

Outsourcing Cayman Islands AML/CFT compliance obligations

Last reviewed: May 2022

Introduction

It is common practice for a managed financial service provider (**FSP**), such as a Cayman Islands mutual fund or private fund (**fund**), to outsource certain anti-money laundering and countering the financing of terrorism (**AML/CFT**) compliance functions to a service provider, such as a fund administrator. This guide provides a practical overview of the relevant steps and considerations which should be borne in mind when an FSP plans to outsource, or is reviewing existing outsourcing arrangements relating to the performance of an AML/CFT compliance function to a service provider.

AML/CFT compliance obligations of FSPs

Within the Cayman Islands AML/CFT framework, the Anti-Money Laundering Regulations (as amended) (the **AML Regulations**) require persons conducting 'relevant financial business'¹ (**RFB**) to establish systems to detect money laundering, terrorist financing and proliferation financing, and therefore assist in the prevention of abuse of their financial products and services.

The Guidance Notes on the Prevention and Detection of Money Laundering, Terrorist Financing and Proliferation Financing in the Cayman Islands (as amended) (the **Guidance Notes**) issued by the Cayman Islands Monetary Authority (**CIMA**) are designed to assist FSPs (ie, all persons conducting RFB) in complying with the AML Regulations. FSPs are expected to follow the Guidance Notes in developing an effective AML/CFT framework suitable to their business and failure to do so may result in the relevant supervisory authority seeking an explanation and/or taking enforcement action under the applicable legislation.

The AML Regulations require FSPs to, amongst other things:

- take measures to prevent and detect money laundering, terrorist financing and proliferation financing;
- establish and maintain appropriate and consistent systems, policies and procedures in order to prevent and report money laundering, terrorist financing and proliferation financing, including establishing and maintaining adequate procedures for:
 - monitoring compliance with, and testing the effectiveness of, its systems and controls (including policies and procedures); and
 - ensuring compliance with targeted financial sanctions applicable in the Cayman Islands;
- appoint an Anti-Money Laundering Compliance Officer (**AMLCO**);
- appoint a Money Laundering Reporting Officer (the **MLRO**) and a Deputy Money Laundering Reporting Officer (the **DMLRO** and, together with the MLRO and the AMLCO, the **AML Officers**) (see below for more detail on AML Officers); and
- establish suspicious activity reporting policies and procedures.²

¹ As defined in the Proceeds of Crime Act (as amended) (the **PCA**).

² See our guide titled '[An introduction to the Cayman AML/CFT regime](#)' for more information.

A breach of the AML Regulations may lead, on summary conviction, to a fine of US\$609,756 or, on conviction on indictment, to a fine and to two years' imprisonment. A breach of certain provisions of the AML Regulations may also lead to administrative fines imposed by CIMA pursuant to the Monetary Authority (Administrative Fines) Regulations (as amended).

Outsourcing of compliance functions

The AML Regulations provide that an FSP may *delegate* the performance of a compliance function to a person or *rely* on a person to perform a compliance function. It should be noted, however, that the FSP will remain ultimately responsible for compliance with the applicable AML/CFT obligations, irrespective of whether the FSP has outsourced the performance of the compliance function to another person.

Delegation vs reliance

The Guidance Notes provide an explanation of CIMA's understanding of the terms 'delegation' and 'reliance' and clarification of CIMA's expectations where a delegation or reliance arrangement is entered into by an FSP.

With a 'delegation', the delegate performs the compliance function in accordance with the internal policies and procedures of the FSP, and not those of the delegate. The delegate would then be subject to the control of the FSP in ensuring the correct and effective implementation of those policies and procedures.

Conversely, in a 'reliance' scenario, the person on whom reliance is being placed would perform the relevant function in accordance with that service provider's own policies and procedures. The FSP must be satisfied that those policies and procedures will enable it to comply with the requirements of the Cayman AML/CFT regime in order to rely upon them. Reliance is the method most commonly used by Cayman Islands investment funds to meet their AML/CFT compliance obligations.

Delegation

The Guidance Notes state that, where an AML/CFT compliance function is *delegated*, the following must be adhered to:

- details of and written evidence of the suitability of the delegate to perform the relevant functions on behalf of the FSP must be made available to CIMA up on request;
- there must be a clear understanding between the FSP and the delegate as to the functions to be performed;
- applicable customer/investor due diligence information must be made available to CIMA on request and to the Cayman Islands Financial Reporting Authority (the **FRA**) and other law enforcement agencies in accordance with the relevant procedures;
- the FSP must satisfy itself on a regular basis as to the reliability of the delegate's systems and procedures; and
- the delegation (or sub-delegation) must comply with the outsourcing principles set out in Section 10C of Part II of the Guidance Notes (the **Outsourcing Principles**).

