Managing cyber risk in the financial sector: Insights from a case study

Chiara Crovini*, Pier Luigi Marchini**

Abstract

Purpose: This article focuses on cyber risk as an emerging issue within the risk management process and the internal control system in the financial sector. It investigates whether cyber risk management (CRM) is (dis)integrated into traditional enterprise risk management (ERM) and analyzes the external dynamics affecting the CRM design.

Design/methodology/approach: This article draws upon institutional theory and the concept of boundary objects. The research examines a listed Italian bank and gathers the data from semi-structured interviews, direct observations, meetings, and archival sources.

Findings: The findings underline that cyber risk rationale plays a crucial role in the CRM process. The interplay between institutional complexity and the need to manage cyber risk is critical for a bank to have a stable and flexible infrastructure. The knowledge boundaries related to the cyber risk culture require further cyber risk talk.

Originality/value: This research furthers the understanding of cyber risk and CRM as an integral part of the ERM and internal control systems in the financial sector, in which there is a shortage of case studies. The financial sector is highly regulated, and managing cyber risk has become crucial as banks usually deal with enormous amounts of personal and sensitive data stored on networks and in the cloud.

Practical implications: This case study emphasizes the crucial role of CRM in the identification and reporting of cyber risk information in annual reports.

Keywords: cyber risk management, internal control system, multi-perspective approach, case study, financial sector, risk information.

JEL: G21, G28, M41, M48

* Aalborg University Business School, Denmark. Corresponding author, e-mail: chiarac@business.aau.dk.

** University of Parma.

Doi: 10.3280/FR2023-001004

First submission: 26 October 2022. Received after revisions: 6 December 2022. Accepted: 20 December 2022.

1. Introduction

Cyber risk is a critical issue that businesses face today (Ashby et al., 2018; Crovini et al., 2018). As a result, the importance of preventative risk management and post-event remediation is growing as stakeholders are increasingly focusing on how companies deal with cyber risks (Eling et al., 2021). With this profound change, brought about by globalization and IT development, it is vital to understand how to manage cyber threats as a hybrid dimension between risk and uncertainty (Brender and Markov, 2013; Crovini, 2019).

Several studies have examined the technical aspects of cyber threats related to computer engineering without considering the fundamental nature of this kind of risk and its impact on the organization and internal control system from a management control perspective (Bojanc and Jerman-Blažič, 2008; Mukhopadhyay et al., 2013; Ruan, 2017). Researchers need to investigate how cybersecurity activities interact with the other internal control activities associated with ERM (Ashby et al., 2018; Gordon et al., 2008).

In light of the multifaceted nature of cyber risk (Aldasoro et al., 2020a; Crovini et al., 2018), this paper aims to fill the gaps in the understanding of cyber risk and cyber risk management (CRM) as an integral part of the ERM and internal control systems in the financial sector (Ashby et al., 2018; Eling et al., 2021; Gordon et al., 2008), in which there is a shortage of case studies (Caldarelli et al., 2016; Giovannoni et al., 2016; Lim et al., 2017). The financial sector is highly regulated, and managing emerging risks, especially cyber risk, has become crucial over the past few years (Ashby et al., 2018). Banks usually deal with enormous amounts of personal and sensitive data stored on networks and in the cloud (Eaton et al., 2019). Furthermore, there is a need to consider the external pressures and stakeholders affecting the formation and design of CRM as a systemic and multi-perspective approach (Boyson, 2014).

Accordingly, this study intends to answer the following research questions:

Research question 1 (RQ1): What are the risk "objects" (e.g., process, tools, conceptualization, organizational arrangements, etc.) and related boundaries that constitute the CRM process?

Research question 2 (RQ2): Is CRM integrated into the existing ERM, pursuing the idea of risk management of everything, or is that an ad hoc method representing a (dis)integrated process?

Research question 3 (RQ3): What are the key external dynamics (or patterns of actions) affecting the formation and design of the CRM process?

To answer these RQs, the analysis focuses on the case of a bank listed on the Italian Stock Exchange (subsequently called "Bank XYZ" for confidentiality reasons). We selected Bank XYZ because of its important role in Italy, where there is great sensitivity to issues related to cyber security.[1] Significant investments have been made to protect companies and those sectors (e.g., financial) that involve critical infrastructures (Italian Ministry of Defence, 2019).

