Politecnico di Torino

Corso di Laurea Magistrale in Ingegneria Gestionale

(*Engineering and Management*)

Tesi di Laurea di II Livello

"Digital transformation in the financial industry"

Supervisor:

Prof. Claudio Demartini

Candidate:

Emilio Salerno

Un caloroso ringraziamento alla mia famiglia, ai miei cari e al mio relatore
che, con il loro sostegno, mi hanno permesso di arrivare fin qui davanti a voi oggi,
contribuendo alla mia formazione personale.

INDEX

INTRODUCTION

In this final work of my studies in Industrial Engineering and Management, started five years ago at Politecnico di Torino, I will deal with the digital transformation of a particular industry, the financial industry, which is mainly composed by the banking sector and the insurance sector.

This thesis, which has the objective to present the current situation of the financial industry worldwide (with a particular focus on Europe), is divided into four chapters that are described as follows.

In the first chapter, I will present the start of the art of the digital transformation in the financial industry, talking about the main challenges the financial institutions are currently facing for the future.

The second chapter will talk about the regulations, directives and legislative procedure that shape the financial industry.

In the third chapter, I will show three case studies, deriving respectively from my professional experience in an international major player of the financial industry worldwide, from my personal experience during the period spent abroad for the Erasmus Extra-UE program in Latin America (Chile) and from the literature available on the net.

The last chapter will present the results obtained and some overall conclusion about the work done in the previous chapters, namely the digital transformation of the financial industry.

Now the natural question that could arise is: what is digital transformation?

Is there any difference with digitalization?

And what about digitization?

I think that the three following terms, digital transformation/digitalization/digitization, are often confused and used interchangeably as synonyms, even if they are conceptually different; therefore, I would like to talk about the difference, which is not just a matter of terminology.

Digitization is the process of converting information from a physical format to digital one. It means converting something non-digital into a digital representation to be used by computer systems and automate processes or workflows. Digitization enables to create value in business activities, which needs data. It helps to lay the foundation for business use cases that leverage the data, nowadays often referred to big data.

A simple example could be the scanning of a paper document and the following saving on computer's hard drive as a digital document, like a PDF format. Another example could be the conversion from analog VHS cassettes to CD, DVD or Blu-Ray discs containing digital data.

Digitalization is the process of leveraging digitization to improve business processes. Digitalization means making digitized information useful for people inside organizations. The term refers to the use of digital technologies and data to create revenue, improve business models, and create a digital culture with digital information as the core.

Most of the times it transforms processes completely to make them more efficient, productive, and profitable for companies.

An example could be the upload of a PDF document from a computer's hard drive to the cloud and therefore sharing it with many people to analyze the data. Or think about the upload of digital movies from CD, DVD or Blu-Ray discs to online services: customer could easily see them directly on a platform such as Netflix or download them as a digital file.

Digital transformation is the transformation of business activities, processes, products, and models to fully leverage the opportunities of digital technologies. The main goal is to improve efficiency, manage risk and discover new monetization opportunities.

Digital transformation is doing things in a new, digital way and it is a broader term than the previous two.

Digitization and digitalization are parts of a digital transformation: the latter one requires digitization and digitalization on the path to build a digital business.

Digital transformation includes all aspects of business, like customer understanding and touch points, growth strategy, enterprise mobile applications, process digitization, worker enablement, new business models, and many other things related to the general performance and growth of the enterprise. Digital transformation often leads to entirely new markets, as well as new customers and business realities.

In general, the digital world has brought a disruption that has heavily affected a variety of habits and behaviors of the professional world. Technology combined with smartphones and the internet provides numerous benefits to the customers as well as to financial institutions.

Previously the implications of digital transformation were unknown as people were concerned about the transition from manual to the digital world.

However, the scenario has changed now. With tighter regulations and changing customer demands, the financial applications and systems have become nimbler and progressive.

For financial institutions, digitalization is more than just adopting technologies such as cloud, big data, social media or mobile. It is aimed more towards creating new business models to develop an eco-system where all markets, consumers and all the stakeholders could participate.

Therefore, organizations focus more on capitalizing with new and emerging technologies that help them in positioning and transforming the teams into high performers.

CHAPTER 1 - STATE OF THE ART OF DIGITAL TRANSFORMATION IN THE FINANCIAL INDUSTRY

1.1 - Digital era

Digital era is characterized by the creation of new business models, enabled by new technologies. In the financial industry, the real change in the business model started in the late 1990s when the incumbents in the industry began to leverage client-server applications, the revolution of Internet and Intranet applications.

Ten years later, the digital revolution had a consolidation thanks to the introduction of mobile devices, cloud computing technologies and instruments for advanced analytics such as Big Data. All the players in the financial industry, incumbents and new entrants, understood that a way back was no longer possible.

Nowadays, digital transformation is still a crucial topic for the industry and the related financial services, because of the exponential development of precedent technologies and the introduction of new technologies, such as artificial intelligence (AI) or distributed ledger networks, on which cryptocurrencies are based. Moreover, a new paradigm is enabled by non-traditional competitors like FinTechs, which entered all parts of the financial industry with their technology-based business models.

Other key factors that are enabling the digital revolution are the regulations and the expectations of the customers.

Regarding the regulations, we will go deeply in details in the second chapter. I will just say here that regulations are authorizing new entities to access consumers' payments accounts to make actions, like normal payments, on their behalf and obviously after their previous consent. This is done through Application Programming Interfaces (APIs) that will be described when talking about open banking.

The other factor is customers' expectations, which significantly grew and will continue to grow thanks to the rise of new technologies that allow an even more digital connected world and even higher capabilities to leverage. It is sufficient to say that in the developed countries of the world everyone owns at least one smart device (laptop or mobile), as many social researches conducted by sociologists show.

For the actors involved in the financial industry like banks, in the digital era the critical success factors that should be appointed are three: having a digital strategy, possessing a capacity of quickly adapting and reacting to fast changing conditions, creating a digital culture inside the organization.

Having a digital strategy means knowing in which technologies invest in an extremely fast changing environment such as the digital one. Moreover, given budget and resource constraints, it is not possible to invest in every new emergent technology. For these reasons, having a clear and well-defined digital strategy today is more important than ever.

One aspect is crystal-clear in the actual digital environment: those who do not adapt will be left behind. Companies must take measures in order to master their entry or consolidation into the digital world. The business model should be optimized according to investments and costumers' needs. Indeed, business models that were successful in the past may not be remain viable and feasible in the new environment.

Nowadays, Information Technology is a key strategic element as a means of guaranteeing an organization's growth, scalability and efficiency.

The second critical success factor is possessing a capacity to quickly adapt and react to changes in the market, which is something crucial today. In the financial industry, for all the players it is extremely important to being agile and lean in order to respond to new technological paradigms. Consider for instance the presence of non-traditional competitors, that is enabled by the digital world we are currently living, to understand the importance of this capacity for banks if they want to maintain their current market share and then growing.

Last but not least, having a digital culture is another key factor to consider carefully. Indeed, if internal structures and processes are proved restrictive and highly time consuming, it is very difficult that innovation could come from within an enterprise itself. Instead, creating and then adopting a digital culture allows the organization to be continuously able to innovate.

In other words, having a digital culture means ensuring that the organization is working collaboratively to ensure that all departments are working towards a common goal. This allows the organization itself to realize its vision of a digital future.

Establishing a digital culture should be seen as a process with a long-term perspective, in order to attain effective implementation of organizational objectives and to make the business lean and adaptable to changes. Organizational goals, values and desired behaviors must be reviewed and converted into work practices and decision-making principles during the daily working life.

Therefore, changes in the culture starts in the everyday actions. However, it's not sufficient to list the rules and the values on a piece of paper, for example. Following behavioral patterns and sharing a clear digital future vision between each member of the

organization creates a sense of trust and belonging to the same organization. It is this sense of trust and belonging to the company the real key success factor when it comes to culture in companies.

Nowadays, we can affirm that some banks are quite mature digitally while other banks are still in the core of the process of digital transformation. Banks try to offer a wide range of functionalities relevant for customers and a compelling user experience.

Concerning the environment in which they operate, the digital challenges that banks are currently facing and will face in the future can be related to three areas:

- Digitalization of the offered services
- Open banking
- Beyond banking

Beyond banking includes the first and the second one; open banking includes digitalization of the offered services; digitalization of the offered services is the core of digital transformation and stands at the basis of the others. This means that without the digitalization of the services, open and beyond banking scenarios are not viable.

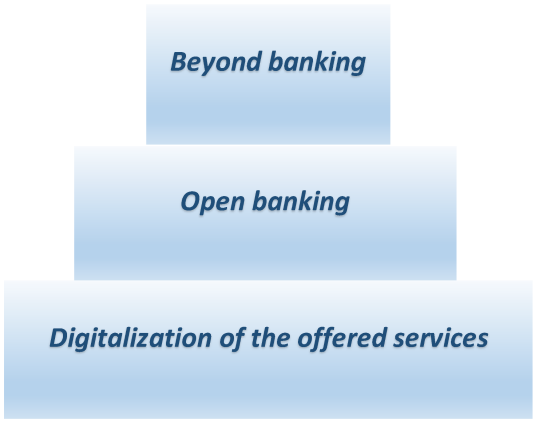


Figure 1

Digitalization of the offered services

The first area refers to all the functionalities that aim to transform traditional banking products and services from brick-and-mortar into internet and mobile.

All the services that were previously offered locally in a branch of the bank are now provided digitally through a digital platform. The bank provides its own financial services on its own platform. Through the digital platform the customer can usually log in into a

private account and see all the relevant information related to his financial status and the financial services he/she paid for.

Another possibility is that the bank provide its financial services on specific platforms chosen according to a selection procedure. For instance, the bank BNP Paribas has introduced the platform *WeChat Pay* to some retailers in Europe with the objective to facilitate the shopping experience for Chinese tourists. Also thinking more in general, consider that a lot of banks provide many e-commerce platforms the option to purchase goods and services from their own website, using the payment methods that the customer is used to deal with.

In this platform, the user can also evaluate the additional products or services offered by the bank (trading, mutual funds, insurance, etc.) and purchase them in case of interest.

Strategically speaking, companies that develop and implement an integrated IT strategy will capture competitive advantages, by strengthening customer relationships and the customer experience. Making the correct investments in the most appropriate technologies brings to a critical competitive advantage in the digital context.

Open banking

Open banking is based on a digital platform where financial services and products from the bank or other third parties are offered to bank's customers.

Open banking functionalities are the ones that make available all the data and information in an ecosystem involving not just banks and customers, but also third-party developers, FinTech startups and other partners. All these actors can have access to data and information and can interact between each other through a digital platform.

In other words, open banking can be defined as a collaborative model in which financial data and information is shared between two or more parties with the objective to improve the capabilities and the services offered to customers. For instance, especially in USA, the open banking ecosystem involves banks and payments networks like Visa or Mastercard.

A fundamental characteristic of open banking, in comparison to the traditional banking, is the sharing of data between banks and other parties involved.

Data sharing is often accomplished through an application programming interface (API) that allows data flowing smoothly. An API is a software intermediary (or set of protocols) that allows two applications to talk to each other. APIs have become crucial for the future of banking because they help to create stronger and more dynamic relationships with

customers. In the world, many industries have used internal APIs for years and technology giants such as Facebook, Uber, Google, and Netflix have experienced tremendous growth using APIs.

In the financial industry, APIs have been used largely by banks in the last years and they will be used even more in the following years for improving the financial services provided both to business and consumers (B2B and B2C markets).

According to a research done by McKinsey, the most common models of API are three: public, private and internal.

The public APIs are the ones used by external partners and developers who build innovative products that can be purchased on the market.

The private APIs are the ones used by all the partners of a company: suppliers, resellers, customers.

Finally, the internal APIs are the ones used by developers within the company.

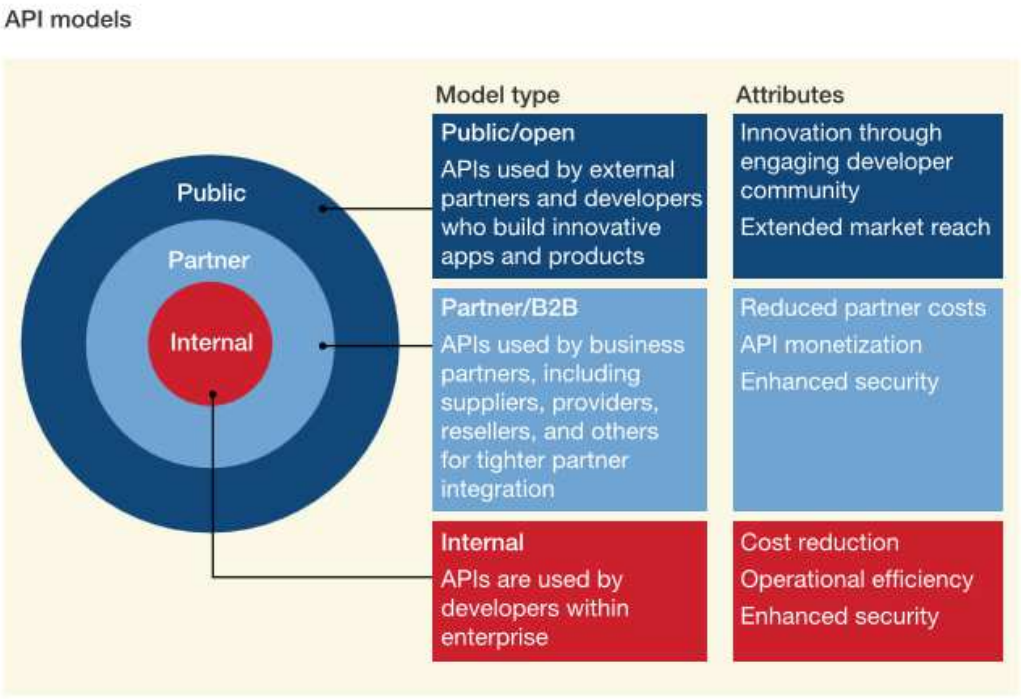


Figure 2

From the point of view of the worldwide developments of open banking, the figure below shows how different parts of the world are currently engaged in.

In Europe and in the USA digital banking is already establishing a new paradigm in the financial industry inventing new business models and rapidly changing the financial market. This is carried out mainly with partnerships with other entities, creating a network based on sharing customers' data and harnessing them in order to make better

decisions. For instance, the Swedish bank Klarna provides online financial services such as lending money or payments solutions for stores and e-commerce.

In South and Southeast Asia digital banks such as FinTechs are growing faster, conquering every year more market share of the financial industry. The case of China is very similar to the European scenario and the scenario in USA: real digital ecosystems such as AliPay and WeChat are moving forward the fully establishment in the financial market. AliPay and WeChat enable enhanced e-commerce through their platforms, offering a more personalized experience and a variety of payments options, including peer-to-peer.

In East Africa, people are starting to use different methods of payments and making transaction thanks to the usage of mobile phone. For example, M-Shwari is is a bank account issued by the Commercial Bank of Africa in Kenya. The uptake and usage of M-Shwari in the last years has been remarkable. There are over 10 million M-Shwari accounts and the Commercial Bank of Africa disburses 50,000 loans every day. One out of five Kenyan adults are active customers of M-Shwari.

The reason why M-Shwari had a huge success in Kenya was the possibility of being able to borrow on demand, in real time, to enlarge families' ability to make ends meet in the short term.

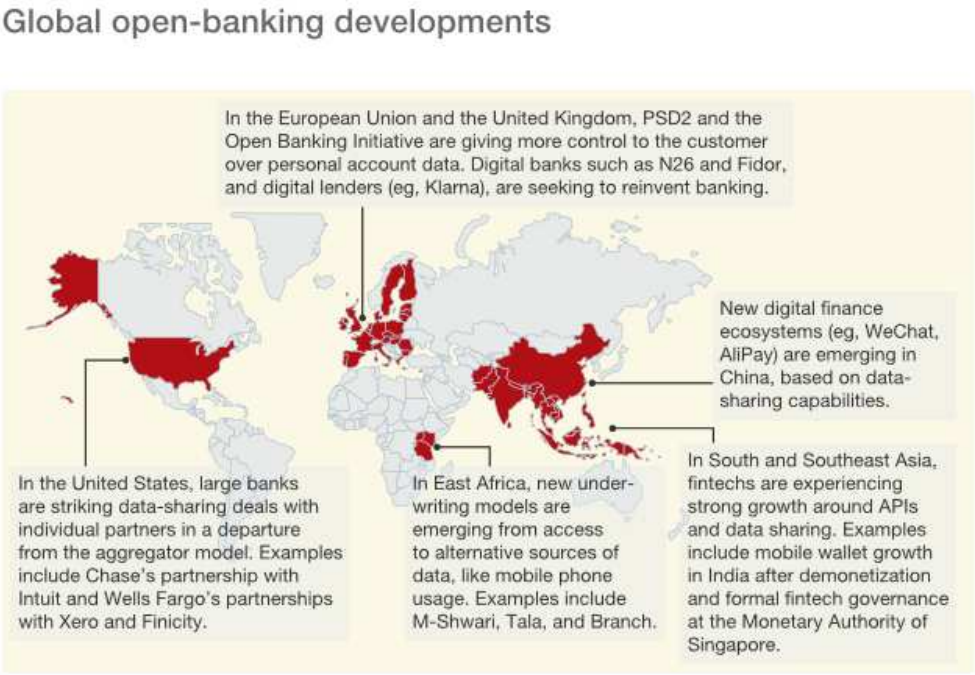


Figure 3

Another example is in United Kingdom, where Barclays provides a service of experiences in lifestyle areas such as culture, arts and travel. Analyzing customers' choices and their

satisfaction after enjoying the experiences, the bank can better understand their preferences and therefore associate the needs and desires with specific targeted offers.

