RISK MANAGEMENT MAGAZINE

Vol. 18, Issue 2
May – August 2023

EXCERPT

https://www.aifirm.it/rivista/progetto-editoriale/

The growing importance of digital risk & governance

Valerio Begozzi; Matteo Oldani; Francesca Terrizzano

The growing importance of digital risk&governance

Valerio Begozzi (Avantage Reply); Matteo Oldani (Avantage Reply); Francesca Terrizzano (Avantage Reply)

Abstract

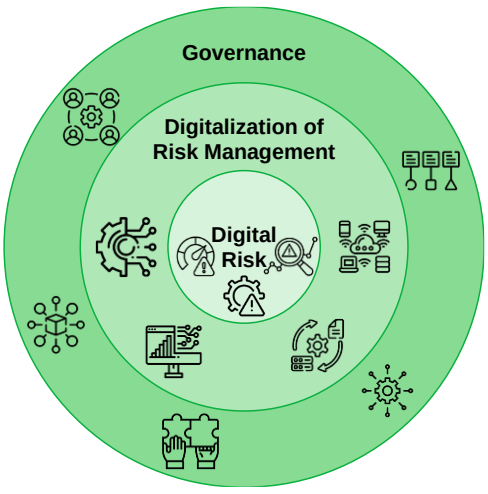
The aim of the paper is to explain what is meant by **Digital Risk&Governance**. For this purpose, it is important to retrace the **technological evolution** that has affected the last few decades: from branches to Mobile Banking, from the digitalization of transactions to the creation of Fintech, from the first process automations to Artificial Intelligence. This evolutionary journey has not only involved and still involves the birth of **new technologies**, but also the possibility of seizing **new business opportunities** and therefore necessarily of facing **new types of risk**, which are not always intuitive and easy to fully understand and manage. In this context, the role of the Regulator is fundamental not only to make available to companies elements for a correct and complete understanding of Digital/ICT Risk, but also to provide guidelines that allow for the construction of an organizational and governance model suitable for gaining awareness risk and to assess, manage and monitor it. A fundamental role is played by the **Digital Operational Resilience Act (DORA)**, which certainly better defines some aspects that until recently did not find a clear place, but - even more important - which allows these aspects to be included in an organic and holistic framework. **Governance and organization** are essential in this panorama, the only functions capable of spreading the risk culture necessary to overcome the silo mentality and to establish the cultural paradigm change essential for managing ICT Risk. Given the extension of the perimeter that is generally included under this risk, the paper goes on to underline the most relevant aspects and suggests in a practical way the components on which companies should concentrate in order to implement and make usable an all-round management framework: from the identification of critical functions to the importance of having tools capable of certifying the correctness, completeness and quality of the data. Another high-sounding and closely related theme, which therefore could not fail to be addressed in the paper, is represented by the **cyberattack** and its impacts on the market. The paper then closes with a theme which, in our opinion, plays an even more stately role than the creation of an overall framework can play: the **Digital Strategy**, consciously accessible only through a Digital Risk&Governance framework, but which represents the ultimate goal to which companies should aspire.

Keywords

Digital Risk&Governance, Risk Management, Risk Management Framework, Digital Risk, ICT Risk, Technological Evolution, Digitalization, Operational Resilience, Cyber Security, Cyberattack, DORA, Digital Operational Resilience Act, Business Continuity, Outsourcing, Data Management, Data Management Framework, Organization, Governance, Organizational Model, Governance Framework, Cultural Paradigm Change, Digital Strategy, Business Strategy

1. Context

In order to better frame the content in the paper, it is essential to define the so-called **"Digital Risk or ICT Risk"**. Generally speaking, it refers to all unexpected consequences that result from digital transformation and disrupt the achievement of business objectives. When an organization decides to scale its operations, its attack surface expands, increasing its exposure to cyber threats. This makes Digital Risk an unavoidable aspect of digital transformation and the advancement of new technology. In the light of this scenario, **Digital Risk protection strategies** have to be developed to mitigate Digital Risk and guarantee that organizations can continue confidently scaling their business. Managing Digital Risk means that the organization understands the implications of adopting certain technologies and acknowledges **Digital Risk as a crucial part of business risk management**. In order to achieve complete comprehension and awareness, the complexity of the Digital Risk landscape can be simplified by clustering risks (e.g., Cybersecurity, Data Leaks, Third-Party Risk). This helps organizations in identifying the most vulnerable areas and targeting risk protection efforts. But how is it possible to adequately manage the Digital Risk? The answer is to be found in **governance**. The Digital Risk context can be fully understood and managed only through setting a proper governance that foresees rules and procedures able to govern how an organization board of directors makes decisions, sets policies, and oversees management.
It is possible to imagine all the elements described above as parts of a puzzle: each component is different and autonomous, but essential to complete the overall picture. The following representation can help to explain this concept.



