PRINCIPAL ACADEMIC TUTOR
Carlo Cambini
DIGEP, Politecnico di Torino

ACADEMIC TUTOR
Stefano Zanero,
DEIB, Politecnico di Milano

EXTERNAL INSTITUTION
Intesa San Paolo

TEAM MEMBERS

Alberto Meneghesso, Management Eng, PoliMi

Giacomo Bima, Industrial production Eng, PoliTo

Alfonso Palmieri, Nanotechnologies for ICTs, PoliTo

Alberto Sivera, Nanotechnologies for ICTs, PoliTo

INTO THE DIGITAL ODYSSEY

Executive summary

The digital revolution is reshaping the financial sector, making new products and services possible for the customers: but this does not come without a cost. More specifically, banks are facing the challenge of reshaping business operations and processes using digital tools and algorithms which are not exempted by what is called the "Regulation Tsunami", an exponential increase in the number of regulations.
In this context, Into the Digital Odyssey, collaborating with the newly created CDT structure (Compliance Digital & Data Transformation) of Intesa Sanpaolo (ISP), aims to support the digital transformation journey of the Chief Compliance Officer Area and to monitor its evolution, in line with the Group's overall digital strategy. The project will address ISP's needs by achieving the following objectives:

- Develop a scenario analysis and a framework to recognize, address and mitigate the risks introduced by new digital technologies (e.g. Artificial Intelligence, Blockchain, Cloud Computing, ...);
- Apply the defined framework to a specific area (e.g. compliance department);
- Define and implement a risk analysis model supporting the above.

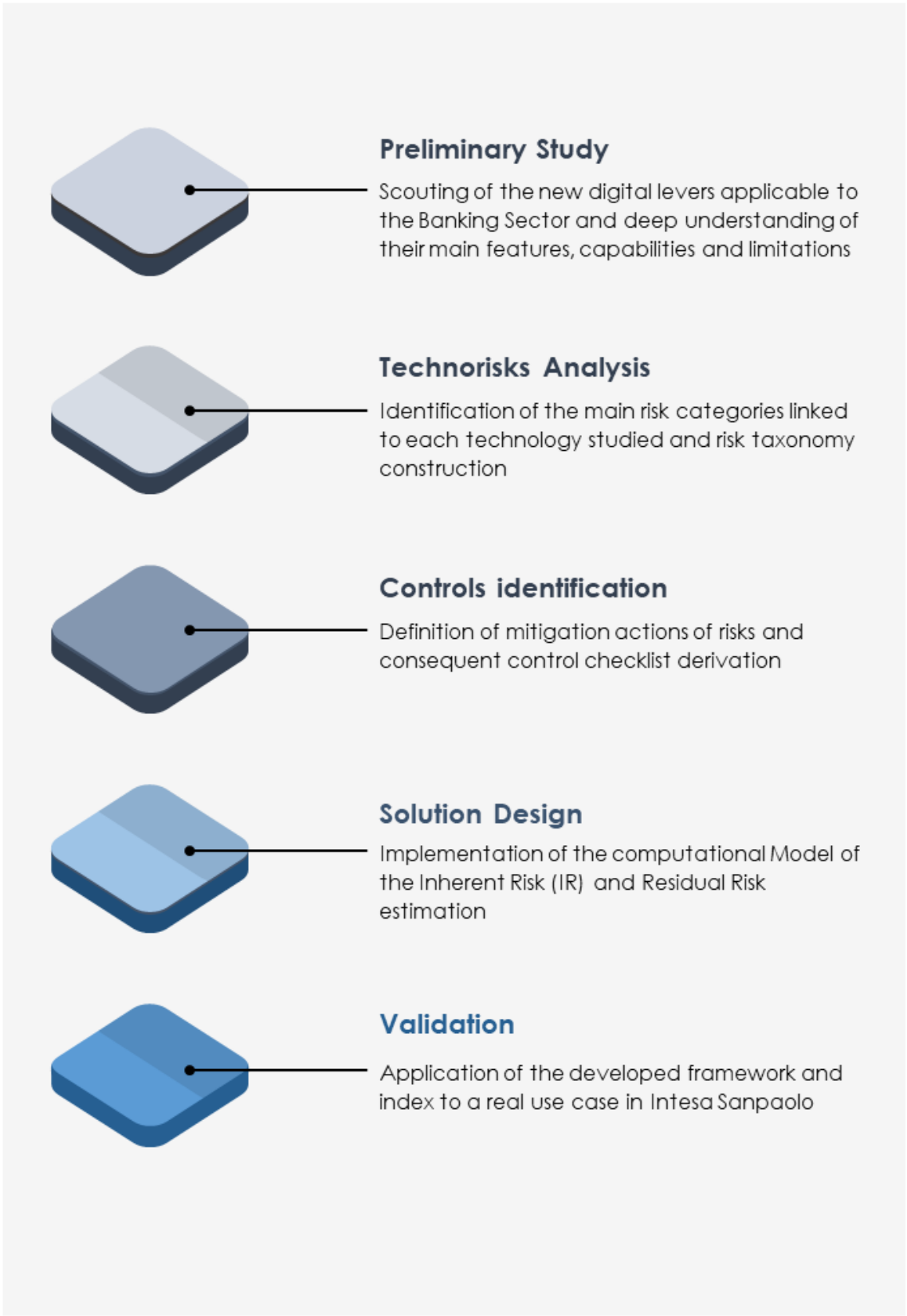
Into the Digital Odyssey brought added value to the state of the art of activities of the compliance function by applying the methods of the compliance risk assessment (CRA) to the new digital technologies (in particular AI), and by designing new mitigation actions that allow the usage of new digital technologies in a way that is beneficial for ISP business and, at the same time, compliant with new European regulations, sustainable, and respectful of the fundamental human rights.

