulage companies, shipping companies, logistics companies, transportation agents, and freight forwarding agents. In addition, even where actors are known and trusted, should the shipping arrangements appear unusual or raise concerns – for example, because the intended route appears overly complex or circuitous – then this should be reported to the relevant STC authorities prior to shipment. Steps should also be taken – both by the exporter and the shipping company – to ensure that transit/transhipment laws and regulations are complied with in relevant jurisdictions along the shipping route.

f) Screening of financial actors

Of growing concern is the role of banks and financial institutions in **'proliferation financing'**. This is the act of providing funds or financial services used in the development, manufacture, acquisition, possession, export, transit/transhipment, brokering, transportation, transfer, stockpiling or use of WMD, their means of delivery, and related dual-use goods and technologies, in breach of national laws and/or international obligations. Also of concern is the risk of contravening financial sanctions levied against states, non-state actors and individuals by the UN, multilateral organisations and states.

All financial institutions that are involved with providing financial services in support of the trade in strategic goods and technologies must carry out the necessary checks to safeguard against proliferation financing and against breaches of applicable sanctions. In addition, all other actors concerned with the international transfer of strategic goods, technologies, and/or services should take steps to ensure that financial institutions that are linked to relevant transactions are legitimate and of good standing.

Box 29: U.S Department of Commerce, Bureau of Industry and Security Red-flag indicators[39] (excerpt)

Things to look for in export transactions:

- The customer or its address is similar to one of the parties found on the Commerce Department's list of denied persons.
- The customer or purchasing agent is reluctant to offer information about the end-use of the item.
- The product's capabilities do not fit the buyer's line of business, such as an order for sophisticated computers for a small bakery.
- The item ordered is incompatible with the technical level of the country to which it is being shipped, such as semiconductor manufacturing equipment being shipped to a country that has no electronics industry.
- The customer is willing to pay cash for a very expensive item when the terms of sale would normally call for financing.
- The customer has little or no business background.
- The customer is unfamiliar with the product's performance characteristics but still wants the product.
- Routine installation, training, or maintenance services are declined by the customer.
- Delivery dates are vague, or deliveries are planned for out of the way destinations.
- A freight forwarding firm is listed as the product's final destination.
- The shipping route is abnormal for the product and destination.
- Packaging is inconsistent with the stated method of shipment or destination.
- When questioned, the buyer is evasive and especially unclear about whether the purchased product is for domestic use, for export, or for re-export.

Awareness and consideration of specialised STC provisions

a) Catch-all

In the field of STC, one of the most difficult aspects to implement is the 'catch-all' clause. Catch-all controls exist in the form of **authorisation requirements or prohibitions on the transfer of goods, technologies, and/or services** not usually subject to control, in situations **where they may be intended for a WMD or sensitive military programme/end-user or may be destined for a restricted or prohibited destination**. This poses a number of challenges for ICPs for several reasons, not least because the nature and extent of the catch-all differs across jurisdictions. The three main variables are:

- the scope of goods/technologies/services covered – listed, non-listed, or both
- the nature of intended end-use – for use in connection with WMD programmes only, or also for use in military programmes in states subject to arms embargo
- the evidence base – the exporter has knowledge of illicit end-use, is informed of illicit end-use by government, and/or has suspicion of illicit end-use

The effective operation of the catch-all is based on having **full knowledge of a customer's intentions** and also an understanding of the techniques adopted by proliferators to disguise their illicit trading activities; unfortunately, commercial enterprises, research institutes, and other relevant entities are not always in possession of all relevant information on these topics. Nevertheless, given the risk of negligence leading to serious STC violations, all ICPs need to include a genuine effort to implement catch-all controls that apply within relevant jurisdictions. This could involve the development of specific guidance on this issue, conducting a thorough review of the end-use of an item for export/international transfer, and monitoring and maintaining control of shipments as far as possible.

In practice much of the responsibility for implementation of the catch-all will fall to governments, in terms of publishing information on how the catch-all operates, taking steps to educate industry on this issue, and alerting industry to specific risks.

b) Intangible technology transfer and technical assistance

Intangible technology transfer (ITT) is generally considered to be the **transmission of technical information via electronic, oral, or other intangible means**. In some contexts ITT is also considered to include the transfer of knowledge and skills by individuals. In other contexts, the sharing of instructions, skills, training, working knowledge and consulting services is referred to, distinctly, as **'technical assistance'**; this **can be transmitted separately or provided pursuant to the export of tangible goods or technology**.

