OFAC and the Role of the Three Lines of Defense

History of OFAC

Throughout history, economic sanctions have been closely linked with war and were intended to weaken the enemy. After World War I, President Woodrow Wilson called for an alternative to armed conflict and economic sanctions were seriously considered. Both the League of Nations and the United Nations used sanctions as a tool of enforcement. The highest profile sanctions were imposed on Iraq following the Gulf War in 1991. In addition to the UN, the U.S. continues to implement economic sanctions. Since 1990, sanctions have been targeted towards political regimes, drug traffickers and terrorists. (Kimberly Ann Elliot 2008)

OFAC Authority and Oversight

The Office of Foreign Assets Control (OFAC) is a division of the U.S. Treasury that has responsibility for administering and enforcing economic and trade sanctions. OFAC operates under Presidential wartime and national emergency powers, as well as authority granted by legislation that allows OFAC to impose controls over transactions and to freeze assets under U.S. jurisdictions. The Secretary of the Treasury has delegated the responsibility to develop, enforce and oversee the various U.S. sanctions programs currently in place. (Federal Financial Institutions Examination Council 2010)

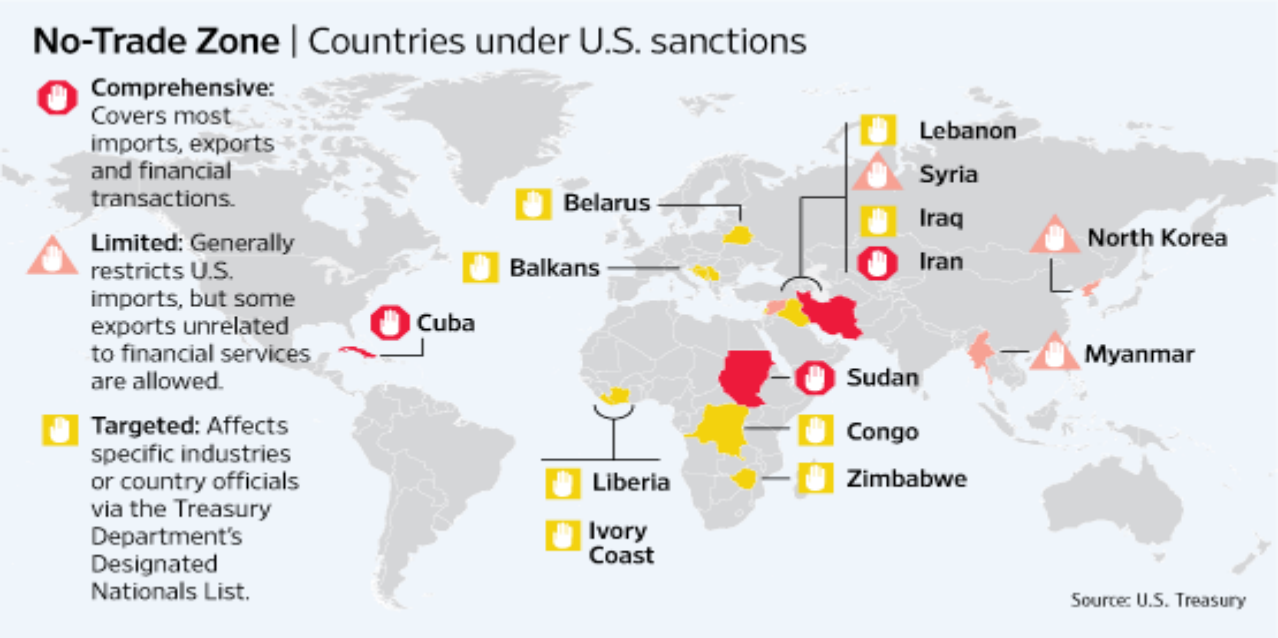
OFAC Exterritorial Impact

Unlike Bank Secrecy Act legislation, OFAC-related regulations have applicability outside U.S. borders. All U.S. persons, to include permanent residents, individuals located in the U.S and U.S. banks, their domestic branches, agencies, international banking facilities, foreign branches and overseas offices and subsidiaries are required to comply with OFAC regulations when transacting in U.S. dollars. This includes U.S. branches for foreign financial institutions, as well as U.S. persons working at foreign corporations outside of the U.S. at the time the transactions are processed. (Slear 2006) At a high-level, OFAC requires the blocking of accounts and property of specified countries, entities and individuals. It also prohibits or requires the rejecting of unlicensed trade and financial transactions with sanctioned countries, entities and individuals. (Federal Financial Institutions Examination Council 2010)

