



Policies, Procedures and Processes

In June of 2005, the Federal Financial Institutions Examination Council (FFIEC) issued the Bank Secrecy Act (BSA)/Anti-Money Laundering (AML) Examination Manual. Even if you have only glanced through the manual, you've probably noticed the phrase "policies, procedures and processes". Those three words appear together no less than three hundred times throughout the manual. What do these terms mean? Are they synonyms? Is it acceptable for a financial institution's BSA/AML program to have separate policies, procedures and processes? Additionally, can the financial institution have procedures and processes that are not approved by the Board of Directors? These are the questions and concepts we will address in this article.

You won't find the terms defined in a regulation. We've formed these opinions from noting how they are used in the regulatory industry and in the new examination manual. Obviously, our experiences lead to the opinions expressed in this article. We have also discussed these thoughts with numerous regulators from various agencies (FDIC, FRB, OCC, OTS and state regulators).

A financial institution's BSA/AML program is made up of the bank's policies, procedures and processes. **Policies** are dictated and approved by the Board of Directors indicating how the financial institution will comply with federal laws and regulations. **Procedures** are guidelines devised and implemented by management to enable the institution's personnel to perform the day to day **processes** necessary to carry out the policy. Policies, procedures and processes are not one in the same; rather, each is a separate and distinct concept not intended to be used synonymously.

How did we get here?

For years BSA/AML compliance was typically nothing more than a policy reviewed and approved by the Board of Directors indicating an assignment of responsibility (the BSA Officer) and statements indicating "we will do this to comply with the law". In addition to the policy, several unwritten controls were put in place by management to carry out the policy statements. This was the status quo until the events of 9/11.

The USA PATRIOT Act, specifically Section 326, requires financial institutions to implement a written Customer Identification Program (CIP) and include it in the institution's BSA/AML program. Additionally, the CIP program requires risk-based procedures to verify each customer's identity. This appears to be where the confusion began.

The initial interpretations of this requirement indicated a financial institution must have a written CIP program, including risk based procedures, which had to be approved by the Board of Directors. As a result, many financial institutions created a CIP policy complete with detailed procedures and had them approved by the Board of Directors. The first thought that should come to mind is, "How can the Board approve something requiring as much detail as the CIP procedures?" The Board isn't involved in the actual processes. Why would they formulate and implement the procedures? The only way this is possible is if the Board was trained with the level of detail necessary for the CIP risk based procedure requirements. Procedures and processes are management's responsibility. Management must formulate procedures and processes in such a way that the policy can be carried out by the financial institution's personnel in a practical and efficient manner.

Furthermore, we've never met a Board that had the knowledge, or desire, to really understand procedures. They operate at a much higher level. Bankers often joke that the Board just signs off on the policy and procedures without really understanding them. That's because it's not practical for them to comprehend the detailed procedures. That's not what they do or should be asked to do.

What do the regulators really want?

On page 179 of the FFIEC's BSA/AML Examination Manual, it states:

"Verify that the bank's policies, procedures and processes include a comprehensive program for identifying customers who open an account after October 1, 2003. The written program must be included within the bank's BSA/AML compliance program and must include, at a minimum...."

If we apply the logic that a financial institution can have separate policies, procedures and processes we would expect to see the following:

1. A CIP program policy approved by the financial institution's Board of Directors and included as part of, or within, the BSA/AML policy;
2. Detailed, risk based, CIP procedures formulated and approved by management in a written format. The procedures should be reviewed, but not approved, by the Board; and,
3. Discussions with the staff performing the procedures confirming the actual processes completed.

Provided the financial institution adequately addresses each of the above items, the Customer Identification Program should be in compliance with the guidance found in the FFIEC BSA/AML Examination Manual. The separation of procedures from the Board of Directors approved policy also allows for adaptability without calling a Board meeting every time a minor exception to procedure is warranted.

Let's look at this from the angle of Currency Transaction Reports (CTRs):

1. The policy states a CTR will be completed.
2. The procedures give guidance on how to complete the CTR.
3. The processes are where forms are kept, how they are completed (handwritten, typed, electronically, etc.), if a supervisor will review the completed form and who and how will the CTR be filed.

Now let's apply this concept throughout a financial institution's entire BSA/AML Program. First, the Board approved BSA/AML Policy must state the financial institution will:

1. Designate an individual, or individuals, responsible for BSA/AML compliance;
2. Instruct management to implement a system of internal controls (procedures and processes) to ensure ongoing compliance;
3. Require appropriate training for all personnel;
4. Provide for annual, independent testing of the BSA/AML program; and,
5. Implement a Customer Identification Program that will verify the identity of any person seeking to open up an account; maintain records of the information used to verify a person's identity, including name, date of birth, address and tax identification number; and, review lists of known or suspected terrorists or terrorist organizations provided to the financial institution by any government agency to determine whether a person seeking to open an account appears on any such list.

Next, we must ensure that written procedures approved by management and reviewed by the Board are in place to enable the financial institution's personnel to perform the processes necessary to carry out the approved policy. For example, each of the following BSA/AML risk areas should have written procedures in place, as applicable:

1. Customer Identification Program,
2. Customer Due Diligence,
3. Suspicious Activity Reports,
4. Currency Transaction Reports,
5. Currency Transaction Reporting Exemptions,
6. Information Sharing – 314(a) and 314(b),
7. Monetary Instruments,
8. Funds Transfers,

9. Office of Foreign Assets Control (OFAC);
10. Trust and Asset Management, and,
11. Non-Bank Financial Institution.

Note: This list is intended to be representative and not exclusive. Written procedures may be required in other areas not mentioned above.

If the financial institution adequately addresses each of the above items, the BSA/AML program should be in compliance with the guidance found in the FFIEC BSA/AML Examination Manual.

Summary:

Policies are statements adopted by the Board of Directors indicating what a financial institution will do to comply with federal laws and regulations. Procedures are formal written guidelines indicating who, when, where and how these policies will be carried out. Processes are informal, unwritten actions to carry out the policy. Even though policies, procedures and processes are each separate and distinct concepts not intended to be used synonymously, they do work together to develop, implement and administer the day to day practices assuring financial institution's BSA/AML compliance program.