The first component, in the centre, is represented by **Digital Risk**, associated with the risks inherent in digital products, services and supporting processes. The component of **"digitalization"** indicates the process of moving to a digital business and, more in detail, the use of digital technologies to change a business model, provide new revenue and/or value-producing opportunities. Its application to the risks field allows to use the digital technologies to **modernize the discipline of risk management to create value-producing opportunities**. Finally, the component that embraces the other two concepts is **governance**, representing the indispensable framework, composed by guidelines and organizational rules, that enables an efficient and proper coordination of the other parts.
Viewed together, the three components represent **key aspects of integrated risk management**, that put together views of strategic, operational and technological risk associated with digital products and services.

2. Introduction

2.1 The technological evolution in the financial sector

Technological innovation is becoming a hallmark in the financial sector: it is becoming increasingly difficult to understand whether a new financial service or product stems from a business idea that technology supports or it is the natural outcome of the practical application of a new technology.

Technology has now become an intrinsic factor of some financial products/services as they would exist only through their specific technology.

But what have been the technology trends in the financial world in recent times?

Evolution of distribution channels: from branches to internet banking to mobile banking
Until the last century, for the customers the Bank is synonymous of **branch**, a physical place where human contact with the bank officer gives tangibility to the Bank-customer relationship. The branch in this period plays both a transactional role (provision of cash, payment and credit services) as well as a relational one. The number of branches of a Bank is used as a non-financial indicator of its size and thus its market share.

In the late 1990s and early 2000s, the spread of the first PCs and the Internet gave the spark to **Internet banking**, a tool in which customers independently can manage their financial position. While services were initially limited to the consultation of asset information, banks later made available banking services (digital payments) and then financial services (investment services).

A decade later, around 2010, a second technological wave began, putting two new tools in the hands of customers: the smartphone and the ability to access the mobile Internet. **Mobile banking** was born, accelerating the trend of digitalization of financial services.

Two phenomena demonstrate this trend[1]:

- **the contraction of the distribution network** with a cut of 34 percent (in Italy between 2012 and 2021 branches decreased from 32.881 to 21.650) and a substitution of the branch functions, which is increasingly focused on providing advisory services to customers instead of traditional banking services that are instead provided mainly through digital channels
- **the dematerialization of currency and digitization of transactions**: the number of POS in Italy from 2010 to 2021 increases from 1.497.000 to 3.910.000 (+ 260%) against a 16% reduction of ATMs (which decrease from 44.878 to 37.405 in the same period).

In 2020, these transformations accelerate rapidly due to the Coronavirus pandemic (Covid-19) when financial institutions need to strengthen their digital communication channels towards their customers when social distancing is the norm.

Among the technologies accompanying this evolution of connecting banks and their customers we find: home banking portals, mobile banking apps, trading platforms, customer service via chatbots, etc.

Evolution of banking and financial products
Technological innovation not only enables the evolution of distribution channels but also drives the evolution of the financial services offered to customers, with new players appearing alongside traditional institutions: **Fintech** companies are born.

Compared to traditional banks where the business model is based on the financial service, relegating technology only to a supporting role, in Fintech companies the paradigm is reversed and technology is the essence of the core business and the financial service its declination.

This has enabled prolific and pervasive product innovation with the creation of numerous new banking/financial services and products. Just to mention a few of the most important ones:

- payments: mobile payment services (Paypal, Apple Pay, Satispay, etc.), virtual credit cards
- credit: digital lending, P2P lending, crowdfunding
- finance: robo advisors, cryptocurrencies, copy trading.

Internal bank technology evolution
In the meanwhile, financial institutions, which in the 2010-2020 decade had to manage a complex situation for their profitability due to the central banks' expansionary policy by means of interbank rates at historic lows, are focusing their strategies on efficiency and optimisation of their operational machine to safeguard their profitability.

[1] ABI Report "Digitalizzazione e retail banking: ottimizzare i modelli di servizio per rafforzare la relazione banca-cliente", March 2023

These strategies, which leverage the use of technology to optimise operating costs, are based on two drivers:

- **Automation of internal processes**: re-engineering processes to make them more streamlined is no longer sufficient. It is necessary to automate all those low value-added operational activities that lengthen process completion times and expose the Bank to operational risks. **Robotic Process Automation** (RPA) and **Process Mining** technologies enable cost savings with improved productivity and flexibility.

- **Outsourcing of application services**: the widespread use of information technology to provide increasingly complex services is increasing the operating costs of ICT Departments. To optimise these costs, new software management models have become increasingly popular over the years: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). These management models make possible to outsource technological complexity from banks and to exploit the scale economies of specialised ICT companies thanks to the scalability of solutions and Pay-per-Use formulas. Among the technological enablers of these management models, we find **cloud computing** technologies in which some IT components (hardware and/or software and/or data) are not located in the bank infrastructure (on premise) but on the ICT provider infrastructure and made available through the Internet.