It's important to say that there are risks in sharing data between partners because of the possible problems of privacy and security: consequently, it's crucial to create an infrastructure which has the role to protect the information exchanged between partners of the collaborative network.

In a nutshell, the main benefits of an open banking model are: an improved customer experience, new revenue streams and a sustainable service model for underserved markets.

Beyond banking

Beyond banking refers to the fact that banks are trying to extend the value chain with the aim to become a crucial part of customers' daily lives. They are offering value-added financial services, integrating their services with others provided by different actors.

Alike the open banking, there is an ecosystem of stakeholders but in this case customers can benefit from various kind of services by different kind of providers, not just financial services. For instance, when offering a loan for a house, banks give buyers other relevant information such as neighborhood resources or information on school located in the area of the house.

Therefore, beyond banking is based on a platform in which multiple actors are present with different roles. This platform, in which customers can benefit from different types of services, is a digital platform where all the services are integrated in order to provide an overall exceptional customer experience.

In this scenario of multiple services, banks develop and maintain the backbone and the infrastructure of financial products that integrate into a wide range of non-financial services.

1.2 - Penetration of smart devices in the industry

When it comes to digital means, we have to mention the ones through which banks, customers and other possible stakeholders (in an open or beyond banking ecosystem) can accomplish many kind of tasks and activities.

The smart devices used can classified into three types:

- PC/laptop
- Smartphone
- Tablet

The penetration of these devices has produced a deep transformation of the habits and preferences of the customers, who are becoming increasingly accustomed to share information about themselves and interacting with other people online through social media platforms.

In particular, in the countries with developed economies, where mobile broadband networks are available at low prices for almost everyone, Internet has become a place where consumers can compare all kinds of products and services and sharing their experiences with others. This is the actual scenario of many sectors, and the financial one is not an exception: customers can compare online different financial services (such as deposits, mortgages or insurance policies) and find relevant information quite easily.

In strategic terms, this brings to a higher competition in the market: if people can compare various services provided by different players in the industry, they can choose the cheapest service or the best service according to their needs easily, without having to go physically in the branch of the banks or insurance companies to acquire the information.

Moreover, with the adaptation of customers to interact via digital media in many areas of their lives, their expectations of an overall higher quality of the services has dramatically increased, especially in the financial area where important factors such as wealth, money and investments are involved. Banks have adapted to this increase in expectations, for instance providing a service of customer service available 24/7 online or providing the possibility to interact through social media or email.

However, banks are still adapting to the fast-changing behaviors of customers and today we are fully in the phase of *Online banking* and *Mobile banking*.

<u>Online banking</u>

Online banking consists in allowing customers to leveraging banking tools and carrying out financial operations from the comfort of the home, office or while travelling. For instance, customers can pay their bills online, download electronic statements, making transfers and buying additional services if desired.

Regarding bills, many banks offer a service of automatic bill payments: all the customer has to do is to make sure the money needed is in the bank account before the scheduled date of payment. In this date, the bank will automatically process the payments on behalf of the customer (for instance sending money to the electric, gas or water provider).

The possibility of checking and downloading statements online allows to save paper, preserving the environment and keeping private and secure the information contained. The customer can also access anytime to the statements and see all the transactions he made, both revenues and expenses.

As a standard service, modern online banking will offer customers an automated (self-learning) record of their income and expenditures which can be presented in chart form or categorized – via mouse click/touch/voice activation – by type or size of expenditure or by date, for instance. On this basis it will then also be possible to interactively calculate customers' differing financial needs in the shape of scenarios. The bank offers proposed are based on the collected and evaluated behavioral data in respect of customer spending patterns or propensity to save or take risks. For example, it is possible to provide calculations showing customers a chart of a consumer loan, property mortgage or retirement plan in line with their financial behavior. Consideration will also be given to external dynamics (interest rates, securities quotations and exchange rates) which can be changed interactively in the scenarios and forecasts. Additionally, customers can configure individualized services, such as alarm signals or text messages, to inform them of overdrafts or unusual account activity which the underlying self-learning algorithm recognizes.

Mobile banking

Mobile banking is the online banking carried out on the go, through mobile devices such as smartphones and tablets. Wireless Application Protocol (WAP) is the technology architecture that makes accessing Internet pages possible from a mobile device. WAP provide a user experience similar to the one conducted on a laptop, but banks have to create mobile friendly websites for customers to guarantee so.

Today some banks offer a free download of a mobile banking application, through the Google play store on Android or the App store on iOS. On these applications, customers can log in and check the balance, manage the bill payments and transfer money between accounts from wherever it is possible to have an internet connection. Moreover, they can manage the credit and debit card’s security settings and many other types of transactions.

The mobile banking applications are a reliable channel and offer users the possibility to conduct more complex transactions compared to a simple access to the bank account from a mobile browser.

A bank, in order to decide which kind of solution adopt, must consider the advantages and disadvantages, the needs of customers and its technology infrastructure. For instance, a mobile banking application brings more development costs but it is typically more reliable and offer a compelling user experience.

1.3 - Digital functionalities

The main digital functionalities that banks carry out today are:

1. Information gathering
2. Account opening
3. Customer onboarding
4. Day-to-day banking
5. Start a relationship
6. Expand a relationship
7. End a relationship

I will now explain briefly each of this one, giving some examples of activities included.

Information gathering

By information gathering, I mean access to information on the various products offered by the banks and the various pricing according to specific groups and needs.

The act of collecting information in the digital world typically occurs through public websites and social media platforms.

Account opening

The experience of opening an account today occurs mainly in the digital world, thanks to the channels and identity verification methods.

However, in the typical traditional bank is still required at least one visit to a bank's branch in order to open a bank account.

We will see in the related chapter that today, there are some Non-traditional competitors of banks that allow customers to open a bank account entirely online.

Customer onboarding

By customer onboarding I mean guidance of the customer in the first steps of the process of fully understanding the potentialities of the digital platform in which he/she will operate daily to check his/her financial data and relevant information.

Day-to-day banking

Activities carried out daily by the users are mainly digital: checking the balance account, withdrawal, deposits, managing the account and making money transfers.

Start a relationship

Even if traditional banks typically requires a visit to their branch to start a relationship with them, today there are the so called *fintechs* which do not have any physical space and are totally online banks. I will go further in details in the related chapter about FinTechs and Non-traditional competitors.

Therefore it's possible to affirm that it possible to start a relationship entirely online with a bank today.

Expand a relationship

Banks can sell to their existing customers additional products and services like saving accounts, term deposits, loans, investment funds and others through digital platforms.

Furthermore, banks can observe the characteristics and the behaviors of the clients and evaluate the potential risks associated to each of them. It's mandatory from the law for banks to make a classifications of customers depending on their level of risk, with the so called KYC (Know Your Customer) process.

For instance, the major Italian player – as we will see on details in the third chapter – in its process of vetting customers classifies them according to three level of risk: high, medium and low.

On the basis of the level of risk associated to a customer, different time frames of repetition of the process will be considered and applied to that specific customer.

End a relationship

Banks can close a relationship with a customer entirely with digital channels. At the same time, customers can voluntarily close their relationships through the digital platform.

1.4 - A new model for banks: Banking-as-a-platform (BAAP)

The three macro-categories described design a new model for banks: the banking-as-a-platform model (BAAP).

As it can be seen in the table, the differences are substantial between the current state of traditional banks and the model of BAAP in a wide range of different aspects inside the firm, from the scope of the firm to the organizational chart.

In the traditional bank, the company itself does everything obviously and doesn't have a lot of relationships with external partners; in the BAAP model, the platform involves a collaborative network between the bank and other partners.

Other partners carry out complementary activities, which can be providing other financial services (open banking) or services/products different from the financial ones (beyond banking).

In the BAAP model, the bank has a collaborative approach with almost all the partners involved in the platform; the platform partners, instead, can have a collaborative approach with some partners and a competitive one with others.

For instance, partners such as MasterCard or VISA will compete between each other in order to offer the best service for payments options to bank's customers.

Regarding the technologies used, the traditional bank normally owns technologies which are not open source, not modular and with no open standards.

In the BAAP model, the interoperability between partners' interfaces and bank's interfaces is key.

Banks own open interfaces and modular, open source technologies with open standards. As also mentioned before, data sharing is accomplished through APIs.

PLATFORM LEVERS	TRADITIONAL BANK	BANKING-AS-A-PLATFORM (BAAP)
SCOPE OF THE FIRM	Does everything	*Bank*: focused only on core competencies and core activities *Platform partners*: perform broad array of complementary activities
SERVICE	Owns 100% of product stack	*Bank*: owns core product stack *Platform partners*: develop and offer ancillary services
PRODUCT	Owns 100% of product stack	*Bank*: owns core product stack *Platform partners*: develop and offer ancillary products
INTELLECTUAL PROPERTY AND DATA	No sharing with anyone	*Bank*: shares information *Platform partners*: share information
TECHNOLOGY	Typically owns technologies, which are not open source, not modular and with no open standards	*Bank*: owns modular, open source and with open standards technologies. Owns application programming interfaces (APIs) and the interfaces are opened *Platform partners*: partners' interfaces and bank's interfaces must be interoperable
INTERNAL ORGANIZATIONAL CHART	Centred on the company itself (divisional or functional)	*Bank*: centred on leveraging core competencies and harnessing the relationships with partners on the platform *Platform partners*: centred on developing the ability to use the same "language" as banks, understanding customer needs and behaviors
RELATIONS WITH PARTNERS	Few relations with external partners	*Bank*: collaborative approach *Platform partners*: collaboration with some partners, competition with others

Table 1

1.5 - Current technology innovations fostering change in the industry

There are three key technologies whose development could have an important impact for the business of banking: advanced analytics, machine learning, distributed ledger technology (Blockchain).

Some of these developments could have an impact in the mid-term, others in the long term. Some will be driven by banks, other by other actors in the financial market. Banks need to evaluate carefully the implications and, as already explained, formulate a good strategy in order to decide in which technology prioritize the investments.

Advanced analytics

Payments in the market generate a lot of transactional data that can have a significant impact on transaction banking. Advanced analytics, such as Big Data algorithms, can help to reach a better prediction and description of what happens in daily life and consequently banks are able to enhance their performance.

In the last few years there has been an exponential increase in the data generated and a continued decrease in the cost of data storage: therefore, it's becoming easier for banks leveraging this information and also having more accurate information on the behavior of the users.

Banks currently concentrate most of their analytics use cases in sales management (for example, next product to buy, digital marketing, and transactional analytics), financial risk management (collections), and nonfinancial risks (cybersecurity and fraud detection).

Machine learning

Machine learning techniques increase the speed of processing data for banks.

Hand-in-hand to advanced analytics, machine learning it's helping banks to optimize performance and retrieve more accurate information than ever from the financial market. Some of the most significant advances brought about by advanced analytics and machine learning are in customer segmentation, which is becoming much more sophisticated and productive. The improvements affect an array of activities, beginning with the prevention and management of bad debt and extending through to internal and external account resolution.

Leaders taking the analytics-based actions that define the new model have already begun to realize gains in efficiency and effectiveness. For instance, a famous European bank automated 90 percent of communications with clients by developing two advanced-analytics models using machine-learning algorithms.

The models use hundreds of variables, including client demographics and information on overdrafts, client transactions, contracts, and collaterals. The bank has realized more than 30 percent in savings with no loss in operational performance thanks to this machine learning algorithms.

Increased investment and subsequent advancement of AI and machine learning in banking help translate this data into pointed insights that help making better decisions.

If step one in the adoption of AI and machine learning was to simplify existing processes with intelligent automation, the future lies in being able to offer bespoke solutions that are tailored to each customer based on their previous interactions. The evolution of chatbots in banking is an example.

Chatbots present a dual benefit to banks. Increased number of interactions and continuous learning over each of those interactions helps the bot transform from a transactional entity offering textbook responses to basic questions into a personal assistant, which can offer intelligent suggestions and personalized recommendations. At the same time, the transactions allow banks to gather a lot more information about customers and target them with relevant products and services that would make sense to them.

For instance, banks such as American Express and Wells Fargo have already introduced Facebook Messenger bots to help their customers with details about their financial transactions over chat. Since bots are programmed to learn based on each transaction and chat conversation, the interactions become far less transactional and human-like with time.

Distributed ledger technology (DLT)

A distributed technology ledger could have a disruptive impact on business models of the banks. The distributed technology ledger is based on a decentralized network in which all the actors can see the transactions occurring on a real time basis. Nowadays, the most known distributed technology ledger is Blockchain, which is leveraging cryptocurrencies in order to develop the distributed network.

Blockchain could have a powerful impact in many industries and the financial one is not excluded, if not one of the most impacted by this decentralized technology.

"Blockchains have the potential to displace any business activity built on transactions occurring on traditional corporate databases, which is what underlies nearly every financial service function. Any financial operation that has low transparency and limited traceability is vulnerable to disruption by blockchain applications. DLT is therefore both a

great opportunity and also a disruptive threat," according to Bruce Weber, dean of Lerner College and business administration professor, and Andrew Novocin, professor of electrical and computer engineering, both at the University of Delaware based at Newark (USA).

Besides that, Blockchain would reduce the massive duplication of information that creates delays, conflicts and confusion in many aspects of financial services. For instance, the massive duplication of information that creates delays, conflicts and confusion in many aspects of financial services could be reduced thanks to the decentralization of the distributed technology.

However, there are no only pros shifting to this new technological paradigm. Indeed, there are some possible bumps and issues to consider along the way of the adoption.

Making use of the Blockchain is not as simple as just buying a new software and running it. All the relevant members inside the bank organization should join the new system.

These members participating in a blockchain may have misaligned incentives and different interests, and this can end up in a gridlock or in a limited adoption of the technology.

Cloud infrastructure

Many financial institutions use cloud-based software-as-a-service (SaaS) applications for business processes that might be considered non-core, such as CRM, HR and financial accounting. They also turn to SaaS for 'point solutions' on the fringes of their operations, including security analytics and KYC (Know Your Customer) verification.

Even so, the technology is quickly becoming predominant also in the core activities in the financial industry. According to the consulting company PwC, by 2020, core service infrastructures in areas such as consumer payments, credit scoring, and statements and billings for asset managers will be based on a cloud infrastructure in a large number of financial institutions.

However, important issues arise when considering cloud infrastructure. First of all, the most important challenge to address is the security of customers data and information. Financial companies should carefully consider how to protect data from cyber attacks when adopting a cloud infrastructure. We have also already explained that one of the main challenges faced today is cyber-security.

Some countries worldwide have imposed strong restrictions on the transfer of client data to the public cloud. For this reason, many financial institutions today are going towards the adoption of a private-cloud solution.

1.6 - Non-traditional competitors: FinTechs and digital lenders

FinTechs and non-traditional competitors are changing the financial services industry today. A pursuit of innovations and paradigms is the only way for banks to survive in the digital era. Therefore, banks are trying to embrace the changes and react quickly to new innovations and technological paradigms in the moment they occur in the market. The competition for banks now is in innovation and no longer in conserving stability or the market share.

FinTechs are financially focused platforms that employ software and technologies to support existing banking and financial services. Moreover, these platforms are fostering innovations in all the area of finance, from retail banking to cryptocurrencies and lending money.

Investments in FinTech have grown exponentially, reaching US$31 billion in 2017 and bringing total global investment to US$122 billion over the past three years.

FinTechs have a lot of strengths: first of all, they are nimble and they put focused efforts on specific services normally offered by banks. Moreover, they don’t have the burden of legacy systems like banks do and they are excellent in removing frictions between customers and banks. Legacy systems are mainly related to systems, dated back to the 1970s, that hinder performances and hamper technological innovation.

Finally, they have a strong understanding of the customer journey. They have demonstrated to be able to provide value in every step in which a potential customer and then a customer finds himself.

When it comes to weaknesses, instead, FinTechs normally have some inability to easily scale and grow by connecting with more customers. This is due to the fact that FinTechs still don’t have the level of trust that banks have. In addition to this, FinTechs don’t have the access to capital that banks have.

Examples of FinTechs around the world include peer-to-peer (P2P) lending services in Asia, or mobile payment solutions in Africa like M-Pesa that allow people who don’t have a traditional bank account to make purchases through their cellphone account. In Europe, the german startup N26 offers potential customers the possibility to open an account entirely from a smart device (smartphone, tablet or laptop) just in some minutes.

Another example is the irish FinTech Leveris that has built a full-stack, standalone core banking and lending platform, that delivers a cloud-based, quick-to-market solution for traditional banks and consumer brands. Leveris platform is built specifically for modern cloud-based infrastructure. Because of that, Leveris does not find issues that normally arise when migrating a legacy core banking system to the cloud system.

Many traditional banks offer some form of digital capabilities around lending, such as loan status, loan payments and basic account information. However, the majority of traditional banks' lending processes, including online application, onboarding, processing, underwriting and funding, have yet to be overhauled through technology. This means there is still a lot of opportunity to improve productivity, close more loans and increase revenue per loan with faster and automated services.

In this context, digital lenders are non-bank alternative lenders which are offering services (mostly loan services) that traditional banks are not yet capable of offering.

However, the real competitive advantage does not stands in the service itself. It stands instead in the use of technology to reduce the time and cost of originating and servicing loans, allowing to grow the portfolios of activities more cost-efficiently.

