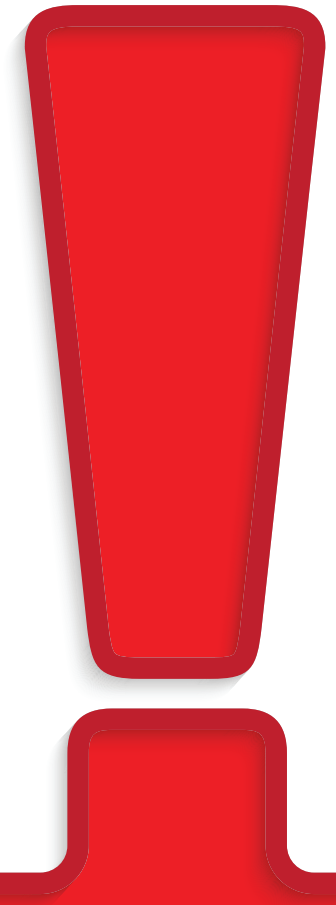
QUICK REFERENCE GUIDE

How to perform a financial institution risk assessment



This quick reference guide walks you through three steps to perform a risk assessment for your FI, and includes examples and best practices.

VERAFIN
A STEP AHEAD.

Sections

TABLE OF CONTENTS

SECTION 1

Risk Assessment Overview

There are various levels of risk for a financial institution. Institution risk takes into account all risk factors and combines them into an overall risk assessment. A financial institution risk assessment is a measure of the potential threats present at, and for, your financial institution. This encompasses:

- Customers
- Entities
- Transactions
- Employee training
- Geographic locations
- Products
- Services

This should also include any other factors that affect the regulatory compliance and fraud risk health of the organization. Your risk assessment should drive your policies and procedures, which help mitigate and manage those risks. A thorough risk assessment considers BSA/AML, fraud, OFAC, and institution-specific factors, such as business lines and subsidiaries and how all of these factors interrelate.

This quick reference guide provides a brief, summarized version of the requirements and can help you perform a financial institution risk assessment. When your examiner asks where your FI stands with risk, this guide can help you feel confident and prepared.

"A risk-based approach requires institutions to have systems and controls in place that are commensurate with the specific risks of money laundering and terrorist financing facing them."[1]

[1] *Study Guide for the CAMS Certification Examination, Ch. 4, p. 183*

SECTION 1

Risk Assessment Overview

Tips and tricks

Ensure your risk assessment is tailored to your FI:

Be as specific as you can with the information at your disposal.

Try not to generalize or be too vague.

For background research and material, ask for a copy of an existing risk assessment.

The following resources can help you get started:

Peers and consultants

Online forums and search engines

Risk assessments are continuous.

Risk changes over time and should be continuously monitored and reassessed.

Learn about any potential exposures and detail a plan.

It's better to know where you stand in terms of risk so you can put appropriate measures in place to protect your FI and your customers.

Ensure you are able to justify your decisions.

Examiners want to see a logical thought process in your risk assessment that justifies your analysis and decisions.

SECTION 2

Performing a Risk Assessment

Performing a risk assessment for your financial institution

Examiners want to know that your financial institution is aware of the risks that are present and is managing them adequately. This quick reference guide walks you through three steps to perform a risk assessment for your FI, and includes examples and best practices.

You know what products and services your FI offers, so your FI risk assessment helps you know:

- the risks they present
- the number of low, medium, and high risk customers
- the types of products and services they use
- their typical transactions and expected behavior
- the geographic locations that are in use by your customer base
- which ones present the most risk to you

You should also be able to talk about the reasons behind your decisions, and have a plan in place to mitigate the risks that you can control. High risk can help you determine which individuals and groups require greater scrutiny.

It's a good practice to start with a clear purpose for the existence of a risk assessment and an awareness of your risk limitations. This will help ensure that your institutional risk assessment is aligned with your FI's intended risk profile. Further to this, when new products and services are added, the risks should be evaluated prior to implementation to ensure they align with your FI's policies and procedures.

SECTION 2

Performing a Risk Assessment

Three steps to complete a risk assessment:

STEP 1

Perform a risk assessment based on risk factors.

a. Identify specific risk categories.

b. Take a deeper dive into identified risk categories and rate them.

STEP 2

Provide narrative guidance to show understanding and justification.

STEP 3

Identify mitigation efforts.

(i.e., monitoring, tracking, acceptable risk levels).

These steps are outlined in more detail on the following pages.