OFAC Sanction Programs

As previously noted, OFAC administers a number of different sanctions programs against various countries and political regimes, all with varying degrees of severity. Currently, there are sanctions programs involving the following countries: Balkans, Belarus, Burma, Ivory Coast, Cuba, Democratic Republic of Congo, Iran, Iraq, Former Regime of Charles Taylor, Libya, North Korea, Somalia, Sudan, Syria, Yemen and Zimbabwe. In addition to the country-specific sanctions, OFAC has also implemented sanctions relating to counter narcotics trafficking,

counter terrorism, non-proliferation of weapons of mass destruction, rough diamond trade transnational criminal organizations as well as Magnisty sanctions. Individuals associated with the various sanctions programs are classified as a Specially Designated Nationals (SDNs). (US Department of Treasury 2012) Although there have been changes to the U.S. Sanctions programs over the years, the illustration below provides a flavor for the scope and breadth of the various countries with U.S. sanctions programs.



(Fritsch 2010)

Recent Enforcement Actions for Non-Compliance with U.S. Sanctions

Since 2010, there has been an increase in the number of enforcement actions where major international financial institutions have agreed to forfeit billions to the United States Government in connection with apparent violations of US sanctions programs. A similarity in three of the major cases is that employees were aware of the activities that led to the violations.

HSBC Holdings plc

In December 2012, HSBC Holdings plc settled potential liability for apparent violations of multiple sanctions programs. HSBC paid a sum of $375,000,000 to OFAC for apparent violations of sanctions relating to Cuba, Burma, Sudan, Libya and Iran. From March 2004 to June 2010, HSBC processed 2,335 wire transfers for approximately $430,078,225 involving various sanctioned entities. HSBC affiliates in Europe, Asia and the Middle East processed transactions through U.S. financial institutions that involved locations, entities or individuals subject to

sanctions. The London head office and Dubai branch were cited with manipulating or "stripping" data from SWIFT messages prior to sending the payment to the U.S. for processing. The U.S. Department of Treasury found that the apparent violations were egregious and that HSBC staff failed to exercise caution in avoiding these transactions and that staff, including senior management were aware of the transactions that were being processed which led to the apparent violations. (US Department of Treasury 2012)

Standard Chartered

A day before the announcement of the enforcement actions against HSBC, Standard Chartered Bank agreed to a settlement with OFAC for $132 million for the apparent violations of U.S. Sanctions relating to Iran, Burma, Libya and Sudan. It was alleged that from 2001 to 2007 that the London and Dubai offices of Standard Chartered Bank omitted or removed references to U.S. sanctioned locations or entities from payment instructions prior to submitting the payment requests to U.S. financial institutions for processing. (US Department of Treasury 2012) (US Department of Treasury 2012)

Royal Bank of Scotland

In 2010, Royal Bank of Scotland N.V. (RBS), formerly known as ABN Amro Bank N.V. agreed to forfeit $500 million to the U.S. in connection with claims made that it conspired to defraud the U.S., violated the International Emergency Economic Powers Act (IEEPA), the Trading with the Enemy Act (TWA), as well as violation of the Bank Secrecy Act (BSA). It was alleged that ABN Amro removed critical information from wire transfers prior to submitting the instructions to U.S. financial institutions. During the course of 10 years, payments worth hundreds of millions were processed on behalf of sanctioned countries and entities. According to court documents, certain offices, branches, affiliates and subsidiaries effectively stripped any information relating to a sanctioned interest from payment messages. They also implemented procedures and a separate queue to repair payments which contain a reference to a sanctioned entity. Procedure manuals were created and included information on how to make changes to these instructions, so that the payments would bypass payment filters maintained by U.S. banks. (US Department of Justice 2010)

Who Owns the Risk?