Reducing operating costs does not represent the only strategy to safeguard profitability. Another technological development has made possible to extract value from what is already available in banks but not adequately exploited: **data**.

In the context we are describing every day financial institutions produce huge amounts of data that can generate value thanks to adequate and sufficiently powerful analysis tools such as **Big Data** and **Machine Learning** technologies.

These technologies enable a better knowledge of customers with two main purposes:

- **marketing**: personalisation of services due to more precise and targeted analyses that allow better customer profiling and enable cross-selling and up-selling of services/products;
- **risk management**: detection of fraud and suspicious transactions, improvement in identifying the correct credit profile of customers.

The new technological frontiers
But what are the next technologies that will change the financial world in the near future?

The technological world is moving faster and faster and new technologies are entering or will soon enter the financial sphere, some even with disruptive impacts.

- **Blockchain or Distributed Ledger Technology (DLT)**: a technology that improves the sharing of information between counterparties while ensuring its inalterability. The financial sector will be impacted in payment services (e.g., in the simplification of payment reconciliation and fraud reduction), in the management of digital currencies (e.g., cryptocurrencies) and in the management of contracts (e.g., smart contracts)

- **Artificial Intelligence (AI)**: a multipurpose technology with a large area of application in financial institutions including improvements in machine learning algorithms, customer behavioural analysis, data mining for a strategic perspective, predictive risk analysis, etc.

- **Quantum computing**: a technology that changes the computational paradigm to perform more complex calculations that are unmanageable with current technologies, regardless of their processing power. The impacts on the financial world will be pervasive and range from solving portfolio optimisation problems to calculating financial risks, from detecting and preventing fraud in digital payments to managing cryptographic security systems.

To close this brief historical excursus on the technological evolution in the financial sector, we quote the prophetic words of Vincenzo Desario, former general director of the Bank of Italy, in a speech he made in 2000, right at the dawn of the story told in this chapter:
"*The banking and financial sector is most involved in the development of the new economy; the immateriality of financial products combines perfectly with new technologies, powerful tools for the collection, processing and distribution of information. Intermediaries play a plurality of roles with the new technology; some more traditional, such as the sale of financial products and the offer of payment services on telematic networks; others innovative, such as the creation of infrastructures for e-commerce, the management of technological services on behalf of third parties, and the provision of advisory services, including non-financial ones, to firms. The scenario outlined for the future of banks is articulated, full of opportunities but also of risks; financial operators need to reflect in depth on the implications for business strategies arising from the ongoing technological evolution.*"

2.2 New technologies, new opportunities, new risks

As we have seen, the increasingly pervasive use of technology leads financial intermediaries to build partnerships with specialised technology companies: the interconnection among the various players is increasingly stronger as their mutual dependency.

The direct consequence of this approach is a greater **systemic risk**, in particular for business continuity: the interruption in the provision of a service by one player could have amplified impacts on the entire financial sector, especially if other market players depend on that service for their business.

This is true when there is a **concentration** of certain services in a **few large ICT companies** that become the unique provider of a given service for the entire sector.

Another source of systemic risk is the **lengthening of the supply chain** of financial services: in fact, technology providers often depend on other ICT companies and, as in all chains, the weakest link determines the robustness of the entire chain. If we add also that IT companies are not always subject to financial regulation, the mix of these factors could be explosive.

While outsourcing of ICT services produces a reduction in the costs of the operational machine, it also entails a **reduction in direct control** by the bank and poses new challenges in the governance of providers.

For this reason, as we will see in the next chapter, regulators have been extending the boundaries of their regulations in recent years to include non-financial companies within a framework aimed at ensuring operational resilience and responsible management of outsourced services.

Besides the outsourcing of activities in terms of process in the supply chain, the health pandemic has also seen a geographical dislocation of work organisation: **remote working**. Above all, the financial industry has been persistently impacted by the new remote/hybrid work made possible by the availability of effective communication and co-working technologies. During the health pandemic, when remote working was an imperative, financial institutions realised that this new organisation of work had minimal impact on productivity and also reduced the costs of office management (real estate). With the pandemic over, hybrid work has become the new normal in the financial sector. However, this new organisation of work brings new risks, especially of an IT nature, since the **attack surface has increased** geographically and at the level of application architecture, which now is **outside the conventional defensive perimeter** of institutions (firewalls, attack detection systems, security of communication channels, hardware vulnerabilities, data breaches, etc.).

But the new work model is not the only source of new risks for the financial sector.

The **standardisation** of technologies for financial services, while on one hand reducing the likelihood of a successful cyberattack (as a standardised technology is more robust because it has had time to correct its weaknesses), on the other hand increases the impact if the attack is successful (as a standardised technology is widely used). In a way, cyber risk could be seen as a **tail risk**, with low frequency of occurrence but high impact.

