



# **SANCTIONS & EXPORT CONTROLS COMPLIANCE POLICY**

**ISSUE DATE: NOVEMBER 2018**

**ISSUE NO. 1**

## 1 About this policy

- 1.1 This policy applies to Luxfer Holdings PLC and its subsidiary companies (“Luxfer”) and to all Luxfer employees, officers, consultants, contractors, casual workers, volunteers and agency workers.
- 1.2 Luxfer’s commercial success relies upon its ability to conduct business in different countries around the world. We are committed to complying with applicable sanctions and export control laws and regulations in every jurisdiction in which we operate. Such compliance is critically important to the integrity of the Luxfer businesses and requires active participation of all personnel.
- 1.3 The purpose of this policy is provide guidance on applicable laws and regulations and to set out measures to help manage and mitigate the risk of sanctions or export law violations.
- 1.4 Failure to comply with this policy carries the risk of:
- significant financial penalties;
  - negative publicity and damage to the Luxfer brand;
  - loss of business;
  - revocation of export privileges;
  - the businesses being blacklisted from certain contracts;
  - adverse impact on share price; and
  - imprisonment of individuals.
- 1.5 Responsibility for this policy:
- **Managing Directors/Presidents** will be ultimately responsible for the implementation of this policy within their businesses, appointing a Sanctions Compliance Manager and allocating adequate resources for this purpose.
  - **Luxfer’s Executive Leadership Team** will review this policy and receive reports from the managing directors/presidents on an annual basis.
  - **Luxfer’s General Counsel** will be responsible for advising generally on this policy and ensuring that it is updated as required from time to time to reflect any changes in the law or best practice.
- 1.6 Successful implementation of this policy will be dependent upon the finance, marketing and sales functions in each business working together, sharing information and collaborating on due diligence.
- 1.7 Each business shall nominate a member of its senior management team as its **Sanctions Compliance Manager (“SCM”)**. The SCM shall be the key contact for all matters relating to exports and sanctions and responsible for ensuring that their businesses comply with this policy on a day to day basis. At the date of this policy, the SCMs for each business are as follows:

<b>Business</b>	<b>SCM</b>	<b>Contact title</b>	<b>Email</b>
Luxfer Gas Cylinders	US, Canada, India & China – Michael Edwards	Divisional finance director	<a href="mailto:Michael.Edwards@luxfer.com">Michael.Edwards@luxfer.com</a>
	UK & Europe– Howard Mead	European finance director	<a href="mailto:Howard.Mead@luxfer.com">Howard.Mead@luxfer.com</a>
Luxfer MEL Technologies	Guy Roberts	Director of sales & marketing	<a href="mailto:Guy.Roberts@luxfer.com">Guy.Roberts@luxfer.com</a>
Luxfer Magtech	Matt Shufran	Vice president of sales	<a href="mailto:Matt.Shufran@luxfer.com">Matt.Shufran@luxfer.com</a>
Luxfer Graphic Arts	Sarah Crump	Financial controller	<a href="mailto:Sarah.Crump@luxfer.com">Sarah.Crump@luxfer.com</a>
Luxfer Superform	Phil Taylor	Sales & engineering manager	<a href="mailto:Phil.Taylor@luxfer.com">Phil.Taylor@luxfer.com</a>

1.8 Although written in the context of the laws of England & Wales, the EU and the US, the principles and requirements of this policy apply to all Luxfer’s operations and are generally applicable to other jurisdictions around the world. When dealing with matters in other jurisdictions it will be necessary to contact Luxfer’s General Counsel and seek specialist advice on a case by case basis.

1.9 This policy does not form part of an employee’s contract of employment or a contractor’s terms of engagement and may be amended at any time. Breach of this policy by an employee may lead to disciplinary action, which may result in dismissal for gross misconduct. If a third party breaches this policy, they may have their contract terminated with immediate effect.

1.10 This policy is intended to supplement and not replace other Luxfer policies. In the event of any conflict between this policy and applicable mandatory law, the applicable mandatory law shall prevail.

1.11 If you have any questions about the obligations or implications of this policy, please contact Luxfer’s General Counsel or your business SCM.

## **2 Background**

2.1 Sanctions and export controls are restrictions and prohibitions imposed by various national and international organisations, including the United Nations, European Union and the US government, to promote foreign policy, limit the supply of

technology, finance or strategic goods to certain countries and to seek to maintain or restore international peace and security.