Proliferators are increasingly **seeking to acquire technologies and know-how** in order to establish engineering and manufacturing capabilities that allow them to produce items of concern, such as missiles, WMD, and sophisticated military equipment. Whereas it is generally accepted that information that is in the public domain and so-called 'basic scientific research' should be exempt from control, in many jurisdictions intangible technology and technical assistance are controlled for export if they are associated with tangible goods and technologies that are themselves controlled. The regulation of intangible transfers of technologies/technical assistance represents a major challenge for government and for industry, academia, and research institutes.

The difficulties that are faced in regulating and monitoring intangible transfers are compounded by the **many ways in which ITT can occur**, including:

- by email
- by fax
- uploading to a website
- storage on a cloud server
- storage on a memory stick that is posted, carried by a person, or shipped abroad
- by oral means – in person through conversation/presentation or detailed description via telephone or internet, etc.
- by means of visual display – electronically, hard copy, etc.

In addition to controlling technologies or information that is transmitted to, or shared with, overseas entities, companies/institutes should seek to include **restrictions on any subsequent onward transfer** of proprietary technology/information. They should also comply with any restrictions that apply to the activities of overseas employees or students concerning access to, or sharing of, controlled information and technology.

The ICP of any company/institute that engages in ITT or provides technical assistance must include the education of personnel as to **the importance of ITT/technical assistance control** and the laws and regulations that apply in this area, as well as the development of procedures and protocols for ensuring compliance with relevant STCs. Some basic elements for an ITT/technical assistance management plan may include:[40]

- clear guidelines as to **which people within a company or institution may/may not undertake** ITT/provide technical assistance and the permitted methods for such transfers of technology/information
- **classification listings for all technologies and technical information** owned or used by a company or institution
- a requirement that export control classification is **established** as soon as a new piece of technology is developed/created
- a process that must be followed to ensure that the **appropriate controls are being applied** to the transfer of technology or technical information, including information that has been uploaded to laptops and other hardware
- a requirement that any email transmission of controlled intangible technology or technical information should include, in the email header, **the relevant export licence/authorisation number**
- restricting the transfer of technology and technical information by allowing it to take place only through **specific controlled areas of the company database**
- restricting the transfer of technology and technical information by creating **physical access controls** (badges, locks, limited access areas) in an effort to limit the potential for unauthorised use or transfer of controlled information
- systems and procedures enabling **monitoring of ITT** and the blocking of certain transfers if necessary
- provisions for **regular internal audit of ITT** and provision of technical assistance

Governments have a significant responsibility to conduct outreach to relevant enterprises and institutions and to raise awareness of controls on ITT and technical assistance – including any restrictions that apply to storage of information on 'cloud' services using servers located abroad, and any mitigating measures that can be taken (e.g. encryption of data).

Ultimately, however, the **onus is firmly on industry, academia, and other relevant actors** to ensure that they have proper guidelines and systems for control of ITT and technical assistance, that the relevant transfer authorisations are obtained, and that proper records are maintained for inspection during an external audit.

Box 30: Elements of an ITT-focused ICP for academia and research institutes (Korean Security Agency of Trade and Industry)

- Management organisation and strategic plan should reflect ITT controls
- ITT control should have the explicit support of the CEO
- Examination of possibilities for technology transfer: at research planning stage, at intermediate or final report stage, when being shared subsequently
- Education and training for staff and students in respect of travel abroad, conferences and seminars
- Ensuring controls are applied to shipping of strategic items
- Regular audit of ITT
- Documentation management
- Ensuring a robust information security system
- Reporting on transfers and possible infractions

ITT should also be factored into any guidelines for:

- Joint or commissioned research
- Technology transfer within the organisation
- Technology, education, and consulting
- Merger and acquisition
- Technology licensing and sales
- Business trips or conferences/exhibitions
- Management of overseas staff/students

c) International brokering of strategic goods and technology transfers

International brokering of strategic goods and technology transfers is an integral part of the international trade in these items. It occurs when one or more entities facilitate the international transfer of strategic goods and technology **between two third parties based in different countries** without the broker (sometimes referred to as an 'intermediary') ever taking physical possession of the items.

Some entities engage in brokering activities as their primary or sole strategic trade-related activity. Others – including MNCs – focus primarily on other aspects of the trade in strategic goods and technologies (e.g. manufacture and export) but engage in brokering as and when necessary, for example, where – as part of a larger order – a customer requires specific items which the MNC supplier does not manufacture or export.

An increasing number of governments now control international brokering in strategic goods and technologies; however the exact nature of the controls varies from country to country. At a minimum, brokering is usually defined as **buying and selling** of controlled items or **facilitating** an agreement between other parties for the international transfer of controlled items. In some cases governments may apply brokering controls to the **financial** or **transportation** aspects of the transfer of controlled goods.