Categorizing Risk

Risk can be broken down into general categories:

Prohibited
(not tolerated at the FI)

High risk
(significant, but not prohibited)

Medium risk
(additional scrutiny is merited)

Low risk
(baseline risk)

SECTION 2

Performing a Risk Assessment

STEP 1 Perform a risk assessment based on risk factors.[2]

The FFIEC BSA/AML Examination Manual outlines three main risk categories: products and services, customers and entities, and geographic locations. The following lists provide the steps for creating a risk assessment and the reasons each category presents risk along with examples of what is included in each risk category.

a. Identify Specific Risk Categories

Products and Services

Products and services have varying degrees of risk at each institution. The riskiest ones involve the heaviest possibility of being used for money laundering or terrorist financing. To help determine how to rate each product and service, you can ask yourself: Does a particular product or service enable significant volumes of transactions to occur rapidly; afford plenty of anonymity; require identification to complete; or have unusual complexity?

Some products and services that are particularly risky include private banking, offshore international activity, loan guarantee schemes, wire transfer and cash-management functions, and transactions in which the primary beneficiary is not disclosed.

Examples of products & services

- Electronic funds payment services
  prepaid access, funds transfers, transactions that are payable upon proper identification, third-party payment processors, remittance activity, automated clearinghouse transactions (ACH), automated teller machines (ATM)
- Electronic banking
- Trust and asset management services
- Monetary instruments
- Foreign correspondent accounts – bulk shipments of currency, pouch activity, payable through accounts, U.S. dollar drafts
- Trade finance
- Services provided to third-party payment processors or senders
- Private banking
- Foreign exchange
- Special use or concentration accounts
- Lending activities, particularly loans secured by cash collateral and marketable securities
- Non-deposit account services – non-deposit investment products and insurance

[2] *Note: The lists of products and services, customers and entities, and geographic locations are not complete. For more detailed information, refer to the FFIEC BSA/AML Examination Manual.*

SECTION 2

Performing a Risk Assessment

Customers and Entities

Customer and entity risk is extremely complex. Certain types of customers may pose heightened risk. Through customer due diligence (CDD), a financial institution gains an understanding of the types of transactions in which a customer is likely to engage. This helps identify potential risk and determine an appropriate level of monitoring. Enhanced due diligence (EDD) is applied to those deemed to pose higher risk and their activity should be reviewed more closely when an account is opened, as well as throughout the term of the relationship. Due diligence is ongoing and assists the bank in risk-based monitoring.

Often, private businesses are more difficult to perform due diligence on. Prior to opening new business accounts, it is important to verify the validity of the business (the Boston Public Library offers a helpful State Corporations Database).[3]

Customer risk depends not only on how much you know about the person or business and their intentions, but also on variables such as transaction volume, services sought, and the geographic location of their birth, residence, employment, and transaction origin and destination.

Examples of customers & entities

- Foreign financial institutions
  banks and foreign money services providers – casas de cambio, currency exchanges, money transmitters
- Non-bank financial institutions
  money services businesses, casinos and card clubs, brokers/dealers in securities, dealers in precious metals, stones, or jewels
- Senior foreign political figures and their immediate family members and close associates
  known as politically exposed persons (PEPs)
- Non-resident alien (NRA) and accounts of foreign individuals
- Deposit brokers, particularly foreign deposit brokers
- Foreign corporations and domestic business entities, particularly offshore corporations (such as domestic shell companies and Private Investment Companies and International Business Corporations) located in higher-risk geographic locations
- Cash-intensive businesses
  convenience stores, restaurants, retail stores, liquor stores, cigarette distributors, privately owned ATMs, vending machine operators, parking garages
- Non-governmental organizations and charities – foreign and domestic
- Professional service providers
  attorneys, accountants, doctors, real estate brokers

[3] *State Corporations Database, Boston Public Library, http://www.bpl.org/kbl/websites/state-corporations-databases/*

SECTION 2

Performing a Risk Assessment

Geographic Locations

Geographic location risk can be broken down into jurisdictions and countries. Where do individuals reside and what are their citizenships? Where are businesses headquartered and where do they conduct the majority of their business?

There is no single way to risk rate geographic locations, so a number of methods are used. Examiners are looking for your reasoning, so it is important to document all of your decisions.

Some methods for determining geographic risk include looking at heat maps or at defined regions such as High Intensity Drug Trafficking Areas (HIDTA) and High Intensity Financial Crime Areas (HIFCA); finding out whether the country is a member of FATF or has AML requirements equivalent to international best practices; question the overall reputation of the countries; access the website knowyourcountry.com; access the U.S. State Department's annual *International Narcotics Control Strategy Report*[4], which rates over 100 countries on their AML controls.