1.7 - The main challenges facing digital banks today

The pressure for players in the financial industry is increasingly growing, both for traditional banks and non-traditional competitors. They all need to face, thorugh their digital strategies, the increasing intensity of the competition in the financial environment, with increasing technology-driven firms entering the market. The priority is to develop a digital platform ecosystem with consider entering into potential strategic alliances with external financial service providers. In this context, the most important challenges are:

1. <u>Trust</u>

Trust from customers in the financial sector is mainly related to the processing of financial transactions: customers want security, privacy and protection of their personal data. Loss of data or relevant information of a customer could break the relationship between the bank and the customer. This is why banks, in the digital era we are currently living, are investing many resources in securing data, systems and processes.

Trust has to be recognized by banks as a critical success factor in the financial market, deciding whether the outcome is success or failure. Indeed, only the banks who can convince clients that their data is secure and won't be sold to third parties or used for

other purposes without their consent, will not only continue to exist in the financial market, but also grow.

2. Transparency

Transparency measures are fundamental to overcome customer mistrust and minimize data protection infringements. It should cover all steps of data analysis, meaning not only the collection of them but also the actual analysis and the following usage and exploitation. In this perspective, customers should have the possibility to follow each step and the communication should be clear and understandable.

Another important point to consider is the *General terms and conditions* that customers accept if they want to use the financial services.

In order to guarantee transparency for the usage of customers' data, many pages of complicated general terms and conditions should be avoided. Unfortunately, this is not the case most of the times. Customers claim their rights to know what happens with their data and what kind of usage banks do.

In this perspective, most of the times there are stringent regulatory regime that oblige banks to adopt measures of data privacy and data protection. However, additional self-imposed and voluntary measures could help banks to become much more transparent, with the effect of establishing better and longer relationships with customers.

Another aspect to consider is that the fact that discussing potential issues in advance with customers and documenting their consent could ensure a long-term relationship based on trust and respect of confidential information between the parties.

3. Cost pressure

Pressure on margins is increasing. Financial companies have to produce and provide services in a more efficient way. The future, not only in the financial industry but in all the sectors, is going toward more automation, industrialization and standardization in the core business.

Generally speaking, banks are breaking up and revolutionizing value chains and increasing the level of standardization and automation of processes.

Besides this, they are relying more on centralization and experimenting different distribution channels. Meanwhile, regarding the typical activities carried on, banks are

driving forward outsourcing of certain functions and shifting other functions from front to back office.

4. Cyber-security

Cyber-security is key in a fast changing digital environment, and the financial industry is not an exception. Banks need to guarantee the security, protection and privacy of customers data and information if they want to build a long-lasting relationship with them. Indeed, trust is based on all of these three factors.

In this perspective, the main technologies involved are the Cloud technology and, more broadly, the Internet Of Things (IoT). Cloud technology stands at the basis of a new infrastructure, in which all the relevant data and information are shared between the actors having access to the cloud itself. Because of issues of security and privacy, many financial companies are opting for private-cloud infrastructure.

Internet of Things refers to all the physical objects (devices, cars, houses, wearables) that contain sensors, software and that are able to communicate between each other. IoT growth in financial services has primarily occurred in payments, insurance and transactions.

5. Regulatory pressure

Banks need to spend a large part of their discretionary budget on being compliant to the increasing regulatory requirements, and on building systems and processes to keep up with the escalating requirements.

I will explain deeply the regulatory pressure in the following chapter, presenting and discussing the most recent regulatory requirements and their consequences on the financial environment.

CHAPTER 2 - REGULATIONS, DIRECTIVES AND LEGISLATIVE PROCEDURES IN THE FINANCIAL INDUSTRY

2.1 Financial instruments regulations

2.1.1 - Markets in Financial Instruments Directive (MiFID)

MiFID is the Markets in Financial Instruments Directive (2004/39/EC). It has been applicable across the European Union since November 2007. It is a cornerstone of the EU's regulation of financial markets seeking to improve the competitiveness by creating a single market for investment services and activities. Another goal is to ensure a high degree of protection for investors in financial instruments.

MiFID sets out:

- conduct of business and organizational requirements for investment firms;
- authorization requirements for regulated markets;
- regulatory reporting to avoid market abuse;
- trade transparency obligation for shares;
- rules on the admission of financial instruments to trading.

The 20th October 2011, the European Commission adopted a legislative proposal for the revision of MiFID, which took the form of a revised directive and a new regulation.

After more than two years of debate, the Directive on Markets in Financial Instruments, commonly referred to as MiFID II, and the Markets in Financial Instruments Regulation (MiFIR), were adopted by the European Parliament and the Council of the European Union. They were published in the EU Official Journal on 12 June 2014.

MiFID II and MiFIR withdrew the Directive 2004/39/EC and the Regulation on Markets in Financial Instruments previously adopted.

2.1.2 - MiFID II improvements

MiFID II and MiFIR ensure fairer, safer and more efficient markets and facilitate greater transparency for all participants. New reporting requirements and tests increase the amount of information available.
The rules governing high-frequency-trading impose a strict set of organizational requirements on investment firms and trading venues.

Besides this, the provisions regulating the non-discriminatory access to central counterparties (CCPs), trading venues and benchmarks are designed to increase competition.

The protection of investors is strengthened through:

- introduction of new requirements on product governance and independent investment advice;
- extension of existing rules to structured deposits;
- improvement of requirements in several areas, including on the responsibility of management bodies, inducements, information and reporting to clients, cross-selling, remuneration of staff, and best execution.

2.1.3 - Why MiFiD II ?

The stated aim of the MiFID is for all EU members to share a common, robust regulatory framework that protects investors. MiFID came into effect prior to the 2008 financial crisis, but changes were made in light of the crisis. One of the issues in the original drafts is that the regulatory approach to third world country firms was left up to each member state, and that led to some firms outside the EU having a competitive advantage and an easier regulatory oversight compared to firms inside the EU.

This issue was addressed through MiFID II, which harmonized the rules for all firms with EU companies. The Markets in Financial Instruments Regulation (MiFIR) works in conjunction with MiFID II to extend the codes of conduct to other types of assets, including for example contract based assets and structured finance products.

2.1.4 - EU Regulatory Vision

MiFID and MiFID II are just one part of the regulatory changes sweeping the EU and affecting the compliance departments of all the financial firms operating there (insurers, mutual fund providers, banks, etc.).

Taken together with other regulatory initiatives like the General Data Protection Regulation (GDPR) and the Markets in Financial Instruments Regulation (MiFIR), the EU is pursuing its vision of a transparent market with clear rights and protections for EU citizens.

Alike many regulatory frameworks, the major part of new rules are slight modifications upon existing regulations, such as the requirements for disclosure where a conflict of

interest exists. However, several best practices, like the appointment of a single officer responsible for protecting client interests from within the firm, are now explicit requirements for firms wanting to access the EU financial market.

2.1.5 - Alternative Investment Fund Managers Directive (AIFMD)

The Alternative Investment Fund Managers Directive (AIFMD) is an EU regulation that applies to hedge funds, private equity funds, and real estate funds. The institutional funds that fall under the AIFMD were previously outside of EU financial regulations for disclosure and transparency, including the Markets in Financial Instruments Directive (MiFID).

The AIFMD sets standards for marketing around raising private capital, remuneration policies, risk monitoring and reporting, and overall accountability. The AIFMD is part of an increased push for investor protections that the EU undertook just before the 2008 financial crisis, when efforts started to increase due to the systematic risks the crisis revealed.

The AIFMD has two major objectives. Firstly, it seeks to protect investors by introducing stringent compliance around how and what information is disclosed. This includes conflicts of interest, liquidity profiles and an independent valuation of assets. The directive points out that alternative investment funds are intended for professional investors only, although some member states can choose to make these funds available to retail investors, as long as additional safeguards are applied at a national level.

The second objective of the AIFMD is to remove some of the systemic risks that these funds can bring to the EU economy. In order to do this, the AIFMD mandates that remuneration policies should be structured in a way:

- that does not encourage excessive risk taking;
- that financial leverage is reported to the European Systemic Risk Board;
- that the funds have robust risk management systems that take liquidity into account.

2.2 Accounting Regulations

2.2.1 - International Financial Reporting Standards – IFRS

International Financial Reporting Standards (IFRS) are a set of international accounting standards stating how particular types of transactions and other financial events should

be reported in financial statements. The International Accounting Standards Board (IASB) issues IFRS, and they specify exactly how accountants must maintain and report their accounts. IFRS were established in order to have a common accounting language, in order to have a better understanding of businesses and accounts from company to company and country to country.

IFRS are standard in many parts of the world, including the European Union and many countries in Asia and South America, but not in the United States.

The Security and Exchange Commission in USA don't want to switch to International Financial Reporting Standards in the short term, but it will continue reviewing a proposal to allow IFRS information to supplement US financial filings.

Countries that benefit the most from the standards are those that do a lot of international business and investing.

Advocates suggest that a global adoption of IFRS would save money on alternative comparison costs and individual investigations, and in the meantime allowing information to flow more freely.

In the countries that have adopted IFRS, both companies and investors benefit from using the system, since investors are more likely to put money into a company if the company's business practices are transparent. Moreover, the cost of investments are usually lower.

2.2.2 - Generally Accepted Accounting Principles – GAAP

Generally accepted accounting principles (GAAP) refer to a common set of accepted accounting principles, standards, and legislative procedures that companies and their accountants must follow when compiling their financial statements. GAAP are focused on the practices of US companies and they are issued by the Financial Accounting Standards Board (FASB).

Generally speaking, GAAP are a combination of authoritative standards set by the FASB and a commonly accepted ways of recording and reporting accounting information in USA. GAAP improve the clarity of the communication of financial information, especially for external investors who want to have a better and more accurate idea on the

companies they want to invest in. GAAP covers such things as revenue recognition, balance sheet item classification and outstanding share measurements.

GAAP must be followed when a company distributes its financial statements outside of the company. If a corporation's stock is publicly traded in USA, the financial statements must also follow rules established by the US Securities and Exchange Commission (SEC).

However, some companies may use both GAAP and non-GAAP compliant measures when reporting financial results. GAAP regulations require that non-GAAP measures are explicated clearly in financial statements and other public disclosures, such as press releases.

2.2.3 - IFRS vs. GAAP

The main differences that exist between IFRS and GAAP accounting rules include:

- LIFO Inventory

  While GAAP allows companies to use the *Last In First Out* (LIFO) as an inventory cost method, it is prohibited under IFRS.

- Costs of Development

  The costs of development of products are to be charged to expense as they are incurred under GAAP. Under IFRS, the costs can be capitalized and amortized over multiple accounting periods.

- Write-Downs

  GAAP specifies that the amount of write-down of an inventory or fixed asset. This quantity cannot be reversed if the market value of the asset increases. The write-down can be reversed under IFRS instead.

As mid-size and big companies increasingly need to operate in global markets and conduct operations around the world, international standards are becoming increasingly popular at the expense of GAAP, even in USA.

2.3 - Banking regulations

Banking regulation is a form of government regulation which subjects banks to certain requirements, restrictions and guidelines, designed to create market transparency between banking institutions and the individuals and corporations, with which banks have relationships and make business.

2.3.1 - Basel Committee on Banking Supervision

The Basel Committee on Banking Supervision (BCBS) is the primary global standard setter for the regulation of banks and provides a forum for regular cooperation on banking supervisory themes.

The Basel Committee, initially named the Committee on Banking Regulations and Supervisory Practices, was established by the central bank Governors of the Group of Ten countries at the end of 1974, after big problems with international currencies and banking markets. The Committee's first meeting took place in February 1975; since then, meetings have been held regularly three or four times a year.

Today the committee has 45 members, including central banks and bank supervisors from 28 jurisdictions. The committee consists of senior representatives of bank supervisory authorities and central banks of the following countries: Argentina, Australia, Belgium, Brazil, Canada, China, France, Germany, Hong Kong SAR, India, Indonesia, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, Russia, Saudi Arabia, Singapore, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom and USA.

It is named *Basel* Committee because it usually meets at the Bank for International Settlements in Basel, Switzerland, where its permanent Secretariat is located.

The main goal of the committee is to strengthen the regulation, supervision and practices of banks around the world in order to enhance financial stability. The BCBS aims to enhance "*financial stability by improving supervisory know-how and the quality of banking supervision worldwide*." This is done through regulations named accords, known worldwide as Basel accords.

These accords are a series of international standards for banks regulation, in particular regarding capital adequacy.

The Basel accords are four and they are: Basel I, Basel II, Basel III and the most recent one Basel IV.

2.3.2 - Basel I

Basel I is a set of international banking regulations written by the Basel Committee on Banking Supervision that sets out the minimum capital requirements of financial institutions, with the overall goal of minimizing credit risk and establish an appropriate risk-weighting of assets. Therefore, Basel I was primarily focused on Credit Risk and Risk Weighted Assets (RWAs).

The Basel Committee classified and grouped the assets of bank in five categories, according to the level of risk that is associated with that class of asset, carrying risk weights of:

- 0% (for example cash, bullion, home country debt like treasuries);
- 20% (securitizations such as mortgage-backed securities (MBS) with the highest AAA rating);
- 50% (municipal revenue bonds, residential mortgages);
- 100% (most corporate debt);
- No rating.

Banks with an international presence are required to hold capital equal or greater to 8% of their risk-weighted assets.

Put in mathematical terms, the capital adequacy indicator of a bank is calculated by the ratio between the capital and the risk-weighted assets. This ratio, according to what established by Basel I, should be equal or greater than 8%:

$$\frac{Capital}{Risk-weighted\ assets} \geq 8\%$$

The implementation of Basel I standards brought positive effects in the financial environment. Besides a relatively simple structure of the standards and the categories, the main effect was an increased competitive equality between internationally active banks, given also the worldwide adoption. The capital of banks started to be managed with greater attention and discipline by banks. Finally, through the capital adequacy ratio, Basel I created a benchmark for an overall accepted assessment of the players in the financial market.

Even though these advantages, some weaknesses became eventually evident. For instance, the capital adequacy ratio depended only on credit risk, while other types of risk such as the market risk and the operational risk were excluded. Consequently, values

involved in the adequacy ratio were considered at their book value and not at their market value. Moreover, when considering the credit risk, there was no difference between debtors of different credit quality and rating.

These considerations brought to an amendment to recommendations from 1993 and 1996, which introduced a new capital adequacy ratio for capital requirement and a new instrument for the assessment of bank's market risk, the Value at Risk (VaR).

Firstly, the new capital adequacy ratio was between the capital and the risk-weighted exposures, including also market risk.

$$\frac{\boldsymbol{Capital}}{\boldsymbol{Risk-weighted\ exposures\ (credit\ and\ market\ risk)}} \geq 8\%$$

Secondly, the new instrument introduced by the amendment, the Value at Risk, is a statistic that measures and quantifies the level of financial risk within a bank over a specific time frame. The VaR of a bank is determined with statistical models and techniques, used to assess the potential loss and the probability of occurrence for the defined loss.

Today, VaR is still commonly used by investment and commercial banks to determine the extent and occurrence ratio of potential losses in their institutional portfolios.

In a nutshell, the VaR, which is a measure of a bank's market risk, is measured by assessing an amount of potential loss, a probability of occurrence for the amount of loss and a specific time frame.

2.3.3 - Basel II

The main objective of Basel II was to align regulation with the best practices in risk management, providing banks with incentives to enhance risk measurement and avoiding all the possible forms of regulatory arbitrage.

As the former chairman of the Basel Committee Jaime Caruana said, "*Basel II is not intended simply to ensure compliance with a new set of capital rules. Rather, it is intended to enhance the quality of risk management and supervision.*"

Basel II is based on three principles:

- Minimum capital requirements
- Capital supervising
- Market discipline

Principle 1: Minimum capital requirements

The definition of bank capital, established with Basel I in 1988, remained the same also in Basel II and it remains largely the same today as well. This definition makes a classification of the capital into three different levels: Tier 1, Tier 2 and Tier 3. These three tiers were born from the necessity of some criteria to ensure the similarity of capital components across all the countries. These criteria are:

- Permanence;
- Freedom, meaning the ability to absorb losses on an ongoing basis;
- Subordination to depositors and other creditors.

The extent to which a capital instrument meet these criteria will determine the tier of capital in which it is categorized.

Tier 1 deemed to have the highest capacity to absorb losses, in order to allow banks continue to operate on ongoing basis. This includes common shareholder equity and disclosed reserves, which are reserves published after tax earnings and dividend payments.

Tier 2 capital is the secondary component of bank capital that compose a bank's required reserves. It cannot exceed 100% of Tier 1 capital and it is designated as supplementary capital. This supplementary capital is composed of items such as undisclosed reserves, revaluation reserves, hybrid capital instruments and subordinated term debt.

Undisclosed reserves are reserves not disclosed publicly by the bank itself, while revaluation reserves are reserves created by the revaluation of the asset (a building for example). Hybrid capital instruments have mixed characteristics of both debt and equity instruments, such as preferred stock. The last component is debt subordinated to other debts, loans or securities with a higher seniority.

Tier 3 capital includes a greater variety of debt than Tier 1 and Tier 2 capitals. Tier 3 capital include a larger number of undisclosed reserves and subordinated term debt compared with Tier 2 capital.

In particular, to qualify as Tier 3 capital, assets must be limited to 250% of a banks Tier 1 capital, be unsecured, subordinated, and have a minimum maturity of two years.

