World Academy of Science, Engineering and Technology
International Journal of Economics and Management Engineering
Vol:13, No:01, 2019

CybeRisk Management in Banks: An Italian Case Study

Authors : E. Cenderelli, E. Bruno, G. Iacoviello, A. Lazzini

Abstract : The financial sector is exposed to the risk of cyber-attacks like any other industrial sector. Furthermore, the topic of CybeRisk (cyber risk) has become particularly relevant given that Information Technology (IT) attacks have increased drastically in recent years, and cannot be stopped by single organizations requiring a response at international and national level. IT risk is never a matter purely for the IT manager, although he clearly plays a key role. A bank's risk management function requires a thorough understanding of the evolving risks as well as the tools and practical techniques available to address them. Upon the request of European and national legislation regarding CybeRisk in the financial system, banks are therefore called upon to strengthen the operational model for CybeRisk management. This will require an important change with a more intense collaboration with the structures that deal with information security for the development of an ad hoc system for the evaluation and control of this type of risk. The aim of the work is to propose a framework for the management and control of CybeRisk that will bridge the gap in the literature regarding the understanding and consideration of CybeRisk as an integral part of business management. The IT function has a strong relevance in the management of CybeRisk, which is perceived mainly as operational risk, but with a positive tendency on the part of risk management to the identification of CybeRisk assessment methods that are increasingly complete, quantitative and able to better describe the possible impacts on the business. The paper provides answers to the research questions: Is it possible to define a CybeRisk governance structure able to support the comparison between risk and security? How can the relationships between IT assets be integrated into a cyberisk assessment framework to guarantee a system of protection and risks control? From a methodological point of view, this research uses a case study approach. The choice of “Monte dei Paschi di Siena” was determined by the specific features of one of Italy’s biggest lenders. It is chosen to use an intensive research strategy: an in-depth study of reality. The case study methodology is an empirical approach to explore a complex and current phenomenon that develops over time. The use of cases has also the advantage of allowing the deepening of aspects concerning the "how" and "why" of contemporary events, on which the scholar has little control. The research bases on quantitative data and qualitative information obtained through semi-structured interviews of an open-ended nature and questionnaires to directors, members of the audit committee, risk, IT and compliance managers, and those responsible for internal audit function and anti-money laundering. The added value of the paper can be seen in the development of a framework based on a mapping of IT assets from which it is possible to identify their relationships for purposes of a more effective management and control of cyber risk.

Keywords : bank, CybeRisk, information technology, risk management
Conference Title : ICRFSB 2019 : International Conference on Risk, Financial Stability and Banking
Conference Location : Zurich, Switzerland
Conference Dates : January 14-15, 2019