International higher risk geographic locations generally include:

- **Countries subject to OFAC sanctions**, including state sponsors of terrorism
- **Countries identified as supporting international terrorism** under section 6(j) of the Export Administration Act of 1979, as determined by the Secretary of State
- **Jurisdictions determined to be "of primary money laundering concern"** by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, through FinCEN, pursuant to section 311 of the USA PATRIOT Act
- **Jurisdictions or countries monitored for deficiencies in their regimes to combat money laundering and terrorist financing** by international entities such as the Financial Action Task Force (FATF)
- **Major money laundering countries and jurisdictions** identified in the U.S. Department of State's annual International Narcotics Control Strategy Report (INCSR), in particular, countries that are identified as jurisdictions of primary concern
- **Offshore financial centers (OFC)**
- **Other countries identified by the bank as higher-risk** because of its prior experiences or other factors – legal considerations, allegations of official corruption

Domestic higher-risk geographic locations may include, but are not limited to:

- Banking offices doing business within, or having customers located within, a U.S. government-designated higher-risk geographic location
- High Intensity Drug Trafficking Areas (HIDTA)
- High Intensity Financial Crime Areas (HIFCA)

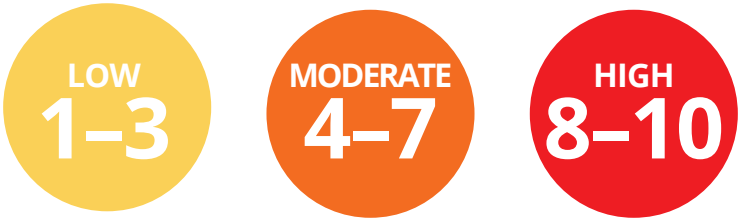
[4] *International Narcotics Control Strategy Report, http://www.state.gov/j/inl/rls/nrcrpt/2015/*

Performing a Risk Assessment

b. Take a deeper dive into identified risk categories and rate them

When you have created a thorough list of the risk categories at your FI, the next step is to determine the risk each category presents. A good way to do this is to create an excel spreadsheet, write the expanded risk factors in one column, and include another column to rate each one as low, moderate, or high. To get an overall rating for each category, average out each category.

For example, you could determine a way to average, or use a rating such as:



Another part of this deep dive is to determine the quality of your FI's compliance risk management. How well is your FI managing the threats that are present? The rating options for this part are strong, satisfactory, and weak.

The complexity of this analysis is up to you, as the risks at each FI are different. The three categories are combined to give a composite score that helps you assess how much risk is present. It's important to note that a determination of high compliance risk is not bad; the management of the risk is the key. Your FI might take on more risks but do a great job handling those risks – an examiner wants to get a sense of the overall circumstances as they pertain to your specific FI and ensure that you are doing a thorough job managing the risks.

Analysis of Specific Risk Categories	Quantity of Compliance Risk			Quality of Compliance Risk Management		
Products and Services	Low	Moderate	High	Strong	Satisfactory	Weak
Customers and Entities	Low	Moderate	High	Strong	Satisfactory	Weak
Geographic Locations	Low	Moderate	High	Strong	Satisfactory	Weak

When you have determined your overall ratings for the identified risk categories, the next step is documenting your analysis and providing the reasoning behind your decisions.

SECTION 2

Performing a Risk Assessment

STEP 2 Provide narrative guidance to show understanding and justification for risk ratings.

Write down reasons for your FI's level of risk for products and services offered, customer activity, and geographic locations of both your FI and of the incoming and outgoing transactions.

Your FI's unique customer base, location, and types of products and services offered make up a risk profile that is different from every other FI. Examiners want to see your decision-making in narrative form – write down why you determined one factor was riskier than another, or why certain customers should be monitored more closely. Often, this assessment is done at account opening, or when new products and services are offered. When the risk factors change, the risk narrative needs to be updated.

For example, a narrative about products and services would include the following information:

- Definition of each product and service
- How to deal with each product and service (who, where, when, why)
- What is an acceptable and manageable level of risk for each product and service
- What is an acceptable and manageable level of risk overall

Risk Tip

Examiners want to make sure that you are in compliance with regulations, and a robust institutional risk assessment helps provide answers about:

How much risk your FI is willing to accept, and why

How much risk is posed, and how you came to your conclusion

How well your FI is managing that risk

SECTION 2

Performing a Risk Assessment

STEP 3 Identify mitigation efforts and acceptable level of risk.

List the policies, processes, and procedures your FI has in place to mitigate risk. Indicate what is an acceptable level of risk for your FI and how your FI manages this risk.

When you know what your risks are, you can determine the steps that are necessary to manage those risks. An important consideration is knowing a comfortable threshold of risk for your FI. What products and services and customer types should be prohibited? Include this rationale in the policy and ensure there is adequate enforcement of that policy.