The research draws upon neo-institutional theory (DiMaggio and Powell, 1983; Scott, 2013) and the relationship between the concept of boundary objects and infrastructure (Arena et al., 2017; Power, 2015; Star, 2010). According to coercive isomorphism and neo-institutional theory, regulations have an essential role in shaping the internal organizational structure of Bank XYZ. However, regulatory pressures need to consider the institutional complexity of financial institutions and the dynamics of (dis)integrated risk. This study also extends the conceptual lens of boundary objects in the specific field of CRM. By analyzing the cyber risk objects and related interactions, this research focuses on determining how corporate actors and their interactions shape the understanding and the CRM process as an ad hoc process that might be (dis)integrated within the existing ERM of financial institutions. Despite the relevance of having an ad hoc CRM process, it is still difficult to distinguish CRM activities clearly from other existing practices. Forming a stable but flexible infrastructure requires financial institutions to deal with knowledge boundaries that limit the cyber risk measurement, assessment, and management. Hence, CRM involves reaching beyond the limits and length of traditional ERM (Eling et al., 2021).

The insights of this study contribute to the existing knowledge on how cyber risk is considered and managed as it investigates the cyber risk practices implemented by a financial institution. Furthermore, the need to develop a multi-perspective approach effectively considering and integrating the interactions with the external environment is closely related to the introduction of cyber resilience and complementary activities to achieve specific

[1] See the new Agency for Cybersecurity in Italy, established with Law-Decree 82/2021 to coordinate all the public and private organizations dealing with the protection of personal data and the promotion of cyber resilience in the country.

objectives even in adverse and unexpected events. Furthermore, CRM requires the commitment of policy makers, public institutions, and the government to develop an appropriate culture leading to a common strategy against cyber threats. This organizational approach will also affect the management decision to disclose financial and non-financial information about cyber risk and the external risk reporting process, which will influence the investors' reactions (De Luca and Phan, 2019; Giner et al., 2020; Crovini et al., 2022a). Therefore, this study sheds light on the practical implications of having a strong link between the internal control system of a bank and its mandatory risk disclosure (Allini and Manes-Rossi, 2014; Aureli and Salvatori, 2013).

The remainder of the paper is organized as follows. Section 2 presents the literature review about the issues and challenges of cyber risk and cyber risk management, focusing on financial institutions. Section 3 introduces the theoretical framework that guides and informs the research design, which is described in Section 4. The case study description and related findings are presented in Section 5, and Section 6 contains the discussion. Finally, conclusions and possible future developments are presented in the last section.

2. Literature review

The debate around the concepts of risk and uncertainty has become particularly important (Crovini, 2019), especially in the IT and innovation fields, in which experience and knowledge of the future and risk quantification are limited (Ashby et al., 2018). Cyber risk is the risk of incurring financial, reputational, and market share losses concerning information and communication technology (ICT; Aldasoro et al., 2020b; Mukhopadhyay et al., 2013; Öğüt et al., 2011). Therefore, it is considered as part of the operational risk, with impacts on the reputational and strategic risks, and it has three fundamental characteristics: vulnerability, threat, and damage (Aldasoro et al., 2020a; Crovini et al., 2018).

The term "cyber risk" also refers to several different sources of risk related to information and technology assets, originating from both the external environment and internal company (mis)conduct (Aldasoro et al., 2020b). For example, the National Association of Insurance Commissioners (2018) included identity theft, disclosure of sensitive information, data breach, and business interruption in cyber risk.

Accordingly, this study considers cyber risk as a hybrid dimension between risk and uncertainty (Crovini, 2019) because companies cannot know what will happen in the future with the probability of occurrence and distri-

bution of the impacts of the manifestation of cyber fraud. Moreover, internal and external cyber fraud cannot always be predicted (Ammirato et al., 2019; Bodin et al., 2018) because of the speed of change in the surrounding environment, globalization, and IT connections. Thus, companies have to deal with a sort of cyber uncertainty, which is difficult to prevent and has several consequences in terms of economic and financial losses and reputational impact (Crovini et al., 2018). In particular, cyber risk disasters have a direct impact on companies' bottom line in terms of loss of opportunity cost; organization brand equity and market capitalization are also adversely affected (Öğüt and Menon, 2005).