Furthermore, the use of communication standards (e.g., API interfaces) has allowed the **disaggregation of application components**: but the more disaggregated a system is, the more vulnerable it is to cyberattacks, since the weakness of a single element can be used to enter the system and quickly propagate the attack within it. This is why it is important to use a "security by design" approach when building the ICT architecture.

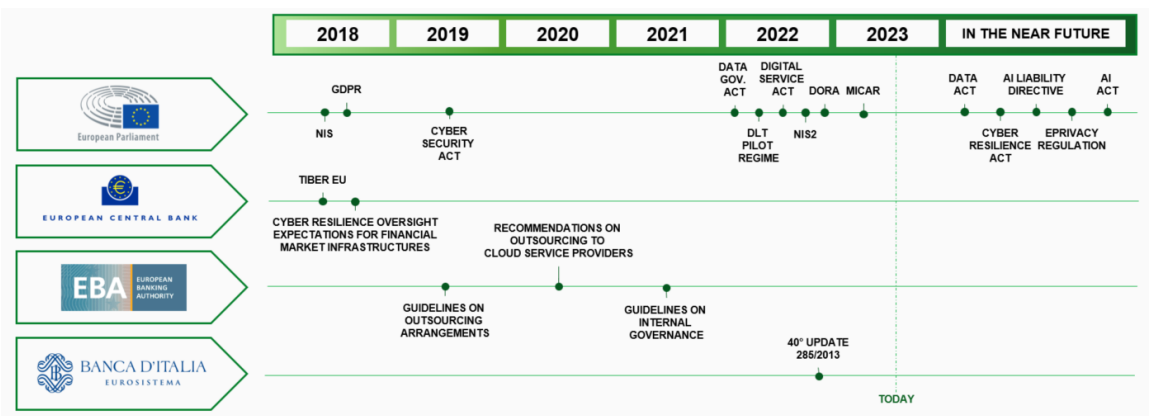
Another source of risk is represented by **pioneering technologies** whose operating mechanics and business implications are not yet well known. Take, for example, Artificial Intelligence, which is increasingly entering the financial world. In some cases, AI is based on recursive logic that reinforces certain tendencies (self-full-filling prophecy) and can lead to a feeling of overconfidence. Using, for instance, AI in the field of KYC to determine a customer credit rating could lead to reputational risks if discriminatory logics arise. Of course, there are also risks more related to the sphere of cyber-security that will be explored in more detail in the following chapters.

2.3 How the Regulator faces the technology evolution

As described above, technological evolution has brought transversal changes to the entire financial sector and new risks to be managed. But how does the legislator address these changes?

In recent years, **traditional Regulators** (e.g., ECB, EBA, Bank of Italy, etc.) have focused on technology governance in banking: regulations have been published on the framework for cybersecurity testing (ECB, 2018), on cyber resilience (ECB, 2018), on ICT outsourcing management (EBA, 2019), on cloud services management (EBA, 2020), on internal governance (EBA 2021) and on ICT management (BoI, 2022).

Furthermore, following the Covid pandemic in 2020, a new political regulator has joined the traditional ones: the **European Parliament** in order to support the EU economic recovery has outlined a strategy for digital finance in which it defines a new approach to encourage responsible innovation in the financial sector. This is the context for the series of regulations from 2022 that will introduce rules on data governance, DLT management, cryptocurrencies and other regulations, now under consultation, that will be issued in the near future.



Among the most recently issued/proposal of regulations we find:

- the **Digital Operational Resilience ACT (DORA)**[2] :
  - strengths the IT security of financial entities such as banks, insurance companies and investment firms by uniform requirements for the security of their network and their information systems
  - creates a regulatory framework on digital operational resilience, whereby all firms need to make sure they can withstand, respond to and recover from all types of ICT-related disruptions and threats
  - consolidates and upgrades the ICT risk requirements addressed so far separately in the different Regulations and Directives

- the **Data Act**[3]**:**
  - makes more data available for use and sets up rules on who can use and access what data for which purposes across all economic sectors
  - gives individuals and businesses more control over their data through a reinforced data portability right, easily copying or transferring data across different services
  - improves the conditions under which businesses and consumers can use cloud and edge services
  - introduces mandatory safeguards to protect data held on cloud infrastructures in the EU. This will avoid unlawful access by non-EU/EEA governments

- the **Artificial Intelligence Act**[4]:
  - addresses risks specifically generated by AI applications
  - proposes a list of high-risk applications and set clear requirements for them
  - defines specific obligations for AI users and providers of high-risk applications
  - proposes a conformity assessment before the AI system is put into service or placed on the market and an enforcement after such an AI system is placed in the market
  - proposes a governance structure at European and national level.

3. ICT organizational governance framework

At the beginning of the paper, governance was mentioned as a key element in managing the Digital Risk and leading an organization through an efficient and aware digitalization process. So, how is it possible to ensure that an organization best manages its Digital Risk? In our opinion, the main steps are the following.

