Standard Commerce Bank, Ltd.[1]

Anti-Money Laundering & Counter Terrorism Compliance Policy

25 Victoria Street (Corner of Bath Road)
Roseau, Commonwealth of Dominica

Implementation Date: May 2016

Version Number: 1.0

Last Updated: May 2016

Approved By: Alex Silver, Compliance Officer

---

[1] Standard Commerce Bank, Ltd. is referred to as "SCB" or the "Bank" within this document.

Table of Contents

1 Policy Statement

1.1 SCB's Commitment

Standard Commerce Bank, Ltd. ("SCB or the "Bank") is committed to preventing, detecting and deterring money laundering and terrorist financing by adhering to all applicable Commonwealth of Dominica compliance requirements. It is the responsibility of every employee (including contract and part-time employees) to comply with this programme and all related legislation for jurisdictions[2] in which SCB operates.

SCB is a registered and licensed Dominica Bank and adheres to the Bank's AML/CTF Compliance Manual, as well as all regulations pertaining to Anti-Money Laundering and Suppression of the Financing of Terrorism as codified by the Commonwealth of Dominica.

SCB maintains a "Zero Tolerance" policy[3] regarding intentional violations of applicable laws prohibiting money laundering, terrorist financing and related financial crimes, and as such, SCB is committed to the oversight of the Bank's employees, payees, customers and service providers. Therefore, SCB requires the discharge of any employee, payee, or service provider who commits such a violation, and SCB may pursue civil and/or criminal charges, based on the facts and circumstances.

1.2 Compliance Programme

SCB is required to have an Anti-Money Laundering (AML) compliance programme that consists of these five elements:

1) **Written Policies and Procedures**: a document that memorializes SCB's responsibilities under the law and what the Bank is doing to meet them.

2) **A documented Risk Assessment**: a document that describes and assesses the risk that SCB's business could be used to launder money or finance terrorism.

3) **The appointment of a Compliance Officer**: a document that designates an individual ultimately responsible to develop and maintain SCB's AML/CTF compliance programme.

---

[2] SCB is located in Roseau, Dominica.

[3] The Bank will discharge any employee or service provider and close accounts of any payee or customer that commits a violation of either the Commonwealth of Dominica's Statutory Rules and Orders regarding AML/CTF or the Bank's internal policy. Additionally, SCB may take a proactive approach in pursuing civil and/or criminal charges, based on the facts and circumstances. *See* AML/CTF Procedures for Compliance Staff.

4) **AML/CTF Compliance Effectiveness Reviews**: a document that summarizes testing and reporting[4] completed, either annually, or every two years (depending on the jurisdiction) that assesses how well the Bank's compliance programme is working.[5]

5) **Training**: a programme conducted at least annually, to ensure that all staff understand their roles and responsibilities, as per AML/CTF compliance requirements.[6]

The procedures that SCB follows are specific to the Commonwealth of Dominica. If the Bank were to expand operations to jurisdictions that do not have current governing legislation, SCB will apply voluntary compliance measures, based on international compliance standards and best practices, including practices published by the Financial Action Task Force (FATF).

1.3 Operational Compliance

In addition to the Bank's documented programme, SCB is required to maintain operational compliance. This includes collecting and recording Client Identification Programme (CIP) documentation, as well as Customer Due Diligence (CDD) information, reporting certain types of transactions to the Bank's regulators and government agencies, as well as keeping records. All procedures detailed within SCB's procedures are mandatory without exception. Any activity that is conflicting with SCB's AML compliance procedures should be brought to the attention of the Compliance Officer immediately.

2 AML Compliance Basics

Money laundering[7] is the process of taking money obtained by committing a crime and disguising the source to make it appear legitimate. Under the Commonwealth of

---

[4] Regulatory reporting to the Commonwealth of Dominica's Financial Intelligence Unit (FIU). *See*: Section 5.7 AML/CTF Compliance Effectiveness Review.

[5] An assessment to determine the efficacy of the current compliance programme. Results are provided to the FIU of the Commonwealth of Dominica, correspondent banking relationships and certain vendors by the Compliance Officer when and where a request is deemed appropriate.

[6] Pursuant to the 2013 Money Laundering (Prevention) S.R.O. No. 4 Part II Sections 6-7, the Compliance Officer must provide education and training for all SCB directors, employees, including part-time, temporary, and contract employees to raise awareness of the Commonwealth of Dominica's AML/CTF compliance regulations, their "personal obligations under those enactments", the Bank's compliance programme (both policy and procedures), and personal liability for failure to report in accordance with internal procedures. *See*: both SCB's All Staff and Compliance Procedures.