An FI's internal policies and risks related to the business must be taken into account in the overall risk assessment. For example, an internal policy to train all employees can help mitigate risk – internal communication ensures everyone does their job to the best of their ability and vital information reaches each staff member who needs to know.

A working example:

Let's say Bank A offers a lot of high risk products and services, but they only offer them to customers who are trusted. They know what's going on with their customers and their transactions due to a CDD monitoring schedule (and EDD in case of unusual activity), so if there is activity that seems suspicious, they can investigate immediately. They know who is new, who sends wires to risky locations (and very few do), and where everyone lives because they have called to verify or conducted site visits.

Let's fill in that table. We know their product risk is high, their customer risk is low, and their location risk is moderate due to the balance of well-known customers and transactions to risky locations. They have excellent customer monitoring and offer products and services selectively, so their compliance risk management is strong for those two categories. Their lowest category of compliance management comes from the wires to risky locations, but they are willing to accept that risk, and have documented the business need (such as a large population of international students in a university town sending/receiving money).

Analysis of Specific Risk Categories	Quantity of Compliance Risk			Quality of Compliance Risk Management		
Products and Services	Low	Moderate	**High**	**Strong**	Satisfactory	Weak
Customers and Entities	**Low**	Moderate	High	**Strong**	Satisfactory	Weak
Geographic Locations	Low	**Moderate**	High	Strong	**Satisfactory**	Weak

SECTION 3

Managing Risk

Threats can lead to reputational and legal risk and damage.

Risk assessments should take into consideration:

- the Board of Directors and senior management
- policies and procedures
- roles and responsibilities
- an internal audit
- external resources
- inventory (purpose and products, actual or expected usage, restrictions on use)
- documentation
- internal controls (which are necessary to prevent fraud)

Helpful hints for managing risk

Policies and procedures – Ensure consistency and discipline with risk management principles, supervisory expectations, and implementation. Have your assessment challenged to identify limitations.

Technology – A data-driven approach helps eliminate assumptions and reveal gaps. Technology is recommended to help with a layered approach to security.

Education – Always educate yourself about Red Flags and investigate them. Risk assessments are highly subjective – every assessment is as different as the individual institution – and should leverage industry best practices and published research.

Risk Model – Development of a risk model is not enough – it is very important to implement it and use it effectively. It is important to always have a fraud monitoring process or system in place.

- *Set up appropriate monitoring*
- *Accept only risks you are willing to manage*
- *Validate your choices and ratings to determine appropriate controls*
- *Designate someone to manage systems, controls, duties, training, etc.*

Ask yourself:

Fraudsters often try to justify their actions through rationalization.

From a fraud perspective, a couple of good questions to ask yourself are:

Is there an opportunity?

Is there a good chance to get away with it?

SECTION 3

Managing Risk

Factors to consider when deciding whether or not to automate

Financial institutions have increased the use of data-driven decision-making tools. Automated tools can help you prevent crime and ease compliance concerns.

Would automation help you with your risk assessment?

- Asset size is not as important as an FI's risk profile for determining whether automation is needed
- An FI's customer base and transactional mix can increase or decrease the need for a solution
- Geographic location is an important factor during risk assessment and can lead to an increase in monitoring (such as HIDTA or HIFCA)
- Automated solutions provide a complete view of customer activity

Save time and money

- Save time by eliminating manual reviews, scheduling, reporting, etc.
- Detect crime faster and give yourself more time to investigate and make decisions
- Reduce IT requirements
- Generate an institutional risk profile automatically when the system is configured
- Improve investigation efficiency by combining AML and fraud detection, case management, customer risk rating, OFAC, and more in one system
- Maximize your resources by unifying processes
- Prevent fraud proactively
- Enhance your audit trail and tools
- Create visibility across your FI and streamline communication
- Stay on top of emerging trends and new regulatory requirements

Verafin is an industry leader in cross-institutional FRaud detection and Anti-Money Laundering (FRAMLx) software with a customer base of over 1200 financial institutions across North America.

Its solution uses advanced behavior-based analytics that help financial institutions stay a step ahead of numerous types of fraud as well as the BSA, USA PATRIOT Act, and FACTA compliance landscape.

Verafin is the exclusive provider of fraud detection and BSA/AML software for the California Bankers Association, Florida Bankers Association, Massachusetts Bankers Association, Illinois Bankers Association, CUNA Strategic Services, and has industry endorsements in 44 states across the U.S.

Resources

The FFIEC BSA/AML Examination Manual details the BSA/AML compliance requirements for a financial institution risk assessment at length.

The Study Guide for the CAMS Certification Examination provides a good, clear breakdown of what's needed to perform a risk assessment.

For more information on how to manage risk, contact us today.

1.877.368.9986
info@verafin.com
www.verafin.com

VERAFIN
A STEP AHEAD.