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

Author: Mr. Antonio Carlo
Tallinn University of Technology, Estonia

Ms. Francesca Casamassima
Italy

GOING DIGITAL, STAYING SECURE: CYBER ERM ACTIVITIES IN A POST-PANDEMIC SETUP

Abstract

The last decades have been characterized by a rapid process of digital transformation, the so-called Industry 4.0. In addition to generating many new opportunities for businesses, it has contributed to the emergence of a new dimension of risk arising from the adoption of new Emerging Disruptive Technologies (EDTs), such as Artificial Intelligence, Internet of Things (IoT), and Cloud Computing. Hence, the need has emerged for enterprises to navigate risk through the adoption of Enterprise Risk Management (ERM) activities that are effective in a digital context. In particular, digital transformation has contributed to the emergence of new cyber threats, thus making cyber risk assessment an enterprise critical in managing ERM programs. Indeed, the development of an integrated and comprehensive ERM program could significantly contribute to enterprises' capabilities to identify risks, manage cybersecurity practices and support their objectives. Moreover, recent years have also witnessed an increase in the number of "Black Swans" and low probability-high impact events such as the Covid-19 outbreak, which require timely interventions in the reorganization of the company in order to ensure Business Continuity and minimize the negative impact of the event on the operation of the enterprise itself. The aim of the paper is therefore to provide a holistic view of the topic, starting from the analysis of how two specific sectors have adapted their cyber ERM activities to the pandemic, and to suggest a way forward for the assessment of unlikely events, which might become increasingly frequent in the coming years.