Key Words

Digitalization, Artificial-Intelligence, Banking, Non-Compliance Risk

Project steps

In the following image it is summarized the initial project structure and the different steps designed to reach the objective of the project.



Project description written by the Principal Academic Tutor

Criminal phenomena in the financial sector are emerging as one of the main limit of digital finance. Anti Financial Crime in particular - including Anti Money Laundering, Countering Financing of Terrorism, Financial Sanctions and Anti Bribery and Corruption - assumes absolute centrality in the criminal economy.

New digital technologies (e.g. Artificial Intelligence, Blockchain, Machine Learning, ...) are an essential tool to fight these increasingly sophisticated crimes. The banking sector is investing large number of resources in digital technology, and primarily in artificial intelligence, to fight these phenomena and thus to strengthen its safeguards with the adoption of internal models for interception of potentially suspicious transactions.

Into the Digital Odyssey» is a multidisciplinary project that involves technology management and ICT knowledge as well as aims regulation and legal topics. The goal is to develop a framework of the risks associated with the use of new digital technologies within a bank. This framework aims at promoting the adoption of these technologies in such a way as to reap their benefits, while mitigating the risks that they may generate.

This project has been carried on in collaboration with Intesa San Paolo, one of the leading bank in Italy, and in particular with the Compliance Unit. The Compliance Unit's task is to conduct business in accordance with applicable laws, rules and standards by overseeing and monitoring the daily financial operations. Within the project, the Compliance Unit of Intesa San Paolo has provided to the research group with detailed information on the use of digital technologies to limit digital fraud and developed with our Team a detailed analysis to deal with the emerging "digital" risk and improve the effectiveness of governance, risk management and control processes in a bank.

Team description by skill

Giacomo Bima: Industrial production and technological innovation Engineering student at Politecnico di Torino. His core competences are related to the management of the supply chain and the standardization of industrial processes leveraging innovative technologies. During his studies he spent one year in Ireland and one year in Barcelona, while now he is currently working in Procter & Gamble in Warsaw.

Alfonso Palmieri: Nanotechnologies for ICTs student at Politecnico di Torino. His core competences are related to industrial processes for nanotechnologies, design of optoelectronic deviecs and electronic devices for structured light. He spent six months in Paris and he is currently working on metasurfaces at Harvard University (Boston).

Alberto Sivera: Nanotechnologies for ICTs student at Politecnico di Torino. His core competences are related to industrial processes for nanotechnologies, and design and simulation of optoelectronic and electronic devices. He spent six months in Paris and he is currently working on neuromorphic self-oganizing networks at Politecnico di Torino.

Alberto Meneghesso: Management Engineering student at Politecnico di Milano. His core competences are related to management subjects in general with a focus on Corporate Finance. During his studies he spent 6 months at the Northumbria University in Newcastle as part of the Erasmus+ project.

Goal

The rapid spread of digital technologies is significantly reshaping business operations and processes in the banking sector, becoming the enabling factor for the offer of new products and services to customers. In this new environment, the boards of financial institutions are facing new digital risks, resulting from the need to combine business objectives with the mission of ensuring compliance with regulations and a responsible, honest and ethical conduct. In this context, Into the Digital Odyssey aims to:

1. develop a scenario analysis and a framework to recognize, address and mitigate the risks introduced by new digital technologies (e.g. Artificial Intelligence, Blockchain, Machine Learning, ...);
2. apply the defined framework to a specific area (e.g. Artificial Intelligence);
3. define and implement a digital index supporting the above.

The initiative will bring value to the digital evolution process that is affecting the entire economic system on a large scale. This goal will be reached by contributing to maximize the opportunities deriving from digital levers, through the management and minimization of the underlying risks in a sustainable, compliant and ethical perspective. Our project is structured as follows:

1. Background analysis: this step aims to understand the technical features, capabilities and limitations of new technologies (including AI/ML techniques) and to assess their cutting-edge applications.
2. Techno-risk analysis: the study carried out in the first step will be further developed with reference to the adoption of Artificial Intelligence solutions
3. Design: this phase will involve a. The definition of a framework to support the assessment and management of the risks generated from the use of digital tools by financial institutions b. The study and definition of a methodology to monitor the behavior and performance of innovative technologies (with a specific focus on AI algorithms) c. The development and implementation of a Digital Risk Index and of the relative maintenance directions on an ongoing basis

Understanding the problem

The compliance function within financial institutions must fulfill a twofold strategy:

a) Constant internal monitoring and development of the appropriate tools to reduce the non-compliance risk against the current legislative framework.
b) Constant monitoring of possible future new laws that could be introduced by the authorities, and that banks must be ready to comply with.