Dominica's 2001 Money Laundering (Prevention) Regulations, supplemented by the 2011 Money Laundering Prevention Act No. 8, as amended by the 2013 Money Laundering (Prevention) Act No. 5 (and No. 2 of 2013), it is illegal to launder money or to knowingly assist in laundering money. Under these Acts, SCB must take steps to be sure that the Bank's business is not used to launder money and if SCB suspects that money laundering may be taking place, the Bank must report it.

Terrorist financing[8] is the process of moving funds in order to pay for terrorist activities. Unlike money laundering, the source of the funds is not always criminal but the intended use of the funds is criminal. Under the Commonwealth of Dominica's Acts, it is illegal to knowingly assist in the financing of terrorism, including the possession of terrorist funds or property. If SCB knows or suspects that the Bank has terrorist property in the Bank's possession, it must be reported immediately.

3 Roles and Responsibilities[9]

Every SCB employee, including part-time, temporary, and contract employees, has a responsibility to ensure that SCB's AML/CTF Compliance Programme is adhered to.

- **Board of Directors and Senior Management**:
  - Overseeing the AML/CTF Compliance Programme;

---

[7] "Money laundering" denotes conduct which constitutes an offence under section 3(1);

"(1) A person who -

(a) receives, possesses, manages or invests; (b) conceals or disguises;
(c) converts or transfers; (d) disposes of, brings into or takes out of Dominica; or (e) engages in a transaction which involves, property that is the proceeds of crime, knowing or believing the property to be the proceeds of crime commits an offence. As amended by the Commonwealth of Dominica's 2013 Money Laundering (Prevention) Act 5." *See also*: 2013 Money Laundering (Prevention) S.R.O. 4 Commonwealth of Dominica.

[7] Dominica Risk & Compliance Report December 2014 pg. 7.

[8] Terrorist financing is funding any act of terrorism or committing any act or omission that facilitates the funding of terrorism.

[9] Addresses the Caribbean Financial Action Task Force's (CFAT's) compliance programme. SCB is required to ensure that the Bank's supervisory and regulatory practices are such within the Caribbean that they act as a deterrent to money laundering and financing of terrorism and proliferation and in cases where it does occur that it can be detected. The Commonwealth of Dominica is a member of the CFATF. In order to assess the status of the anti-money laundering framework of their member countries, both the FATF and the CFATF undertake detailed reviews referred to as mutual evaluations.

- Receiving regular (at least annual) status reports on the AML/CTF Compliance Programme;
- Consulting the Compliance Officer, as needed, where AML or CTF related issues arise;
- Ensuring that the Compliance Officer has the resources to implement and execute an effective AML/CTF Compliance Programme;
- Ensuring that the Compliance Officer is adequately qualified to manage the AML/CTF Compliance Programme (understand Dominica's AML/CTF requirements and SCB's business model); and
- Signing off on the results of completed AML/CTF Compliance Effectiveness Reviews (within thirty (30) days of the issue of the report).

Compliance Officer:

- Developing and maintaining the AML/CTF Compliance Programme and Risk Assessment, which includes regularly reviewing and updating these documents and maintaining a record of all updates;
- Ensuring that all employees and other relevant parties receive appropriate AML/CTF training at least annually;
- Reporting to Senior Management on the status of the AML/CTF Compliance Programme, including any AML/CTF Compliance; Effectiveness Reviews (within thirty (30) days of the issue of the report) and regulatory examinations;
- Overseeing AML/CTF Compliance Effectiveness Reviews and ensuring that the reviewer has sufficient knowledge of Dominica's AML/CTF requirements and SCB's business to conduct the review;
- Maintaining complete and accurate records;
- Maintaining current registration in good standing with Dominica;
- Corresponding with Dominica's regulatory bodies[10];
- Maintaining up to date knowledge of Dominica's AML/CTF compliance requirements, as it applies to SCB's business model; and

[10] The FSU is the authority regulating the SCB's compliance programme, the FIU is the "Unit" to whom the Bank submits all AML/CTR required reporting. FSU - http://fsu.gov.dm/ and FIU - http://fiu.gov.dm/.