Cyber risk has to be quantified and managed throughout the organization by enhancing data and information sharing and knowledge sharing (Eling et al., 2021). However, low-quality data points and data sharing (Ammirato et al., 2019) make a comprehensive risk assessment and evaluation almost impossible (Aldasoro et al., 2020b; Ruan, 2017), although many cyber risk management frameworks exist (Institute of Risk Management [IRM] 2014; ISACA 2012; ISO/IEC 2018).

Some frameworks (National Institute of Standards and Technology [NIST] 2018) specifically provide risk assessment methodologies (Alali et al., 2018), quantitative risk models (Alali and Almogren, 2017), industry surveys, security analytics tools in the market, and even regulations regarding IT risk, particularly for the financial sector. However, the absence of a standard reference makes it challenging to compare different approaches to reduce exposure, evaluate countermeasures' cost-effectiveness, optimize the return on cyber risk spending, and structure the risk databank consistently. Moreover, the majority of people involved in managing risks do not have the proper skills to deal with cyber risk (Ashby et al., 2018; Eling et al., 2021; PricewaterhouseCoopers [PwC], 2018) since it usually stems from information technology (IT) problems. Hence, cyber risk awareness and analytics are crucial to help firms identify weaknesses and threat scenarios, identify consequential countermeasures, and put appropriate measures in place, even though the insurance capacity remains limited (Bodin et al., 2018; Eling, 2018).

As Gordon et al. (2008) argued, researchers concerned with management control systems can and should play a key role in addressing issues related to cybersecurity because little is known in this field. One of the few authors to have focused on cyber risk from the management control perspective is Boyson (2014). Investigating cyber supply chain risk management, he developed a model that revealed a significant interaction between different functions within the companies analyzed. This interaction consists of extensive enterprise risk practices, continuous communication between IT, supply

chain, and corporate risk functions, and an emphasis on customer engagement in the risk surveillance/due diligence process. This analysis reinforces the idea that CRM should be a systemic, transversal, and multi-perspective process, necessitating a profound change in every organization.

A standard methodology for analyzing cyber risk would also assist internal communications between corporate cybersecurity professionals, from the control room to the boardroom, and facilitate external communication with other firms, investors, and regulatory agencies (Ammirato et al., 2019). Therefore, passing from the business domain of identifying cyber risk through the CRM process would directly affect risk reporting, representing the link between management accounting and control and financial accounting (Crovini and Ossola, 2021).

In their literature review, Eling et al. (2021) concentrated on three phases of the CRM process: risk identification, analysis, and treatment. They did not analyze environmental scanning (i.e., the first step related to incorporating the risk management process into the overall corporate governance), risk monitoring, and process review. Nevertheless, they provided interesting insights into integrating cybersecurity programs and the general ERM framework because the CRM process is often implemented with a silo view. This misalignment results in unsuccessful CRM and severe risk governance failure (Eling et al., 2021: 113). Hence, they recommended more studies on the interactions between cyber risk and corporate risk governance.

Regarding the financial sector, the traditional risk management process, with its interplay with the management control system, has become inadequate, especially since the 2008 financial and economic crisis, which brought new kinds of risks, such as cyber risk (Boyson, 2014; Crovini et al., 2018; Gordon et al., 2008).

Researchers have analyzed the tools and processes involved and the activities (i.e., boundary objects) carried out by risk management in the banking sector (Mikes, 2009, 2011) by focusing on the concept of ERM (Caldarelli et al., 2016) and the evolution of the role played by this function in banking organizations (Giovannoni et al., 2016). Specifically, Power (2004, 2009) underlined the shift from *risk management of everything* to *risk management of nothing*. Instead, *risk management of everything* is mainly characterized by secondary risk management, in which reputational risk reflects a new sense of vulnerability.

The consequence is that everyone inside a company is considered a risk manager. This progressive involvement in managing both primary and secondary risks has influenced the internal control systems of companies, pushing them to implement control and risk activities to comply with risk man-

agement frameworks and regulations (Pérez-Cornejo et al., 2019). More specifically, the two areas that risk managers and internal control systems need to emphasize are risk communication and the development of explicitly risk-based regulatory systems. This dual risk management (Kaplan and Mikes, 2016) involves groups of people providing independent scrutiny of compliance activities and risk managers advising business decision makers about the risk exposure of the overall company.

