In 2016, the private banking scene in Singapore has witnessed a series of events such as the sale of Barclays Wealth to Bank of Singapore and the Monetary Authority of Singapore (MAS) revoking the banking license of BSI Bank in Singapore for its Anti-Money Laundering (AML) / Counter-Terrorism Financing (CTF) lapses linked to 1MDB.

In addition, we have the Panama Paper leak, exposing a staggering number of 4902 intermediaries in Hong Kong alone. This left the private banks in the region under an increasing amount of pressure to monitor the activities of the Politically Exposed Person (PEPs).

Amidst this are rising compliance costs and tighter regulations, but this does not stop Asian wealth firms from benefiting from the “positive” business momentum created through economic growth, as mentioned by Tan Su Shan, co-chair of MAS’s private-banking industry group.

In the wake of these events, Kristen Lim from Huxley Banking & Finance has hosted an inaugural roundtable discussion with the Operational Risk Leaders in Singapore on how they manage risk for the banks in this challenging period.

Alex Sim, COO of UOB Private Bank: I am a firm believer of having a strong risk manager who understands and is part of the business, clearly distinct from the second and third line. In any case, regulators expect the business to be accountable for risks they take on and manage them accordingly. We need good risk practitioners working in and supporting the business, rather than police them.

There is a school of thought that suggests integrating the first and second line due to the common business view that the second line fails to understand in terms of the business, to provide effective risk management solutions or mitigations. The distinction between the first and second line (i.e. Compliance, Operational Risk) is left blurred in some banks and as a result, we often hear the phrase “1.5” line of defense. To me, this does not help – where does one draw the line of independence? We end up placing an unrealistic expectation on a risk manager in the first line to be independent, yet reporting into the business head.

Ultimately, I think the shift into having a strong first line to make the business accountable will continue. This must be derived from the ability of risk managers to provide sound advice or solutions to the issues at hand. I think that is the real value of the first line. With this in place, the second and third lines can concentrate on their roles as checks and balance.

*Head of Business Risk Management, Private Bank: One of the leading private bank in Singapore has been observed investing heavily within the first line the past year. Having a Business Control Management team who performs over a larger sample base control now allows the Business Risk Manager (first line) to perform checks on the business, while the Operational Risk Managers (second line) perform checks on the first line.

HUXLEY: HOW CAN WE ACHIEVE A SUCCESSFUL ENTERPRISE RISK MANAGEMENT (ERM) AND BUSINESS MODEL INTEGRATION?

Chee Keong Tan, Head of Operational Risk, Royal Bank of Canada: I think there are two key elements Risk Managers must demonstrate to show the value they can add during business discussions and outcomes. As practitioners, we will need to establish credibility to earn that right. What is equally important is the tone from the top by the senior management as most people behave and act in accordance to the management’s focus and priorities. In order to have a successful risk management and business model integration, these two components need to be working hand in hand.

Alex Sim: Risk management can only be part of the process when the business recognizes the value of the first line thereby explaining the reasons for a strong first line. With a strong team on the first line, we are definitely one step closer to achieving a successful ERM.

Eva Gessner, Chief Risk Manager of UBS: In terms of business model integration, our risk managers in the first line are often involved in advising the business on risk impact and what they need to look out for in the context of cross-border, regulations, etc. We partner with the business to find the best model for the firm.
HUXLEY: HOW IS EVENT PROBABILITY DEFINED OR MEASURED ON SCENARIO ANALYSIS?

Kevin Headley, Global Markets Head of Operational Risk: When I was dealing with certain global regulators in the context of cyber and infrastructure failures, they expect a very realistic viewpoint. In effect, you are given the probability factor of one. This means that you must expect that this event will take place and your stress test must factor in that expectation. This is not just the traditional expectation of 1 in 1000 years or 1 in 10 years. I’ve seen situations where regulators have gone to the point of expecting clear thresholds in terms of dollar impact that comes out between a few scenarios. It can be a very interesting situation on how they may be offering a hint to the amount of capital that is potentially affected. If you create a scenario with a number that is too low in terms of impact, it may very well get rejected. This is one factor in how the Government collates stress tests that can emerge at a global level outside Asia.

*Group Head of Operational Risk, Global Bank: There are banks which have recently published their operational risk’s stress-testing framework. Inputs from the business are usually gathered from the operational risk managers covering the business while scenarios are stretched to cover probability of event. This probability is always defined as the following: most likely, likely and unlikely to happen. However, there hasn’t been any scientific calculation around it yet.

HUXLEY: HOW IS CYBER SECURITY RISK HANDLED WITHIN THE OPERATIONAL RISK FRAMEWORK - IN TERMS OF INTERACTION WITH IT, INFORMATION SECURITY AND DATA LEAKAGE UNIT?

Eva Gessner: For UBS, cyber security risk is generally handled globally and the individual countries are involved through implementations of policies and frameworks relevant to them. As an industry we have to acknowledge that cyber risks are very real and growing. Communication channels such as WhatsApp or WeChat have become very popular and the industry will have to learn to adapt to this.

Chee Keong Tan: The recent Bangladeshi incident highlighted the growing cyber security threat. SWIFT has also reported several similar incidents. As such incidents are usually fairly technical in nature, the operational risk practitioners would need to work closely with technology experts, and act as an important interface to bridge the gaps between technical and business stakeholders.
HUXLEY: WHAT ARE THE EMERGING OPERATIONAL RISK IN THE NEXT 1-2 YEARS?

• Cyber security risk

In one of the leading private banks in Singapore, verification through video conference meetings are valid as long as an independent part is present. Although the bank still requires a hard copy of the passport eventually, despite the verification of the client’s identity through an e-meeting, there is a need to strike a balance and understand that the ease of communication is a risk the client must take as technology platforms may not be fully encrypted.

Alex Sim: I see cases where Relationship Managers (RM) communicates extensively with clients via mobile messaging applications. With technology advances and increasing convenience, at some point, clients will be expecting to use this mode of communication to transact. Imagine the use of video capabilities on mobile devices to fulfil client verification instead of a RM heading down personally. Are we comfortable, as risk managers, to embrace such platforms as the norm rather than exception?

• Fraud risk

Chee Keong Tan: While we consider the client’s experience, we should also be mindful of the internal fraud dimension. In terms of devising a solution or making a decision, there is a need to have a good understanding of the circumstances and consequences. I would deem the use of some of these technology solutions not advisable with the current state of technology. Some banks may have higher risk appetite thereby choosing a higher acceptance on certain types of cyber risk. They would need to consider the various scenarios that may lead to internal fraud risk, litigation risk and many others. As long as there is a robust risk identification and mitigation process, you would be able to derive the optimal solutions for your business.

WHAT’S NEXT?

After a round of speaking with the Operational Risk Leaders within the industry, it is important for the banks to set the tone from the top while having Risk Managers in place who could help the business make better decisions. Defining a good Risk Manager: one who understands the business would no doubt bring a greater contribution towards the strategies of the business. They should be a trusted advisor to the business, and a go-to person for business solutions.

If you have any questions, please contact:

Kristen Lim
Audit, Risk and Governance Recruitment
+65 6572 4500
k.lim@huxley.com
https://sg.linkedin.com/in/kristenlim
www.huxley.com

*Industry personnel who wish to be kept anonymous.

Disclaimer: The views and opinions expressed in this article are those of the authors and do not necessarily reflect the official policy or position of any company.