- Obtaining appropriate training, including continuing education, in order to develop and maintain knowledge of AML/CTF compliance requirements and industry best practices.

All Employees:

- Complying with the requirements set out in the AML/CTF All Staff Procedure document;
- Reporting certain types of transactions[11] to the Compliance Officer;
- Keeping up to date and accurate customer[12] records;
- Obtaining customer identification when required;
- Completing AML/CTF training when required (at least annually); and
- Identifying and reporting potential money laundering or terrorist financing activities.

If you are not sure what to do to meet these responsibilities, speak with your manager or the Compliance Officer.

4 Commonwealth of Dominica Regulatory Background and Requirements

4.1 The Money Laundering Prevention Act (MLPA) & Regulations

The MLPA, including its subsequent amendments and its enacted regulations, describe requirements related to AML and CTF compliance. The MLPA facilitated the creation of relevant regulatory and oversight authorities, a framework for compliance, and penalties for non-compliance[13].

---

[11] Suspicious Transaction and Currency Reports.

[12] For the purpose of this programme and its accompanying Risk Assessment, and procedural documentation, the term "customer" is considered to include "business relationships", unless otherwise specified. A business relationship is defined as "…formed by a person acting in the course of relevant financial business where that person has obtained, by procedures maintained by him in accordance with regulation 5, satisfactory evidence of the identity of the person who, in relation to the formation of that business relationship, was the applicant for business." 2013 Money Laundering (Prevention) S.R.O. No. 4 Part I Section 2.

[13] "The failure of the Compliance Officer of a relevant business to maintain such procedures in accordance with this regulation shall not constitute an offence but

4.2 Suppression of the Financing of Terrorism Act (SFTA)

The SFTA establishes the offence of terrorist financing, the designation of terrorist persons and groups, the freezing of assets, and duties to disclose certain information.

4.3 Money Laundering Supervisory Authority (MLSA), Financial Services Unit (FSU) & Financial Intelligence Unit (FIU)

The Money Laundering Prevention Act (MLPA) established two (2) statutory entities: the Money Laundering Supervisory Authority (MLSA) and the Financial Intelligence Unit (FIU). The core functions of the MLSA are to supervise and regulate financial institutions (FIs) and designated non-financial businesses and professions (DNFBPs) listed in the Schedule to the MLPA, whereas the core functions of the FIU include analysis and investigation of financial crimes. In 2011, the Financial Services Unit (FSU), became Dominica's MLSA.

Dominica's FIU is a member of the Egmont Group[14], and international network of FIUs. In accordance with the Egmont Group's principles, the FIU "serves as a national centre for the receipt and analysis of: (a) suspicious transaction reports; and (b) other information relevant to money laundering, associated predicate offences and financing of terrorism, and for the dissemination of the results of that analysis."

4.4 Financial Action Task Force (FATF)

The Financial Action Task Force (FATF) was established in 1989 to combat money laundering. The FATF seeks to set standards and promote effective implementation of legal, regulatory and operational measures for combating money laundering, terrorist financing and other related threats to the integrity of the international financial system. FATF developed forty (40) recommendations which have become the internationally accepted standards on combatting money laundering and the financing of terrorism & proliferation.

4.5 Caribbean Financial Action Task Force (CFATF)

The Caribbean Financial Action Task Force (CFATF) is a regional organisation, which had its genesis out of the Financial Action Task Force (FATF). Its mandate is to ensure that the supervisory and regulatory practices in the Caribbean jurisdiction effectively deter, identify and, if necessary, prosecute money laundering and financing of terrorism . The Commonwealth of Dominica is a member of the CFATF. In order to assess the status of the anti-money laundering framework of its member countries, both the FATF and the CFATF undertake detailed reviews referred to as mutual evaluations.

---

will be subject to a penalty of fifty thousand dollars." Money Laundering (Prevention) Act No. 8 of 2011, PART V, Section 4.

[14] http://www.egmontgroup.org/about

4.6 Regulator Examinations and Compliance Assessment Reports

SCB's regulators are responsible for ensuring that the Bank (as a reporting entity) is meeting the Bank's obligations. To do this, they will periodically request information. SCB may receive these requests by email, phone or in writing. All requests should be forwarded to the Compliance Officer for prompt review.

Most information requests require a response within thirty (30) calendar days. Late responses may be subject to penalties.