However, Power (2009) argued that there are several limitations of traditional ERM, intended as a transversal process dealing with risk identification, assessment, and management. First, ERM cannot process and represent internally systemic or emerging risks since this task involves reaching beyond the parameters and the progressive attention paid to quantification models defined by established frameworks. Arena et al. (2017) addressed this issue by introducing the concept of *(dis)integrated risk management*, the dynamics of which explain the difficulty of balancing plasticity and robustness in ERM. Robustness requires companies to adopt ad hoc processes to deal better with specific risks (e.g., energy and extreme events). Plasticity makes the distinction of risk management activities from other internal control processes challenging.

Nevertheless, companies are under continuous pressure because of knowledge boundaries that highlight the limited nature of ERM procedures (Durst et al., 2018). Throughout the ERM process, a standardized and shared context inevitably (dis)integrates the risk management process into ad hoc processes for specific risk categories that do not fit the ERM reporting cycle because they need to be managed at the operations level (Arena et al., 2017). The risk is that ERM cannot aid decision making, thus losing its managerial relevance (Arena et al., 2017).

Power (2009) stated that governance failure derives from intellectual failure as traditional risk management and internal control systems cannot represent the interconnectedness between risks, requiring a continuous exchange with the external environment. This interconnectivity with the external environment may be made possible through the development of business continuity management (BCM), which involves hybrid IT and emergency management specialists attentive to systemic risks. Power thus emphasized that ERM can be defined more accurately as *risk management of nothing* because there is the risk that ERM, especially in the financial sector, operates as a boundary-preserving model that cannot adapt to the complex and continuously changing environment.

Research has found that risk management practices have sometimes been implemented superficially to meet regulatory requirements and appease

stakeholders (Lim et al., 2017; Mikes, 2011). However, regulation and formal structures are less important than the imbalance of power within the organizational structure and the deployment of content-specific knowledge (Robalo, 2014).

Uncertainty is linked to knowledge management and boundaries (Durst and Henschel, 2020; Power, 2004), revealing that knowledge about certain risks needs to be localized (Carlile, 2002, 2004). The build-up of specific risk identification and assessment practices is required at a more operational level (Arena et al., 2017).

Questions have progressively emerged about how different risk governance functions interact and the extent to which risk management staff can exercise influence and control over the risk-taking behavior of financial entities (Lim et al., 2017). Information flows, data recording, and internal and external reporting systems are crucial risk objects to track all operations and management events promptly and provide complete and up-to-date information on business activities and the evolution of risks (Arena et al., 2017). In addition, information flows ensure the integrity, completeness, and accuracy of data and risk information communicated to enhance an effective risk talk (Circolare 285/2013 Bank IT – First part, Tit. IV, Chap. 4, section V; Giovannoni et al., 2016).

The capability of financial entities to identify, assess, and manage new kinds of emerging risks in this challenging environment needs to be improved. ERM was conceived to rely on historical knowledge and not look forward, thus focusing on what companies do not know (Ashby et al., 2018:3). In this sense, the need emerges to expand ERM to include knowledge risk management to identify, analyze, and respond to the risks associated with the creation, application, and retention of new organizational knowledge (Durst et al., 2018; Tsang and Lee, 2020).

According to the Financial Services Authority (2006), significant time is needed to develop a common and universally recognized standard that would enable financial companies to measure and mitigate their cyber risk. Thus, all stakeholders must engage in a meaningful dialogue addressing cybersecurity threats. In addition, the cybersecurity response should be system wide, enhancing interconnectedness instead of prescribing specific activities for each function (Ashby et al., 2018). In this way, efficient and consistent responses to regulatory requests would be facilitated, thus concentrating additional resources on improving the risk culture (Palermo et al., 2017). The expertise and technical competencies of the actors involved in assessing and managing cyber risk are fundamental. Policy makers also actively need to

enhance communication among institutions and promote information sharing to improve the company's internal control systems (Ashby et al., 2018).