Principle 2: Supervisory review

This principle is based on the foundation upon which banks should have a process for assessing their overall capital adequacy according to their risk profile and a strategy for maintaining their current level of capital.

This process is carried out by one or more than one professional figures, called supervisors, that have the specific duty to review and evaluate banks' capital adequacy and the strategies related. Supervisors should monitor and ensure banks' compliance with regulatory capital ratios required from the Basel committee; in case the ratios are not respected, they should take appropriate action to require banks to hold capital in excess of minimum requirements.

However, if possible, supervisors should seek to intervene at an early stage to prevent capital from falling below the minimum levels required to support the risk characteristics of a specific bank. They should require a fast remedial action if capital is not maintained or restored over time.

On a national level, when considering the set of banks within the scope of the implementation, supervisors should take into account quantitative as well as qualitative criteria such as a bank's size and risk profile, the complexity of its activities and its international presence.

Principle 3: Market discipline

The purpose of the third principle, market discipline, is to complement the operation of minimum capital requirements and the supervisory review process.

The Basel Committee has the objective to encourage market discipline by developing a set of disclosure recommendations and requirements which will allow market participants to assess key pieces of information on the scope of application, capital, risk exposures, risk assessment and management processes, and therefore the capital adequacy of the institution.

The disclosures that the bank must make are greatly increased. This is designed to allow the financial market to have a better picture of the overall risk position of the bank, increasing the transparency of the banking operations. The disclosures on which is based the principle of market discipline allows the counterparties, partners, and all the other possible entities with which the bank could have a relationship, to be able to set prices and deals appropriately in the financial market.

2.3.4 - Basel III

Basel III is the internationally agreed set of measures developed by the Basel Committee in response to the financial crisis started during 2007.

Like all Basel Committee standards, Basel III standards are minimum requirements that apply to internationally active banks. Members are committed to implementing and applying standards in their jurisdictions within a period of time established by the committee.

Being a response to the financial crisis, Basel III addresses a number of shortcomings in the previous regulatory framework and provides a foundation for a strong banking system, which will help avoid the presence of systemic vulnerabilities.

As the document of Basel III itself says, "*The objective of the reforms is to improve the banking sector's ability to absorb shocks arising from financial and economic stress, whatever the source, thus reducing the risk of spillover from the financial sector to the real economy.*"

Therefore, the framework described aims to allow the banking system to support the real economy, even in the most difficult and demanding circumstances.

Basel III also aims to improve risk management and governance as well as strengthen banks' transparency and disclosures. Finally, Basel III reflects the Committee's efforts to regulate significant cross-border banks. These efforts include the recommendations to reinforce national resolution powers and their cross-border implementation.

Consequently, the committee mandated its Cross-border Bank Resolution Group to report on the lessons from the crisis, on recent changes and adaptations of national frameworks for cross-border resolutions and on the most effective elements of current national frameworks.

2.3.5 - Basel IV

The 7th December 2017, the Basel Committee published a document finalizing Basel III reforms, also known as Basel IV. This document concludes the proposals and consultations ongoing since 2014.

The purpose of the Basel IV was to establish a global minimum standard for dealing with the past financial crisis and, at the same time, to prevent new crises by increasing the capitalization of the institutions. Another important goal was to reduce high variability of risk-weighted assets (RWAs).

The finalization took place by the Group of Central Bank Governors and Heads of Supervision.

Key points of Basel IV are referred to:

- Credit risk;
- Risk weights;
- Operational risk;
- Leverage ratio;
- Capital floor.

Credit risk

Basel IV sets forth a revision of the standardized approach for credit risk and a revision of the internal ratings-based (IRB) approach.

The regulations meet the consistency goals by removing the option to use the advanced IRB approach for asset classes that are not subject to robust and prudent modeling. These restrictions apply to three type of entities:

- Large and mid-size corporates (with consolidated revenues above €500m), restricted to Foundation IRB (F-IRB) or Standardized approach (SA) only;
- Banks and other financial institutions, restricted to F-IRB or SA only;
- Equities, restricted to SA only.

Risk weights

Risk weights become classified according to newly defined risk categories; a standardized approach aims to improve granularity and risk-sensitivity.

For instance, for banks, risk weights are driven by an external rating, ranging from 20%-150%. For jurisdictions that do not permit ratings for banks, or for unrated exposures, the risk weights range from 20% to 150%, depending on newly defined risk categories.

Similarly, for corporates, the risk weight is driven by external ratings, ranging from 20% to 150%. For jurisdictions that do not permit ratings for corporates, or for unrated exposures, the risk weights range from 65% to 100%.

Small and medium enterprises are separately identified and apply an 85% risk weight. For subordinated debt and equity, the risk weight is categorized based on exposure type and varies between 100% and 400%.

Operational risk

Regarding the operational risk of banks, Basel IV removes all existing approaches and started to require a single, risk-sensitive standardized approach. This approach involves a combination of the bank's income and the historical losses.

Therefore, the previous approach used for operational risk was redesigned and all alternative approaches were eliminated.

Leverage ratio

The leverage ratio is defined as the capital divided by the exposure measure. The exposure measure is the sum of the on-balance sheet exposures, derivative exposures, securities financing transactions exposures and off-balance sheet exposures.

The leverage ratio is set at 3% of Tier 1 capital against total exposure. The capital and the exposure measure should be calculated on a quarter-end basis; even though, supervisors may allow more frequent calculations if they are consistent calculations.

Basel IV introduces also an additional requirement for global systemically important institutions (G-SIIs). G-SIIs are required to meet a higher leverage ratio: in particular, the leverage ratio must be greater of a particular percentage that equals the half of the percentage level of add on Common Equity Tier 1 capital. For example, if a G-SII has a 2% of add on Common Equity Tier 1 capital, the institution itself will face an additional 1% leverage ratio required.

Capital floor

One of the most important and new elements introduced by Basel IV is the capital floor, or output floor, designed to reduce variability in risk-weighted assets and to improve comparability of capital ratios among banks. Moreover, the capital floor is designed by regulators to ensure that risk-based capital requirements do not fall too much.

The Basel Committee advocated using the standardized approaches to calculating RWAs as a floor for the outputs from internal modelled approaches. The initial suggestion was that internal model RWAs should not fall below 60% to 90% of standardized outputs. The aim was to reduce the variation of internal model outputs between banks and to mitigate model risk and measurement error. After more than 18 months of negotiations, the Basel Committee agreed in December 2017 to set a floor of 72.5%.

This was a compromise between US regulators who had argued for a higher level, and European regulators who wanted a lower level.

Therefore, Basel IV require that RWAs should be calculated as the higher of the approved approaches and 72.5% of the total RWAs, using only the standardized approach.

The standardized approach includes credit risk, counterparty credit risk, securitization, market risk and operational risk.

All banks are also required to disclose their RWAs and capital ratios on two bases: one without the capital floor, and another with the floor applied, along with additional and more detailed information.

The future impact of capital floor depend on business models and on the approach banks are using for calculating capital requirements. For large banks using internal models to calculate most of their capital requirements, the impact will be larger. For them the floor is likely to result in a significant increase in capital requirements.

Basel IV: implementation dates

The implementation dates are confirmed as 1st January 2022 for all the key points considered above, plus the revised market risk framework already published in 2016 by the Basel Committee itself.

The only exception to this date is the output floor of 72.5%, which will be phased over the following years as shown in the table below.

1st January 2022	50%
1st January 2023	55%
1st January 2024	60%
1st January 2025	65%
1st January 2026	70%
1st Jauary 2027	72.5%

Table 2 – Output floor phases

In addition to this, there will be a 25% transitional cap on the increase of firms' risk-weighted assets. This cap applies until the 1st January 2027.

2.4 EXTRA-UE regulations: USA, Brazil and Japan cases

International standards set by the Basel Committee are required to ensure that all banks which can transmit risks across borders meet sufficiently stringent solvency and liquidity requirements. This is carried out with the objective to facilitate the operation of international banks at a global level, and to favour the integration of global banking markets.

Basel I, II, III and IV are not designed to be applied to the whole banking system in all jurisdictions. The Basel core principles for effective banking supervision do not require jurisdictions to apply the capital adequacy rules to non-internationally active banks.

The Basel framework therefore follows the concept of proportionality, which refers to tailoring regulatory requirements to non-internationally active banks, especially the smaller and less complex ones. Indeed, Basel I, II and III already incorporate some limited elements of proportionality by offering a variety of approaches for calculating risk-weighted assets, as we have already seen previously.

The application of proportionality implies that regulatory requirements may differ significantly across banks in the same jurisdiction, depending on the size or other characteristics. The impact of these differences in a competitive environment can partially explain why, when implementing the Basel framework, some countries chose to apply the standards to all banks in their jurisdictions, meanwhile other countries decided to apply the full Basel standards only to internationally active banks.

Below there are some example of proportionality approaches in countries outside Europe.

<u>The case of United States</u>

The USA has applied the full Basel standards to a specific group of banks and bank holding companies. In particular, these are banks with an advanced approach banking organization. They are typically banking organizations with consolidated total assets equal or greater than US$ 250 billion or with foreign exposures on the balance sheet equal to US$ 10 billion or more.

A proportional application of the international standards in the USA is the one related to the market risk and credit risk frameworks. Only banking organizations with aggregate trading assets and liabilities equal to or above US$ 1 billion (or representing 10% or more of total assets), calculated quarterly, are subject to the US implementation of market risk-based capital requirements reflecting Basel II standards.

The case of Brazil

Brazil used to apply the minimum capital standards to the country's whole financial system.

This included more than 1,400 institutions that range from large and complex banks to credit unions and securities dealers.

However, Basel III brought the country to a change of approach.

The Central Bank of Brazil, the country's regulatory and supervisory authority, abandoned the approach taken since Basel II and undertook a comprehensive and public segmentation of the Brazilian financial system, starting to introduce regulatory requirements on a proportional basis.

The Brazilian regulation that establishes the new regulatory framework and divides the Brazilian financial system into five segments was issued in January 2017; it takes into account the size, the international activity, and the risk profile of the subject institutions.

The segmentation is applicable at the consolidated level to institutions operating in and from Brazil, which means that a foreign institution is assessed from the perspective of the operations of its Brazilian subsidiary.

The goal of the segmentation is to provide a simple categorization of the financial system. Linked to that, the categorization must be suitable for a variety of regulatory topics, ranging from prudential supervision to recovery and resolution issues.

Once the segmentation has been established, the next step for Brazil is to establish different regulatory requirements using the five segments as drivers for deciding on the appropriate proportionality for each specific situation.

The case of Japan

Japan applies the Basel frameworks to all internationally active banks. Japan's Financial Services Agency defines them as financial institutions if they have one or more branches or subsidiaries outside Japan, including bank holding companies, credit cooperatives, investment banks and regional banks.

On the other side, non-internationally active banks are subject to rules similar to the Basel standards, including the definition of capital; even though, a less stringent capital requirement with a minimum capital adequacy ratio of 4% applies.

2.5 Payments Regulation: Payment Services Directive (PSD)

The Payment Services Directive (PSD) was adopted in 2007. This legislation provides the legal foundation for an EU single market for payments, with the objective to establish safer and more innovative payment services across the EU. The idea behind was to make cross-border payments easy, efficient and secure as the national payments within a state member of EU.

Since 2007, this Directive on payment services brought substantial benefits to the economy in Europe, making access for new market entrants and payment institutions easier than before. Therefore, the result was an increase of competition that meant more choices to consumers. The PSD focuses on electronic payments, which are more cost-efficient than cash and which stimulate economic growth and consumption. Indeed, there are other payment means (for instance cash and cheques) not falling within the scope of the Directive.

The directive helped to make the Single Euro Payments Area (SEPA) in practice. The SEPA makes smooth the way cashless euro payments are made across countries member of EU. It allows European consumers, businesses and public administrations to make and receive under the same basic conditions the following types of transactions:

- Credit transfers;
- Direct debit payments;
- Card payments.

This makes all cross-border electronic payments as easy as domestic payments, in accordance with the overall goal of establishing efficient and easy payments of the PSD. The SEPA covers all the countries in the EU. It also applies to payments in euros in other countries: Iceland, Norway, Switzerland, Liechtenstein, Monaco and San Marino.

The establishment of this single area for payments have some advantages. Firstly, it allows the presence of a single system for both domestic and cross-border bank transfers. Secondly, it allows cross-border transactions by direct debit, which means charging directly a bank account in one country for services provided in another country. Finally, it allows people working or studying in another country to use an existing account in their home country to receive the salary or pay bills in the other country where they live.

An important principle covered by the SEPA is the principle of equal charges, which requires banks to apply the same charges for domestic and cross-border electronic payment transactions in euro.

The principle of equal charges, both for national and cross-border payments, applies to all electronically processed payments in euro, including:

- Credit transfers;
- Direct debits;
- Withdrawals at cash machines (ATMs);
- Payments by debit and credit cards;
- Money remittance.

The PSD and the SEPA brought more transparency and information for consumers during the last ten years in the industry, for example regarding execution times and fees. Execution times were reduced, refund rights were strengthened.

Another very tangible benefit is that payments became easier and quicker throughout the whole EU; today payments are usually credited to the payment receiver's account within the next day.

Revised Payment Services Directive (PSD2)

The European Commission proposed to review PSD to modernize it, with the objective to take into account new types of payment services, especially new online payments on internet previously unregulated.

Updated definitions ensure a level playing field between different providers and address in a more efficient way the consumer protection and privacy needed in the context of modern type of electronic payments.

The revision of the Payment Services Directive was proposed in July 2013. The result was the Revised Payment Services Directive (PSD2), which complements and updates the previous directive.

The main difference is that PSD2 widens the scope of PSD by covering new services and players by extending the scope of existing services. PSD2 regulates payment instruments issued by payment service providers, which do not manage the bank account of the user of the service.

The revised Payment Services Directive requires banks to give Account Information Service Providers (AISPs) access to bank account information and to allow payment service providers to start payment transactions.

By enabling customers, consumers, and businesses alike to use third-party providers to manage their finances, PSD2 removes the monopoly banks held over their customers' account information.

Moreover, by providing third-party providers with access to consumer banking data, a host of new financial products and services can be built on top of existing bank infrastructures. This gives customers more convenience and control of their payment options through a single service.

Finally, with the purpose of making electronic payments safer and more secure, PSD2 introduces enhanced security measures to be implemented by all payment service providers. In particular, as a general rule, PSD2 requires payment service providers to apply strong customer authentication for electronic payment transactions.

In a future perspective, PSD2 will allow companies and consumers to benefit fully from the EU market, particularly in terms of electronic commerce (the well-known and widely fast growing e-commerce).

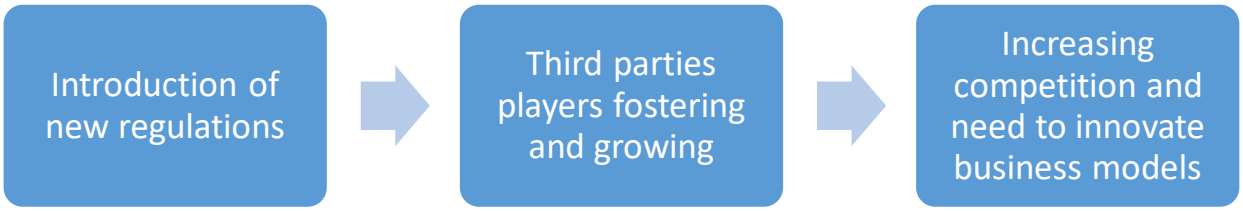
The Directive aims to help develop a single market for electronic payments, in line with the idea of a wide digital market where different parties such as retailers, consumers or other market players can meet each other and carry out transactions efficiently.

2.6 Effects of regulations: increasing competition and fostering banking innovation

Regulations aimed at increasing competition and openness in the financial services industry are encouraging banks to collaborate with new players to innovate and improve offerings from a strategic point of view.

Removal or relaxation of entry barriers has spurred the growth of new players by fostering a safe environment to innovate and gain ground in the value chain of banks.

A variety of innovation labs and new FinTech platforms have been springing up globally.



Therefore strategically speaking, with increasing competition and decreasing margins, banks have prioritized the innovation of business models: they are moving forward the digitalization of the processes and they are outsourcing big parts of the value chain in their middle and back offices.

Financial institutions are investing in innovation and vying to collaborate or establish partnerships with new players in the industry to develop innovative products and services, improve digital offerings and extend their reach into untapped markets.

For instance, traditional banks are acquiring or investing in FinTechs and digital-only challenger banks, such as the digital lenders described in the first chapter of the thesis. This new environment offers a win-win situation through which new players learn to thrive in the banking value chain by becoming platforms and marketplaces as incumbents diversify their product portfolios.

An example could be the Australian financial environment, in which regulators are following suit, and they announced recently an overhaul of the country's financial system and a comprehensive package of reforms to strengthen accountability and competition. For instance, there were reforms regarding the use of application programming interfaces to facilitate the sharing of customer and business data.

In Singapore, the Monetary Authority of Singapore built a FinTech Innovation Lab in 2016, and relaxed some regulatory requirements to give FinTechs the flexibility to innovate in a responsible environment. In a similar way, a regulatory framework for FinTechs in Japan was set up to support progress and development in the financial industry.

In South Korea, the Financial Services Commission opened a FinTech Open Platform to encourage startups throughout the country.

2.7 - Anti-Money Laundering (AML)

Money laundering is the process of creating the appearance that large amounts of money coming from criminal activity have been originated from a legitimate source, such as a legal business activity.