- 2.2 Frequently applied measures include:
  - 2.2.1 embargoes on exporting or supplying arms and associated technical assistance, training and financing;
  - 2.2.2 bans on exporting equipment that might be used for internal repression;
  - 2.2.3 financial sanctions on individuals in government, government bodies and associated companies, or terrorist groups and individuals associated with those groups;
  - 2.2.4 travel bans on named individuals;
  - 2.2.5 bans on imports of raw materials or goods from the sanctioned target; and
  - 2.2.6 other measures applied according to individual circumstances.

### 3 Export controls overview

- 3.1 Export controls:
  - 3.1.1 restrict the export of '**controlled**' goods and goods that are intended for a particular end use;
  - 3.1.2 apply to the supply of certain goods **to all destinations**, not just those countries subject to sanctions; and
  - 3.1.3 apply not only to the export of physical items but also to the transfer of intellectual property (e.g. taking a laptop overseas with controlled items, such as software, stored on it).
- 3.2 In the US the Export Administration Regulations ("**EAR**") are administered and enforced by the US Department of Commerce. In the UK, the Export Control Joint Unit ("**ECJU**"), part of the Department for International Trade, administers the UK's system of export controls and licensing for controlled items.
- 3.3 If export controls apply, a licence must be obtained. Licence requirements will be largely determined by the following factors:
  - 3.3.1 **nature of the product**: if a product is subject to a national or international legislative control regime and included on an applicable controlled items list – a 'controlled' item – it will require a licence. Controlled items generally include those designed or modified for military end use, dual use items that can be used for civil or military purposes, associated technology and software and items that could be used for torture;
  - 3.3.2 **destination**: depending on the sensitivity of the item, separate licences may be required for individual destination countries. Certain 'non-sensitive' products may require a licence if the country is subject to sanctions; and
  - 3.3.3 **End use**: products that are not included on a controlled items list may still require a licence if the product could be used for certain controlled or prohibited purposes (e.g. in the development of weapons of mass destruction).

**3.4** *Anybody involved in handling ITAR controlled items, ITAR controlled data or any other military supplies must do so strictly in accordance with Luxfer's approved ITAR manuals.*

#### **4 Sanctions overview**

4.1 Sanctions restrict the flow of money and economic resources to individuals, entities and countries that are subject to those sanctions.

4.2 Sanctions only apply to individuals, entities and countries that have been targeted with measures by the UN, EU, US or other government, organisation or supranational body.

4.3 Every country that implements sanctions does so by maintaining lists of individuals and entities with whom it is illegal to do business, for reasons which may include country association, terrorism and weapons proliferation.

4.4 Financial sanctions may be imposed by the UN Security Council through UN Security Council Resolutions. These are implemented in the EU through regulations. In the UK the Office of Financial Sanctions Implementation ("**OFSI**" - part of HM Treasury) may designate domestic individuals or entities as 'targets'. Examples of actions that constitute offences under the Terrorist Asset-Freezing etc Act 2010 ("**TAF**A") include:

4.4.1 dealing with funds or economic resources owned, held or controlled by a target, or where we know or have reasonable grounds to suspect that a target is holding or controlling those funds or economic resources;

4.4.2 making funds, financial services or economic resources available, directly or indirectly to targets;

4.4.3 making funds, financial services or economic resources available, directly or indirectly for the benefit of targets; and

4.4.4 knowingly and intentionally participating in activities that would directly or indirectly circumvent the financial restrictions imposed by the financial sanctions regime or enable or facilitate the commission of any of the above.

4.5 In the U.S., trade restrictions are imposed pursuant to U.S. economic sanctions regulations, which are administered by the U.S. Treasury Department, Office of Foreign Assets Control ("**OFAC**"). U.S. sanctions range from comprehensive (e.g., prohibiting nearly all transactions with a particular country) to selective (e.g., prohibiting certain transactions with certain entities or individuals).

4.6 U.S. sanctions regulations cover the conduct of 'U.S. Persons', being all persons in the United States, regardless of nationality, all U.S. citizens and lawful permanent residents, wherever located, and all companies and organizations incorporated in the United States, as well as their foreign branches. In the case of Cuba and

sometimes Iran, U.S. economic sanctions extend to non-U.S. entities that are owned or controlled by U.S. persons.

