Iakyara vol.312

Special Edition

Risk-based approach to AML/CFT

- Interview with Hiroshi Ozaki by Ryuichi Matsushita -

3.February.2020

Nomura Research Institute, Ltd.

Executive Summary

With financial services now globalized, countries around the world have to coordinate with each other to prevent money laundering and terrorist financing. Their AML/CFT regimes are evaluated by the Financial Action Task Force (FATF), an international organization. If a country were to fail an FATF evaluation, its international reputation would be tarnished. We spoke to Hiroshi Ozaki, Director of the Japanese FSA's ALM/CFT Policy Office, about what Japanese financial institutions' immediate priorities should be.

Hiroshi Ozaki

Director
AML/CFT Policy Office
Strategy Development and Policy Bureau
Financial Services Agency

Appointed Director of FSA's AML/CFT Policy Office in February 2018 following 30-year career with Sumitomo Mitsui Banking Corporation (originally Mitsui Bank), including stints in New York, London and Dubai. Concluded tenure at SMBC as head of AML/CFT compliance. Holds MBA from New York University and Certified Anti-Money Laundering Specialist credential.

Ryuichi Matsushita

General Manager
Global Financial Solution Business Department
NRI

Joined NRI in 1992. Headed NRI Singapore's financial systems business and served as Vice President of iVision Shanghai, a joint venture between NRI and Mitsubishi Corporation, before assuming current position in 2017.

AML/CFT starts with KYC

Ryuichi Matsushita: Thank you for taking the time to meet. I know you've been busy with the FATF's just-completed on-site visit as part of its evaluation of Japan. I want to talk about anti-money-laundering and countering financing of terrorism (AML/CFT).

The FSA recently reported that the FATF's 2019 evaluation would assess Japan's AML/CFT legal and regulatory regime and the effectiveness of AML/CFT measures in Japan. Since the last FATF evaluation, Japan has made considerable progress on the AML/CFT front, including enactment of various legislation and publication of the FSA's Guidelines for Anti-Money Laundering and Combating the Financing of Terrorism in February 2018. What are the keys to more effective AML/CFT?

Hiroshi Ozaki: I believe the first priority is to strictly adhere to a risk-based approach, the minimum standard for AML/CFT. Financial institutions need to comply with the FSA's AML/CFT Guidelines in addition to applicable laws such as the Act on Prevention of Transfer of Criminal Proceeds. We want them to expedite implementation of the Guidelines' required actions.

The first step in AML/CFT is verification of customers' identity. It's crucial for financial institutions to diligently verify identity as a routine step in the process of opening a new account or initiating transactions. Particularly when dealing with a corporation, financial institutions must ascertain the corporation's beneficial owners and screen them against lists of sanctioned parties and criminal organizations to prevent illicit transactions. Next, financial institutions must do a customer risk assessment that takes into account customer attributes, products/services, transaction modalities, geographic locations and other relevant factors.

Even existing customers need to be monitored in accord with their respective risk levels by IT systems and/or customer-facing employees. If any unusual transactions are detected, a suspicious transaction report should be filed. Vigilance is required because even customers who were not being red flagged when their identity was initially verified can subsequently become problem customers. To detect such cases, financial institutions must be able to spot changes in transaction patterns. These changes are generally detected electronically, so monitoring systems' ability to detect

various scenarios must be tested regularly. Lastly, due diligence on customers has to be periodically updated at a frequency commensurate with customer risk.

Matsushita: So the key is to improve and maintain the accuracy of identity verification, which ultimately comes down to the quality of individual financial institutions' customer data.

Ozaki: Exactly. If customer attribute data are outdated, you cannot count on identity verification and customer risk assessments to be effective. To update customer attribute information, you have to check in with customers, demanding their time. We understand that keeping customer information up to date is a huge task given how many customers financial institutions have, but doing so helps to protect customers, Japan's financial system and, in turn, the financial institutions themselves. We want financial institutions to get customers on board with keeping their information up to date.

Matsushita: I understand identity verification is the first step in AML/CFT, but what about the recent talk about going beyond KYC (know your customer) to KYCC (know your customer's customer)?

Ozaki: KYCC is not required under the FSA's Guidelines. KYCC is most clearly illustrated in the context of correspondent banks. If Japanese Bank A enters into correspondent agreement with foreign Bank B, both are required to monitor each other. Their respective KYC mandates do not extend to each other's customers, but both must ascertain how the other one screens and monitors its customers and conducts risk management.