Often times there is confusion among management and compliance as to who owns the risk relating to sanctions, to include ongoing monitoring and reporting. This can be caused by a lack of clearly defined roles and responsibilities across the three lines of defense. The challenge is to find the right balance between the various control functions to ensure that there are no gaps in coverage, while at the same time avoiding duplications in coverage and oversight. Due to the

nature, size and complexity of various financial institutions, each organization may have a slightly different way in which the work of the three lines of defense is implemented and coordinated. Noted below is a summary of the underlying role of each group as part of the compliance risk management process. (Institute of Internal Auditors 2013)

FIRST LINE OF DEFENSE	SECOND LINE OF DEFENSE	THIRD LINE OF DEFENSE
Risk Owners/Managers	Risk Control and Compliance	Risk Assurance
• operating management	• limited independence • reports primarily to management	• internal audit • greater independence • reports to governing body

Source: IIA Position Paper on the Three Lines of Defense in Effective Risk Management and Control

First Line of Defense

The business unit responsible for onboarding customers is the first line of defense responsible for embedding a strong risk and control environment into the daily business as usual activities. In relation to sanctions controls, as the first line of defense, it is the responsibility of the business to understand the customer's source of funds and wealth, expected account activity, ownership structure, as well as the associated and/or controlling parties. In the case of affiliates, it is imperative for the financial institution to know their customer's customer. If sufficient information is not obtained at the time of account opening, there is an increased risk that the customer screening against the OFAC list at the time of account opening is ineffective and increases the potential for on-boarding a sanctioned party or interest. If a foreign affiliate or correspondent has poor KYC and onboarding controls, the exposure and risk of processing a transaction on behalf of a sanctioned interest increases significantly.

Areas to be reviewed and tested by Internal Audit:

- How robust is the account opening procedure and process for the unit under review?
- Are accounts opened with missing information and documentation?
- Is there is a process in place to identify the ultimate beneficial owners, controlling and interested parties?
- How well do affiliates or foreign correspondents collect Know Your Customer (KYC) information?

Second Line of Defense

Compliance as the second line of defense is responsible for implementing and maintaining a robust OFAC compliance program to include risk assessments, written policies and procedures, interdiction software, creation of customized training, acting as a point of escalation and reporting the blocking of funds to OFAC at the time of blocking and on an annual basis going forward. A compliance testing function should also exist as part of the second line of defense, which will oversee the first line and opine on their ability to comply with OFAC requirements.

OFAC/Sanctions Compliance Program

Risk Assessment

When starting the scoping and planning for an examination of the OFAC function within an organization, the first document to obtain and review is the OFAC risk assessment. A well thought out and organized risk assessment will assist in identifying and understanding the organization's OFAC risk profile. During the planning and scoping phase, the auditor should determine if management has adequately considered and captured the various risk categories. If management has not completed an OFAC risk assessment, the audit team should perform one based on their knowledge of the business prior to commencing the review. A completed risk assessment will provide a detailed roadmap for control testing during the course of the audit. It is critical that the auditor responsible for reviewing the risk assessment understands the following factors that could have an impact on the level of OFAC risk across the organization:

- **Business Activity** – The nature and extent of business activities, including growth at a rapid pace, delivery channels, third party relationships, and significant merger and acquisition activity. If the business is expanding at a rate faster than they can fully implement controls to mitigate the risk, this could be an area for concern.
- **Products and Services** – Cross border/international wire transfers, cash letter, Trade Financing, Remote Deposit Capture, Internet banking are examples of products which heighten a U.S. financial institutions' exposure to potential OFAC violations.
- **Customer Types** – Correspondent Banks, Affiliates, Private Banking customers, Politically Exposed Persons (PEPs), Personal Investment Companies, Bearer Share accounts, Nonresident Alien, Offshore and corporate accounts with complex ownership structures are just a few examples of accounts which pose a higher risk to financial institutions.