- 4.7 U.S. economic sanctions on entities and individuals present particular compliance challenges because sanctions targets often do not reside in countries otherwise subject to sanctions. It is therefore essential to screen Transaction Parties against OFAC's List of 'Specially Designated Nationals' (SDNs) and 'Blocked Persons'. The SDN List is updated regularly, so parties should be screened on a regular basis even if they are well-known to Luxfer.

## **5 Risk assessment.**

- 5.1 Each business will take steps to monitor compliance with this policy and review the effectiveness of its procedures at least once every 12 months as part of its general risk management process to ensure its sanctions and export control procedures are proportionate to the risks it faces.

## **6 Role of the SCM**

- 6.1 The SCM is primarily responsible for ensuring that its business complies with the requirements in this policy. The role will involve:

- 6.1.1 management and supervision of due diligence and risk assessments;
- 6.1.2 delegating tasks and co-ordinating activities between business functions;
- 6.1.3 addressing and reporting any deficiencies in compliance to the managing director or president of that business; and
- 6.1.4 consulting with Luxfer's General Counsel regarding any sanctions or export compliance risks in pending international business activities.

## **7 Our procedures.**

### **7.1 Determining which sanctions or export controls apply**

- 7.1.1 Assessment of the following 5 factors will be key in determining whether sanctions or export controls apply:

- 1. Places** – Where do you do business?
- 2. Persons** – Who do you do business with?
- 3. Products** – What goods/services do you supply?
- 4. Purpose** – What are your goods/services used for?
- 5. Payments** – Is your business going to get paid?

### **7.2 Export licences**

- 7.2.1 Each business shall implement an export management system to ascertain clearance requirements, apply for and maintain applicable licences and ensure that all necessary steps are taken to avoid export violations.

### 7.3 Due diligence

7.3.1 Third party screening (as described in paragraph 7.4) must be undertaken before engaging with or supplying to any new customer, supplier, distributor, agent, freight forwarder, customs broker or any other business partner (“**Transaction Party**”).

7.3.2 During due diligence of any Transaction Party, and throughout the life of the relationship, each business shall monitor for any compliance red flags suggesting that the transaction is likely to violate sanctions or export control laws. Any unusual situation or activity involving a Transaction Party must be reviewed further. Examples of such red flags include:

- Transaction Party or its address is similar to that of a party found on any restricted party list;
- Transaction Party or purchasing agent is reluctant to provide information about the end-user or end-use of a product;
- Transaction Party intends to pay cash when the terms of sale would usually call for financing;
- Transaction Party has little or no business background;
- Transaction Party is unfamiliar with the purchased product; or
- Transaction Party declines routine installation, training, or maintenance services.

7.3.3 If anybody encounters any of the red flags listed above or any other unusual circumstances without adequate explanation, the transaction must be halted, and Luxfer’s General Counsel must be consulted for guidance.

### 7.4 Screening

7.4.1 Each business shall implement procedures (using AEB Compliance software or other similar tools approved by Luxfer’s General Counsel) to ensure that all relevant transactions are adequately screened against applicable sanctions, restricted party lists and export controls list including at a minimum, (1) **Office of Foreign Assets Control (OFAC) US sanctions list**, (2) **EU Consolidated Financial Sanctions list**, (3) **Office of Financial Sanctions Implementation lists (OFSI)**, including the UK Consolidated List of Financial Sanctions Targets and (4) the **UK Strategic Export Control Lists**.

7.4.2 It shall also be necessary for each business to ensure that it does not engage in any transaction that directly or indirectly involves countries that are subject to sanctions, unless and until such transaction has been screened and approved in accordance with this policy.

7.4.3 The level of screening required in each case will depend upon the risk profile of the particular relationship or transaction. In circumstances involving a

party located in a high-risk jurisdiction, greater due diligence will be required in comparison with a situation involving an internationally recognized business in a territory that is not subject to sanctions or export controls.