1. Identify key assets

First need is represented by the identification of critical assets within the organization and all the ways they may be exposed or vulnerable to threats. Critical assets can be tangible, such as IT systems, or intangible, such as stakeholders and those people who influence organization goals.

2. Understand the potential threats

Second step consists in understanding the threats that the organization is facing, also considering the fact that threats prioritize their attacks based on the shortest path or least effort needed.

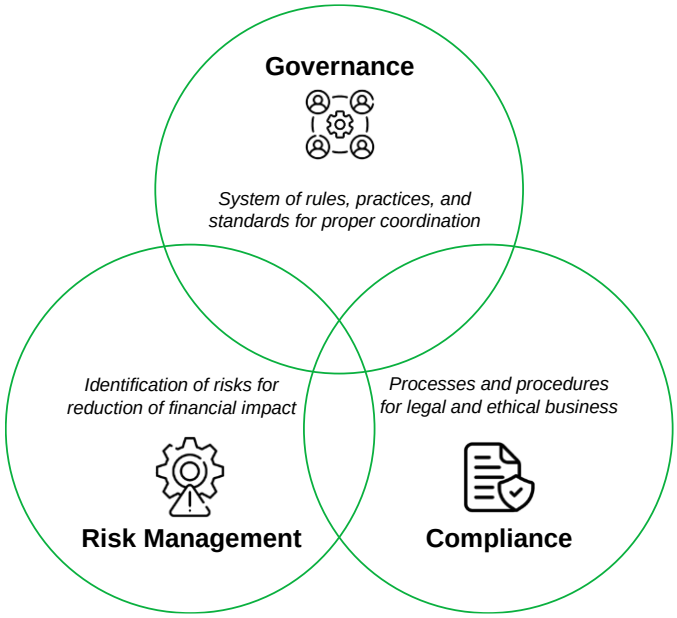
3. Monitor for intolerable exposure

After understanding the overall situation, it is essential to consider sources for any intolerable digital exposures (e.g., social media and dark web pages) in order to detect exposed assets.

4. Mitigate the risk

The monitoring process enables the possibility to define a mitigation strategy, that can set short, medium or long-term objectives according to the priority and the stability of the intervention over time. One of the broadest and most effective mitigation actions is certainly represented by the governance, risk and compliance strategy, that can be considered as a cross organizational approach. The three components allow to set an overall system of rules, practices, and standards that guide a business (Governance), to identify potential risks and act to reduce/eliminate their financial impact (Risk Management) and to have processes and procedures that make it possible to conduct business in a legal and ethical manner (Compliance). The strength of this corporate management system is that it is able to overcome the reluctance of sharing information and resources among different departments, avoiding the efficiency reduction and encouraging the development of a positive company culture. The overall purpose of governance, risk and compliance strategy is to reduce risks and costs as well as duplication of effort. It requires company-wide cooperation to achieve results that meet internal guidelines and processes established for each of the three key functions.

[2] https://www.digital-operational-resilience-act.com/
[3] https://www.eu-data-act.com/
[4] https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai



Within this context, also DORA acknowledges the **centricity of organizational model** in order to guarantee a resilient view, even if it highlights the importance of requiring the introduction of more complex governance mechanisms only to financial entities that are not micro-enterprises (proportionality principle). More in detail[5]:

- Organizations shall establish an **internal management and control framework** which ensures effective and prudent management of all IT risks in order to achieve a high level of digital operational resilience; this means that the search for synergies and the necessary coordination and integration mechanisms between all the players involved takes on particular importance. Moreover, an **adequate chain of command and control** must be ensured, such as a decision-making architecture capable of governing the entire value chain.
- The management body of the financial entity shall define and approve the implementation of all provisions relating to the Digital Risk management framework, supervise and be responsible for such implementation. This means that the management body is called to:
  - **assume ultimate responsibility** for the IT risk management of the financial entity
  - **prepare policies** aimed at guaranteeing the maintenance of high standards of availability, authenticity, integrity and confidentiality of data
  - **clearly define roles and responsibilities** for all ICT-related functions and establish appropriate governance arrangements to ensure effective and timely communication, cooperation and coordination between these functions
  - **have overall responsibility** for defining and approving the digital operational resilience strategy, including determining the appropriate level of tolerance for IT risks of the financial entity
  - **approve, supervise and periodically review** the implementation of the **ICT business continuity policy** and the ICT-related response and recovery plans of the financial entity
  - **approve and periodically review the internal ICT audit plans** of the financial entity, the ICT audits and the most important changes made to them
  - **allocate and periodically review adequate financial resources** to meet the financial entity digital operational resilience needs across all types of resources, including relevant ICT security awareness programs and digital operational resilience training activities
  - **approve and periodically review the financial entity policy** on how to use the ICT services provided by the third-party ICT service supplier
  - **establish company-wide communication channels** that allow it to be duly informed about agreements concluded with third-party ICT service providers on the use of such services, any significant and relevant planned changes relating to third party ICT service providers and the potential impact of these changes on the critical or important functions subject to the agreements in question, including a summary of the risk analysis to assess the impact of these changes, as well as at least the major ICT incidents and their impact, measures of response and recovery and corrective measures.
- Organizations establish **a role in order to monitor the agreements concluded with service providers** for the use of such services, or designate a senior manager to be responsible for overseeing the related risk exposure and relevant documentation
- Members of the financial entity management body **actively maintain adequate knowledge and skills to understand and assess cyber risks** and their impact on the operations of the financial entity, including by undergoing specific training on a regular basis, commensurate with the manged IT risks.