Outsourcing Principles

The Outsourcing Principles provide certain required controls for outsourcing an AML/CFT compliance function, particularly the outsourcing of the AML Officer functions, including the following:

- each FSP should maintain policies and procedures in relation to outsourcing;
- where an FSP proposes to outsource its compliance function, or the MLRO or DMLRO position, a risk assessment (including country risk) should be conducted prior to entering into the arrangement;
- the FSP must conduct due diligence on the proposed service provider to ensure that the service provider is fit and proper to perform the function in question;
- the outsourcing/service agreement must:
 - clearly set out the parties' obligations;
 - require regular reporting by the service provider to the FSP and ensure that the FSP has access to all information and documentation maintained by the service provider in relation to the outsourced function(s);

- require the service provider to file a suspicious activity report with the FRA if a suspicion arises during the performance of the outsourced activity;
- if sub-contracting is permitted, require that the service provider follows outsourcing standards equivalent to those imposed on the FSP; and
- not be likely to impede access to data without delay due to the imposition of confidentiality, secrecy, privacy or data protection restrictions;
- the FSP should have a contingency plan and an exit strategy in place in case the service provider fails to perform the outsourced function as agreed; and
- where the service provider (or a sub-contractor) operates from a jurisdiction with AML/CFT standards lower than those of the Cayman Islands, the service provider (and any sub-contractor) must adopt and apply the Cayman Islands standards.

The Guidance Notes also refer FSPs to CIMA's Statement of Guidance on Outsourcing (the **Statement of Guidance**) for further guidance.³ The Statement of Guidance, amongst other things, contains detailed provisions relating to the terms which should be included within an outsourcing agreement.

Reliance

Where an FSP will *rely* on a third party to fulfil any AML/CFT function, it is required to:

- ensure that the service provider or other person has adequate and appropriate knowledge and experience to be able to perform the function;
- conduct a risk assessment of the person before entering into any service agreement and, where the person operates from outside the Cayman Islands, document and demonstrate the consideration of country risk;
- enter into a formal service agreement setting out the responsibilities of each party;
- review the policies and procedures of the service provider prior to entering into the service agreement, and test them on an ongoing basis, to ensure that they:
 - are consistent with the nature of the FSP's business;
 - adequate in relation to the function to be performed; and
 - will meet the Cayman Islands AML/CFT standards; and
- where the service provider operates from a jurisdiction with AML/CFT standards lower than those of the Cayman Islands, ensure that the service provider adopts and applies the Cayman Islands AML/CFT standards in the performance of the relevant function.

Intra-group arrangements

Whilst CIMA recognises that an outsourcing arrangement with an FSP's related entity may present fewer risks as compared to an outsourcing arrangement with an unrelated party, the Statement of Guidance sets out certain minimum requirements relating to intra-group outsourcing arrangements. Those requirements include the following:

- a written outsourcing agreement which details, amongst other things, the scope of the arrangement, the services to be supplied, the nature of the relationship between the FSP and the service provider, and procedures governing the subcontracting of services;
- an appropriate business continuity plan that is designed to handle foreseeable risks;
- an appropriate process for monitoring, reporting and oversight;
- an exit strategy from the outsourcing arrangement and ability to choose another outsourcing provider if risk is deemed too high by the FSP's board of directors or general partners (as the case may be);
- location of books and records that will meet legal requirements and be available for review by CIMA;
- the arrangement must be subject to appropriate internal and external audit and risk control measures which are substantially equivalent to those applicable to the FSP; and
- the FSP must follow any additional expectations CIMA may have depending on the risks related to the outsourcing arrangement and the conclusion of any supervisory review conducted by CIMA.

³ Available at <https://www.cima.ky/upimages/commonfiles/1499756196StatementofGuidanceOutsourcingRegulatedEntities.pdf>

Where an FSP is a branch which is covered by outsourcing arrangements entered into by its head office, the Statement of Guidance sets out the minimum details which such branch should receive in a written confirmation. The relevant branch should also assess the applicability of the various elements in the Statement of Guidance bearing in mind the risks posed to its operations and clients by the outsourcing arrangement.

The Guidance Notes further require (amongst other things) that, where an FSP is a branch or subsidiary entity whose business is conducted in accordance with a group-wide AML/CFT programme, a gap analysis should be conducted before relying on the group-wide programme, and whenever any changes are made to the group-wide programme or to applicable AML/CFT obligations, to ensure that the programme complies with the Cayman Islands requirements.