- **Geographic Locations** – Countries with sanction programs, or countries known to be transshipment hubs for the purposes of disguising the final port of shipment, countries with a low Transparency International Corruption Index rating, countries with strategic deficiencies according to FATF and offshore financial centers/tax havens should be considered when assessing the country risk.
  (Federal Financial Institutions Examination Council 2010)

Once evaluation of the risk assessment has been performed, the auditor can begin to focus on the design, implementation and embeddedness of the various controls put in place to manage OFAC risk. This can be accomplished by performing detailed testing surrounding the key areas of the OFAC Compliance Program across the two lines of defense. In cases where the first and second lines of defense are considered to be mature and have processes in place to self-identify issues, audit may supplement or decide to rely on the results of the work performed. The results of this testing and monitoring can assist audit in forming its view of the control environment. If it is determined that reliance cannot be placed on the first or second line, audit will have to perform detailed testing of controls across the program to support their overall conclusions of the effectiveness of the control environment across the organization for OFAC Compliance.

OFAC Compliance Officer

As part of the overall OFAC Compliance program, a dedicated OFAC Compliance Officer should be appointed to oversee the day to day operations within the OFAC Compliance Program. The individual appointed to this position should have prior experience managing and overseeing an OFAC Compliance program with a similar risk profile.

Areas to be reviewed and tested by Internal Audit:

- The auditor should obtain a copy of the OFAC Compliance Officer's resume and opine on their experience relating to OFAC Compliance.

OFAC Governance Forum

A governance forum or committee should be established consisting of representation from the business lines, as well as compliance and information technology departments. The mandate and committee charter should include approval of policies and procedures, review of management reporting, potential violations of law and/or voluntary self-disclosures, changes to the interdiction software/OFAC filter and approval of any processes that are outside of the established policy. The forum should be informed of emerging risks changes in legislation and have metrics or key risk indicators to assist management in the decision making process.

Areas to be reviewed and tested by Internal Audit:

- The auditor should obtain the committee charter, meeting minutes and determine if all of the committee's objectives have been met, there is effective challenge and the membership includes representation from the various lines of business and compliance functions.
- Obtain the MIS reporting provided to the committee and opine on the effectiveness and if it is designed to assist in the management decision process.

Risk-based approach to scanning for OFAC Compliance

While a specific OFAC compliance program is not required to be implemented by U.S. Financial institutions, it is a matter of sound banking practices that a written compliance program be implemented to effectively mitigate the OFAC risk faced by the institution, which is determined based upon the products, services, customers and geographic locations in which the organization operates and does business. The program should include written policies and procedures, establish protocols for screening customers and transactions, blocking, rejecting and reporting transactions to OFAC, designated OFAC Compliance Officer, Governance and Oversight Committees, training for employees and independent testing for compliance. (Federal Financial Institutions Examination Council 2010)

Areas to be reviewed and tested by Internal Audit:

- Review the OFAC Compliance Program Manual and ensure all key functions processes and controls are properly documented. The manual should be reviewed and updated on a regular basis.

Most major financial institutions will use interdiction software or more commonly known as an OFAC filter to scan transactions for compliance with the various OFAC sanctions programs. Interdiction software includes an element of "fuzzy logic", which would identify misspellings in sanctioned countries, ports, vessels or individual names. An example of fuzzy logic that would generate an alert for most interdiction software would be Cuba spelled as Kuba.

Areas to be reviewed and tested by Internal Audit:

- Prepare a list of variations to the names on the current SDN list to determine if the filter is generating alerts for exact matches and partial matches. Where a partial name match does not generate an alert, research should be performed into the reason why. Was this deliberate on the part of OFAC Compliance, Information Technology or Payment Operations?

- Have exclusions been built into the filter due to the number of alerts that would be generated?
- Is the filter sensitivity threshold set to manage the number of alerts based on staffing levels, rather than risk?
- Is there a "if then" rule in place, which requires not only the name to be a match but other details, such as date of birth to generate an alert.
- If there are special exclusions or rules built into the filter, ensure that there is a process in place to have these items approved by an Oversight Committee and that the rationale is adequately documented.

The OFAC compliance officer in conjunction with input from information technology, operations and AML compliance will prepare a number of lists to be included in the routine screening processes. For instance, there may be individuals from an AML perspective that the organization elects not to do business with. The OFAC Compliance team has the flexibility to input a series of names not related to sanctions into the filter, which will generate an alert if the individual tries to open an account or process a transaction with the organization.