Matsushita: So having a database suitable for managing customer information is important, as is data governance given the sensitivity of the information involved.

Ozaki: System requirements vary depending on the financial institution's size, but customer information for AML/CFT compliance requires a database capable of managing customer risk scores and updating them based on customer risk assessments. A hard-copy filing process is not adequate. The database needs to

be able to handle identity verification tasks also, such as expiration date tracking to keep customer information from becoming stale. We strongly encourage financial institutions to maintain databases compatible with their size and industry.

Additionally, you cannot just install a database or IT system and then leave it. You have to periodically test your systems and upgrade them as dictated by the test results. It's also advisable to have personnel with expertise in database/system administration and maintenance. From such a perspective, I see an important role for IT-system sharing and joint back-office arrangements that make the requisite IT more accessible to financial institutions irrespective of their size. The Japanese Bankers Association has been researching such arrangements since last year. I believe financial institutions need to seriously look into putting the JBA's research findings into actual practice.

Matsushita: AML/CFT is an issue for all financial institutions, not just depository institutions. In this sense, sharing of IT infrastructure across different financial subsectors based on the JBA's research may be worth considering.

Ozaki: I agree. Promoting IT-system sharing more broadly than just among depository institutions would be beneficial.

Risk-based approach to AML/CFT

Matsushita: While a risk-based approach is fundamental to AML/CFT, financial institutions tend to favor rules-based approaches to regulatory compliance.

Ozaki: As I mentioned at the outset, the risk-based approach (RBA) is literally the minimum standard. I'll now go into more detail on the RBA and how to implement it.

The RBA starts with identifying what types of risks exist with respect to at least four factors: customer attributes, products/services, transaction modalities and geographies. Next, you assess the risks' magnitude either qualitatively or quantitatively (e.g., through risk scoring). The key point is to be comprehensive.

In financial institutions, the compliance department may not actually be well versed in all available products and services. First, organizational units that deal in products and

services must identify every single one of them in specific terms, not general terms like “deposits” or “electronic funds transfers.” Once a detailed and comprehensive list of products and services has been compiled, the risks associated with each must be identified and assessed. The compliance department then thoroughly checks whether risk mitigation measures commensurate with the risk assessments are in place. This is the first step.

The second step is customer risk assessment. It entails pulling together information on individual customers’ attributes, the types of transactions they engage in and the products/services and geographic locations involved. This information is used to comprehensively assess customer risk.

Matsushita: Those risk assessments form the basis of risk mitigation measures, correct?

Ozaki: Yes. The risk mitigation measures take one of two forms: measures focused on transactions themselves and measures specific to individual customers. From an RBA standpoint, what I’ve described so far is the minimum standard. We’ve recently been looking at speeding up this process.

Matsushita: I’ve heard, for example, that when financial institutions do customer risk assessments they sometimes incorporate too many risk factors into their models and consequently end up with little variation in risk scores among customers. They need to upgrade their assessments by initially focusing on a small handful of risk factors to clarify the most salient risks and then iteratively adding more risk factors.

Ozaki: Yes. Another key point about the RBA is that it’s a dynamic process, analogous to the PDCA (plan-do-check-act) cycle. You first assess risks and devise risk mitigation measures. You then check those measures’ effectiveness. Did they adequately reduce risk with respect to products and services? Did suspicious transaction reports decrease or increase?

At least once a year, you assess the overall program and make adjustments as

needed, adding corrective measures in response to deficiencies and zooming out to a higher-level perspective if risk assessments are too granular. It's important to go through this process every year.

Matsushita: Do you have any pointers for performing such reviews?

Ozaki: The key is identifying the risks that your own institution is facing. If you analyze suspicious transaction reports and fraud losses to determine whether risk is decreasing or increasing and how your institution compares in this regard with financial institutions in general, you should end up with a realistic risk assessment. It's also a good idea to refer to the National Public Safety Commission's national AML/CFT risk assessments.

Matsushita: I imagine that sharing knowledge with other banks will also play an important role in upgrading risk analyses and AML/CFT in general.

Ozaki: Indeed. We want industry organizations to take the lead in promoting such sharing within their respective industries. The FSA intends to likewise publish essential information, such as reports on financial institutions' current state and issues they are facing. Other valuable resources include the FATF's RBA guidance, which recommends best practices on a country-by-country basis, and similar information from overseas.

IT vendors' expected role

Matsushita: As a provider of information systems to financial institutions, we at NRI would like to know what you expect of IT vendors from an AML/CFT standpoint.

