Australian Banking Association

December 2021

ABA Sanctions Guidelines

A guide for industry practice

Australian Banking Association, PO Box H218, Australia Square NSW 1215 | +61 2 8298 0417 | ausbanking.org.au

Australian Banking Association

Table of Contents

Australian Banking Association

1. Introduction

The ABA Sanctions Guidelines (Guidelines) are intended to provide a set of good industry practices for Australian Banking Association (ABA) Member banks (Members) in meeting their legal and regulatory obligations. Non-Members and other members of the Australian financial services industry may also benefit from the Guidelines.

The Guidelines are not legally binding, nor are they approved by Australian regulatory bodies or the Department of Foreign Affairs and Trade (DFAT). However, they have been developed in consultation with regulators, and set out industry good practice domestic sanctions requirements and incorporate global regulatory guidance. Members should therefore adopt into their Sanctions Compliance Framework elements of these Guidelines which are in keeping with their risk profile, having regard to the nature, size and complexity of their business.

These Guidelines are limited to obligations applicable to Australian financial institutions under Australian sanctions laws administered by DFAT. They have nevertheless been developed with reference to the broader Australian legislative and regulatory framework, including but not limited to obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) and Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (AML/CTF Rules), which are the subject of separate industry guidance. While these guidelines reflect sanctions regulation, organisations should ensure they also consider obligations under the AML/CTF Act, including overlap between certain sanctions requirements and anti-money laundering and counter-terrorism financing obligations and suspicious matter report (SMR) obligations triggered in relation to contraventions or attempted contraventions of Australian sanctions laws. Organisations should also consider the sanctions obligations imposed by other jurisdictions where applicable.

As the Guidelines leverage the Wolfsberg Guidance on Sanctions Screening, it is recommended both documents be read in conjunction with each other. There may be other guidance, obligations, and/or requirements that members will need to consider having regard to the nature, size and complexity of their business.

Members are also encouraged to be familiar with relevant Financial Action Task Force (FATF) guidance such as Guidance on Proliferation Financing Risk Assessment and Mitigation which urges private sector entities to have in place processes to identify, assess, monitor and manage proliferation financing risks, adding that private sector entities may do so within the framework of their existing targeted financial sanctions and/or compliance programmes.[1]

Members should also refer to the various resources and fact sheets available on the Australian Department of Foreign Affairs and Trade, Australian Sanction Office (ASO) website.[2]

2. Sanctions Overview

Sanctions are measures not involving the use of armed force that are imposed in situations of international concern.

Australia implements two types of sanctions:

1. United Nations Security Council sanctions (often referred to as multilateral sanctions), which Australia must impose as a member of the United Nations. United Nations Security Council sanctions are implemented by means of regulations made under the *Charter of the United Nations Act 1945* (Cth) (COTUNA), and
2. Australian autonomous sanctions which are imposed as a matter of Australian foreign policy. Autonomous sanctions are implemented by means of the *Autonomous Sanctions Regulations 2011* made under the *Autonomous Sanctions Act 2011* (Cth).

[1] INTERNATIONAL BEST PRACTICES (fatf-gafi.org) page 3 para 1 and Guidance on Proliferation Financing Risk Assessment and Mitigation (fatf-gafi.org) page 3 para 2

[2] Australia and sanctions | Australian Government Department of Foreign Affairs and Trade (dfat.gov.au)

Examples of sanctions measures which may be relevant to the Australian banking industry include:

- Targeted financial sanctions (including asset freezes) on designated persons and entities
- Restrictions on trade in goods and services (including 'arms or related materiel'), and or
- Restrictions on engaging in certain commercial activities.

Australian sanctions laws apply to all activities in Australia as well as to all activities undertaken by Australian citizens and Australian registered bodies corporate overseas. It follows that these Guidelines developed for ABA Members will also capture all activities of all persons in Australia as well as the activities of Australian citizens and Australian registered bodies corporate overseas.

The consequences of failure to comply with Australian Sanctions are serious for individuals and bodies corporate. Sanctions offences are strict liability offences for bodies corporate, meaning that it is not necessary to prove any fault element (intent, knowledge, recklessness or negligence) for a body corporate to be found guilty. On this basis, and because sanctions laws reflect UN efforts to engender international peace and security and Australian Government foreign policy, compliance with sanctions laws is considered part of corporate and social responsibility good practice.