## 7.5 Banking covenants

- 7.5.1 In addition to legal and regulatory obligations, businesses must ensure that they comply with the covenants set out in Luxfer's financing and facility agreements. These covenants apply to all Luxfer businesses and prohibit Luxfer from operating in certain territories. The covenant in the current facility agreement is as follows:

*The Company represents and covenants that it will not, directly or indirectly, use the proceeds of the transaction, or lend, contribute or otherwise make available such proceeds to any subsidiary, joint venture partner or other Person, to fund any activities of or business with any Person, in Burma/Myanmar, Cuba, Iran, Libya, North Korea, Sudan, Syria, Crimea or in any other country or territory, that, at the time of such funding would result in a violation by any Person (including any Person participating in the transaction, whether as underwriter, advisor, investor or otherwise) of Sanctions (being any other countries / persons sanctioned by OFAC, UNSC, EU ,HMT (UK) or any other relevant sanction authorities).*

## 7.6 Record keeping

- 7.6.1 Each SCM will ensure that all relevant records are maintained, including export licences, correspondence with the authorities relating to exports and imports, records of the dates on which export licences expire and any other records that need to be retained specifically for the purposes of such licence.
- 7.6.2 Records must be kept for **five years** from the end of the year of export or such longer period as may be required by appropriate authorities or agreement between relevant parties.

## **8 Contract management**

- 8.1 Contracts must include appropriate trade compliance language to ensure that the Transaction Party understands and complies with applicable sanctions and export laws and its obligations under this policy. Applicable contracts should include:
- 8.1.1 a statement that the Transaction Party is not a restricted party or otherwise subject to sanctions;
- 8.1.2 an undertaking to comply with all applicable sanctions and export laws and the obligations in this policy;
- 8.1.3 an undertaking not to do anything that would cause Luxfer to breach any laws or regulations to which it is subject; and



8.1.4 the option to terminate the contract in the event of a sanctions or export controls violation or breach of the above undertakings.

## **9 Training and awareness**

9.1 Managing directors and presidents shall be responsible for committing sufficient resources to support the development and operation of an effective trade compliance program within their business units.

9.2 Introductory training on sanctions and export compliance shall be provided as part of new employee orientation to personnel with international business responsibilities. Certain personnel will be required to undertake additional training on sanctions and export compliance issues on a periodic basis.

9.3 Employees must not arrange, approve, or effect any export or other trade compliance activity unless he or she is satisfied that the transaction complies with all applicable legal requirements and Luxfer policies and that all documentation and recordkeeping requirements have been satisfied.

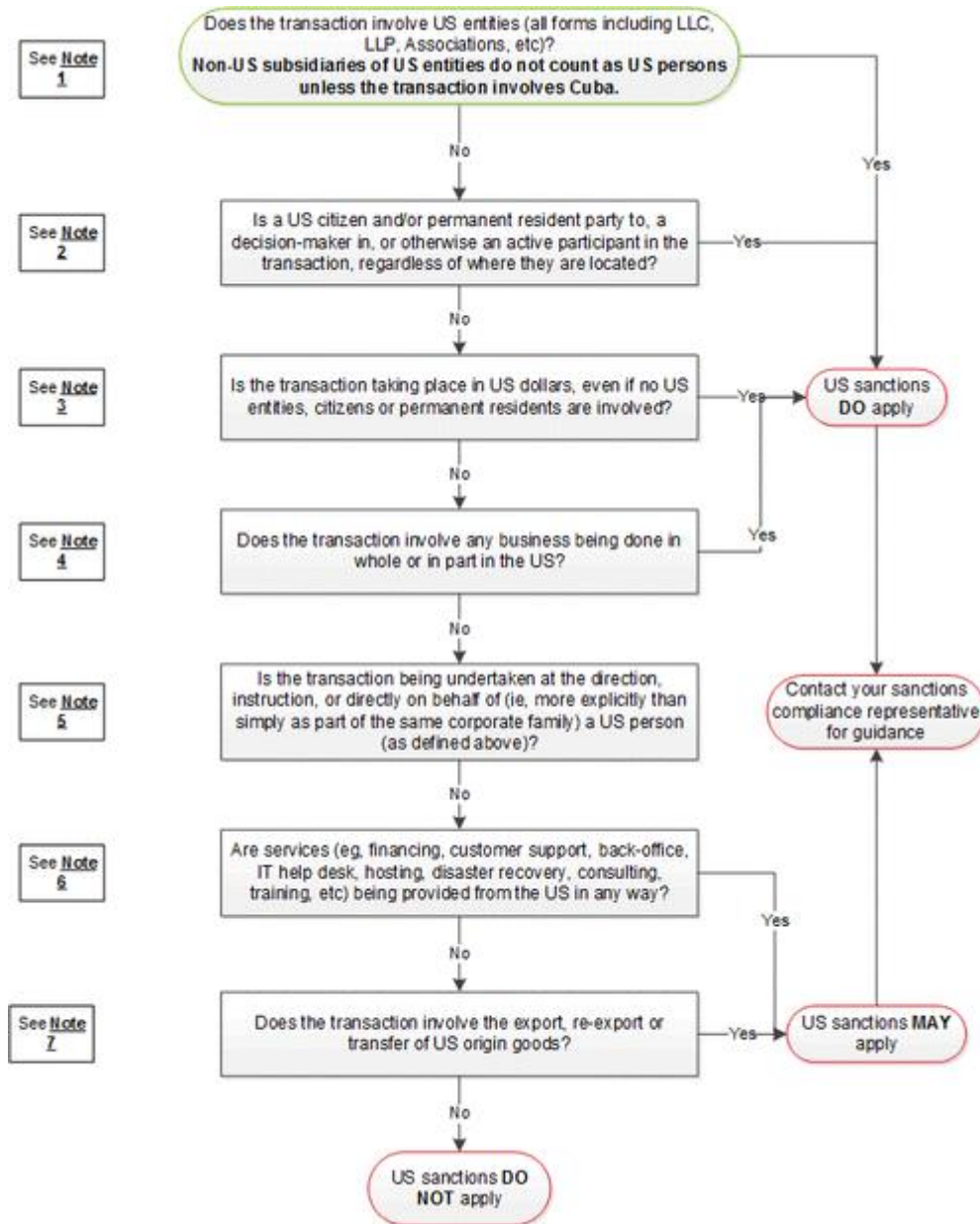
9.4 Each employee should seek guidance from their SCM or Luxfer's General Counsel when in doubt about his or her responsibilities under this policy.