Most governments will impose some or all of the following requirements upon brokers operating within their jurisdiction:

- a requirement to **register** as an international broker with the STC authorities
- a requirement to **obtain a licence** for each individual transaction
- a requirement to **keep records** of all relevant transactions

In most states the principal focus of brokering controls relates to the trade in **conventional arms**; however, under the EU Dual-Use Regulation[41] the brokering of dual-use goods and technologies outside the EU is controlled where a broker has been informed, or is aware, that the goods or technology in question are to be used for the production or delivery of WMD.

The **geographical application** of brokering controls is also variable. At a minimum, controls will apply to activities that take place within a country's territory; however, in some contexts, controls have an extra-territorial application so that residents or nationals are subject to brokering controls at home or abroad.

It is vital that companies and institutes that play any role in facilitating the international movement of strategic goods and technologies between third-party countries are fully cognisant of both the export controls *and* the brokering controls that apply within their country/countries of operation and any other jurisdictions where the transfer has been arranged or executed. Failure to do so could lead to multiple breaches of STCs in different countries, with potentially serious implications for the viability of future business activities.

A record-keeping system

Record-keeping should be an essential part of any company/institute's internal management systems and ICP, irrespective of the nature or size of its operations or the types of licences or authorisations it normally uses. The nature of the records kept and the length of time they must be retained vary from one jurisdiction to another and will depend on the nature of a company's business or the nature of an institution's research. A company/institution should **keep comprehensive records relating to all controlled activities** and may see benefits in maintaining some or all records beyond the time specified in law.

In many cases either the regulator and/or national enforcement authorities have a right to inspect records. The objective is to ensure that traceable records of each transaction made under an export licence or authorisation are maintained, so that queries about any transactions may be readily checked and an adequate audit trail followed through. To facilitate record-keeping, a company/institute's ICP needs to **establish a policy on the time, the means, and the locus for maintaining and storing records** to ensure that the information required by law is kept and can be readily retrieved. In addition, clear responsibilities for record-keeping should be allocated among staff along with rights of access to records and procedures for sharing confidential information.

A good standard of internal accounting and record-keeping is particularly important if a company is involved in the use of **bulk permits**, given the likelihood that relevant STC authorities will wish to conduct compliance visits to ensure that exporting activities are consistent with the terms of the permits granted. Being able to prove compliance is a key function of any ICP.

Box 31: Key requirements of a record-keeping system

Records required to demonstrate compliance with licences or authorisations include:

- Details of export licence applications, authorisations and refusals, including email and documentation records.
- Details of the physical export of goods that has taken place under an export licence.
- Electronic transfers of technology/technical information; individuals who share licensable information should be made responsible for maintaining transaction records.
- Oral presentations – where an individual is presenting controlled information at an event where attendees receive copies, or are free to take notes, the presenter must ensure that everyone who receives the information is authorised under all relevant jurisdictions, and that records are kept.
- Provision of services – if services are licensable, records will also need to be kept to demonstrate that the terms and conditions of those licences have been complied with.
- Recording compliance with access restrictions of those working with licensable items; this might include records of physical and IT access controls that document which individuals have been afforded access to controlled technology and information within the company/institute.

Box 31 continued

Other areas where records need to be maintained include:

- Export control classifications – as well as the finished article, each part and component must be classified, along with the technology related to the software, design, and manufacture of the parts and components; production equipment and services may also require an export control classification.
- Screening – a fundamental part of export compliance and a regulatory requirement in some jurisdictions; the screening date and result should be recorded and retained for as long as possible, and at least as long as the records of the relevant exports are kept; screening results should be readily available for scrutiny during internal audits and compliance visits.
- Training – awareness and training are also mandatory components of some governments' compliance requirements and should be recorded; this might include a record of the list of attendees, the names of trainers, the dates of training, the topics covered, and the issues and questions raised by employees.

A **database** provides a legal record of classifications and auditable evidence that the exporter is performing its legal obligation to understand how its products are controlled. For a large organisation, a central point for recording this information may be advantageous to minimise unnecessary repeat classification exercises for the same items used at different locations. The development of an in-house database to catalogue the proper classification associated with all products and services produced by a company/institute can also be useful.

SMEs may require a simple database or IT system; it may be easier for companies to develop their own system that meets their particular requirements. Sole traders and very small enterprises may choose to rely on paper records; medium-sized enterprises are more likely to require some form of electronic record-keeping system, and this might involve looking at what enterprise management systems they already have and exploring what record-keeping system might complement these.