2.1 Designated Persons/entities

Australian sanctions laws include targeted financial sanctions which prohibit persons from making assets available to 'designated persons and entities', and from dealing with or using their assets (freezable or controlled assets). The DFAT Consolidated List contains the names of all persons and entities designated under Australian sanctions law.

The DFAT Consolidated List is available on the DFAT website: http://dfat.gov.au/international-relations/security/sanctions/Pages/consolidated-list.aspx. The List changes frequently and Members should monitor for updates on a regular basis. Members can also subscribe to the Australian Sanctions Office's mailing list to receive notifications on updates to DFAT's Consolidated List.

Members should be aware that certain targeted financial sanctions apply to non-designated persons or entities acting at the direction of or on behalf of designated persons, and to non-designated entities that are owned or controlled by designated persons.[3]

2.2 Asset Freezing, Screening, Transaction Monitoring and Reporting

Where Members become aware that they hold freezable or controlled assets, Members are legally required to provide the Australian Federal Police with specific information about the assets under the *Charter of the United Nations (Dealing with Assets) Regulations 2008 and the Autonomous Sanctions Regulations 2011*. Members should also inform DFAT's Australian Sanctions Office (ASO).

Members' AML/CTF Programs should effectively identify, mitigate and manage money laundering and terrorism financing risk, including where such risks arise from the potential breach, non-implementation, or evasion of sanctions obligations. In particular, members should ensure that their Screening and Transaction Monitoring Programs include appropriate risk-based systems and controls, including to identify any transactions or attempted transactions that may be relevant to the investigation of a sanctions offence and which trigger an obligation to submit a suspicious matter report (SMR) to AUSTRAC. It is important to regularly assess the design and effectiveness of these controls in mitigating the sanctions risks.

2.3 Permits

In certain circumstances, a bank's customer may apply to the Minister for Foreign Affairs (or the Minister's delegate) for a sanctions permit to authorise activities, such as a transaction or making a

[3] Some jurisdictions further specify a default rule to determine the scope of ownership and control, such as the UK, EU or the US. In the US, for example, any entity that is 50% or more owned or controlled by sanctioned persons is also itself sanctioned. It is not clear whether such a rule applies under Australian law or regulations, and there is no guidance issued by Australian regulators on this point.

facility or finance available, that would otherwise be prohibited under Australian sanctions law. Members should consider the processes they have in place when a customer seeks to undertake an activity which requires one or multiple sanctions permits.

While there is no exhaustive definition in law of *arms* or *related materiel*,[4] restricted goods or services that a bank's customer may seek to import or export can include equipment, weapons, military vehicles, spare parts, computer technology or software related to such items. A good starting point is to check whether goods are listed on the Defence and Strategic Goods List which sets out various goods, software or technology subject to Defence Export Controls.[5]

Before a Member provides financial services to a customer that could result in a breach of a sanctions law, the Member should obtain from the customer full details of the transaction and a copy of the sanctions permit. Members are not required to facilitate transactions/relationships outside of their risk appetite even if there is an applicable sanctions permit.

When seeking the transaction details and sanctions permit, it is good practice for the Member to:

- confirm the authenticity of the permit with the ASO if this is in doubt
- check that the counterparty holding the permit is the party to whom it was issued
- check that the details of the permit correspond with the details of the transaction and documentation provided by the customer, and that the permit remains current
- ensure that the permit includes the Member as a party to the relevant transaction (either by name or by description), and if it does not, either apply to the ASO for a permit for the financial services relating to the permitted transaction or request the customer to seek an amendment to the original permit to include the Member as a party to the transaction.

Any discrepancy should be investigated and where appropriate reported to the ASO. Where the Member suspects that the discrepancy may be relevant to the investigation of an offence, the Member should submit a suspicious matter report to AUSTRAC.

2.4 Offences and Penalties

Banks are subject to sanctions offences including the following, unless otherwise authorised:

- Making an asset available to designated persons or entities
- Dealing with or using freezable or controlled assets, and
- Providing financial services in relation to activities subject to sanctions.

These offences are strict liability offences for bodies corporate (including banks), meaning that it is not necessary to prove any fault element (intent, knowledge, recklessness or negligence) for a body corporate to establish an offence. A defence is however available for bodies corporate that can prove they took reasonable precautions and exercised due diligence to avoid contravening the relevant law.

Members should have in place procedures to manage the risk of breach, non-implementation or evasion of Australian sanctions law. Inadequate due diligence by an employee could leave both the employee and the employer open to prosecution if the employee's actions were judged to be reckless. This includes individual criminal liability for employees, even if the proven application of due diligence and reasonable precautions exonerates the employer. In addition, where an employee does not meet the threshold for recklessness, the employer may be found liable if it is shown that the employer failed to take reasonable precautions or exercise due diligence.