## **10 Reporting concerns**

Anybody who becomes aware of a sanctions or export law violation should immediately report the concern to: (i) the SCM; (ii) Luxfer's General Counsel; or (iii) the anonymous hotline. Please refer to the Luxfer Whistleblowing Policy for further information about anonymous reporting and for details of the hotline telephone numbers. ***Luxfer will not tolerate any form of retaliation against any employee who reports a violation in good faith, even if the reported matter is ultimately determined not to be a violation.***

**APPENDIX 1  
DECISION TREES**

**US DECISION TREE**



**NOTES**

The following notes explain why each question is asked and why affirmative answers may lead to the potential applicability of sanctions. For additional clarification, please contact your SCM.

**NOTE 1—US ENTITIES**

<i>Legal entities</i>	<i>All US sanctions programs apply directly to entities incorporated in the United States or any of its territories and to their activities anywhere in the world. This includes non-US branches or offices of US entities (i.e., establishments of a US entity that are not separately incorporated in the non-US jurisdiction).</i>
<i>Non-US subsidiaries of US entities</i>	<i>US sanctions on Cuba apply directly to the activities of all entities that are directly or ultimately (i.e., through one or more intermediaries) owned or controlled by US persons anywhere in the world. Since January 16 2016, US sanctions on Iran do not directly prohibit non-US subsidiaries of US entities from undertaking most Iran-related activities provided no US persons or ‘touch-points’ described below are involved. Similarly, other US sanctions programs do not apply directly to non-US subsidiaries, unless one of the other jurisdictional ‘touch-points’ applies.</i>

**NOTE 2—CITIZENS, PERMANENT RESIDENTS, AND PERSONS IN THE TERRITORY**

*All US sanctions programs apply directly to all US citizens or permanent residents, wherever in the world they are located. The Office of Foreign Assets Control (OFAC) also has jurisdiction over all persons in the US, even temporarily. Thus, a US citizen or permanent resident employed by a non-US entity and living in a third country, or a non-US citizen located in the US, would be subject to personal OFAC compliance obligations. Any US person would need to be formally ‘recused’ from any transactions with sanctioned persons or embargoed jurisdictions.*

**NOTE 3—CURRENCY**

*Almost all US dollar denominated transactions in the traditional financial system flow through US-based correspondent accounts. OFAC will assert jurisdiction over the US correspondent account and the US financial institution maintaining it. OFAC will also assert jurisdiction over any non-US persons participating in the transaction on the basis that the non-US person caused a potential sanctions breach by sending the transaction through the US financial system. This is the primary basis on which OFAC has asserted jurisdiction in its recent enforcement actions over European financial institutions.*