As we will also read in the next chapter, **an ICT organizational governance framework at 360 degrees allows to change the cultural paradigm and to respond to the "silo mentality"**. It can be defined as the reluctance to share information with employees

[5] https://www.digital-operational-resilience-act.com/

of different divisions in the same company. This attitude is seen as reducing the organization efficiency and, at worst, contributing to a damaged corporate culture. In order to be able to understand the current situation of companies facing Digital Risk, it is essential to analyse the complexity of digital landscape, the nature of the information and its location. To do this it is fundamental to prefer social exchanges rather than the individual ones: this means, for example, a decision-making centre acting with others or a mesh network where each, in turn, uses information shared by others. In general, companies are called to make people understand that **having no risk culture creates culture risk** and does not allow them to have sufficient skills to deal adequately and effectively with the context that technological evolution, understood in the broadest sense, is creating.

4. ICT Risk Management framework

4.1 Cultural paradigm change

Risk management structures in financial institutions, due to their mandate of second-level control office, built over time a dialogue with business offices aimed at defining and implementing risk management measures.
Until now, the main sources of risks in a Bank have been identified in the functions, processes and products of the core business, hence the focus on credit risk, market risk, liquidity risk, etc.
From this view comes the fact that ICT risk has not its own dignity but it has always been included, at the regulatory level, in the broader spectrum of operational risks.
Even at the organizational level, ICT security management has never been included among the objectives of risk management but has always been associated with a "security" structure often located in the Bank ICT area, with which risk management structures have only in rare cases built a stable and structured channel of communication.
The increasingly strategic role of ICT technologies within each financial institution and the resulting impact on the business requires an evolution in the vision of ICT risk and its management: in this context, it becomes essential to **change the cultural paradigm** that Risk Management and Security structures have had toward ICT risks.
The former will have to broaden their scope on issues hitherto left at the borders of their activity scope; the latter must adopt a risk-based approach in ICT risk management.
From this point of view, the **synergy between risk management and information security structures** is high: one could contribute with its risk approach, the other with its technical expertise.

4.2 What to do to create an ICT Risk Management Framework

On the basis of the change in the cultural paradigm, in the terms just described, it is essential to have guidelines for the creation of a framework that can manage ICT Risk at 360 degrees. Here below the main steps.

STEP 1: Perimeter
The first step is to define the perimeter of the critical or important functions and the relative processes.

A function is critical or important when its disruption "*would materially impair the financial performance of a financial entity, or the soundness or continuity of its services and activities, or the discontinued, defective or failed performance of that function would materially impair the continuing compliance of a financial entity with the conditions and obligations of its authorisation, or with its other obligations under applicable financial services law.*"[6]

In order to define the perimeter, it is essential to have a mapping of all ICT functions, their linkage to the company process taxonomy, and all the interrelationships among the various ICT components since the interruption of one service can lead to the failure or interruption of other services.

In doing this, both risk and technical competencies are required

STEP 2: Data
The perimeter of critical functions is also reflected in the data used in the processes: risk analysis should be also conducted by assessing data confidentiality, integrity and availability. Implementations to ensure operational resilience should in fact be proportionate to the degree to which the three aforementioned drivers have been assessed: for example, highly confidential data or 24/7 available data requires greater security and resilience measures than public data or non-urgent data.

STEP 3: Tolerance thresholds
ICT risk should also be considered in the Risk Appetite Framework, in order to define specific threshold for risk appetite, risk tolerance and risk capacity. A clarification is needed: since ICT risk involves only costs and no revenue, theoretically its risk appetite should be zero. However, as we saw in the introduction, new technologies have embedded some risks due to their innovative nature so the Bank willingness to have a cutting-edge technology leads to define a risk appetite, even if unintentionally.

STEP 4: Security testing
From a preventive point of view, it is fundamental to carry out testing campaigns on ICT infrastructures to assess their resilience from cyberattacks.

Although this is not the place to deep dive into the testing typologies and how they should be performed, we would like to recall what was said in the opening of this chapter: testing activities should not only involve the Bank ICT security functions but should also actively involve the risk management as they provide realistic evidence of the Bank exposure to ICT Risk and its operational resilience.