4.7 Non Compliance & Penalties

Compliance with all regulatory requirements is mandatory. Failure to do so may lead to civil and criminal penalties. Depending on the nature of non-compliance, penalties could be applied to SCB, or to specific individuals, including individual staff members.

4.8 Requests from Law Enforcement

SCB collaborates fully with legitimate requests from law enforcement agencies, including all law enforcement agencies. Such requests should be forwarded to the Compliance Officer for prompt review.

5 Commonwealth of Dominica AML/CTF Compliance Programme Components

As a bank operating in the Commonwealth of Dominica, SCB is required to have in place a Compliance Programme comprising the elements described below. SCB's AML/CTF Compliance Programme has been designed to conform to the elements required under the guidance provided by Dominica and CFATF. SCB's procedures for implementing the policies listed are described in separate documents, which have been designed for:

- Compliance Staff and
- All Staff.

In addition, SCB has developed a Risk Assessment and employee training manuals which are applicable to all staff. Moreover, the Bank's employees have completed relevant compliance Training Programme(s).

5.1 Reporting

Certain types of transactions must be reported to the FIU. Reporting to the FIU should always be completed by the Compliance Officer, or a delegate (a person that has been trained to submit reports in the Compliance Officer's absence). All other employees should use the internal form included in this programme to submit reports to the Compliance Officer. If the employee is not sure whether to submit a report, speak with the Compliance Officer for clarification. If it is not possible to speak with the Compliance Officer at that time, err on the side of caution by

collecting the required information, complete and and submit the report to the Compliance Officer. This may include collecting the customer's identification information.

All reports have specific timelines in which they must be submitted to the FIU. All internal reports should be submitted to the Compliance Officer on the same day that the incident or transaction takes place.

Report Type	Timing	Reported To
Suspicious Transaction Report (STR)	Initial STR filing must be submitted within five (5) calendar days	FIU
Currency Report (CR)	Initial CR filing must be completed at the point that currency and/or negotiable instruments valued in excess of $10,000 enter and/or leave Dominica	FIU

5.2 Record Keeping

In order to pass a Compliance Effectiveness Review, SCB must be able to prove that the Bank has met its obligations. Records must be maintained for at least seven (7) years in a format that can be retrieved and sorted easily.

Generally, when the regulators make a request, the information must be delivered to them within 30 calendar days. Depending on the type of information request and the way that the information is stored, the Compliance Officer or a delegate may need time to format and organise the information. For this reason, the following information must be stored in a format that can be retrieved and delivered to the Compliance Officer quickly:

- Complete customer identification information;
- Complete records for Politically Exposed Persons (PEPs)[15];

[15] Pursuant to Dominica's statutory rules and orders, this has been defined to mean in pertinent part:

- Internal Unusual Transaction Forms (whether or not they were reported by the Compliance Officer) and a record of the Compliance Officer's investigation process, including a rational that describes why the transaction or attempted transaction was or was not reported;
- A record of the content, date and completion/attendance of any AML/CTF related training sessions, including internal staff training sessions;
- AML/CTF Compliance Effectiveness Review reports, including a record of Board of Directors and Senior Management sign-off on the final report;
- All regulatory correspondence and reporting;
- All AML/CTF Compliance Programme documents, including Policies, Procedures and SCB's Risk Assessment;
- All Customer Risk Ranking documentation;
- All records of enhanced due diligence for higher risk customers;
- All records of transaction monitoring for higher risk customers;
- Records related to business relationships; and
- Copies of signed agreements with the Bank's service providers.

5.3 Customer Identification[16]

In certain instances, SCB needs to identify and record specific information about the Bank's customers. This includes, but is not limited to, cases in which the Bank is required to make a regulatory report. Identification information must be collected for:

- Any customer with whom the Bank has an ongoing service agreement and/or business relationship; and

---

> …any individual who is or has been entrusted with prominent public functions in Dominica or in any country or territory, including Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials including family members or close associates of the politically exposed person. 2013 Money Laundering (Prevention) S.R.O. No.4.

[16] All existing clients are associated with a Director of the Bank. All new clients will be referrals from the existing client base.

- Any customer that is not recognised and/or authenticated[17] at the time that a transaction is requested by the customer.

Additionally, without letting the customer know that the Bank may have suspicions about the nature of their activities, in instances of:

- Suspected money laundering or terrorist financing activity (including activity that is attempted, but not completed); and

- Confirmed terrorist property.

