IAF BUSINESS INNOVATION SYMPOSIUM (E6)
Strategic Risk Management for Successful Space & Defence Programmes (4)

Author: Ms. Marina Pokrovskaya
Germany

RISK MITIGATION BASED ON INNOVATIVE SOLUTIONS

Abstract

Considering current challenges to the well-being of an enterprise, practitioners tend to evaluate them through the prism of risk management frameworks. These include a wide array of tools to mitigate risks arising from the distinct risk factors that are further consolidated under the risk strategy of a specific enterprise. Any firm in space industry and outside of it faces risks that can be associated with the following key areas: strategic, reputational, regulatory, financial, operational, and cyber. Integrating high tech innovative solutions into the risk mitigation process has now become available by implementing tools based on artificial intelligence technology. Recent advances in risk management are numerous and include Regulatory Technology (RegTech) and Financial Technology (FinTech) solutions that are necessary in the competitive environment. Conservative risk mitigation methods are not fast paced enough to conduct numerous iterations in a split second timeframe and tackle arising risks. For instance, the new regulatory framework design for the company will be more efficient if it grounds on the RegTech concept. The latter automates the state-of-the-art risk mitigation methods and allows for integrating human expertise and newest technology. As for the operational risk mitigation, converging to new technological solutions would also prevent massive problems of the past. The hacking attack on the Bank of Bangladesh in February, 2016 led to a substantial theft of $81m. A number of transactions were blocked due to simple spelling mistakes that eventually prevented higher extent of losses. Hackers made use of gaps in local IT infrastructure of Society for Worldwide Interbank Financial Telecommunications (SWIFT)-member banks to send fraudulent messages. Currently Customer Security Program (CSP) would avoid similar situations. Compliance of members from SWIFT-network to sixteen mandatory standards makes it possible to raise their local IT security, whereby compliance is also enforced through random checks and external audits. Information sharing aims at avoiding future hacking attacks by means of collaborating on preventive measures and implementing the baseline standard for all member firms. Future implementation of blockchain technology is a possible solution to ensure cyber integrity of SWIFT network. Faster and safer funds transfer with increased efficiency and transparency will also allow for maintaining constant information sharing and real-time monitoring. Its functionality is dependent on degree of automatization and centralization of members. Furthermore, better governance and information management are key in the strategic risk management of any enterprise. Finally, risk mitigation plays a crucial role in reaching the organization's goals.