Indeed, criminals need a way to deposit their money in financial institutions, but they can do it only if the money appears to come from legitimate sources.

Dishonestly earned money coming from illegal activities is considered dirty, and the process of laundering "launders" the money to make it look clean (i.e. honestly earned).

During the last years, the financial industry witnessed a rise in regulatory pressures concerning Anti-Money Laundering (AML). Compliance with AML, Know Your Customer (KYC) processes and sanctions requirements continues to be a key focus area for management of the financial institutions, which have to ensure they are following appropriate compliance procedures to meet the increasing regulatory demands. Companies operating on a global scale have to demonstrate also a strong compliance framework, ensuring that each country in which they provide financial services has sufficient management oversight. In addition to that, global companies have to ensure that AML requirements are being met both at local and global level.

Money laundering investigations focus on analyzing financial records for inconsistencies or suspicious activity, and these financial records often relates perpetrators to criminal activity. In today's regulatory environment, extensive records are stored about every significant financial transaction in order to prevent organized criminals, drug smugglers or terrorists relying on money laundering to maintain cash flow for their illegal activities.

According to a survey done in 2018 by the global consulting company PwC, money laundering transactions account for roughly 2% to 5% of global GDP, which means roughly $1 trillion to $2 trillion every year.

Financial Action Task Force (FATF)

Concrete and permanent actions against money laundering began in 1989, when the seven industrialized countries composing the G7 formed an international committee called the Financial Action Task Force (FATF), with the purpose of fighting money laundering on an international scale. The FATF sets standards for contrasting money laundering and it promotes the implementation of these standards. In the early 2000s, the scope of the international committee was expanded into fighting the financing of terrorism as well. That happened because money laundering is one way in which terrorists finance their activities; therefore money laundering goes hand in hand with terrorism.

Today the FATF comprises 38 members, in particular 36 jurisdictions and 2 regional organizations. During the last decade, the FATF developed a series of recommendations that started to be adopted at the beginning of 2012. The goal was to give to its members a comprehensive set of measures to implement in the fight against money laundering, terrorist financing and financing of proliferation of mass destruction weapons.

It is important to highlight that the FATF promotes the implementation of these measures, but the leaders of each country member of the FATF has to carry out the measures at a national level.

Indeed, each country must adapt the measures to make them appropriate for its own financial and political environment. To help members implement the recommended anti-money laundering measures, the FATF provides them with guidance and best practices.

International Monetary Fund (IMF)

The International Monetary Fund (IMF) is an international organization that aims to promote global economic growth and financial stability, encourage international trade, and reduce poverty.

It is based in the USA in Washington D.C. and currently consists of 189 member countries, each of which has representation in the IMF's executive board in proportion to its financial importance; consequently, the most powerful countries in the global economy have the most voting power.

The IMF describes its mission with these words: "*to foster global monetary cooperation, secure financial stability, facilitate international trade, promote high employment and sustainable economic growth, and reduce poverty around the world*."

Since 2000, the IMF started to increase the efforts in relation to anti-money laundering measures and activities for its members. Moreover, from the 11th September of 2001, the IMF started to pay particular attention to the relations between money laundering and terrorist financing on the economies of its member countries.

Therefore, it began immediately to assess the compliance of the members with the international standard for combating terrorist financing.

The IMF points out that people who launder money and finance terrorism have, as target countries, the ones with weak legal and institutional structures; they use the weaknesses to their advantage to move big quantities of money. Ways in which the IMF helps its members stopping money laundering and terrorist financing include serving as an international forum for the exchange of information.

In addition to that, the IMF contributes to the evaluation of each country's compliance with anti-money laundering measures and contributes to identifying where each country needs improvements.

The IMF focuses its work on assessing the strengths and weaknesses of each member's financial sector in complying with the FATF recommendations.

An important activity of the IMF is to provide members with the technical assistance needed to strengthen their legal and financial institutions, and offering advice to members in the process of developing policies directed toward compliance with FATF measures.

Know Your Customer (KYC) process

The Know Your Customer (KYC) process carried out by financial institutions is strictly related to anti-money laundering measures and regulations.

In traditional banking, KYC involve every type of procedure done before starting business with a customer or before renewing the relationship with a customer. The customer, independently from the size, must be verified: banks have to know who their clients are and, especially, if they truly are who they say they are. Banks need to verify if the intent to transact is for legal business activities or not. This is known as Customer Due Diligence (CDD) or Enhanced Due Diligence (EDD).

Currently, the types of documents needed to verify identities for KYC varies from institution to institution. Some require passports or birth certificates, while others want Social Security cards or other types of national IDs, or even the driver's licenses. For businesses, the process becomes even more complicated. In conclusion, customers looking to sign up for financial services find that most KYC procedures create friction and result in a poor user experience.

Therefore, a crucial question becomes: how can be achieved effective KYC and AML processes while creating the least amount of friction? Is possible for financial institutions reducing fraud and providing a frictionless user experience?

The answer is that an increasing amount of friction causes more checks that can be made to improve KYC and AML. However, the principal aim should be achieving the right balance between a positive user experience from the side of customers and a more effective fraud prevention from the side of financial institutions. This is a situation of win-win for both parties, leaving off obviously the criminals and their illegal activities.

Nowadays, best practices include employing automated identity verification during the onboarding process to safeguard customer identity information; however, this type of verification can provide a more accurate check than if performed with manual review.

KYC procedures can be updated with new technologies as well. For instance, there is the possibility to deploy information systems that can assess the risk associated with a device used to sign into a financial institution's system. These new technologies, typically easy to implement and simple to maintain, are able to evaluate how likely a device will be used to commit fraud. This is especially useful in an account takeover situation and will help preventing criminals from doing business.

CHAPTER 3 - CASE STUDIES IN THE FINANCIAL INDUSTRY

In this chapter, I will present three case studies. The first one is based on my professional experience in an international major player of the financial industry. The second one is based on my personal experience during the period spent abroad for the Erasmus Extra-UE program in Latin America (Chile). The last one is based on studies conducted by consulting firms in the insurance sector.

3.1 Case study: KYC process of an international major player in the banking sector

3.1.1 - The KYC process

The KYC process, which stands for Know Your Customer, is a process through which customers of the bank are investigated through the collection of various kind of information.

The KYC process is based on a procedure called *vetting*.

A vetting permits the bank to acquire information about the customer when they start a new relationship, store it in an information system and update it when needed.

With a variable frequency of one, two or three years, the bank retrieves the information stored in the system about the customer and repeats again the vetting for the same customer.

This is done with the objective to verify the information previously stored, and to change it if something relevant happened.

The graph below shows the four steps that compose a *vetting* procedure and, therefore, the KYC process:

Figure 4

The KYC process has two triggers that could start it:

1. For new clients with no previous vetting done, the KYC process is triggered by a new KYC Request, which is also the way of doing the customers' onboarding process. There is the possibility that the client becomes KYC relevant when the onboarding process itself is done for a long time;

2. For clients who have been previously vetted, the KYC process is triggered automatically due to the approaching re-vetting Due date or manually via a pre-due-date re-vetting request by a stakeholder.

A system application supports and leads the user through all the steps of the KYC process, while BRE (Basic Risk Engine) is the tool that calculates the risk classification of a client.

3.1.2 - Attributes of a vetting procedure

For each vetting procedure, the attributes that are stored and displayed by the system are:

- NDG
- Priority Client
- Client Type
- Name of Client
- City and Country
- Location (all the locations a vetting exists for, displaying the associated risk class)
- Business area
- Risk Class
- Due Date
- Status
- KYC Delegate

The NDG is the unique code that identifies a client. In particular, for banks, it is the number of the general direction of the bank itself.

The Priority Client is a capital letter that indicates the priority with which the KYC process has to be carried out. There are three letters for priorities: A, B and C. The first one gives

the maximum priority to the vetting procedure, while the C priority type is associated to the least urgent customers.

The Client Type could be: Bank, Corporate or Retail. Bank clients are financial institutions further divided into Correspondent Banks and Non-correspondent Banks. The difference lies in the fact that the former ones could assume the role of intermediary between two banks that don't have any kind of relationship between each other; the latter ones cannot do that. Correspondent banks are typically large multinational financial companies that have at least one branch in almost all the countries around the world.

Corporate clients are big corporation with more than 500 million of euros in revenues. Retail are single extremely wealthy individuals, typically with a large patrimony or heredity.

After the name of the client, the systems application shows the city and the country in which the client is legally registered. The concept of location is related to the fact that a client could be present in more than one country (for example a bank could have branches in different countries). However, this concept will be explained better and further in details when talking about *Multilocation* with a specific paragraph.

Business area is the field of business in which the client operates.

Risk class is an important parameter because, depending on that, the system will carry out again the entire vetting procedure, and therefore the overall KYC process. The Risk class could be High, Medium or Low:

- HIGH: the KYC process is repeated after one year;
- MEDIUM: the KYC process is repeated after two years;
- LOW: the KYC process is repeated after three years.

The following attribute, the Due Date, is dependent to the Risk Class. The Due Date is the date in which the validity of the vetting procedure done for a particular customer expires. If the Risk Class of the customer is HIGH, the due date will be one year from the date of the end of the KYC process. If the Risk Class is MEDIUM, the due date will be two years from the date of the end of KYC process. If the Risk Class is LOW, the due date will be three years from the date of the end of KYC process.

The Status of the vetting refers whether the vetting procedure is in InWorkQueue status, Started status, Four Eyes Check status or Completed status.

Eventually, the last attribute KYC Delegate appears only if the KYC Specialist has delegated another user to continue the process on behalf of him: the KYC delegate assumes the same access rights and roles of the KYC Specialist who delegated him.

This attribute introduces the concept of KYC user: indeed, there different are types of users with different access rights, roles and activities that they carry out. The next paragraph explains all the possible types of users in the KYC process.

3.1.3 - KYC Users

In the KYC process there are nine types of users, which correspond to the profiles with which it is possible to enter into the system application. Each of them has different access rights and can do a certain kind of activities:

- *KYC Specialist*: he is responsible for the execution of the KYC process, therefore of the execution of the entire vetting procedure;

- *KYC Configurator*: he can configure some parameters of the system in a dedicated section of the tool and he cannot visualize customers' information;

- *KYC Supervisor*: he has the role of performing the four eyes control on the vetting. The KYC Supervisor must be a different user from the KYC Specialist; therefore, the same user cannot assume both roles of KYC specialist and KYC supervisor for the same vetting;

- *KYC Leading Supervisor*: he has the role of performing the four eyes control on the vetting and the role of checking the work of the other supervisors. Moreover, in the case a vetting is composed by two or more locations, and at least one of them has risk class HIGH, the vetting goes mandatorily to the KYC Leading Supervisor check;

- *KYC Head*: he can visualize in read mode only the section where the total amount of customers is shown. For each of these customers, he can visualize the current vetting ongoing and the previous ones done, called historical vettings;

- *KYC Requestor*: he has the right to create a new KYC request for new clients registered in the system application. As it will be discussed later, the new request could be an individual request or a massive request;

- *KYC Delegate*: it is not a self-consistent role, but he is a user that has been delegated from a KYC Specialist, KYC Supervisor or KYC Leading Supervisor in order to do the respective activities;

- *Compliance/Internal Audit:* user that can visualize in only read mode the section where the total amount of customers is shown; for each of these customers, he can visualize the current vetting and the previous ones (historical vettings);

- *Relationship Manager/Client Support (RM/CS):* user that can visualize in only read mode a section where a limited number of customers is shown; in particular, this means that the system will not show information about customers that do not belong to the perimeter of the Relationship Manager currently logged in the system application. For each of these customers, the RM can visualize the ongoing vetting and the previous ones (historical vettings).

3.1.4 - KYC New Request

The KYC Requestor, who is the user with the right to create a new KYC request, in order to proceed for investigating a new client, opens a new page of the system application. The KYC requestor can access:

1. Directly starting the application;
2. Via link from an external onboarding tool present in the Intranet of the enterprise.

The KYC vetting can be requested as:

1. **Individual request**. This means that the request is related to a single NDG only;
2. **Massive Request.** This allows requesting a KYC process for multiple NDGs (NDG codes must be known). A Massive Request needs an offline approval by the KYC Head before starting a vetting and going to the In Work Queue status.

From a functional the point of view, the KYC perimeter is defined in two lists, the Short List and the Commercial Banking List. Hence, if an NDG is KYC relevant it will be present in at least one of the two lists. If it is not present, that NDG is not in the KYC perimeter, and it is classified as *not KYC relevant*. The Short List contains the main customers of the

bank, including those with more than 500k annual revenues. The Commercial Banking List, contains all the customers that have at least one bank account and all types of partners of the company, even the ones owning shares of the financial company itself.

In case the NDG is not relevant a pop up will inform the user.

In the figure below, it is shown the flux diagram of a client, starting from the top. As shown, if a client has not a relationship with the institution at all, obviously it is not possible to proceed. If a client is not present in one of the two lists, it is not KYC relevant and therefore the KYC process does not start.

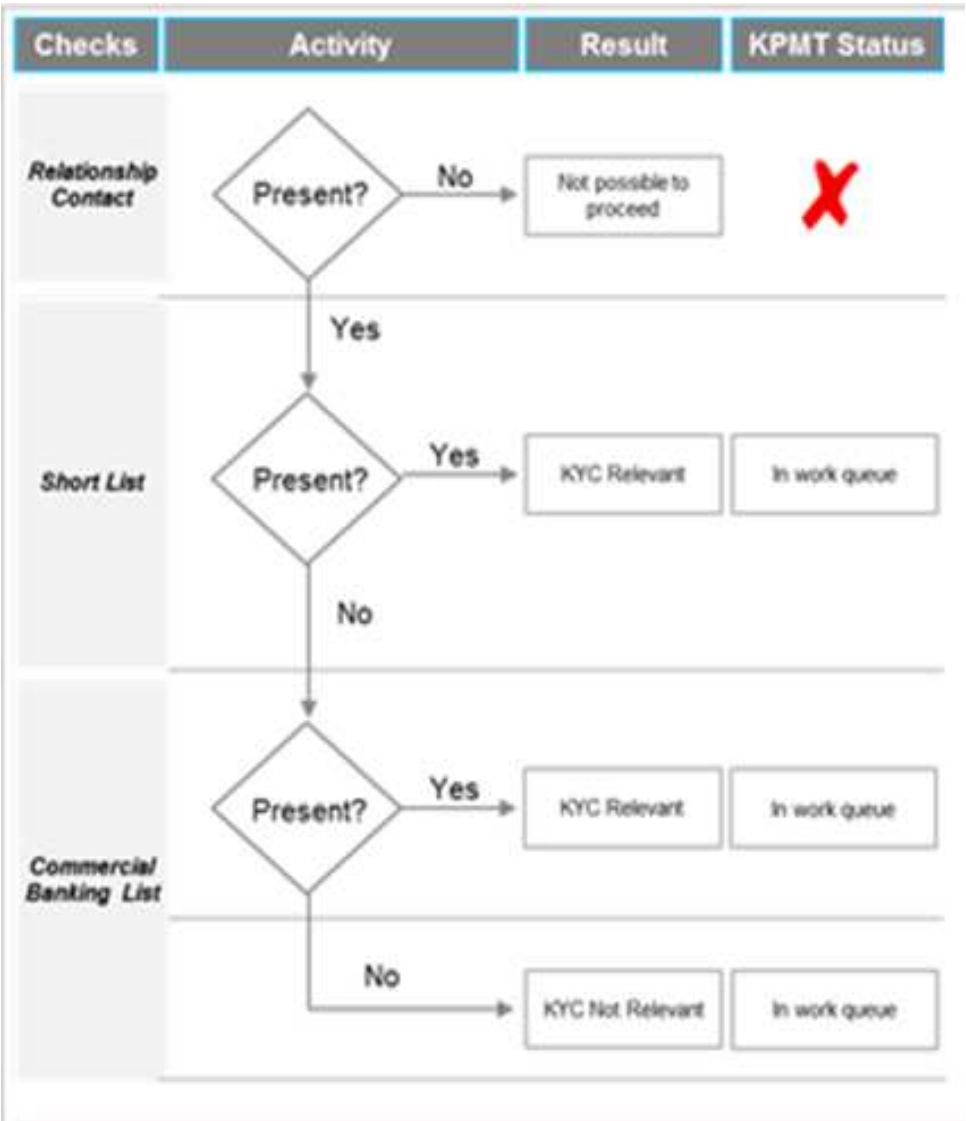


Figure 5

After a successful KYC request, the system application creates a work item and adds it in the first status IWQ, which is the first status of the vetting procedure as already said.

3.1.5 - In Work Queue status - IWQ

In the *In Work Queue* status, there are two tabs: Anagraphic Info and Centralization Data.

Anagraphic Info

In the Anagraphic Info tab, there are all the detailed information related to a customer: general information, location information, activity information and additional information (if required).

General information includes the NDG code, the NDG status, the Corporate Name and the complete name of the reference Manager of the company.

Location information comprises the address of the client: country, city, street address, Zip code or other possible geographic information needed.

Activity information refers to the sector in which the client operates and the typology of relationship established with the client.

Additional information includes specific mandatory information such as the SWIFT code, if a client is a bank.

Centralization Data

The Centralization process is applicable only in case the customer is a bank, and therefore it is characterized by the presence of the SWIFT code. In addition to that, the customer must have more than one location in order to be centralized and must give his consent to the bank to be centralized.

Given that the customer has given the consent, he can be centralized when, reached the due date of the vetting for a particular location (therefore the KYC process must be repeated) the KYC process itself for that customer has been already carried out for another location.