Regular audits of STC compliance and responding to non-compliance

Given the potential for relevant STC authorities to make short-notice compliance visits to companies/institutes engaging in the export and international transfer of strategic goods, technologies, and related services, regular audits of companies and institutions are an important facet of an ICP. Broadly speaking, there are three main types of audit:

- Self-audit – where different departments within a company or institution review each other's business procedures and records using an audit checklist to identify any compliance issues.
- Internal audit – where a company's headquarters carries out checks on internal compliance procedures of their subsidiaries or conducts an audit of records kept among a group of companies or subsidiaries.
- External audit – where an external audit firm (hired by a company) or the company's customers, business partners or STC authorities undertake an audit of compliance (these audits tend to be most useful when conducted by auditors who have an understanding of STCs).

SMEs may rely primarily on self-auditing; larger enterprises are more likely to have a regular internal or external audit. Provisions for regular auditing are also an important element of an enterprise's due diligence requirements and of building a suitable pro-compliance culture.

Audits should involve checking that correct procedures have been followed in respect of all transfers subject to STCs; identifying mistakes or areas for improvement; and enabling a company to demonstrate their compliance with relevant STCs. Should any errors be found, **prompt disclosure** should be made to the relevant STC authorities so as to mitigate the potential for severe penalties. Companies/institutes should have **clear procedures** for responding to cases of potential or actual non-compliance, including the designation of senior personnel who will be responsible for prompt reporting of the information to government authorities and initiating the necessary steps to identify and address deficiencies in policies and/or practices.

Some large corporations engage in **'benchmarking'** exercises where they share information with each other on the systems and resources allocated for compliance with STCs. For example, they may share information on:

- the number of staff involved in ensuring STC compliance
- the number of export licences applied for during a given period
- how many voluntary disclosures have been made in respect of any potential STC compliance problems that have been identified

This information can be useful to senior management, enabling them to ensure that their STC compliance practices are of a similar standard to that of comparable enterprises.

Training

In order for an ICP to achieve its purpose of identifying proliferation risks, all relevant staff and, in particular, those directly concerned with export or international transfer of goods, technologies, and/or the provision of technical assistance should be educated on applicable STCs and trained in how to conduct **screening processes** (see 'Understanding how to screen for proliferation risks' on page 62). Training should be provided regularly – given the potential for personnel changes – and existing staff should have the opportunity to refresh and update their knowledge of this field.

For companies with limited time and resources, updates could be obtained by way of online export control courses. For those with greater resources, **annual training days** for staff – and possibly also for representatives of relevant companies in the supply chain – could be a useful option. Staff should also be subject to regular performance reviews to ensure consistent and effective application of procedures; they should understand why STCs exist, what they do, and how to identify red flags that indicate a possible proliferation risk; they should also learn what questions to ask a prospective customer and how to ensure they obtain satisfactory answers. Relevant employees should also understand what courses of action they should follow in the event of identifying any proliferation risks or suspicious enquiries.

Opportunities for training can often be provided by government; however there is also significant **private sector involvement in STC education**, including industry associations and large companies that provide training to SMEs in order to help ensure STC compliance throughout their supply chains. In the latter case, by sharing information and knowledge of STC issues with supplier companies and by checking their ICP, MNCs can help to create a robust and resilient supply chain – providing the information that is shared is relevant to the concerns and challenges faced by SMEs.

Ultimately, however, all companies and institutions are responsible for their own STC compliance regardless of who provides training or other educational resources.

NOTES

37 Process guidance for commodity classification can be found on the EXBS Internal Compliance Program Guide website: http://icpguidelines.com/index.php/the-elements-of-an-internal-compliance-program/transaction-screening-process-and-procedures/152-item-classification-and-screening

38 Information drawn from a 'New Customer Questionnaire' developed by John Buckler, Managing Director, SCUDO Consultants Limited.

39 U.S Department of Commerce, Bureau of Industry and Security, 'Know Your Customer Guidance' (https://www.bis.doc.gov/index.php/all-articles/23-compliance-a-training/47-know-your-customer-guidance)

40 For further information on the establishment of an ITT control system, see CEEC Draft Working Group Standards (2011), 'Intangible Exports (Exports of technical information)', November (http://www.ceecbestpractices.org/uploads/9/1/2/6/9126226/ceec_-_intangible_exports.pdf)

41 European Union Council Regulation (EC) No 428/2009 (2009) (https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:134:0001:0269:en:PDF)

5

Addressing challenges to the development, adoption, and maintenance of an ICP

Challenges to the development and adoption of ICPs vary and depend upon many factors, including the size of the company/institute, its product range/activities, and where it is based.