These guidelines provide advice to Members in relation to what may constitute reasonable precautions and due diligence for the purposes of a defence to the offences under Australian sanctions law.

[4] Factsheet: Arms or Related Matériel | Australian Government Department of Foreign Affairs and Trade (dfat.gov.au)
[5] Defence Export Controls (DEC) regulates the export and supply of military and dual-use goods and technologies. See here for more information: https://www1.defence.gov.au/business-industry/export/controls

2.5 Extra Territorial Considerations

Members should ensure that their sanctions compliance frameworks cover the sanctions laws of foreign jurisdictions that may apply to their foreign branches and subsidiaries (such as sales or representative offices), or where there may be an extra-territorial impact on the Member.

In conducting payment screening, Members should consider the facts of each transaction. The facts of a transaction may include indications that the recipient could be in an industry or geography where sanctions concerns are likely heightened, for example a shipping company in North Asia or a mining company in Africa. Alternatively, the data available in the transaction payment text or instructions may indicate a nexus to various jurisdictions, which in turn may (depending on the nature of the nexus) bring the sanctions laws of those various jurisdictions to bear on the transaction.

In particular, Members should be aware of the extra-territorial considerations when dealing with the United States. Transactions that involve a US Person or the US financial system may activate the jurisdiction of the US for sanctions purposes, even though those transactions may originate and end outside the US (e.g., USD denominated transactions cleared in the US).

Also, US "secondary sanctions" may apply even where there is no effective nexus with the US – simply dealing with certain US sanctioned jurisdictions, designated persons or industries may activate these extra-territorial sanctions whether a US element exists in the transaction or not.

2.6 Sector-specific sanctions

Australia imposes sector-specific sanctions. These sanctions are usually imposed on a specific sector of the economy of a sanctioned jurisdiction, in respect of certain activities only. For example, sanctions may prohibit certain activities being undertaken with named members of certain industry sectors, such as finance, energy and defence, in a particular jurisdiction.

Members' sanctions compliance frameworks should distinguish between sector-specific sanctions and other targeted financial sanctions, such as asset freezes.

3. Due Diligence and Know Your Customer (KYC)

Customer due diligence, to know your customer, requires collecting information about a customer, and checking it to confirm that the customer, and where applicable, a person connected to the customer (e.g. the beneficial owner or an ultimate controller or persons acting on behalf of the customer), is not a designated person. When providing AML/CTF Act designated services, customer due diligence must be conducted in line with requirements under the AML/CTF Act and Rules and where sanctions risks are higher, the Member should consider applying enhanced customer due diligence where required under the AML/CTF Act. In addition you may wish to consider additional due diligence from a sanctions perspective where appropriate

It should be noted that Member banks may provide services to customers which lie outside of the obligations of the AML/CTF Act and Rules. It is not expected that in those circumstances additional information should be collected beyond that which is already obtained during the normal course of business, or which is specified in any existent regulatory guidance, unless the assessment of sanctions risk undertaken by the business for such non-designated services indicates that a higher risk may warrant additional information collection.

Consistent with this, sanctions due diligence will vary depending on the individual Member's organisational risk profile, customer base demographic, physical and operational location and domestic and international regulatory obligations.

Members' sanctions compliance frameworks should have regard for the risk presented by customer relationships and customer activities, including transactional activity. The sanctions compliance framework should be designed to identify, manage and mitigate sanctions risks end-to-end and throughout the customer relationship and life cycle.

3.1 Assessing Customer, Vendor, Connected Parties' and Beneficial Owner Sanctions Risk

Members should consider the criteria to be factored into a customer/vendor/connected party sanctions risk assessment, including but not limited to industry sector, geography, product type and customer/relationship type. These criteria should ideally be reflected in an enterprise-wide or group-level sanctions risk assessment. In some instances, customers and connected parties will require more due diligence.

A Member may consider a customer, vendor or connected party to be a higher risk from a sanctions perspective and subject to enhanced sanctions due diligence if that customer/vendor/connected party:

- has substantive business activity involving sanctioned countries or regions
- operates in an industry or sector that involves goods or services which, if provided to a particular sanctioned country, region, person or entity, would be subject to sanction restrictions, and/or
- is an entity that is domiciled or registered in a sanctioned country/region

Having regard to sanctions risks associated with customers, vendors or connected parties, Members should, during the establishment of the relationship, collect the names of beneficial owners of the customers, vendors or connected parties, in line with their AML/CTF Programs or other Financial Crime Programs (e.g. Anti-Bribery and Anti-Corruption (ABAC) compliance programs).