**NOTE 4—TRANSACTIONS WITHIN THE TERRITORY**

*OFAC will assert jurisdiction over all transactions that take place in the US, whether in whole or in part.*

**NOTE 5—TRANSACTIONS AT THE DIRECTION OF OTHER PERSONS**

*OFAC will assert jurisdiction over all transactions undertaken at the direction of US persons. This includes, for example, transactions by non-US subsidiaries that are undertaken at the request of, or on behalf of, a US based parent company. It also includes all transactions in*

*which a US person undertakes any type of action to facilitate a non-US person undertaking a transaction that could not be undertaken by a US person.*

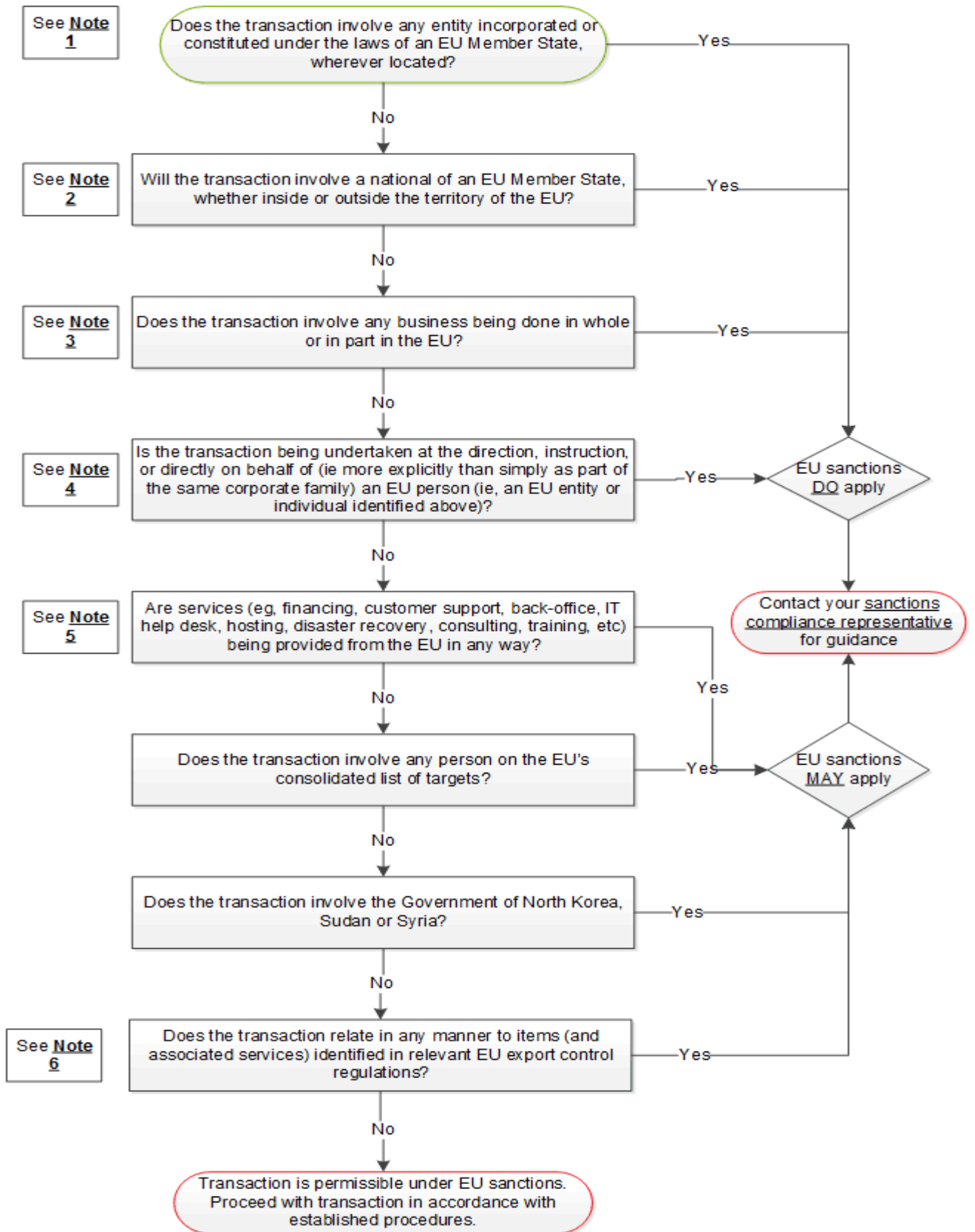
**NOTE 6—SERVICES**

*Any US-based service can potentially bring a transaction within US jurisdiction. This includes US-based approvals for non-US transactions, US insurance, US call centres, and/or US back-office support. OFAC will assert direct jurisdiction over any US person involved in the US-based service. OFAC may also assert jurisdiction over any non-US person involved in the transaction on the basis that the non-US person caused a US person to breach sanctions (the same theory it employs with respect to US dollars as described above).*

**NOTE 7—GOODS**

*In general, US-origin goods are subject to US export controls administered by the US Departments of Commerce and State. However, separately, OFAC generally prohibits the provision of any goods by a US person to sanctioned persons and/or embargoed countries. OFAC can assert primary jurisdiction over any US person involved in the transaction and can assert jurisdiction over non-US persons involved in a US export on a basis that they caused a sanctions breach.*