5.4 Training

Every SCB employee, including part-time, temporary, and contract employees that interact with customers, customer funds or transactions must receive AML/CTF training at least annually. New hires must receive AML/CTF training within their first 30 days of employment as SCB. Anyone that is on a leave of absence that causes them to miss regularly scheduled training will complete training within 30 days of their return to work.

The Compliance Officer will track the completion of all training and may require additional training sessions if compliance issues arise.

AML/CTF training will cover (at minimum) these elements:

- What is money laundering?

- What is terrorist financing?

- What is the Financial Services Unit (FSU)?

- What is the Financial Intelligence Unit (FIU)?

- What are the Bank's responsibilities under the law of the Commonwealth of Dominica?

    - Compliance Officer
    - AML/CTF Compliance Programme
    - Risk Assessment
    - AML/CTF Compliance Effectiveness Review
    - Training
    - Reporting

[17] Refer to All Staff Procedures.

- Record keeping
- Identifying Customers
- Customer Risk Ranking
- Transaction Monitoring

- Who is SCB's Compliance Officer?
- What do I do if I believe that money laundering is taking place?
- What data indicators should staff look for in the Bank's transactions and customer behaviours?

The completion of this training is mandatory (non-negotiable) and training must be completed within the timeframes communicated by the Compliance Officer or its delegate. Failure to complete training could expose the company to regulatory penalties. For this reason, it is vital that you contact the Compliance Officer immediately if you believe that you may not be able to complete your scheduled training session.

If you have any questions about AML/CTF compliance, please contact the Compliance Officer.

5.5 Risk Assessment

SCB's Risk Assessment is summarised in a separate document but pertinent sections include:

- The risk that the Bank's activities could make us vulnerable to money laundering or terrorist financing and
- The controls that SCB has in place to prevent, detect and deter money laundering and terrorist financing.[18]

The Risk Assessment is reviewed and updated by the Compliance Officer at least every two years. The Compliance Officer should also update the assessment more often where there are changes to local legislation or to the products and services that the Bank offers or the Bank's controls.

5.6 Customer Risk Ranking and Transaction Monitoring

Most of the Bank's customers are considered low risk, however, certain customers will be considered higher risk than others. High-risk customers are not treated

[18] SCB's controls are described in an overview format in the Risk Assessment documentation. More detailed descriptions are contained in the Bank's procedural and technical documentation. Specific controls will vary by region, based on regional requirements and laws.

differently when they interact with the Bank's staff, but their activities are reviewed more carefully post-transaction.

High-risk customers are subject to regular transaction monitoring and enhanced due diligence. The Compliance Officer, or a delegate, completes these activities. Transaction Monitoring involves the review of customer transaction patterns to look for suspicious indicators. Enhanced Due Diligence (EDD) involves additional investigation, and in some cases, the Compliance Officer may ask for additional information from the customer, such as details about a specific transaction.

5.7 AML/CTF Compliance Effectiveness Review

An AML/CTF Compliance Effectiveness Review is similar to an audit that tests the Bank's AML/CTF Compliance Programme. The review tests two elements: the programme documentation and the Bank's operations (what SCB has actually done during a specific period of time). These reviews must be completed at least once every two years. The results of the review must be shared with, as well as signed off by, the Board of Directors and Senior Management. This must be completed within thirty (30) days of the date that the final report is issued.

The information gathered for these reports is very specific. If you receive a request related to a review, please check to be certain that you are able to provide all of the information that was requested. The review process may also include interviews with staff. If you are interviewed, it is permissible to reference SCB's AML/CTF compliance programme and other documentation.

The Compliance Officer will work to correct any issues that are noted in the report. This may include:

- Updating the AML/CTF Compliance Programme;
- Creating new controls;
- Updating processes;
- Updating client records; or
- Providing additional staff training on specific topics.

The results of AML/CTF Compliance Effectiveness Reviews may also be shared with potential business partners, financial service providers and the Commonwealth of Dominica. It is a best practice for the Compliance Officer to keep a record of the updates that have been made based on the AML/CTF Compliance Effectiveness Review results.

6 Appendix 1: Definitions & Acronyms

AML: Anti-Money Laundering

Anti-Money Laundering: Actions taken to detect, deter and prevent money laundering from occurring through the Bank's business.