This implies that the team, which still has to carry out the vetting process, can send a request to the team that has already carry out the process in order to update the information for the same customer, and then going directly to the Completed status.

Let’s make an example in order to clarify better the concept.

For instance, imagine that the client under investigation is a multinational company operating in the Food & Beverage sector. This company has its headquarter in Germany but it is located also outside Europe (in USA).

The company has a bank account in Germany with the German branch of the bank and at the same has a bank account in USA with the American branch of the bank itself. The company has given its consent to the bank to be centralized.

If in Germany the due date of the vetting process is reached, the KYC process must be repeated; but, if the KYC process itself has been already carried out by the American branch of the bank, the German branch could send the request for centralizing the customer to the American branch.

The American branch, that has already done the process for the customer, checks the process and sends an answer with the information about the customer to the German branch of the bank. The customer, in the system application, goes directly to the Completed status if the centralization is accepted.

Having clarified the concept of centralization of a customer, three possible scenarios can be identified when the KYC Specialist reaches the Centralization Data tab:

1. If the customer has the SWIFT code and he has already been centralized in the past, the user must follow the centralization process. This scenario implies that the customer has already given the consent to be centralized, and therefore the tab Centralization Data will be editable.
2. If the customer has the SWIFT code but he has not been centralized, the KYC Specialist can decide to centralize him or not. If he decides to do so, he has to ask the consent to the customer in order to proceed.
   However, the presence of the consent is not a technical constraint for the user to carry out the centralization process on the system, but it is mandatory to guarantee the following of the legal steps for the centralization process and avoid possible lawsuits. The tab Centralization data will be editable in this case.
3. If the system does not retrieve the SWIFT code (because the customer is not a bank or because the code is not stored), the customer cannot be centralized; in this case the tab will not be editable. The only possibility is to proceed with a local KYC process, meaning a process without sending a request for information to a KYC team located in another country.

The Centralization Data tab contains an email that will be sent to the KYC team to centralize the customer.

The email is automatic, meaning that the majority of the fields are pre-filled.

In particular:

- Additional recipients can be added, but the pre-filled default recipients cannot be deleted;
- Object is pre-filled and cannot be changed;
- Email text is pre-filled but it is editable;
- Attachments can be uploaded.

After completing the updates, the KYC Specialist can send the email. The KYC Central team receives it and the vetting goes in Started status. In the meantime, the KYC Central team is notified of the request and can start the Centralization process.

Once the KYC Central team completes the vetting and notifies by email the KYC Specialist, the latter has two possibilities:

1. Accept the result of the Centralization and send the vetting to Completed status;
2. Do not accept the result; under this scenario the KYC Specialist can close the vetting, and a new vetting can be initialized. When the new vetting starts, the KYC Specialist has to specify the reason why the old centralized vetting has not been accepted. The KYC Central team will repeat the vetting process, and then will communicate the new result.

IWQ views based on the type of user:

- KYC Specialist can see:
    i. All active vettings in his ownership;
    ii. All active vettings not in Four eyes check status.

- RM/CS will see the work queue via Historical vetting requests:
    i. All vettings involving the respective RM/CS

- KYC Leading Supervisor can see and assign all the vettings in IWQ status.

- All other user profiles will see the full work queue via Historical vetting requests.

3.1.6 - Started status

The Started status contains five tabs: Risk Evaluation, Documents collection, Connected Person, Checks, First Level Control.

Risk Evaluation

The first tab *Risk Evaluation* is made up as follows:

- *Last completed vetting table*: here there are the list of locations for the customer, each one with the related Risk Class and Due date, of the last vetting performed. These fields are not editable. The table guides the user to track the location performed in the past; the closest location to expire is highlighted in bold;

- *Ongoing vetting table*: here there are the list of locations, each one with the related Risk Class and Due date, of the vetting currently in progress. For customers, the KYC Specialist can add other locations by flagging them, and can insert the Risk Class; in this case, the Due date will be automatically calculated and inserted by the system.

When the KYC Specialist adds or removes one or more locations, he has two different possibilities:

- press the button “Pre-potentially closed” (PCL status): this action allows the user to send in PCL only the locations that are selected; these locations will pass to PCL status and therefore they will not be provided with the Due date attribute.
  If the user needs to process a vetting with these locations, he will be able to do it starting a new vetting process and selecting them in Started status. In the *Last completed vetting* table of the tab, the user will have evidence of the locations previously sent in PCL or Closed.

  The action of putting a location in PCL status is carried out by the KYC specialist. It is important to note that, for the case of multilocation, this action must be done for each individual location. An item can stay in PCL status for a maximum of 30 days, then it will be automatically put in Closed status. However, during the 30 days, the user can recuperate the item putting it back in IWQ status.

Instead, once an item goes in Closed status, the action is irreversible: this means that the customer is no longer a client of the bank and therefore no longer has a relationship with the bank itself;

- press the button “Proceed to Four Eyes”: this action allows the user to work the selected locations normally, meaning according to the standard KYC process.

Documents collection

The second tab *Documents collection* contains the list of the documents to be collected for the customer under analysis.

The list of necessaries documents depends on a configuration matrix set by a dedicated role, the KYC Configurator. The matrix contains a set of parameters (type of customer, level of risk, branch…) that determines a list of documents as output; upon saving, the configuration is stored and it is automatically queried by the system.

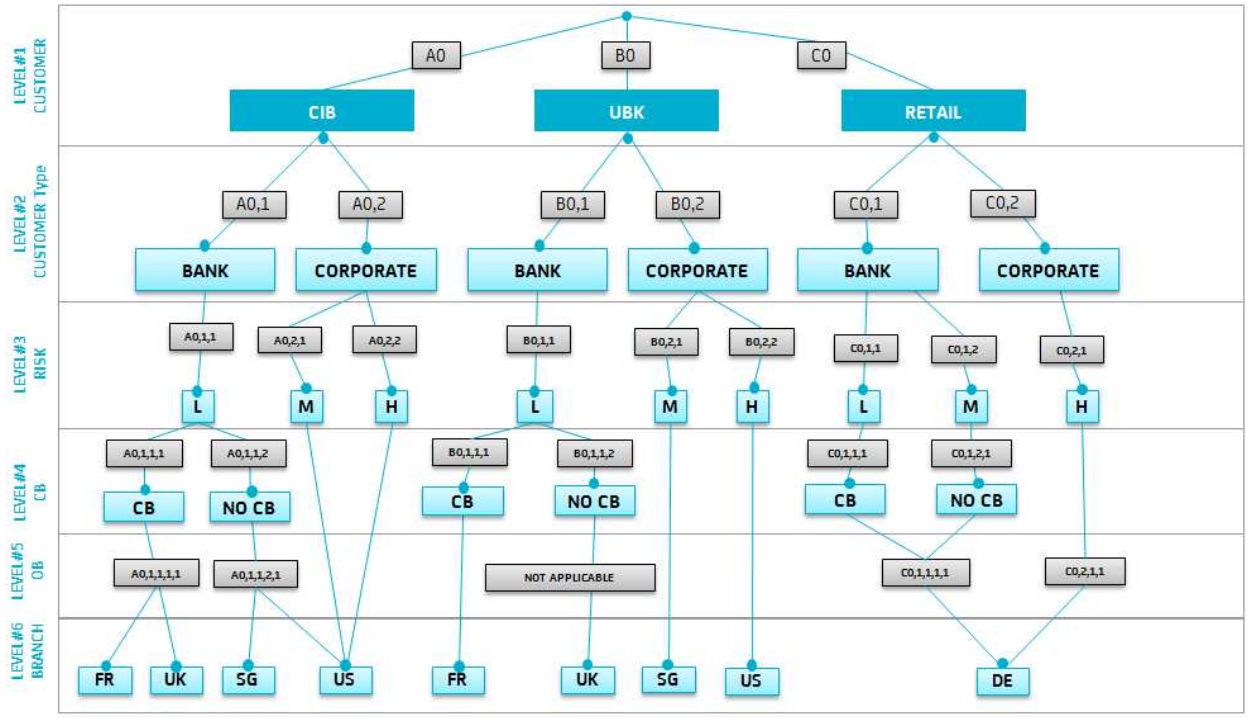


Figure 6

Each node in figure 3 represents a self-consistent set of documents that the system queries and the user must collect; being positioned on one node or another depends on the identity of the customer and the attributes associated.

In particular, from top to bottom, the following levels build the matrix:

- Level 1: Customer
- Level 2: Customer type
- Level 3: Risk Class
- Level 4: Correspondent Bank (CB/no CB), applicable only if level 2 is a Bank
- Level 5: Onboarding phase (OB), meaning whether it is the first vetting for that customer under analysis
- Level 6: Branch location (e.g. FR, IT, US…)

The first three levels discriminate the set of documents and the configuration set up of the customer; the last three levels can be considered as "add-on", meaning that independently by the previous configuration, all the documents are added on top.

In the table inside the tab, the KYC Specialist has the possibility to check the list of documents to be delivered, attach it and flag the field next to what has been uploaded. If one or more documents are not available, he can specify the reason as a note.

Finally he can confirm and proceed to the following tab, which is the Connected people tab.

Connected people

The connected people are all the individual entities that have a relation with the NDG under evaluation in the vetting. There are different typologies of connected people:

- BO: Beneficial Owner
- LE: Legal Representative
- IO: Intermediate Owner
- OC: Other Controllers
- RP: Related parties
- PO: Person placing order
- EN: Entity

The identification of the connected people is a pre-requisite to the *Checks* activity; each of the person is checked according to three different levels: Embargo, Politically Exposed Person (PEP) and Negative Information about the person.

Independently by the typology of the following check in the vetting process, the connected person can be provided in two ways:

- Automatically by the system application itself;
- Manually inserted by the user, most of the times the KYC Specialist.

When the connected person is automatically provided by the system application, this means that the application itself retrieves the relevant information about that person from an internal database, called *Customer Information File* (CIF).

On the other side, a manual addition of a connected person occurs when the user needs to evaluate someone not previously stored in the database. In this case, the user has to complete the following fields to successfully insert the connected people:

- *NDG*: not mandatory
- *First name/Company*: mandatory
- *Last name*: mandatory
- *Date of birth*: mandatory
- *Typology of connected person*: mandatory

Independently whether the connected person is retrieved automatically or manually added by a KYC user, the KYC Specialist has the possibility to remove a connected person if not necessary for the ongoing investigation. However, this action is under his responsibility.

<u>Checks</u>

The precondition to start the checks is fill in the previous tab “Connected person”.

The checks allowed are:

I. Embargo check;

II. PEP check;

III. Negative Information check.

The Embargo check verifies whether the current customer analyzed through the vetting procedure has a prohibition of having some kind of business activity with the country in which the financial institution is located. If that is the case, the system does not allow

continuing the KYC process and the vetting is stopped because the customer cannot have a business relationship with the bank.

The second one is PEP check: PEP stands for Politically Exposed Person. The application checks if the customer is involved in politic affairs and therefore has a relevant public exposure. It is important to highlight that this check is not limited only to particular wealthy individuals but it is extended to legal entities as well (e.g. corporations).

Finally, the Negative Information check verifies whether the customer under investigation recently had some generic negative news about him/her. It could be for example a negative news appeared on some national or international financial newspaper.

The KYC Specialist performs all the three checks through an external tool, which returns to the system application a result and a reference code for the check.

The reference code of a check is used to track all the checks carried out for the ongoing vetting procedure.

RM/Compliance Opinion Request (OR)

In this tab the KYC Specialist can send an Opinion Request (OR) to the Relationship Manager (RM) and Compliance team.

The operator clicks on the tab “RM/Compliance opinion”, fills in the field “New opinion request” with a short description of the request, and then presses the button “Submit” in order to finalize the OR submission.

A notification email is sent to the RM and Compliance team simultaneously.

In the meantime, the operator has the possibility to skip through the tabs and perform the activities included in Started status.

It is not possible to proceed to Four Eyes Check status until one or more ORs are opened.

An Opinion Request can have three different status:

- *Open*: the KYC Specialist opens a new OR when further analysis are necessary, asking for an opinion to the RM and Compliance team;
- *Closed*: after RM and Compliance team has provided at least an answer in their dedicated section, one of them has to close the OR;
- *Canceled*: the KYC specialist can withdraw an OR if he does not need anymore that information. He can do it until the RM or Compliance team have not already provided a feedback to the request.

The tab RM/Compliance opinion shows the list of the requests of the related Vetting, identified by an ID number.

The tab contains the following information:

- Opinion Request ID number
- Created by
- Status
- Creation date
- Outcome/Cancellation reason
- Reason
- Follow-up date
- Closure date
- Closed by
- Notes

By clicking on one Opinion Request ID number, a dedicated pop-up, which shows in details all the requested information, is shown.

The information shown is:

- *Starting data*: this section is pre-valorized; the info are related to the ongoing vetting;
- *Outcome*: these sections depends on the RM/Compliance results; they can provide an answer and insert additional notes;
- *Cancellation*: the KYC specialist has the possibility to cancel the request by clicking on the dedicated button “Cancellation” and indicate the reason of the OR closure (mandatory). The OR is blocked, and the reason is shown in the dashboard of the RM and Compliance team.

Once all the ORs are closed, the KYC Specialist is enabled to proceed to Four Eyes Check status.

3.1.7 - Four Eyes Check status

The Four Eyes Check status represents the activities carried out by the KYC Supervisor and, if needed, revised by the KYC Leading Supervisor. As also said before, the KYC Supervisor cannot be the same user that started the vetting process, which is the KYC Specialist.

Even though, the same user could have the role of KYC Specialist for a vetting, and the role of KYC Supervisor/Leading Supervisor for another vetting.

The KYC Supervisor has access to all the tabs of the vetting in only read mode until the Four Eyes tab; therefore, he cannot modify the previous tabs, but he can only accept or reject what has been done by the KYC Specialist.

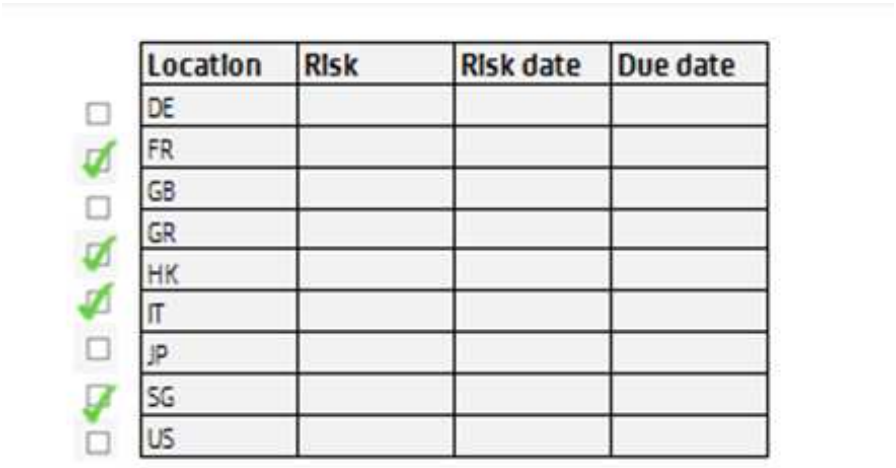
In this tab, all the principal information compiled by the KYC Specialist and calculated by the system are shown.

The KYC Supervisor has to check that everything is correct and, in the case if it is not, sends back the vetting to the first status, IWQ status, giving a detailed explanation of the motivations to the users that processed that vetting (KYC Specialist or other possible delegates). The KYC Specialist will have to repeat again the process of the vetting, taking into account the indications or errors pointed out by the KYC Supervisor or KYC Leading Supervisor.

When everything has been adjusted, the vetting passes into Completed status under the responsibility of the KYC Supervisor (or KYC Leading Supervisor).

3.1.8 - Completed status

This status is the final status of the vetting, in which all the locations and risk information (Risk Class and Due date) of the ongoing vetting are summarized in a table. Therefore, it is a visual recap of what has been done so far by the KYC Specialist and then approved by the KYC Supervisor for the customer under investigation. The Completed status represents the actual situation of that customer inside the whole banking group. All the locations of the client are shown and the ones with the tick box selected are the ones investigated in the current vetting procedure.



	Location	Risk	Risk date	Due date
☐	DE			
☑	FR			
☐	GB			
☑	GR			
☑	HK			
☐	IT			
☐	JP			
☑	SG			
☐	US			

Figure 7

3.1.9 - Multi-location case: requesting a vetting for a new location

The system application used in the KYC process allows the user to execute a vetting procedure for more than one location at the same time. This can be done only when the vetting is in status Started, even if the due date is not reached yet in the previous location. The user, in order to do so, needs to flag the locations that he needs to investigate in a table shown.

Besides that, all the locations will have the same information as checks, attached documents and risk date except for Risk class and Due date, that is always calculated based on the level of risk of each specific location of the client.

When the user requests a vetting for more than one location, the main location is the leading one, for which the KYC process is requested at the beginning, while the others are secondary.

3.1.10 - Closure of a vetting

When the due date comes for a particular customer, if the same customer is no longer a client of the institution, the vetting goes automatically into the *Closed* status.

This means that an investigation is no longer needed and it is no longer possible doing the KYC process, and therefore carrying out a vetting procedure: there is not a relationship between the two parties anymore.

3.2 Case study: Banco Falabella in Latin America

3.2.1 - My experience in Latin America

This case study is related to my experience of Erasmus EXTRA UE in Latin America, precisely in Santiago (Chile), from March 2018 to August 2018.