3. Theoretical framework

This study draws upon neo-institutional theory (DiMaggio and Powell, 1983; Scott, 2013) and the relationship between the concept of boundary objects and infrastructure (Poon, 2009; Power, 2015; Star, 2010). According to institutional theory, organizations continuously seek legitimacy by conforming to the external pressures influencing the management control system (DiMaggio and Powell, 1983; Scott, 2013). The process of isomorphism explains this interplay between companies and the external environment (DiMaggio and Powell, 1983). In particular, "coercive isomorphism stems from political influence and the problem of legitimacy; mimetic isomorphism resulting from standard responses to uncertainty; and normative isomorphism, associated with professionalization" (DiMaggio and Powell, 1983: 150). As a result, the internal structures and practices reflect the rules, procedures, myths, and norms prevalent and generally perceived as "right" by society.

Over the past few years, the ongoing economic and financial crisis has increased the attention paid to risk management and internal control systems, especially in financial institutions (Caldarelli et al., 2016; Giovannoni et al., 2016; Mikes, 2011). At the same time, aspects of economic and political systems "make up the context within which an organization functions" (Dillard et al., 2004: 511) and influence the organizational field. As a result, regulatory authorities have gradually implemented stricter and stricter supervision of risk management and risk awareness (European Banking Authority [EBA], 2017; European Union [EU], 2016; National Institute of Standards and Technology [NIST], 2018).

National and international laws are complex and include directives such as the EU Data Protection Regulation (GDPR), which force companies to ensure that their governance structures demonstrate an awareness of the legal and regulatory environment. As regulation strives to follow the speed and complexity of the threat, organizations face financial and technical challenges to meet compliance requirements. Because of the regulatory environment, financial organizations may put growth over protecting security interests and undertake the "minimum to get by," thereby running a high reputational and regulatory risk (Ammirato et al., 2019).

However, while regulations represent external pressure to provide organizational conformity in banks' internal control system and corporate govern-

ance (Bromley and Powell, 2012), moderate flexibility in modeling the CRM process remains. It has been noted that "organizations may adopt policies to conform to external expectations regarding formally stated goals and operational procedures" (Bromley and Powell 2012:484) but without changing their behavior in practice. Organizations and people can continue to operate according to the existing values, rules, beliefs, and taken-for-granted assumptions (Barley and Tolbert, 1997).

The overall uncertainty around cyber risk, the flexibility in modeling the related process, and the perception of supervisor roles mean that "compliance inducement" actions from rules are likely to be partial (Palermo et al., 2017). The institutional complexity of financial institutions and the intra-organizational dynamics (i.e., the activities carried out and the actors involved) need to be considered. In particular, building on Star's work, Power (2015) concentrated on the relationship between boundary objects and infrastructure.

In this article, the concept of boundary objects (Star, 2010) is extended and used to analyze the different objects (e.g., process, ideas, tools, and organizational arrangements) forming the context of CRM. Specifically, these objects need to balance their plastic and robust characteristics to develop a common infrastructure and consider the contingencies of each organization (Arena et al., 2017).

Understanding the relationship between objects and organizational boundaries is crucial to help overcome problems with information processing and knowledge sharing (Arena et al., 2017:68). Thus, extending the theoretical implication to this study, CRM might be seen as a resource for action that is also contingent upon the institutional environment (Power, 2015).

The concept of infrastructure (Star, 1999) is characterized by certain properties (Arena et al., 2017:68): embeddedness into other structures, visibility only upon breakdown, links with conventions of practice, and uses that reach beyond a single event or one-site practice. Therefore, infrastructure is usually defined by an underlying idea that influences the risk rationale (i.e., the cyber risk definition) and the description of patterns of action (in terms of risk identification and assessment activities).

4. Research design

This research is based on data and materials from a single organizational context (Otley and Berry, 1994; Scapens, 1990). However, the richness of the data justifies the case being mono-site (Ahrens and Chapman, 2006; Scapens, 1990). In addition, the case helps to problematize an emerging phe-

nomenon in the financial sector, in which there is currently a shortage of case studies (Caldarelli et al., 2016; Giovannoni et al., 2016).

Semi-structured interviews were the primary information sources, but direct observations, meeting attendance, and archival sources also provided valuable data (Eisenhardt, 1989; Scapens, 1990). The company's internal documents included ERM policies, framework documents, and organizational charts. In addition, reference to publicly available data, such as annual reports and the company's published information, was made.