Even for SMEs that understand the rationale behind an ICP, there may be **difficulties in allocating the necessary resources**, while finding well-trained compliance personnel may be a challenge. In such situations, external assistance should be sought from government and/or from industry associations/partners.

For MNCs there may be challenges in securing **commitment to compliance at senior levels** and difficulties in ensuring compliance throughout the supply chain. In such circumstances it could prove useful to alert relevant personnel to the consequences of STC failures and point to certain high-profile cases where entities were prosecuted for STC violations.

Box 32: Potential consequences of STC violations for companies/institutes

- Fines and/or imprisonment
- Compound penalties for acts of recidivism
- Negative publicity and damage to corporate image/reputation
- Loss or suspension of licensing privileges
- Repeated government audits
- Placement on a watch list

One priority for all types of enterprise is the desire to **minimise the administrative burden** of an ICP. Companies should create an ICP that is adequate for their specific needs. In the case of a small-scale enterprise with only a few employees, it may be necessary for just one or two people to be fully trained in proliferation screening. Even so, it will be important for all company staff to be aware of the need to adhere to STCs and there should also be a system of record-keeping and periodic audit.

Another ongoing challenge common to all companies/institutes is that any ICP will need to be maintained and updated in response to a shifting regulatory environment. There is no 'one size fits all' for ICPs, and changes will be required in order to facilitate **organic growth and development** in line with the needs of the company or institution and with developments in STCs in relevant jurisdictions and in international sanctions. Failure to update information and procedures could undermine the whole system and lead to penalties and/or prosecutions. In addition, **open reporting of potential STC violations** should be encouraged, without attributing blame to individuals and with a commitment to taking remedial action. Records should be kept of the changes made to an ICP so that if an STC violation does occur, the reasons for this can be better understood.

Fundamentally, an **ICP must be seen as an ongoing commitment** for any company/institute engaged in the international transfer of strategic goods/technologies and should be embedded in the culture, systems, and practices of the whole organisation. An ICP should not, however, be seen as an end in itself; rather it should be viewed as an essential contribution to a global trade regime that safeguards international peace and security by preventing the proliferation of WMD, conventional arms and related strategic goods and technologies.

Chinese Academy of International Trade and Economic Cooperation (CAITEC)

CAITEC is an interdisciplinary and multifunctional institution of social science research and a consultative body directly under the Ministry of Commerce of China, which undertakes research, information consultancy, publishing, education and training. CAITEC conducts research on the world economy and international trade, economic cooperation, regional economies, country-level economies, domestic trade and market development. It also conducts important research relating to export controls. It is one of the first national high-end think tanks in China and in recent years has played an essential role in academic research, expert team building, personnel training and international communication.

Chinese Academy of International Trade and Economic Cooperation
No. 28, Dong Hou Xiang, An Ding Men Wai Avenue, Beijing, P.R. China (100710)

Tel: +86-10-64245741 | Fax: +86-10-64212175 | Web: http://en.caitec.org.cn/

Saferworld

Saferworld is an independent international organisation working to prevent violent conflict and build safer lives. We work with people affected by conflict to improve their safety and sense of security, and conduct wider research and analysis. We use this evidence and learning to improve local, national and international policies and practices that can help build lasting peace. Our priority is people – we believe in a world where everyone can lead peaceful, fulfilling lives, free from fear and insecurity.

We are a not-for-profit organisation operational in nearly 20 countries and territories across Africa, the Middle East and Asia.

Saferworld, The Grayston Centre, 28 Charles Square, London N1 6HT, UK
Tel: +44 (0)20 7324 4646 | Fax: +44 (0)20 7324 4647 | Web: www.saferworld.org.uk

The Center for Policy Research, University at Albany, State University of New York (SUNY)

The Center for Policy Research (CPR) was formally established in September 1987. Research conducted under the auspices of CPR addresses policy-relevant topics in the fields of international affairs, political science, public administration, and public policy. CPR serves multidisciplinary and cross-departmental needs at the Rockefeller College of Public Affairs & Policy and promotes the goal of increasing the University at Albany's level of sponsored research activity. CPR supports fundamental research, applied research, and outreach activities. CPR's Project on International Security, Commerce, and Economic Statecraft provides those forms of support in the area of strategic trade controls and non-proliferation.

Center for Policy Research, University at Albany, SUNY
Milne Hall 300, 135 Western Avenue, Albany, NY 12222, US

Tel: +1 (518) 442-3852 | Fax: + 1 (518) 442-3398 | Web: http://www.albany.edu/cpr/index.shtml

ISBN 978–1–912901–06–7