Ozaki: The databases and IT systems used for AML/CFT compliance include analytical systems that perform filtering, screening and monitoring and enterprise systems for case management.

IT systems require continual updates. Screening systems must be tested to ensure their fuzzy search settings are properly calibrated. Monitoring systems' scenarios must undergo validity testing. If test results are unsatisfactory, the systems must be re-tuned. Additionally, financial institutions' IT systems are not one-size-fits-all. They

vary in accord with the institutions' respective operational characteristics. Financial institutions should work together with IT vendors to customize their IT systems to their businesses.

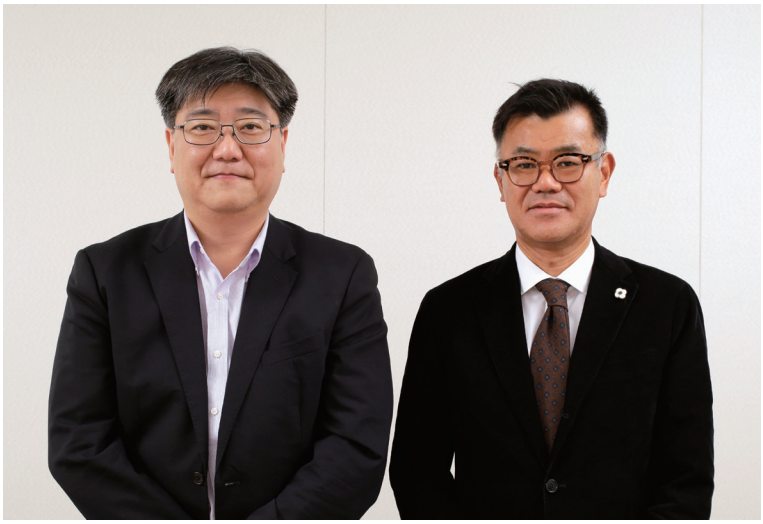
I would also like to see IT vendors come up with effectiveness testing tools for IT systems and databases–for example, tools that would enable internal auditors or independent auditors to independently test IT systems and databases. Please develop such tools.

Matsushita: Do you mean, for example, tools that assess how well financial institutions' IT systems detect red flags by inputting test datasets containing customer information and/or transactions that meet detection criteria?

Ozaki: Yes, among others. I would like internal auditors to be able to check screening systems' false alarm and missed detection rates through test data runs. It would be nice if support for such testing were available from independent IT vendors or consultants. Testing performed by third parties such as independent auditors is another option from the standpoint of objectivity and independence.

Matsushita: At Singapore FinTech Festival 2019 in November, I sensed a change from the previous year with respect to KYC. I saw a lot more vendors and products using external data, including alternative data, to improve KYC accuracy or efficiency.

Ozaki: I believe next-generation KYC will tap into bigger data troves by virtue of automated collection and analysis of information associated with customers, including



even unstructured data such as social media content, for example. To reach that point, financial institutions must first maintain data freshness by continually updating customer-attribute data and information they are legally required to collect.

Matsushita: Digital transformation (DX) has become a management priority not only among financial institutions but across all industries. KYC and data governance are at the heart of DX. From such a perspective, the KYC and data governance expertise, know-how and experience that financial institutions have amassed in their AML/CFT compliance programs should be valuable assets in terms of DX also.

Ozaki: I agree. I believe even AML/CFT will transition to the world of DX, given how information intensive it is. Needless to add, however, adequate safeguards to protect personal information are essential.

Matsushita: Thank you for an enlightening conversation.

about NRI

Founded in 1965, Nomura Research Institute (NRI) is a leading global provider of system solutions and consulting services with annual sales above $4.5 billion. NRI offers clients holistic support of all aspects of operations from back- to front-office, with NRI's research expertise and innovative solutions as well as understanding of operational challenges faced by financial services firms. The clients include broker-dealers, asset managers, banks and insurance providers. NRI has its offices globally including New York, London, Tokyo, Hong Kong and Singapore, and over 13,000 employees.

For more information, visit https://www.nri.com/en

Inquiries to : Financial Market & Innovation Research Department
Nomura Research Institute, Ltd.
Otemachi Financial City Grand Cube,
1-9-2 Otemachi, Chiyoda-ku, Tokyo 100-0004, Japan
E-mail : kyara@nri.co.jp

http://fis.nri.co.jp/en/publication/special.html