Areas to be reviewed and tested by Internal Audit:

- In addition to preparing a list of names to test against the filter, the auditor should also understand and document, via a process flow or narrative the process to update the filter when there are additions to the various sanctions programs or SDN list. A few questions to consider when reviewing the change management process:
    - Who in the organization is responsible for obtaining changes to the various sanction programs/lists?
    - Where does the information come from?
    - How is the information communicated across the organization?
    - Who is responsible for updating the filter?
    - What is the turnaround time?
    - A sample of recent changes/additions should be selected for further review and the auditor should ensure all changes/additions were made to the filter in a timely manner and properly communicated across the organization.

Customer Screening

Typically, customers will be scanned against the OFAC filter at the time of account opening and when there are any changes to theSDN List. When opening an account, the ultimate beneficial owner(s) and controlling/related parties should be scanned for OFAC compliance. This would include authorized users, such as bookkeepers on commercial accounts and joint account holders for personal accounts.

Areas to be reviewed and tested by Internal Audit:

- The auditors should examine how the UBOs and associated parties are identified and documented in the system of record. There should also be a test to ensure that all names are included in the scanning process, whether real time or as part of a nightly batch process.

Transaction Screening

International wire transfers and trade related transactions should be subject to real-time screening against the OFAC filter prior to processing. Cross border wire transfers and letters of credit are high risk for financial institutions, making it imperative that the U.S. bank has all of the required information to fully understand the purpose of the transaction and the involved parties when an alert is generated. Where the payment is either blocked or rejected, depending the on the sanctions program, the filter should be programmed to flag a similar transaction if resubmitted with missing/different information or a variance in dollar amount. Resubmission of the same payment instructions, with a difference in country origination or destination or dollar amount, may be an indication of information stripping.

Areas to be reviewed and tested by Internal Audit:

- The auditor should obtain a list of all products and services offered and determine if the individual transactions are subject to sanctions screening either real time or as part of a daily batch process.
- The auditor should also determine if management has performed a system mapping, to ensure that all transactions from the various banking platforms and systems are subject to screening against the filter.
- If gaps have been identified, obtain management's action plan and assess the process made against key deliverables and target dates.
- Focus should be geared towards transactions that are subject to manual scanning and determine the rationale for the manual monitoring, such as volume or risk to the organization.

Alert Review and Disposition

Alerts generated as part of the customer or transaction screening should be reviewed and cleared by individuals with sufficient knowledge and resources. Standard procedures and detailed instructions for clearing alerts should be documented and made available for all alert clearing staff. Where the alert is determined to be a false positive, supporting documentation and a rationale should be clearly documented justifying why there was not a true match to a sanctioned country, port vessel, individual or entity. When the first level reviewer is in doubt or

needs additional information to determine the status of the alert, a clear line or point of escalation should be established. Management should also have a mechanism to identify and age alerts.

Areas to be reviewed and tested by Internal Audit:

- A sample of alerts closed as false positives should be selected for further review. The auditor assigned to this task should review the alert and the supporting documentation on file used to close the alert.
- Determine the information that is used to determine if the alerts generated are true false positives.
- Select a sample of aged alerts and determine the cause for the delay and the escalation process in place.

Blocking and Reporting of Transactions

A central point of contact should be established in the Compliance function that is responsible for opening interest bearing accounts for all blocked assets. The same team should also be responsible for notifying OFAC of the blocked funds at the time of blocking and as part of the annual report of blocked funds.

Areas to be reviewed and tested by Internal Audit:

- A sample of blocked transactions should be selected for further review to determine if the funds have been placed in an interest bearing account and that OFAC was notified in a timely manner.
- A reconciliation should also be performed comparing all blocked assets as per the system of record to the annual report of blocked accounts, to ensure that annual report of blocked accounts is accurate.

Training

At a minimum, OFAC awareness training should be provided on an annual basis to all employees across the organization. Employees who work in higher risk business lines, such as Trade Finance, Private Bank or Payment Processing should receive customized training to assist with their day-to-day activities and identification of potential OFAC violations.

Areas to be reviewed and tested by Internal Audit:

- The auditor assigned to training should review the course content to determine if it is appropriate for the audience, the general awareness training, as well as the customized training for staff in the higher risk business lines.

- Determine the completion rate across the organization.
- Determine the methodology used by compliance and the business to identify the staff that requires customized training.
- Obtain and review the needs analysis that was performed by the training department.