Caribbean Financial Action Task Force: An organisation of twenty-seven (27) jurisdictions of the Caribbean Basin Region, which has agreed to implement the international standards for Anti-Money Laundering and Combating the Financing of Terrorism (AML/CTF). These standards are the Financial Action Task Force Recommendations (FATF Recommendations).

CFATF: Caribbean Financial Action Task Force

CTF: Counter Terrorist Financing: actions taken to detect, deter and prevent terrorist financing from occurring through the Bank's business.

Currency: The coin and paper money of any country that is delegated as legal tender and that circulates and is customarily used and accepted as a medium of exchange in the country of issuance. The official currency for the Commonwealth of Dominica is the Eastern Caribbean Dollar (XCD).

Currency Transaction: The physical transfer of currency from one person to another (a transaction which does not include the physical transfer of currency, is not considered a currency transaction for this purpose).

FIU: Financial Intelligence Unit

Financial Services Unit of the Commonwealth of Dominica: the sole regulatory authority for the Non-Bank Financial Sector in Dominica and the Money Laundering

Supervisory Authority. The Financial Services Unit, as a department within the Ministry of Finance, covers the financial sector in Dominica with the exception of Commercial Banks and Securities Business.

FSU: Financial Services Unit

Money Laundering: the process of taking property that represents the proceeds of some form of unlawful activity and conducts, or attempts to conduct, a financial transaction, which involves the proceeds of a specified unlawful activity. Under the Dominica Money Laundering Prevention Act, it is illegal to launder money or to knowingly assist in laundering money.

Money Laundering Prevention Act No. 8: In 2011, under Section 7, the FSU became the Money Laundering Supervisory Authority. Their mission is to ensure that every financial institution conducts a risk assessment, develops policies, procedures and controls that prevent and mitigate the money laundering and terrorist financing risks identified.

Money Laundering Prevention Act No. 8 of 2011 Schedule Part 1: includes activities of financial institutions that are 1) "banking business" and "financial business" as defined in the Banking Act of 2005 and 2) "banking business" as defined in the Offshore Banking Act 1996.

Suspicious Transaction Guidelines: pursuant to the meaning assigned in Section 2 of the Money Laundering (Prevention) Act 2011.

Suspicious Transaction Report: a report required to be made under Section 15 of the Money Laundering (Prevention) Act 2011 and Section 19A of the Suppression of the Financing of Terrorism Act of 2003.

Terrorism: is any attempt to influence or intimidate a government or the public at large through violent or illegal means or means that are intended to induce fear or panic.

Terrorist Financing: funding any act of terrorism or committing any act or omission that facilitates the funding of terrorism.

Unusual Transaction Report: An internal form that is used by the Bank's staff to record the details of any customer activity, whether completed or attempted, that is suspected of being related to money laundering or fraud. The completed form is provided to the Compliance Officer, on the same day the activity took place, in order to make a determination of whether the customer activity is deemed to be suspicious.

UTR: Unusual Transaction Report

7 Appendix 2: Programme Update Log[19]

This log can be used by the Compliance Officer to track the updates to the AML/CTF Compliance Programme documents. If the programme is reviewed and no significant changes are made to a document, then there should still be a line item that states that the programme was reviewed and no significant changes were made.

This document may be used as evidence for reviewers or regulators that the scheduled programme updates have occurred.

Document	**Changes**	**Reviewed and Approved by**	**Date**
Anti-Money Laundering & Counter Terrorism Compliance Policy	Programme developed by Outlier Solutions Inc. edited with the Compliance Officer and key members of the Board of Directors to reflect SCB's business model and practices.	Compliance Officer	Q2 2016
Anti-Money Laundering & Counter Terrorism Compliance Procedures for Compliance Staff	Programme developed by Outlier Solutions Inc. edited with the Compliance Officer to reflect SCB's business model and practices.	Compliance Officer	Q2 2016
Anti-Money Laundering & Counter Terrorism Compliance Procedures for All Staff	Programme developed by Outlier Solutions Inc. edited by the Compliance Officer to reflect SCB's business model and practices.	Compliance Officer	Q2 2016
Anti-Money Laundering & Counter Terrorism Risk Assessment	Programme developed by Outlier Solutions Inc. edited with the Compliance Officer and key members of the Board of Directors to reflect SCB's business model and practices.	Compliance Officer	Q2 2016

[19] Senior Management approves programme updates where there are significant changes. Minor changes, such as phrasing or process improvements may be approved by the Compliance Officer, without the approval of Senior Management.