The constant innovation in the financial sector has focused the attention of media, academics, and practitioners in particular on this second point. Digital innovation and the development of new technologies provide the basis for improvements in the real economy, which, in turn, influences and is influenced by financial innovation. Financial innovation has recently become double-tied with technology and data. Fintech startups, Big Techs and even incumbents from non-financial sectors constantly leverage on huge amounts of heterogeneous data and analytics, creating new and more suitable products, improving the accurateness of pricing, lowering the costs of the intermediation process and introducing new business models. At the same time, in addition to the objective operational benefits, the introduction of innovative technologies within the financial industry has opened up several types of new challenges for the compliance activities:

a) Mitigate the regulatory risk in the use of these technologies and put in place the appropriate safeguards for compliance with the possible regulatory framework.
b) Implement new technologies within the compliance function itself to better fulfil its internal role (here we focus on the regtech movement).

Exploring the opportunities

Typically, banks are characterized by three lines of defense against the non-compliance risk: First line of defense, daily risk management, operations and development practices. This includes ensuring to know the customers, monitoring activity for unexpected behaviour and reporting suspicious activity to relevant authorities.

Second line of defense, compliance and risk functions. These functions ensure banks conduct business in accordance with applicable laws, rules and standards by overseeing and monitoring the daily operations and providing advice to the first line of defense.

Third line of defense, internal audit. It performs independent assurance activities to evaluate and improve the effectiveness of governance, risk management and control processes. Recent assessments show that, while banks have made some improvements to their compliance frameworks, progress is still needed in three main areas:

1. governance,
2. dedicated resources (in terms of number and quality), and
3. implementation of policies and processes. Into the Digital Odyssey aims to target this third element, generating a comprehensive framework to assist the second line of defense in assessing quantitatively the compliance risk in the digital world.

Scheme of the three line of defense

Generating a solution

Given the Artificial Intellicence Act as regulatory framework, the risk of non-compliance to that regulations is evaluated in terms of residual risk, following the **Compliance Risk Assessment (CRA) methodology**.

The Compliance Risk Assessment (CRA) assesses the risk of non-compliance of each monitored regulatory area in terms of residual risk. The value is derived from the association between the inherent risk and vulnerability of the organizational and controls system.

- The **inherent risk** (or gross risk) is the level of risk at which the bank is exposed only on the basis of the nature and the extent of its business, regardless of the implemented mitigation measures (safeguards). As it is explained more in detail below, it is evaluated using, in general, a six-level scale, where 1 corresponds to «low inherent risk» and 6 to «very high inherent risk». The methodology adopted for the assessment of inherent risk involves the compilation of a questionnaire based on eleven qualitative/quantitative indicators which can assume a value from 1 to 6. Then after a value has been associated to each indicator in the questionnaire, the inherent risk index value is computed combining these values, and mapping the result from the six-level scale to a percentage scale.
- The **vulnerability of the organizational and controls system** is an index related to the robustness of the implemented safeguards to mitigate the inherent risk. Vulnerability can be evaluated using a four-level scale and it can assume the following values: “Not significant”; "Not quite significant"; "Quite significant"; "Very significant". The vulnerability of the organizational and control system is computed by assessing the level of the implemented safeguards, and then calculating the vulnerability as the complementary to it with respect to the maximum value of the adopted scale. The assessment of the safeguards is carried out according to risk-based criteria, through the “Mapping of the Safeguards and Controls”. The process of "Mapping of safeguards and controls" is aimed at a precise and careful assessment of all procedural safeguards and controls aimed at the management of the risks of non-compliance of the regulatory framework under analysis.
- The **residual risk** (or net risk): is the level of risk after the application of the mitigating effect of the implemented safeguards, in terms of governance and controls. The residual risk level is obtained from the combination of inherent risk and vulnerability.

Into the Digital Odyssey focusses its attenction particularly on the assessment of the compliance inherent risk and on the definition of safeguards starting from requirements coming from the Artificial Intelligence Act.

Main bibliographic references

European Banking Authority, EBA analysis of Regtech in the EU financial sector, June 2021.

Kessler, J. (2022, June 23). Digital transformation: the future of banking & financial services. NeuroSYS: AI & Custom Software Development. https://neurosys.com/blog/digital-transformation-in-banking

Armour, J., Awrey, D., Davies, P. L., Enriques, L., Gordon, J. N., Mayer, C., & Payne, J. (2016). Bank governance. Principles of Financial Regulation (New York/Oxford: Oxford University Press, 2016), European Corporate Governance Institute (ECGI)-Law Working Paper, (316)

Woolard, C., Saidenberg, M., & Goyne, E. (2022, January 14). How can regulation keep up as banking transformation races ahead? EY. https://www.ey.com/en_gl/banking-capitalmarkets/keep-up-on-banking-regulation-during-transformation