[6] Digital Operational Resilience Act, European Parliament, 2022

STEP 5: Mitigation plan
With the outcomes from the testing activities and additional evidences gathered over time, banks must activate a remediation plan to address the identified weaknesses: priority should be given to those activities that most mitigate the impacts of a possible cyberattack.

As ICT Risk is a part of Operational Risk, this plan should be integrated in the operational mitigation plan, giving value to possible synergies

STEP 6: Monitoring
Some institutions already have dashboards for technical monitoring of application security: the most effective way to improve their operational resilience is to evolve these dashboards by integrating new risk-based metrics.

Evolving current dashboards instead of creating new ones not only has time and cost advantages, but also ensures a holistic view in monitoring: keeping technical security dashboards separate from risk dashboards would in fact lead to inconsistent and unambiguous monitoring.

5. Data Management Framework

The availability of high-quality data is very important both to define new digital strategy and to predispose effective Risk Management analysis with meaningful Key Risk Indicator (KRI). In fact, every financial service or industrial activity generates a big amount of data; however, a study[7] estimates that less than 40% in the best case or even less than 30% of these data are used by companies to create business insights or key indicators. In order to guarantee the data availability, it is important to ensure also the security of data. In detail, the critical components are the following:

- **Confidentiality of data**: Data need to be maintained confidential and protected from unauthorized access; they also need to be encrypted if they are personal, also in consideration of GDPR regulation.
- **Integrity**: data need to be integer as they are acquired and captured in the system the first time; this is also connected to the point of ensuring high quality data.
- **Availability**: data need to be accessible only to the authorized persons, but data need to be accessible on-time.

However, this is only the starting point to have high-quality data available, since it is fundamental also that data are of high-quality to use it for Business analysis. So, to define an effective Data Management framework, an important part is represented by the data quality controls that need to be performed to ensure it.

In more detail, the **high-quality data assurance** could be achieved by implementing the following controls:

- **Zero values check:** it checks for the anomalous presence of zero values, in cases where the zero value does not belong to the domain.
- **Univocity checks:** it checks the uniqueness of some variables, both singularly and in tuple; it is essential to avoid data duplicates and any potential relation between them.
- **Anomalies:** verification of possible anomalies on data with respect to the context in which they appear (e.g., data equal to the one of the previous periods in the case it was expected to change or the opposite).
- **Discontinuity in historical series:** it checks on the trend of the data historical series to identify discrepancies or jumps in the numbers.
- **Accuracy:** it aims at calculating percentage of values to check if this percentage is outside the variable domain (out of range).
- **Missing data:** it checks on the completeness and availability of the input data.

Finally, it is important to protect all these data from the possibility to lose them, that could come both from internal issues (e.g., physical damage of the hardware in case are not on the cloud) and from external sources (e.g., cyberattacks). Some examples of the important components to protect the security of data are the following:

- **Access limited through authentication rules:** segregation of the access to the data on the basis of functions, responsibilities, etc.;
- **Change traceability:** traceability through logs of all the changes made to the data (e.g., who has done it, when, how was the previous datum);
- **Secured back-up of the data**: back-up of all the relevant information and storage in a secured location.

6. Impact of the cyberattacks

The increased amount of available data has increased the attention to the possibility of the cyberattacks and their impacts.

A study of Morningstar Sustainalytics[8] shows that there has been an increase in the frequency and in the impact of the cyberattacks.

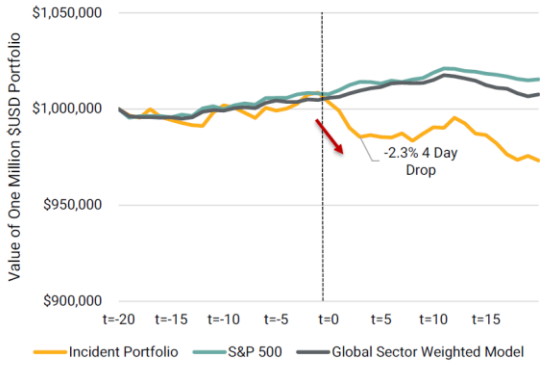
In detail, this study shows that cyberattacks have impact, among others, on the following aspects:

- Share price on the market
- ESG Ratings.

[7] https://www.forrester.com/blogs/hadoop-is-datas-darling-for-a-reason/
[8] Morningstar Sustainalytics: "The impact of Cyberattacks on stock prices", October 2022

The study shows that there is a drop of around 2.3% on average compared to the index (S&P500 in this study) performance in the first 4 days after the news of successful cyberattacks with a consequent increase in the volatility of stock prices.

Exhibit 3: Time Series (Short-Term) - Share Price Reaction to Cyberattacks



*Companies are selected based on clear evidence describing a cyberattack
**Duplicate companies were permitted, given that each cyberattack is unique for that company
Source: Morningstar Sustainalytics

The same study shows also that the portfolio of companies that has had a cyber-attack shows an annualised return of around 12% less that the reference index.