Confidentiality

The Statement of Guidance sets out certain confidentiality duties of FSPs in respect of customer information in an outsourcing arrangement, including, amongst other things, the following:

- an FSP should be satisfied that the service provider has in place policies, procedures and physical and technological measures to protect information that a customer of the FSP might reasonably expect to be confidential;
- an FSP should be satisfied that the service provider has proper safeguards in place for the collection, storage and processing of customers' confidential information and to prevent unauthorised access, misuses or misappropriation;
- an FSP should consider whether it is appropriate to notify customers regarding how it maintains effective control and oversight of the outsourced material function or activity; and
- when an FSP decides to outsource a material function or activity, it should provide prior notification to customers that data or information pertaining to them is to be transmitted to a service provider or a sub-contracted provider, unless terms and conditions of the agreement between the customer and the FSP allow for outsourcing and disclosure to a third party.

A service provider (and any sub-contractor) should also be restricted from:

- using the FSP's proprietary information or customer information unless it is necessary for providing the contracted service;
- making any disclosure to a sub-contracted provider without the prior consent of the FSP and subject to applicable law,

and should be required to notify the FSP (if allowed by applicable law) as soon as practicable prior to any disclosure of customer information being made where that disclosure is required by law.

Conflicts of interest

The Statement of Guidance requires an FSP, which has outsourced a material function, such as compliance function, to a service provider, to properly assess the service provider to identify any conflicts of interest and ensure that preventative measures are taken to manage any such conflicts. An FSP should also ensure that the service provider will periodically review, identify, disclose, monitor and manage all its conflicts of interest with respect to the relevant outsourced activity.

AML Officers

As noted above, the AML Regulations require FSPs to appoint an AMLCO, a MLRO and a DMLRO, and these AML Officers are often provided to Cayman funds by third party service providers. The Guidance Notes provide additional detail on the eligibility requirements relating to the AML Officers, an overview of which is set out below. For details as to the key functions of the AML Officers, please see our guide titled '[An introduction to the Cayman AML/CFT regime](#)'.

AMLCO

An FSP must designate a person at managerial level as its AMLCO to act as the point of contact with the supervisory and other competent authorities in the Cayman Islands. An AMLCO must have the authority and ability to oversee the effectiveness of the FSP's AML/CFT systems, compliance with applicable AML/CFT legislation and guidance, and the day-to-day operation of the AML/CFT policies and procedures.

An AMLCO must be a natural person who is fit and proper to assume the role and who:

- has sufficient skills and experience;
- reports directly to the board of directors of the FSP (the **Board**) or equivalent;
- has sufficient seniority and authority so that the Board reacts to and acts upon any recommendations made;
- has regular contact with the Board so that the Board is able to satisfy itself that statutory obligations are being met and that sufficiently robust measures are being taken to protect the FSP against money laundering or terrorist financing risks;
- has sufficient resources, including sufficient time and, where appropriate, support staff; and
- has unfettered access to all business lines, support departments and information necessary to appropriately perform the AML/CFT compliance function.

MLRO

An FSP must designate a suitably qualified and experienced person as the MLRO at management level, to whom suspicious activity reports (**SARs**) must be made by the staff.

A MLRO must be a natural person who:

- is autonomous (ie, the MLRO is the final decision maker as to whether to file a SAR with the FRA);
- is independent (ie, with no vested interest in the underlying activity);
- has and shall have access to all relevant material in order to make an assessment as to whether activity is or is not suspicious; and
- can dedicate sufficient time for the efficient discharge of the MLRO function, particularly where the MLRO/DMLRO has other professional responsibilities.

An FSP may designate its AMLCO to act as an MLRO, or vice versa, provided the person is competent and has sufficient time to perform both roles efficiently. Where an individual is both an MLRO and AMLCO, that person should understand the roles and responsibilities of each function.

DMLRO

An FSP must also designate a DMLRO who should be a staff member of similar status and experience to the MLRO, to discharge the MLRO functions in the absence of the MLRO.

Contacts

A full list of contacts specialising in Cayman Islands regulatory law can be found [here](#).

This guide is only intended to give a summary and general overview of the subject matter. It is not intended to be comprehensive and does not constitute, and should not be taken to be, legal advice. If you would like legal advice or further information on any issue raised by this guide, please get in touch with one of your usual contacts. You can find out more about us, and access our legal and regulatory notices at [mourant.com](#). © 2022 MOURANT OZANNES ALL RIGHTS RESERVED