Member vendor and connected party relationships may also present sanctions risks. Appropriate due diligence processes to identify and assess these risks should be in place. Ordinarily, these would be in keeping with the due diligence and KYC procedures applied to customer relationships, appropriately designed to address the uniqueness of vendor and connected party relationships.

Members should also have risk-based processes in place to periodically update the details of names of beneficial owners and controllers as collected.

4. Sanctions Screening

Sanctions screening is not mandated by law. Rather sanctions screening is a tool which assists Members to comply with sanctions laws and may form part of risk-based systems and controls to identify, mitigate and manage the risk of breaching sanctions laws and to support Members' in meeting their obligations to submit SMRs. As a result, Members should assess their risk of breaching sanctions laws based on their location(s), size, business, customer types, products, delivery channels, geographic risks and other relevant factors and adopt a sanctions screening regime that is most likely to assist them in complying with obligations under applicable sanctions laws.

This risk-based and highly individualised approach to sanctions screening means that Members may in some instances adopt similar approaches to sanctions screening, while differing in others. By way of example, while there is broad industry consensus regarding some aspects of payment screening (such as the need to sanctions screen international transactions) there are differences of opinion regarding other things (such as sanctions screening of domestic transactions).

It is generally accepted that Members should sanctions screen two data sources, being transaction and reference data. Transaction data is the data contained in payment instructions / messages and trade transactions. Reference data includes all other data known to Members, which may be relevant to complying with sanctions laws. It includes customer data but may also extend to employee data, vendor data, and other information in the Member's records which could, if screened, mitigate against breaches of sanctions laws. In line with the risk-based approach to screening, Members may elect to screen as many or as few relevant transaction data elements and reference data elements as reasonably necessary to mitigate their sanctions risks.

Despite the divergence in approaches to sanctions screening by Members, the Wolfsberg Guidance on

Sanctions Screening is generally regarded as best practice for sanctions screening. It contains valuable insights into:

- what constitutes sanctions screening
- the place for sanctions screening as part of a wider integrated financial crime compliance programme
- screening technology and generating productive alerts
- reference data screening
- transaction data screening
- list management, and
- lookbacks.

The Wolfsberg Guidance on Sanctions Screening (as amended) forms part of these Guidelines.

4.1 Screening Timing, Methods and Considerations

Screening can take many forms, from basic methodologies to more sophisticated algorithms. As a result, screening can be automated or manual, use exact name matching or fuzzy matching logic. Members should consider the screening methods that are appropriate for the scale and risk faced by their institution.

Members may design their own screening solutions which should be applicable to transaction data and reference data. These solutions should consider:

- The operational context within which transactions are presented, i.e., real-time, near real-time and/or batch processing
- The inherent and residual risks within the customer base such that these inform the level and/or likelihood of sanctions risks present in business and transactional activity
- The product and/or channel parameters that influence the way in which a screening capability can be designed such as source data, including rich text format and overlay service information, and whether that is helpful to identifying sanctions risks and consequently the sensitivity of detection rules and thresholds
- The means through which it may be possible to identify re-submitted transactions or transactions that have been subject to text manipulation and/or stripping
- Other compliance frameworks that may supplement and support the Member's sanctions compliance framework, for example correspondent banking due diligence activities
- Legislative and regulatory frameworks that may supplement and support the Member's sanctions compliance framework and obligations incumbent within those frameworks, such as customer due diligence obligations under the AML/CTF Act
- Standardised procedures including escalation models for due diligence activities related to domestic and cross-border transactions
- Enhanced monitoring to determine the customer, vendor, connected party, or employee and/or transactions that require enhanced levels of investigation and developing specific escalation processes
- Consideration of measures such as whitelisting or system rules to appropriately manage false positive volumes, and
- Quality assurance and data integrity checks as part of the internal compliance management arrangements.

4.2 Transaction/Payment Screening

At a minimum Members should screen the names of the payer, payee and each intermediary recorded in international payments against designated person lists. Members should consider whether it is appropriate to screen other payment instruction/message fields to identify links to jurisdictions or activities sanctioned by Australia or other relevant jurisdictions.