	Annualized Returns	
	1 Year Before Incident	1 Year After Incident
Incident Portfolio (a)	7.82	-0.65
S&P 500 (b)	14.44	11.58
Sector Benchmark Portfolio (c)	11.73	10.15
Difference to S&P 500 = (a) - (b)	**-6.62**	**-12.23**
Difference to Sector = (a) - (c)	**-3.90**	**-10.80**

*Currency in use: Base Currency[7]

Source: Morningstar Sustainalytics

The high level of impact on stock prices shows the importance of having a Digital/ICT Risk&Governance framework in place in order to prevent cyberattacks and limits its impact in the case it happens. In addition, the same study indicates also that companies that have implemented more rigorous Data Protection and Security Programmes are more prepared to deal with cyberattacks. This will lead to a double positive effect: one on the stock price and the other one on ESG Ratings. In fact, one methodology adopted to define the ESG rating is a score model based on each of the three dimensions: Environmental, Social and Governance. As discussed in the previous chapter, the cyber incidents have a high probability of negative impact on stakeholders and especially on shareholders; this is also one of the factors considered to define the Governance score inside the ESG Ratings. In particular, this will impact the second-dimension of ESG rating methodology adopted by Morningstar Sustainalytics: the management assessing of the exposure to ESG risks.

7. The importance of digital strategy alignment with the business strategy

As discussed above, the **technology infrastructure** has become **strategic** for the financial services institutions, since it allows to transform a big amount of raw data into analytics and visualization in order to have business insights.

Business insight could be obtained both with **traditional IT models** with a formula developed and considered inside the code or through the **new IT models** such as Generative Artificial Intelligence (Natural Language Processing, Machine Learning, etc.). An example of the potentiality of the Generative Artificial Intelligence (in the following also "AI") has been shown by the recent diffusion of ChatGPT, an AI that is able to answer to questions with indistinguishable human-like outputs.

However, since all these models need a strong technological infrastructure to work it is important that financial services institutions **consider their Digital Strategy together their Business Strategy**. The first point to highlight is the fact that Digital Strategy is not the IT Strategy, but a more widespread concept; in fact, the digital strategy considers **how to leverage on technology evolution to meet the business goals**. In fact, digital technologies have changed the way we communicate and now customers expect a more personalized experience and instant gratification.

Furthermore, a Digital Strategy aligned with business strategy and connected with an effective execution plan will most likely help to improve internal collaboration through different teams and it would **break the silos to have a more holistic view of the company**.

On the other side the increase in digitalization will bring also an increase in the Digital Risk of cyberattack, so it is important to align also a **Risk Management Strategy together with the Business Strategy and the Digital Strategy**. In detail, it is important to define a **resilient ICT Risk Management framework** (see paragraph 4).

8. Conclusion

In this paper we have seen how technology evolution is pervasive in the financial sector and has become a strategic resource due to the deep changes in the core business and in the organization of all financial institutions.

Technology brings new risks that must be addressed with a risk-based approach from both regulatory, organizational, and cybersecurity perspectives. This new approach is made possible only in light of a shift in the cultural paradigm that requires new forms of collaboration, especially between Risk Management and ICT Security units.

New frameworks are required from the point of view of organization, governance, risk management and data management because there is only one certainty: **the question is not "if it will happen" but "when it will happen"**, so you need to be ready for the next cyberattack and the sooner the financial institutions adopt the appropriate frameworks, the lower the impacts will be.

This readiness could be reached through **integrating Risk Management Strategy** with **Digital Strategy** and **Business Strategy**, since one of the points is the mitigation of cyber risk through having a wide data management framework that includes not only the high-quality data checks, but also the guarantee of confidentiality, integrity and security of the data.

In fact, it is becoming every day more important to **break down the silos** and to consider the activities inside a **comprehensive view** of the **company**.

References

- Associazione Bancaria Italiana, "*Digitalizzazione e retail banking: ottimizzare i modelli di servizio per rafforzare la relazione banca-cliente*", March 2023
- Bank of Italy, "*The digital transformation in the Italian banking sector*", April 2022
- European Systemic Risk Board, "*Will video kill the radio star? – Digitalisation and the future of banking*", January 2022
- European Parliament, "*Regulation (EU) 2022/2554 of the European Parliament and of the council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011" - Digital Operational Resilience Act (DORA)*, November 2022
- European Parliament, "*Proposal for a regulation of the European Parliament and of the council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*", April 2021
- European Parliament, "*Proposal for a regulation of the European Parliament and of the council on harmonised rules on fair access to and use of data (Data Act)*", February 2022
- European Banking Authority, "*Guidelines on Internal Governance*", March 2018
- Vincenzo Desario, "*La Banca d'Italia e lo sviluppo dell'e-banking*", September 2000
- EBA, "*Guidelines on ICT and security risk management*", November 2019
- Morningstar Sustainalytics: *"The impact of Cyberattacks on stock prices"*, October 2022