OFAC Compliance Series

(A five-part series)

Part II: OFAC Risk Assessment Methodology

Risk-Based OFAC Programs

Your company's OFAC risk assessment is what drives your OFAC program's policies and procedures and allows examiners to identify the strengths and weaknesses of your program.

- The FFIEC BSA/AML Exam Manual says that examiners may utilize a risk-based approach, however, OFAC's enforcement standards remain a strict liability for violations and executive orders are not risk-based.
- That being said, your OFAC program should be tempered by the Institution's risk appetite and available resources to avoid both regulatory and OFAC violations.
- Your program's policies and procedures must match or exceed the risk.

We are told that everything is risk-based – that the risk assessment is the backbone of any well-built OFAC compliance program – and that an efficient and effective program cannot be developed without knowing where the risks reside. Many businesses, both financial and non-financial institutions, are conducting OFAC assessments to uncover risks, design strong compliance programs, and mitigate their exposure. There are many decisions and much preparation that needs to be made when you embark on conducting an OFAC risk assessment.

Risk-Based Methodology

Every financial institution should also have a documented OFAC risk assessment methodology. Most institutions possess an OFAC risk assessment, but the actual methodology for how to appropriately conduct the risk assessment is often missing.

Think of the methodology as a user-friendly guidebook that helps you by explaining in detail your risk assessment's approach to the who, what, when, where, why, and how steps that are involved in assessing risk. The methodology also establishes standards for execution of the qualitative and quantitative analysis in the OFAC risk assessment. Additionally, the methodology describes the process of conducting a risk assessment so that financial institutions can follow established guidelines and replicate or modify the risk assessment on a periodic basis in order to accurately reflect the Institution's risk. The value derived from investing the time to develop a risk assessment methodology is priceless.

The risk methodology will help you establish your line of succession. It will be much easier for someone to step into the role and complete future risk assessments if there is a guide to understand how your risk was calculated. This line of succession ensures continuity of OFAC operations.

The methodology should detail four primary areas that will formulate the basis for the risk assessment:

1) **Inherent Risk:** How and where inherent risk will be assessed
2) **Change Risk:** How and where change risk will be assessed
3) **Controls:** How and which controls will be evaluated
4) **Residual Risk:** How the resulting residual risk will be calculated. Residual risk will determine the risk direction in which your Institution is headed.

And, formulation of a risk scoring system within the risk assessment methodology, with defined levels of risk, sets the framework for analyzing risk and controls in the risk assessment.

Inherent Risk

In order to determine inherent risk, you should evaluate the OFAC risk inherent within your customers, geographies, products, services, and transactions.

Some categories within these groups will pose a higher OFAC risk. Within each of these risk categories, risk should be assessed across multiple factors. For example, risk-based on the length of the customers' relationship with the institution might be one factor to be evaluated within the customers' risk category. After ascertaining the inherent risk present within each of the risk categories, the overall inherent risk for the institution can be calculated.

Change Risk

Change risk can be defined as the change in inherent risk resulting from a comparative analysis of your past and present metrics. Institutions should assess change risk to measure how the overall risk has shifted and which metrics are responsible for the change. For instance, substantial growth in your Institution's portfolio from the previous year may lead to an increase in your Institution's current inherent risk.

You should anticipate future change risk based on projected metrics for the following year. To illustrate, the projected introduction of new products and services for the next year has the potential of increasing your Institution's inherent risk. If you can predict with relative certainty where inherent risk will increase, you can begin to establish appropriate mitigation early on or begin to create a plan of action as to how to account for the anticipated increase in risk.

Controls

In your assessment of existing OFAC controls, an Institution's task is to evaluate the effectiveness of the controls at mitigating the inherent risk. At a minimum, the results of your Institution's most recent regulatory examination, audit/independent testing results, and compliance testing results should be assessed. Since each of these sources has already come to a conclusion of the OFAC inherent risk from their own independent examinations, most of the time each component addressed will be associated with a unique risk score based on established guidelines set forth by your examining agency. You should always attempt to remain aware of what potential deficiencies or shortcomings can be identified by independent examinations, so you can avoid regulatory penalties.

Residual Risk

Finally, let's address residual risk and how it's calculated. Residual risk can be defined as the risk that remains after controls are applied against the inherent risk. The level of inherent risk and the effectiveness of the controls the financial institution has implemented to mitigate risk will determine the residual risk and the ultimate risk direction in which the institution is headed.

Financial Institutions will often determine risk solely based on categorical inherent risk defined by evaluating the previously mentioned components of inherent risk (remember, this will be customers, geographies, products, services, and transactions) without taking controls into account to accurately calculate residual risk. Failure to consider your controls may result in an incorrect depiction of your risk. In fact, actual risk may differ substantially once the residual risk is identified. Time and effort spent in developing a risk assessment methodology that guides the development of your risk assessment will be worth the investment for your Institution.

Conclusion

A preexisting risk assessment methodology provides the structure for conducting the risk assessment and will make it easier to build a new risk assessment or update an existing. One that is based on meticulous standards that have already been instituted and approved in the methodology, as opposed to starting fresh or lacking an understanding of how the prior risk assessment was conducted.

Arc-Serv can help you build both your OFAC Risk Assessment and the Risk Assessment Methodology. **Contact us** to learn more.

Our next installment in the OFAC Compliance Series will be “Tips and Tricks for a Successful OFAC Risk Assessment.” Stay tuned and **follow us** to get regular updates.