To support sanctions screening activities across the industry, and in keeping with payments systems rules and guidelines, Members should ensure that all outward payment instructions / messages they create contain all available name and relevant address information for beneficiary, remitter and intermediaries, using Latin characters and verified KYC details where possible. Consideration should be given to the approach to screening payment instructions that contain non-Latin characters.

Where beneficiary and remitter information is missing from an inward payment message / instruction, Members should consider how to mitigate sanctions risk, particularly where involving jurisdictions subject to sanctions or higher diversion risk.

Where multiple transfers are bundled into a single batch file, the payment instruction / message may not contain the beneficiary and remitter information or full transparency of the end-to-end payment. Members' risk assessment and controls should take account of the risk of such payments being for the purpose of sanctioned activity.

4.3 Trade Transaction Screening

Members should consider the various forms of information presented to an institution during a trade transaction that could be screened, for example, trade SWIFT messages as well as the content of trade documentation received in the normal course of business. Information in trade documentation, in addition to names of all involved parties, that may assist in identifying potential sanctions risks for further assessment include such things as dual-use goods, shipping routes/methods/vessels/goods and red flags, such as transhipment.

4.4 Customer/Name Screening

Members should consider the industry wide practice of two-way screening of customers. Customer screening should take into consideration changes to data and list information, the frequency of periodic screening and the justification for the chosen frequency. The industry appears to be moving towards two-way daily or weekly periodic screening.

Generally, new customers should be screened before providing services as well as when there is any material change to the customer record. However, in circumstances where it is not reasonably possible to screen customers before providing services, Members should ensure they take reasonable measures to mitigate any potential breach of sanctions laws. Periodic re-screening should be the standard y for all Australian financial institutions, with more frequent re-screening being more appropriate for those with greater sanctions risk.[6]

Members should screen the names of customers, beneficial owners, associated parties, employees, and vendors against designated person lists during the establishment of a relationship or account, and on an ongoing basis over the course of the relationship.

[6] A Delta-Delta screening refers to the practice of rescreening a customer base when there is a change to the regulator list to identify new customers identified, and a rescreening when there has been a change to customer's profile (new/changed information to an existing record or the creation of a new record). True Delta-Delta screening would occur daily on either of the two triggers. Where Delta-Delta is not happening, Members should at a minimum implement institutional wide screening (i.e., rather than just new records) at a frequency matching their risk to identify any potential sanctions risks.

5. Sanctions Alert Management

5.1 Requests for Information (RFI) and Customer Contact

Members should consider screening scenarios where further information is required to determine a potential true match alert. This may include RFI sent to other financial institutions. Members should consider their approach to share information with financial institutions to assist in sanctions investigations where permitted under AML/CTF and privacy regulations. Members should consider their approach for customer contact, including whether questions asked are to be specific to the alert or follow a generic template. When asking sanctions related questions, Members should consider the risk of exposing internal processes that would assist users of the financial system to process transactions in breach of sanctions laws and avoid detection and the AML/CTF tipping off provisions in their interaction with customers.

It should be noted, however, that conducting reasonable inquiries into customer activity that may be unusual is not by itself considered 'tipping off' and Members should use their judgement in communicating with customers to avoid any conclusions being drawn that a transaction or customer may become the subject of an SMR. AUSTRAC has provided guidance to clarify that asking a customer for more information, including about their identity or the source or destination of their funds, is not considered 'tipping off' in and of itself, and can often be managed in a way that avoids this.[7]

5.2 Potential Matches and False Positives

Members should consider putting minimum standards in place for reviewing alerts generated from sanctions screening activities and disposing of false positives. These may differ depending on the Member's risk appetite and customer base, but for individual customers as an example, could include name, residential address and date of birth differences. Members should ensure that records of completed due diligence adequately set out the factors informing final alert decisions.

5.3 True Matches

Members should consider the timeframe for actions taken after a true match is confirmed to ensure that these are reasonable and in keeping with regulatory obligations such as asset freezing or the submission of terrorism related SMRs. Actions may include confirming the true match at an appropriate management level, undertaking additional customer due diligence, reporting the true match internally or externally as required, and freezing assets.

5.4 Freezing Assets and Accounts

Members should consider their process for managing frozen accounts and assets, including but not limited to reporting and transferring of funds (where they are subject to action under State or Commonwealth proceeds of crime legislation) and reporting to regulatory bodies. Members should be aware of their reporting obligations.