Second Line of Defense Testing Function

As noted above, a compliance testing function should also exist as part of the second line of defense, which will oversee the first and second lines with an objective to opine on their ability to comply with OFAC requirements. The testing function may perform reviews similar to Internal Audit, but should not be considered as an Internal Audit Function. The testing function should report directly to the Chief Risk Officer or Chief Compliance Officer. Depending on the quality of work, Internal Audit may be able to place reliance on the work performed by the second line. Internal Audit should work closely with the second line testing functions to understand their review plan, scope, objectives and timing of the reviews in order to minimize duplication and overlap.

Areas to be reviewed and tested by Internal Audit:

- Determine if the second line of defense testing function sufficiently staff with individuals who have requisite technical expertise.
- Obtain and review the annual testing plan and ensure all key controls are included in plan.
- Select a sample of completed reviews and review the work papers to determine if the key controls were tested and where control weaknesses were noted, they were properly reported.

Third Line of Defense

Internal Audit serves as the third line of defense and is required to provide an independent assessment of the controls put in place across the first and second lines of defense to mitigate the OFAC risk and exposure across the organization. Where there is overlap of testing or monitoring activities to those undertaken by the first or second lines of defense, these are undertaken as part of Internal Audit's independent assurance role and should not be relied upon by management as a substitute for, or supplement to, first or second line of defense activities. The result of the reviews performed by Internal Audit should be provided to the Audit Committee of the Board of Directors. It is imperative that the audit plan is risk based, covering the highest risk areas within the organization. The plan should be considered as a living document and reviewed on a periodic basis to ensure coverage is appropriate and all emerging risks have been considered. The Internal Audit function should also be staffed with individuals

who possess the requisite subject matter expertise, having worked in compliance, the business as a consultant or for a regulatory agency.

Results of Internal Audit reviews, to include work papers and reports will be reviewed by the Regulators and in some cases; they will look to rely on the work performed by Internal Audit when completing their examinations or targeted reviews of the financial institution's AML/OFAC compliance program. It is imperative that all work papers completed by Internal Audit are well documented and provide support for decisions made. The documents should be able to stand on their own. A third party should be able to read the work papers and walk away with a clear understanding of the scope, objective and results of the test work performed. The reports should also be written in a clear and concise manner, which articulates the issues and risks to the organization.

In recent years, there have been instances in which US Regulators have criticized the AML/OFAC coverage performed by Internal Audit for failure to identify control deficiencies. Many of these criticisms stem from insufficient risk-based audit coverage, lack of individuals with the requisite subject matter expertise and experience, as well as the inability escalate issues and effectively challenge senior management. (Abel 2009)

Bibliography

Federal Financial Institutions Examination Council . *FFIEC BSA/AML Examination Manual .* 2010. http://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2010.pdf (accessed October 28, 2013).

Institute of Internal Auditors. *The Three Lines of Defense in Effective Risk Management and Control.* IIA Position Paper , Institute of Internal Auditors, 2013.

Kimberly Ann Elliot, Gary Clyde Hufbauer and Barbara Oegg. *Library of Economics and Liberty [Online].* 2008. http://www.econlib.org/library/Enc/Sanctions.html (accessed October 28, 2013).

Slear, Judith Lee and James. *Beware of OFAC.* Washington DC, September 2006.

US Department of Justice . *US Department of Justice - Office of Public Affairs .* May 10, 2010. http://www.justice.gov/opa/pr/2010/May/10-crm-548.html (accessed Septmeber 16, 2013).

US Department of Treasury . *US Department of Treasury Press Center .* December 11, 2012. http://www.treasury.gov/press-center/press-releases/Pages/tg1799.aspx (accessed September 18, 2013).

—. *US Department of Treasury Resource Center.* December 10, 2012. http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/12102012_scb.pdf (accessed September 18, 2013).

US Department of Treasury. *US Department of Treasury Press Center .* December 10, 2012. http://www.treasury.gov/press-center/press-releases/Pages/tg1792.aspx (accessed September 16, 2013).

—. *US Department of Treasury Resource Center.* December 11, 2012. http://www.treasury.gov/resource-center/sanctions/CivPen/Documents/121211_HSBC_posting.pdf (accessed September 16, 2013).