I had the privilege to study at the number one university of Latin America in the rankings of 2018, the *Pontificia Universidad Catòlica de Chile*, located in Santiago. Among the courses, I've attended an intensive program called GNAM, which stands for Global Network for Advanced Management.

The purpose of the program was to expose participants to understand the political and economic context of businesses in the main Latin American markets, as well as evaluating innovative business models in specific industries and identifying the key success factors for these models. In order to do that, professors explained the consumer cultures in Latin American markets, which are very different from European cultures, and they exposed

the impact of social media in the marketing actions of the small-medium enterprises (SMEs) and big corporations in Latin America.

In the morning and in the early afternoon there were scheduled lessons in the classrooms of the university, while in the late afternoon we visited two companies per day. For instance, we visited the Latin American headquarters of the global players Nestlé, Enel and Coca Cola Bottling.

From a human point of view, I met people from all over the world and made long lasting friends; therefore, it was absolutely an amazing experience and opportunity to widen my knowledge that the Chilean university gave to me during my Erasmus months.

3.2.2 - An innovative business model

Among the innovative business models studied, I will present here the case of Falabella and its presence in the financial industry with Banco Falabella. By the beginning of 2018, Falabella was amongst the Latin American corporations with the largest market capitalization, with more than USD 24 billion. Moreover, it was one of the main retailers in terms of annual revenues and EBITDA (respectively USD 15 billion and USD 2 billion).

The company is headquartered in Santiago (Chile) and has more than 110.000 employees in Latin America, including the countries of Mexico, Colombia, Peru, Brazil, Argentina and Uruguay. The interesting fact and the huge difference with the business model in the European financial industry is that Falabella offers a wide range of products and services in five business divisions: financial services, department stores, real estate, supermarkets and home improvement. In Europe, banks are present exclusively in the financial sector and they don’t have any presence in other type of industries.

All business segments of the company operate in Latin American countries and, over time, Falabella has used different ways to expand into businesses and countries. In the financial industry, Falabella entered the credit business in 1980 and became the first store to introduce its own credit card, usable to purchase things only in its stores.

To start a relationship with a new client without a financial history (onboarding of a new client), Falabella offered a credit card with a small quantity of money to be spent. As a result, Falabella acquired valuable information about customers from the very beginning.

In 2010, it established strategic partnerships and alliances with Visa and MasterCard, which allowed the credit card to be used in third party stores as well.

The credit card of Falabella was introduced and offered to customers in all the businesses in which the company was present. In 2017, the percentage of sales with the credit card was very relevant, representing more than 45% in department stores. Falabella had been the largest credit card issuer in Chile: the strategy behind was to offer a large set of products and one of the best loyalty programs in all Latin America.

Banco Falabella

Falabella expanded into the banking sector with the launch of Banco Falabella in 1998. The strategy pointed out by the board of directors of the company was to combine the stability of a traditional financial business (bank) with the proximity to customers that characterizes a retail company.

In particular, the chairman of the board, Carlo Solari, said: "The financial area has always been very relevant within the group. We realized that to maintain a relationship with customers, we had to go from being a credit card company to be a bank for people, which means personal banking."

In 2018, twenty years later, Falabella announced the full integration of its credit card business with Banco Falabella. The Chief Financial Officer of Falabella, Juan Manuel Matheu, said: "The integration has the goal to give an additional boost to the growth of the credit card business and Banco Falabella, improving their future perspectives."

Regarding the own credit card of Falabella, it expanded into Peru in 1998, and then to Colombia and Argentina in 2006. By the end of 2017, the active accounts with a credit card were almost 5 million and Banco Falabella had 264 branches along Chile, Peru, Argentina and Colombia.

Always in 2017, Falabella concluded the acquisition of 50% of the shares of the Mexican company Soriban (Servicios Financieros Soriana) for approximately USD 35 million: the goal was to offer services and credit products in more than 800 Soriana stores in Mexico.

Shopping malls

In 1990 Falabella entered the shopping mall business in Chile. At that time, there was only one mall in Chile, Parque Arauco, launched in 1982 by an independent mall developer.

Since then, the shopping mall industry had been growing in Latin America. One of the main reasons behind the growth was the increasing preference towards purchasing different goods and services in the same place, the so called "one stop shopping".

To be successful in the “one stop shopping”, malls should have a good variety and mix of offerings and stores. With this strategy, Falabella today owns department stores, home improvements store and supermarkets. However, the business model of the shopping malls in Latin America developed differently from the US, where most of them are isolated from the cities. In Latin America, most of the shopping malls are located inside the cities. For instance, in Santiago, the Costanera center is very well known because the shopping mall is located inside the tallest tower of Latin America (300 metres), which is in the very heart of the Chilean capital and, in my personal opinion, in the very heart of the financial business of all Latin America.

3.2.3 - The art of negotiation in the financial industry: the hidden challenges of cross-border negotiations

Another great argument I dealt with, in the intensive program I attended at the *Pontificia Universidad Catòlica de Chile*, was strategy of negotiations.

Being able to communicate effectively is a crucial skill, whether vis-à-vis with people, talking at the phone, or with a website page online. It is not relevant having a great product or providing an outstanding service if you cannot present it in an effective and understandable way to a potential customer. In addition to that, the product of the service you have doesn’t matter if you cannot communicate the value you are going to give in exchange of the money you will receive.

This is true in all the world of business, therefore in all the industries, and the financial industry is not an exception at all. Actually, in today’s world, where all people are submerged with any type of advertising and information possible during all day, it’s even more crucial than ever being able to reach effectively the recipients of your message and being able to distinguish yourself from the competition.

In negotiations, international deal makers have long bowed to local traditions and costumes. But new research suggests they also need to understand something deeper, which is the subtle yet potent ways through which the national culture shapes the governance and decision-making process during the deals.

Decision-making and governance processes, which determine either a “yes” or a “no”, can differ widely from culture to culture, not just in terms of legal technicalities but also in terms of behaviors and core beliefs. In international negotiations, it is not rare that a promising agreement fails because people involved ignored or underestimated the relevant differences in processes across cultures; differences that later on became barriers and obstacles impossible to overcome.

The first useful advice is to know exactly who is involved in the negotiation and which role or roles is playing. In particular, the all decision-making process could be drilled down into these questions:

i. Who are the players?
ii. Who decides that?
iii. What are the informal influences that can make or break a deal?

Who are the players?

Depending on the country you are negotiating terms and conditions for a business deal, there are typically extra players involved that could have an influence, beyond those representing the two companies.

For instance, at the level of top management, labor union in Germany has virtually equal representation on many supervisory boards of directors. Inside the European Union, various Brussels commission may get involved in business negotiations.

Outside Europe, instead, for example in China, local party officials play an integral part in Chinese negotiating teams in the People's Republic, even when the Chinese company is nominally "private". In USA, legal entities such as the Federal Trade Commission or the Justice Department could be involved in case of business deals between big corporations.

In the financial industry, extra players are typically involved when there are merger and acquisitions (M&As) negotiations on the table. For instance, when banks want to expand their presence abroad in other countries, they have to deal also with other players in the negotiation, such as trade union or government representatives.

Who decides that?

Even if you know who is playing in the negotiations, a failure to understand each player's role and who owns which decision can be very costly.

Considering again the example of M&As, owning the majority of the equity shares in USA often allows the buyer to control effectively the company purchased.

In Germany, this is not the case instead. German corporate governance provides a structure in which other key players, owning some shares of the company, can block even the actions of the majority of shareholders. While the management board in most large German companies has daily management responsibilities, it is only one of four sets of

players (along with shareholders, a supervisory board and labor union) that can play a significant role in any major decision.

Furthermore, in many cases in Germany labor union elects fully half of the members of the supervisory board, which in turn elects the management board. At the same time, the management board can prevent any single shareholder from voting more than 5% of the total company share, independently from how large the quantity of shares held is.

What are the informal influences that can make or break a deal?

It is fundamental to understand which kind of people must sign the contract to finalize a deal, but that is often not enough. Many countries have networks of influence that are more powerful than the actual parties making the deal, even though these parties don't have a formal standing, such as for instance governmental bodies normally have.

In Germany's financial industry, for example, the insurance giant Allianz has a strong influence on the majority of business deals. In Russia, it can be the Russian mafia and other protection rackets that have a relevant influence. In Japan, it can be the *keiretsu*, industrial groups that are linked by business ties, lending and cross-shareholdings.

US companies, typically coming from a culture with a strong legal system, frequently underestimate the power of informal influences because they assume that foreign legal systems will enforce formal contracts just as they are expected to do at home. In Japan, for instance, which has a relatively small legal system and few lawyers, most of the times companies rely only on relationships and negotiations to resolve business disputes.

3.3 - Case study: cybersecurity in the insurance sector

3.3.1 - Overview

The exponential development of the technologies over the past ten years, leading to new emerging assets being at risk such as robotics, cloud, the internet of things, augmented reality and wearable technology, is having a powerful impact on the insurance sector as well. Some of these may include apps in which insurance companies may transact customer data or new forms of payment.

At the customer level, this opens the door for insurers to introduce or redesign insurance products and technology related to face the latest trends in insurance exposures and losses. Firstly, many of the insurance products will be cyber. Risk managers of physical assets are now collaborating with risk managers of virtual assets, which will be a major shift for insurance organizations. Responding to cyber and data breaches is creating a new

way of analyzing risk, supported by processes and operational models that are becoming more agile in adapting to changes.

As consumers continue to demand services in real time globally and insurance companies expand internationally across borders, insurers are developing disruptive tools to help manage the risks. These technologies include increased usage of tablets and mobile-to-mobile payments, big data analytics, third-party contracts and personal digital devices that offer customers an outstanding experience. The digital world in the insurance sector is causing a fundamental shift from a product or service offering to a more personalized, user-driven strategy that focuses on customer needs and preferences.

While access to technology for the consumer is available, the main issues for insurers are back-end processing systems, legacy technology and manual processes.

As well as issues, insurance companies face many diverse risks that present opportunities and challenges. Security around networks, cyber threats and regulatory uncertainty are currently the biggest ones. This comes at a time when the industry continues to deal with low economic growth, high costs, low investment returns and market volatility. The market environment, continuously and rapidly changing, is leading to more complex business boundaries in the form of consolidation, innovations and disruptive technologies in order to support consumer demands and the increasing use of third-party agents.

Expansion and increased M&A activities are prevalent in the insurance sector, and reinsurers are increasing their share in direct access to domestic markets. This is combined with a drive to consolidate existing businesses, including outsourcing and shared service centers using third parties.

The need to support consumers across multiple platforms and channels is leading to the creation of third-party models for technology platforms and FinTech payments, as explained in the first chapter as well. Future channels and disruptive models are emerging that are changing the insurance ecosystem and laying the groundwork for digital transformation and meeting changing customer demands.

Since new platforms are replacing the traditional ones, insurers need to rethink distribution channels, market segmentation and go-to-market strategies. Continual advances in disruptive technologies empower consumers and provide easier access to markets and, at the same time, empower industry consolidation among insurers and technology companies.

In addition to that, insurers have to invest in improving their internal processes and restructuring their legacy systems in order to be responsive and effective. The regulators' main concern regarding these issues is the insurer's ability to control client data and maintain visibility.

The need to protect sensitive data is attracting more attention than in the past with the recent introduction of the Notifiable Data Breaches scheme in Australia and Europe's General Data Protection Regulation (GDPR). Insurance companies are particularly affected because they have access to incredibly sensitive customer data. They need to protect it to comply with privacy and data breach laws, as well as to maintain their customers' loyalty.

The insurance sector is becoming an increasingly attractive target due to the valuable data insurers hold on individuals. Customers of insurers and customers being serviced and managed by brokers, are really getting aware about data privacy. They need a warranty that the information they share is protected and not used or passed on without their knowledge and consent. Insurers possess a lot of data on individuals: they have data about their health, anagraphic information, properties, cars and other vehicles, and even their pets.

If banks hold the money, insurers hold the data; therefore, identity fraud is a significant risk in the sector. Cyber hackers usually attack the point of least resistance: since banks are currently strengthen their defenses, they are moving their focus to the insurance sector. Thus, given that the sector provides an attractive target for cyber criminals, a strong cyber security is more important than ever.

Insurance providers should focus on five key areas to address cyber risks:

1. Strategy

Insurance providers need to ensure their cybersecurity posture is strong, strategically speaking. This means reviewing the capabilities that are already in place, identifying any gaps and then plugging the gaps as needed.

In addition to that, new and improved cyber security capabilities are likely to be required. Where best practices are already in place, insurers need to spread them throughout the whole organization, establishing values and a culture on respecting and strictly following them. Indeed, leading insurers in the sector are starting by ensuring that their existing capabilities are being properly utilized.

2. Responsibility

Insurers cannot leave cybersecurity to the IT department in isolation. Cyber security is a business issue, not only an IT issue. Most organizations have elevated cybersecurity to a boardroom issue and insurance providers must do the same: the most successful insurers have their Chief Security Officer reporting directly to the Chief Operating Officer, creating clear sights between the business and the risk.

Therefore, the best practice seems to be appointing one or more responsible of cybersecurity in the companies; in this way, stakeholders can get a clear picture of cyber risk and what is being done to address it.

3. Communication

Every employee of the organization needs to understand that security is his or her responsibility, from the Chief Executive Officer down to the new entrants. This includes understanding where vulnerabilities could come from, such as third-party suppliers and partners, agents, and people with access to sensitive data. In particular, insurers need to focus on improving their understanding of their ecosystem of third party participants, such as non-affiliated agents, outsourced service providers or other non-employees with access to data, with the goal to manage their risk in a consistent manner and always having the complete control.

Furthermore, insurance brokers and advisers are right at the frontend, thus insurance companies need to make sure that they are across the topic and understand it at the same level.

4. Collaboration

Leaders throughout the organization need to work together to understand how to meet the cyber challenge in the most effective and efficient way. Distributing resources appropriately and helping each other, especially when needed for understanding the potential origins of the cyber-attacks, are crucial points in the overall strategy of the insurance companies.

5. Planning

Organizations need to develop a cyber response plan and review it regularly to ensure they are prepared for any possible incident. Successfully activating a response and recovery program takes practice, commitment and clear responsibilities inside the organization. From exercises that simulate the way attackers behave through to improved employee training and more frequent drills, insurance companies need to carefully consider how to ensure their organization remains prepared.

This includes delineating responsibilities, training all team members, and practicing for potential scenarios. Chief Executive Officers should work with their business leaders to understand the right balance between centralized and decentralized services to most appropriately meet the cyber risks in the sector. Creating the right structure for robust and consistent cyber security is key to have a responsible and defendable response.

3.3.2 - Anthem Insurance Companies Inc. data security breach

Anthem Insurance Companies Inc. is the largest health benefits company by membership in the United States, with member insurers licensed to conduct business in all 50 states and the District of Columbia. Anthem Insurance discovered a major data security breach. The breach was eventually thought to have potentially exposed the data and records of around 78.8 million customers.

Data affected reportedly included names, birthdays, social security numbers, addresses and email addresses, as well as employee information, but not credit card or medical data. Anthem immediately alerted its principal regulator as well as the FBI, and called in a firm of consultants to help it assess remediation steps required.

The costs of the incident have been highly considerable for Anthem. The initial cost of security improvements, remediation and clean up after the breach have been estimated to be around $260 million. This estimation is despite the fact that there is no evidence to date that any customer data has been bought or sold on the dark-net by cyber criminals. Indeed, this has led some observers to speculate that a nation state rather than a cybercrime gang could have initiated the attack to Anthem IT systems.

In addition to these immediate costs, Anthem also faced very high costs for the slow-burn effects. It was announced that the insurer would be paying $115 million to settle litigation stemming from the attack. This settlement was subject to the approval of the presiding US district judge and the money will be used to pay for two years of credit monitoring for stakeholders potentially affected by the attack.

In 2018, Anthem agreed to pay the US government $16 million to settle potential privacy violations stemming the data breach. The data breach had a huge impact on almost 80 million customer records and resulted in the leak of sensitive, personal information belonging to former and active customers three years ago.

In particular, hackers managed to infiltrate a database and covertly steal records containing client names, dates of birth, physical and email addresses and Social Security numbers. The attack took place over a number of weeks before being detected and shut down. Under the terms of the agreement, Anthem is currently undertaking a corrective action plan, in order to enhance internal security procedures and practices. In addition to that, the government is monitoring the adoption of those practices as well.

The privacy settlement follows the closure of a class-action lawsuit levied against Anthem on behalf of customers impacted by the data breach. Anthem settled the suit for $115 million. However, after legal costs, it has been estimated that customers who claimed compensation will receive little more than a dollar each one.

CHAPTER 4 - CONCLUSIONS

"Data! Data! Data! I can't make bricks without clay!"

Sir Arthur Conan Doyle

This thesis, my final work of studies in Industrial Engineering and Management, had the objective to present the digital transformation of the financial industry, focusing on the banking sector and the insurance sector.

In the first chapter, I exposed the state of the art of the industry: there was an explanation of how the digital era has changed – and it is still changing – the financial market, with a deep penetration of smart devices. This penetration of smart devices allows several digital functionalities to be carried out quite easily.

Digital functionalities bring to a redefinition of business models, especially the ones of the banks in the sector: I discussed the Banking as-a-platform (BAAP) model and the establishment of new non-traditional competitors in the industry, fully basing their business model on the digital world (e.g. digital lenders).

The initial state of the art explained as well the main challenges that the digital players in the industry are facing and possible ways to overcome them.