**EU DECISION TREE**



## NOTES

The following notes explain why each question is asked and why affirmative answers may lead to potential applicability of sanctions. For additional clarification, please contact your SCM.

### NOTE 1—LEGAL ENTITIES

EU sanctions apply to all legal persons or entities located inside or outside the EU which are incorporated under the laws of a Member State. The EU does not extend its sanctions directly to non-EU subsidiaries of EU companies, unless a separate jurisdictional nexus applies.

### NOTE 2—CITIZENS, PERMANENT RESIDENTS, AND PERSONS IN THE TERRITORY

The EU exercises jurisdiction over any national of an EU Member State located inside or outside the EU. The EU also exercises jurisdiction over any individual within the EU.

### NOTE 3—TRANSACTIONS WITHIN THE TERRITORY

The EU asserts jurisdiction over all transactions that take place in whole, or in part, within the Union territory, including its airspace.

### NOTE 4—TRANSACTIONS AT THE DIRECTION OF OTHER PERSONS

The EU will exercise jurisdiction over any EU person undertaking a transaction to circumvent or otherwise facilitate the circumvention of sanctions.

### NOTE 5—SERVICES

The EU will assert direct jurisdiction over any EU person involved in the provision of services to sanctioned persons or entities. Such services include EU-based approvals for non-EU transactions, EU insurance, EU call centres, and/or EU back-office support. To date, the EU has not applied a similarly broad jurisdiction over non-EU entities that may 'cause' a sanctions breach.