Members must have processes in place to consider requests regarding the dealing with or use of freezable and controlled assets for basic expenses, legally required dealings, contractual dealings, required payment dealings or extraordinary expense dealings. Such dealings can only be authorised by a sanctions permit issued by the ASO.

Where Members become aware that they hold freezable or controlled assets, Members are legally required to provide the AFP with information about the asset. Members should also inform the ASO, and give consideration as to whether a suspicious matter arises and any obligation to submit a report to AUSTRAC.

[7] Tipping off | AUSTRAC

Notwithstanding whether a name match is a true match or a false positive, following a sanctions alert investigation, Members should still separately consider whether the facts of the transaction are anomalous, out of normal behaviour for the customer or are otherwise unusual and consider conducting Enhanced Due Diligence or submitting a Suspicious Matter Report as appropriate.

6. Quality Assurance

Members should ensure they have appropriate and independent quality assurance processes in place to monitor the adequacy and effectiveness of sanctions processes and decision making on an ongoing basis. As detailed further in Section 8, assurance should be conducted in adherence with requirements set out in the Member's policy documents, procedures and standards. Assurance activities should consider appropriate sample sizes and provide inform regular feedback to front-line staff through forums and communications and/or refresher training sessions.

7. Circumvention of Sanctions

Members should be aware of the various forms that sanctions circumvention can take, including structuring of transactions, deleting, omitting, or concealing information (also known as stripping), or resubmitting transactions. There is an obligation on Members, staff, and customers to provide accurate information that is not deliberately changed, false or misleading.

Members must not knowingly structure transactions, or give instructions to customers, in a way that would result in the avoidance of sanctions prohibitions or restrictions or result in the concealment of activity in breach of sanctions laws. Members should provide appropriate staff training on how to identify and escalate potential sanctions evasion and attempts to resubmit payment instructions to their relevant compliance departments. Members should consider the benefits of system screening controls which detect potential stripping and resubmission attempts.

Members should consider what processes they have in place to ensure timely and appropriate senior escalation of suspected or actual sanctions evasion including the submission of SMRs. Further consideration could also be given to customer education in terms of the Member's policies on sanctions compliance.

Where a Member is concerned that the financial services it is providing are being used to avoid, circumvent, or conceal activity that may breach sanctions, the Member should consult their own legal advisors or the relevant government agency. Sanctions breaches should be reported as required by local and foreign laws.

8. Governance, Oversight, Training and Record Keeping

8.1 Senior Management Governance and Oversight

Member Boards, Executives and Senior Management should be committed to compliance with sanctions laws and foster and communicate a culture of compliance in all respects. This should include making available sufficient human and information technology resources and providing adequate independence and authority to sanctions personnel.

Members should have a documented policy setting out the high-level principles for sanctions risk management, the practical approach taken, and employee responsibilities to ensure compliance with sanctions laws. This may be a standalone policy document or form part of a broader suite of policy documents.

Members should also define the accountabilities of Senior Management in relation to the Sanctions Compliance Framework. Areas for consideration include appropriate levels of senior management decision making, oversight and approval of sanctions policy and procedures. Oversight should include management information that assists with assessing the performance of the controls within the

sanctions framework, with the framework and controls subject to regular and ongoing design and effectiveness testing.

8.2 Staff training

Members should consider enterprise-wide staff training on sanctions risk, specifically covering the institution's sanctions obligations, internal policy and the escalation process for evasion/stripping attempts. Consideration should be given to providing training at the commencement of employment, ongoing training periodically, and additional training to staff with a higher exposure to sanctions risk, such as customer-facing or compliance roles.

8.3 Procedures and Record Keeping

Members should consider maintaining documented procedures designed to identify and manage sanctions risk relevant to the Member and that provide specific practical guidance for employees. Best practice approaches to maintaining procedures include regular review of content to ensure the procedure is designed effectively with respect to the risk to which it is applied, clearly documented approvals at an appropriate management level.

Members might consider including procedure steps on how to comply with information requests from government agencies, and guidance on sharing legally permitted information Members should also consider procedures that specifically comply with information requests from government agencies or other parties involved in the value chain in a timely manner.

When designing procedures Members should consider how decision making and key sanctions matters are evidenced with an audit trail.

9. Outsourcing of Sanctions Controls

Where sanctions controls are outsourced, Members should ensure that the materiality of the outsourcing has been assessed, regulatory notification has been provided where appropriate, and that there is ongoing assurance over the outsourced activity. This should include on-going monitoring, reviews of service level agreements and regular engagement.