In the second chapter I exposed the regulations, directives and legislative procedures that control and define the laws that the incumbents have to or should follow and respect. In particular, regulations are mandatory while directives are general indications or advices that financial institutions should follow for having better financial ratios in their balance sheet and income statement.

In this chapter I divided these financial "rules" into five categories: financial instruments regulations, accounting regulations, banking regulations, payments regulations and anti-money laundering regulations. Financial instruments regulations refer mainly to the Markets in Financial Instruments Directive (MiFiD).

For accounting matters, there are two big standards adopted from financial institutions around the world: the International Financial Reporting Standards (IFRS) and the Generally Accepted Accounting Principles (GAAP). Banking regulations are the four Basel accords, provided by the Basel Committee on Banking Supervision based in Basel (Switzerland).

Payments regulations consist in the Payments Service Directive (PSD) and its development PSD II. Finally, anti-money laundering regulations are guaranteed by the Financial Action Task Force (FATF) and the International Monetary Fund (IMF).

In the third chapter I presented three case studies deriving from my professional experience in an international major player in the financial industry, from my personal experience of studies abroad in Santiago (Chile) and from the literature on the financial industry. The experience of studying abroad was a great opportunity offered to me by my university, *Politecnico di Torino,* and I will always be thankful for that.

This experience allowed me to grow a lot as a person and to make long-lasting relationships, while perfecting Spanish skills as well.

Lastly, the current chapter has the goal to bring forth general considerations about the industry and final overall conclusions.

I chose to deal with the financial industry because it is an industry that have always attracted me since I was very young: discovering how the overall financial system works, including the central bank, banks and insurances, fascinates me. In my opinion, to do that, it is required a lot of study and practice in order to fully internalize the concepts and theories behind the different financial instruments and to understand macroeconomic and microeconomic variables as well.

For these reasons, I wanted to make an experience in this industry and, when the opportunity came, I did not hesitate. I am still learning new procedures and mechanisms inside the bank I am working in now, and I had the opportunity to do also a training about the insurance sector recently, with a general overview and comparison to other European countries.

My job as a consultant allows to work on different projects at the same time; therefore allows me to learn and quickly improve new skills, understanding different realities, challenges and situations inside the industry (indeed projects could be with different companies, not necessarily the same one).

Secondly, among the various possibilities, I chose a project related to the digital transformation area, since I am very passionate about technology, its new developments and the future trends for the imminent future. In particular, my desire was to find out at which step of the digital transformation journey banks has arrived so far and find out how much needs to be done yet for the implementation of the latest technologies in the processes of financial organizations.

From the professional experience previously described in the third chapter, I learned the importance of standards and the processes in a big corporation. Regarding this, Jack Ma, CEO and Founder of Alibaba, the giant Chinese retailer with almost 40 billion of euros of revenues in 2018, said: “If you start working for a big company, you are part of a big machine. If you start working for a small company, you learn to dream and follow a vision.”

That could seem an intuitive statement but, according to my personal opinion, it is crucial for understanding how daily life in companies really works. My experience in a big player in the financial industry confirms this statement. Indeed, big corporations, perfectly comparable to machines, move smoothly just in case the internal processes and standards are respected. Internal processes correspond to the gears that put in motion the machine itself.

However, it is not just sufficient observing and respecting processes. Processes must be clear and well-designed, according to the internal culture of the enterprise. I found out the importance of clarity while working for the KYC process, largely described in the third chapter: if processes are not clear, employees struggle continually to achieve the quality or time to market expected in the final delivery of the project.

Lack of clarity in the processes manifest in bureaucratic complications most of the times: the documents to be collected are not well defined and very few people know how to fill them. This makes difficult discovering all the steps of the process and almost impossible following them smoothly without delays or complexities.

The importance of people, as an important factor in digital transformation setting, is unquestionable. Financial companies digitize processes and develop new digital services and solutions, which could not be possible without an efficient operational system in the background to ensure information flow between different digital solutions and applications.

Technology assets that serve as enablers for digital transformation could be divided into two categories: operational back-bone and digital services platform. Managing changes coming with digital transformation can be over-whelming, and most of the financial institutions agree that employing a change-management process is even more important than ever in this digital age. Employees get used to specific work patterns and changing their habits without properly communicating and implementing those changes can undermine digital efforts. Change management, HR conversations, events and education help employees adapt to the change and contribute to a digital culture in the company.

In general, digital transformation enables digital tools to enhance productivity, efficiency and change of hard paper documents to secured PDF or HTML formats. The days with an application form and product sheets are far away. Sales teams and field officers are now empowered with smartphones and other portable devices where information can easily be stored and displayed whenever the user wants.

Nowadays, many financial services providers have embraced digital transformation. However, many companies have taken hold up approach of observing the developments of the technologies and then decide on whether investing and in what investing: this is a

reactive approach, which stands at the opposite of a proactive approach, with which companies act as pioneers of technologies bringing digital transformation.

It is possible to affirm that in the financial industry the greatest number of companies adopts a reactive approach: they first wait for the new technologies emerging and arriving into the market and then they decide in what investing. They do not develop digital technologies inside the organization, which means that most of the times they do not have a research and development department.

To clarify better the concept, this is the opposite of the behavior of proactive firms: for instance, companies such as Google, Amazon, and Facebook continuously invest large part of their profits into research and developments of new technologies and digital ways to enhance their value proposition to subscribers and customers.

The digital transformation in the financial industry has positively affected the economic growth and has accelerated the growth of innovations. Many financial experts are discussing that there is no economic growth, but the signs of potential positive impact are quite visible; the best examples are the mobile banking apps, mobile money and e-wallets. With the introduction of banking apps, mobile money and e-wallets have taken a central stage in finance all across the world.

From what described so far, it is possible to list the six following characteristics that the digital transformation has brought and is still bringing in the industry:

1. <u>High standardization</u>
   Financial services are always considered as high performing. When these are integrated with technology systems with standardized processes and data, this leads to a high standardization;

2. <u>Highly automated functions</u>
   Adoption of new technology tools lead to higher process automation for services such as money remittance, procurement orders, invoice generation, and KYC processes;

3. <u>Faster Performance</u>
   With the adoption of big-data and other machine learning tools in finance, it is easier to predict and forecast budget allowing teams to finish month-end cycles before time.

4. <u>Insight-driven functions</u>
   Digitalization has modified financial models in such a way that the resources concentrate more on deriving insights rather than focusing only on transactions.

5. Improved customer and employee experience
   The same level of information is available with customers and employees and thus less chaos in transactions.

6. Better service delivery
   The legacy systems integrated with new technologies have changed the finance's operating model and the structured processes have improved service delivery.

A closer look at the three case studies in the previous chapter reveals that one of the main value proposition of the financial business is capitalizing on technology to improve customer experience.

The primary aim of digital transformation in the financial sector is to be more customer-centric.

In financial services, competition is not just with other financial services providers but with anyone offering a real technology and consumer experience. The focus while digitizing financial services or while developing financial mobile applications should be to make the customer's lives easier. It is essential to make a point that digital transformation is not a technology strategy but an overall business strategy that makes business swift and quick to respond to the market.

Digitalization has unlocked newer opportunities in the banking, credit and capital market functions of the financial domain. There are multiple branch locations, and it is hard to keep a branch right next to the consumer. As a result, mobile apps have become extremely popular during the last five years.

The IT systems used, however, cannot be upgraded or updated as the developers too have moved to the newer and latest technologies. It is a considerable challenge for some financial services companies to pull out the data and get on to the modern technology-based system. Other than the integration of the legacy system with advanced technology, the keenness to embrace digitalization by company workforce was also a challenge. In addition to that, with the digital disruption in existing services and products, it is essential for companies to focus on acquiring new skills and technologies. Indeed, even though the right technology will outgrowth the efficiency, it is the workforce that ensures successful implementation. The key to surviving in a digital environment is to adapt and adjust to the changes: the Chief Information Officers of financial institutions take this responsibility to adopt the changes and lead the transformation.

The digital tools meant for financial services industry focus more on improving and updating the existing competencies and core systems. There are other exponential tools too that are intended to deliver new capabilities.

The growing technologies disrupting the financial system includes the cloud, robotic process automation, advanced and predictive analytics, cognitive computing, in-memory computing and blockchain technology.

The benefit of adopting cloud in finance is unquestionable. Cloud brings further acceleration and swiftness. Cloud technology in financial services expedites new digital workflows enabling effective collaboration between departments or collaboration between business and third parties. The financial institutions use cloud-enabled applications for business processes such as HR and accounting. As the workforce and the team becomes get comfortable with the application, it gets integrated with the core systems.

However, with cloud-enabled applications, it is easy to scale data for critical functions such as credit scoring, consumer payments, statements and billings for essential account functions. Also, data speed is vital for financial firms to stay competitive and in effect. Financial services industry is the primary target for cyber criminals, owing to sensitive personal information. Therefore companies operating in this industry find security and compliance as crucial problems. The quickness of cloud safeguards the critical data, digital financial assets, and user information while protecting the employee performance.

Regarding robotic process automation, many financial institutions work on multiple technology systems and process robotics assist in automating transaction processing and communication across various systems.

Robotic process automation efficiently replaces human involvement and consequently reduces human errors in the process. It addresses the key challenges of the financial sector and can be effectively utilized for billing and collection operations, accounts receivable functions, financial transactions, financial reporting. Automation will enhance the functionalities of legacy systems by lessening inefficiency and addressing the manual intensive activities. Although process robotics is at a testing state at a few organizations, it is working exceptionally well to support legacy systems.

Another important development of technologies is the one related to advanced and predictive analytics. Today, there are several different channels through which the customers interact with their financial services provider. Because of these multiple channels, there is a load of customer data being collected by financial organizations. This data can be effectively leveraged using advanced or predictive analytics to gain insight into consumer behavior. Advance/predictive analytics can assist financial establishments to optimize their processes, therefore reducing costs.

Cognitive computing is yet another constant disruption in finance. It is the technology that makes use of natural language processing, machine learning, speech recognition and computer vision to stimulate human thinking. For financial organizations, it is essential to collect, analyze and use data to improve decision making.

An idea inspired by cognitive computing. While chatting or performing financial transactions through cognitive computing, the avatar responds in different facial expressions according to the content of the conversation. It makes it appear more like a face-to-face conversation, enhancing the facial expression/emotion that is usually missing.

Some of the basic elements of cognitive computing are in the following list:

- It enables financial organizations to obtain personalized information about the customers and use the same to notify about payments, bills, and other reminders. Cognitive computing also offers suggestions regarding exceeding customer payments and other intelligent automation services.
- It ensures the creation of conversation interfaces for placing customer queries and responding to them. Chat-bots are the best example of AI-powered digital assistants, developed to respond to customer queries thereby improving consumer services and CRM.
- Robo-advisors too are a part of cognitive computing but are not AI-powered. The Robo-advisors use algorithms to read through data and come up with a suitable suggestion.
- Cognitive technology works similar to human thinking but is considered as key to security. Protection of financial data is vital; hence cognitive computing is the solution.

With complex laws and regulations within the financial sector, poor knowledge of data policies can make finances a challenge for customers. With cognitive computing, real-time updates on rules and real-time implementation of the policies help in keeping policy documents updated and encourage good compliance.

Cognitive computing has enabled real-time trading analysis and improved trading systems so that customers can be served faster and better.

Cognitive computing has been beneficial for both the company and customers. Apps enabled with algorithms, machine learning, digital advisors and improvement in cyber security have positively impacted customers to manage their finances.

With financial companies dealing an enormous amount of data, higher transaction volumes and increasing compliance; there arises a need to address real-time data analysis

challenge. If it is finance, it has to be high performing, but with enormous data load, the efficiency can be at stake.

The massive amount of trading and accounting data calls for a robust infrastructure, with high speed of transactions and in real-time.

In-memory computing platform addresses these challenges. The information is stored in the main random access memory of specialized servers. This means that it eliminates the delay while retrieving data from servers.

The 24-hour mobile banking pile up huge data and at the same time the regulations, exchange rates, interest rates, share prices, etc. are also required to be updated. In-memory computing platform offers users with real-time information and calculation. It also provides information around commodity trading in real-time at an excellent speed for the users to experience a never before financial experience.

Last but not least, one of the most trending digital tool these days is Blockchain. With the advent of Blockchain technology, the financial services industry is considered to have entered into a new digital era. This new technology has changed the way we think about transactions and has revolutionized the economy.

Blockchain technology stands out of all the technologies that have disrupted the finance vertical.

Blockchain powers decentralized digital currency also called as cryptocurrency.

In Blockchain technology, encrypted blocks of data are considered as currency and are shared during transactions. Blockchain technology makes use of advanced encryption techniques to verify currency and transaction. Blockchain technology ensures that only the authorized users who own the part of Blockchain can edit the data using the private key.
Smart Contract is one of the most attractive applications of Blockchain technology. It automates the execution of commercial agreements and transactions. As Blockchain technology entertain no middlemen, smart contracts are considered more secure than the traditional agreements that adds up cost for the middlemen. It is also believed that the Blockchain technology will assist in fraud reduction, enable one time KYC process, efficient & cost effective trading, and many more.

The technology may sound a promising one, but still many challenges need to be addressed to transform the finance and banking sector with Blockchain technology completely.

Finally, as conclusion, it is possible to affirm that digital transformation encompasses optimization of the current business by digital technologies utilization and disruptive

innovation of business by employing new business models, products, or services that are based on the digital technologies. Experiences show that in order to excel in a process of digital transformation, organizational changes and changes regarding HR department have an important role.

On the other hand, projects' scope, goals and success depend on the IT maturity of an organization, its business niche, environment and people readiness to adopt changes.

Thus, the digital transformation is a complex and multi-dimensional concept, involving almost every aspect inside an organization, independently whether a small, medium enterprise or a big corporation.

In addition to that, I think that digital transformation is today unavoidable for companies and organizations.

Failure to participate not only in digitalization but also in the customer-centered innovation, means failure with regards to a decision that has many and important direct effects on competition in markets and especially in the current fast evolving world.

“The biggest impediment to a company’s future success is its past success.”

Dan Schulman, CEO of PayPal

BIBLIOGRAPHY/SITOGRAPHY

CHAPTER 1 - STATE OF THE ART OF DIGITAL TRANSFORMATION IN THE FINANCIAL INDUSTRY

The state of digital lending, Results of an American Bankers Association research study

Digital Banking Maturity 2018: how to become a digital champion and why only a few succeed? Deloitte Digital report

Deloitte Luxembourg Digital Banking Benchmark: improving the digital performance, Deloitte Digital report

Digital Transformation in European Private Banking, Cognizant reports

Current challenges and solutions in banking & capital markets, EY report

Building the bank of 2030 and beyond: the themes that will shape it, EY report

Beyond Banking: New Business Models for the Digital Era, Criterium group report

Fintech reloaded – Traditional banks as digital ecosystems with proven walled garden strategies into the future, Deutsche Bank Research

Financial Services Technology 2020 and Beyond: Embracing disruption, PwC report

The Digital Transformation of the Banking Industry, BBVA research

CHAPTER 2 – REGULATIONS, DIRECTIVES AND LEGISLATIVE PROCEDURES IN THE FINANCIAL INDUSTRY

Payment Services Directive: frequently asked questions, European Commission, Brussels 12nd January 2018

Impatti tecnologici derivanti dall'introduzione della MiFID II, PwC report <www.pwc.com/it/it>, 8th June 2019

Basel III: A global regulatory framework for more resilient banks and banking systems, Basel Committee on Banking Supervision

Pillar 3 (Market Discipline), Basel Committee on Banking Supervision

The consequences of Basel IV – a quantitative impact study, VÖB German public banks

Proportionality in banking regulation: a cross-country comparison, Financial Stability Institute

Basel IV: finalizing post-crisis reforms, EY report

Financial Services Risk and Regulation: "Basel IV", Leverage ratio revisited, PwC report, <www.pwc.co.uk/fsrr>, 8th June 2019

Know Your Customer: Quick Reference Guide, PwC report <www.pwc.co.uk>, 8th June 2019

CHAPTER 3 – CASE STUDIES IN THE FINANCIAL INDUSTRY

Know Your Customer: Quick Reference Guide, PwC report <www.pwc.co.uk>, 8th June 2019

Lecturas seleccionadas: Curso Estrategias de Negociacion, Pontificia Universidad Catolica de Chile, Escuela de administraciòn (Authors Carlos Kubrick and Ennio Romanini, academic year 2017/2018)

Cyber strategy for insurers: managing physical and digital assets to protect brand and reputation, EY report

Closing the Gap: Cyber Security and the insurance sector, KPMG report, <www.kpmg.co.uk/closingthegap>, 8th June 2019

CHAPTER 4 - CONCLUSIONS

Digital Transformation Is Risky, But Not Transforming Is Even Riskier, <https://www.forbes.com/sites/joemckendrick/2019/05/27/digital-transformation-is-risky-but-not-transforming-is-even-riskier/#754e24ad3f3a>, 8th June 2019

Banche e digitalizzazione, a che punto siamo? I dati del report Capgemini, <https://www.zerounoweb.it/cio-innovation/banche-e-digitalizzazione-a-che-punto-siamo-i-dati-del-report-capgemini/>, 8th June 2019

The 5 Digital Transformation Identities of Financial Services Organizations, <https://www.gartner.com/smarterwithgartner/the-5-digital-transformation-identities-of-financial-services-organizations/>, 10th June 2019

Digital Transformation in Finance, <https://engineerbabu.com/blog/digital-transformation-in-finance/>, 10th June 2019