### NOTE 6—GOODS

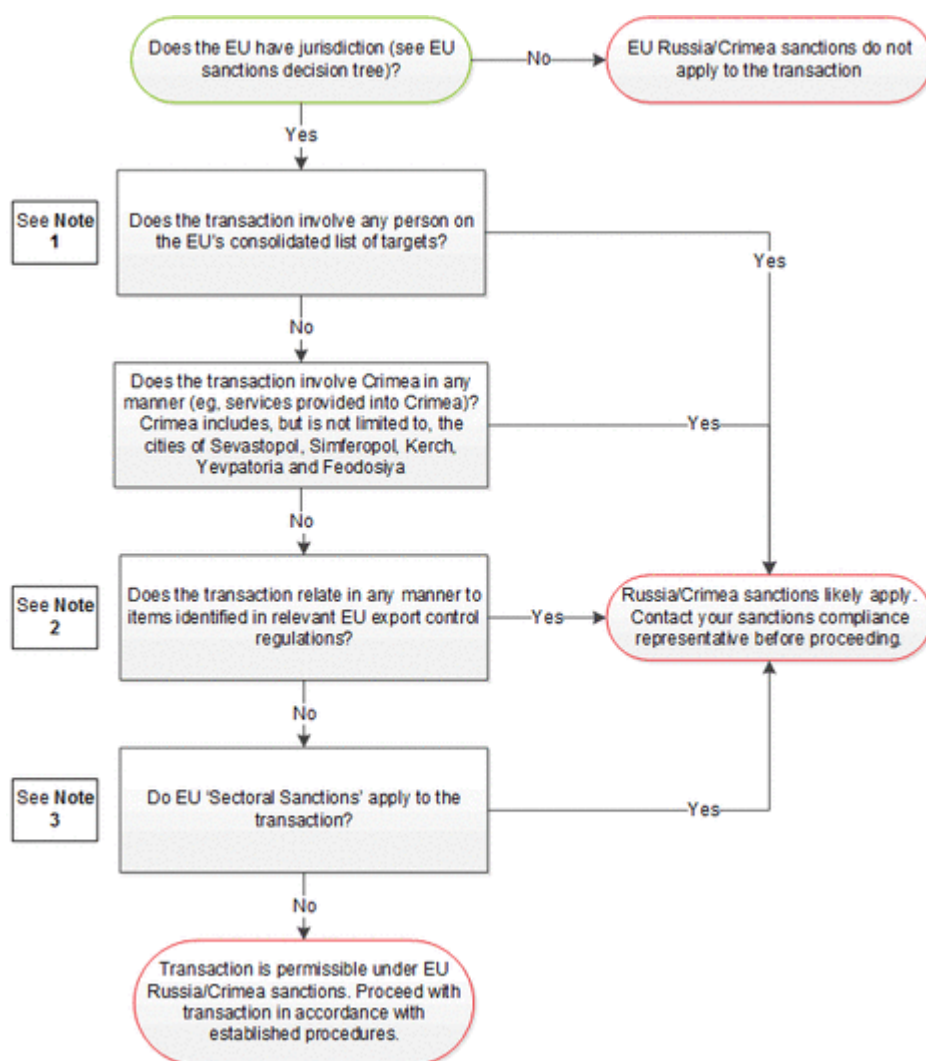
A similar analysis applies with respect to goods. The EU imposes its own export control regime for all EU-origin items as well as all items transiting the EU. With respect to sanctions, the EU will apply jurisdiction directly to any EU person involved in the provision of goods to sanctioned jurisdictions. To date, the EU has not applied a similarly broad jurisdiction over non-EU entities that may 'cause' a sanctions breach.

Specifically, for countries embargoed under EU sanctions regulations:

<i>Iran</i>	<ul style="list-style-type: none"><li>—items identified on the EU Common Military List</li><li>—items identified by the Nuclear Suppliers Group list</li><li>—certain dual-use goods that could contribute to reprocessing or enrichment-related activities</li><li>—items on the Military Technology Control Regime list</li><li>—raw or semi-finished metals</li><li>—enterprise planning software for nuclear and military industries</li></ul>
<i>North Korea</i>	<ul style="list-style-type: none"><li>—arms and related material</li><li>—Korean banknotes and coins</li></ul>

	<ul style="list-style-type: none"> <li>—luxury goods</li> <li>—gold, precious metals and diamonds</li> <li>—items that could support North Korea’s nuclear, ballistic missile or other weapons of mass destruction programs</li> </ul>
<i>Sudan</i>	<i>Items identified on the EU Common Military List or on the EU dual-use list used for military purposes</i>
<i>Syria</i>	<ul style="list-style-type: none"> <li>—items that might be used for internal repression</li> <li>—telecommunications monitoring equipment</li> <li>—crude oil and natural gas related exploration and production</li> <li>—steam and gas turbines</li> <li>—gold, precious metals and diamonds; luxury goods</li> <li>—cultural, archaeological and other products</li> </ul>

## RUSSIA & CRIMEA DECISION TREE



### NOTES

The following notes explain why each question is asked and why affirmative answers may lead to potential applicability of sanctions. For additional clarification, please contact your SCM.

#### NOTE 1—SCREEN

Screening required on individuals/entities involved in transaction -undertake due diligence.

#### NOTE 2—GOODS AND SERVICES

Generally related to goods (and associated services) identified on the EU Common Military List or on the EU dual-use list used for military purposes.

#### NOTE 3—TRANSACTION

Sectorial sanctions will apply if the transaction involves:

- an entity subject to EU Sectorial Sanctions, **and** either (i) the provision of investment services, transferable securities, money market instruments, or loans or credit with a maturity exceeding 30 days, to the identified entity (note: payment terms are not considered loans or credit) or (ii) support (in any manner) for the exploration or production of oil from Arctic offshore, shale or deep-water locations.