The data collection covered the period 2018-2020. The respondents in IT functions reported that cyber risk became an issue only a couple of years before the data were gathered. Interviews were conducted with the Risk Management Function, Business Continuity Management (BCM), IT Function, Compliance Function, and Internal Audit as they were actively involved in managing cyber risk (Appendix A). The interviews varied in length between 30 and 90 minutes. They were recorded and then transcribed for analysis later (Appendix A). The interviews were divided into two parts – the first covered general information about the internal organization of the Bank and its business management and the second was more specific and concerned the definition of cyber risk, its assessment, and management within the Group.

The three coordinates used to build the specific parts of the interviews were: (A) conceptualization of cyber risk; (B) CRM with respondents' perspectives on organizational structure and CRM procedures; and (C) relationships with external pressures and stakeholders (public institutions, government, customers, and suppliers). In addition, to increase effectiveness, ensure coherence, and provide complete coverage of the issues related to the CRM process, questions also focused on internal and external dynamics in terms of power dynamics and roles, actors' perceptions, and environmental and regulatory pressures.

Following Saldaña (2012), the data were coded to identify crucial elements related to the CRM process. The characteristics of the general business environment, the Bank's internal control system, and specific cyber risk activities carried out were identified. The information and data gathered were linked to the identification of cyber risk objects and related boundaries in the CRM process. The analysis then further linked evidence from the data to the concepts of internal and external institutional pressures.

The following section describes the empirical evidence in detail.

5. Cyber risk management in Bank XYZ

5.1. Setting the context

This study examines the case of Bank XYZ, a bank listed on the Italian Stock Exchange. It is one of the leading Italian private and listed companies with over a century of history. Founded in early 1900 by a group of entrepreneurs, it became the holding of a medium-sized and multiregional group with more than 5,000 employees after several mergers and acquisitions. Today Bank XYZ is present in 19 regions across Italy. It grew by opening new branches and acquiring small- and medium-sized banks in which it became interested in the early 1990s. It mainly provides banking services for retail and small businesses and insurance and real estate services. Thanks to its commitment to anticipating customer needs and creating new services and skills, the Group has always been able to combine technological innovation with attention to individual customers. Another distinctive element of Bank XYZ and its Group is its multi-channel distribution network: remote banking systems and advanced remote banking solutions exist alongside traditional branches to meet the need for speed and security of transactions.

Bank XYZ was chosen as a case study because of its crucial role in Italy, its wide range of activities, and its mission and values. XYZ is attentive to its customers, human relationships, detail, and concreteness. Italy is currently a good context for analysis: it is incredibly attentive to problems related to cyber security, and the government has made significant investments aimed at reducing cyber risk, in particular in those sectors, such as the financial one, that involve critical infrastructures (Italian Ministry of Defence, 2019; Law-Decree 82/2021).

5.2. Cyber risk objects and the CRM process in Bank XYZ

In this section, the paper presents the main findings related to RQ1 (What are the risk "objects" and related boundaries that constitute the CRM process?) and RQ2 (Is CRM integrated into the existing ERM, pursuing the idea of risk management of everything, or is that an ad hoc process representing a (dis)integrated process?).

Bank XYZ has recognized issues deriving from cyber risk very recently. As a result, the Bank defines cyber risk negatively as a pathological aspect of the IT risk and linked to external attacks undertaken to violate the IT systems. The Bank has defined roles and responsibilities within the internal con-

trol system (Table 1). In addition, it has invested in training employees and directors to raise awareness of the sensitive nature of cyberattacks.

Table 1 – Main bodies and their roles in the cyber risk management process in Bank XYZ

Bodies	No. of people	No. involved in the CRM process	Role/function
IT Function	300	4	Active role. This operating function bears the most responsibility for assessing and managing cyber risk.
Compliance	65	2	Complementary to an internal audit: monitors compliance with laws and regulations.
Internal Audit	64	1	Monitors the BCM plan and processes, suggesting changes when necessary.
BCM	4	4	Close collaboration with the IT function. Identifies critical processes and crisis scenarios and tests recovery procedures.
Risk Management	50	2 (focused on operating risk, of which cyber risk is a part)	Marginal role. Receives the overall assessment of IT risk and defines the level of operational risk.

Cyber risk is assessed and managed by the IT Function, which follows the COBIT framework. Out of 300 people, 15 concentrate on IT security and four focus on cyber risk.

The Chief of the IT Function stated:

External threats are changing, and we had to modify the assessment as also required by the supervisory bodies.

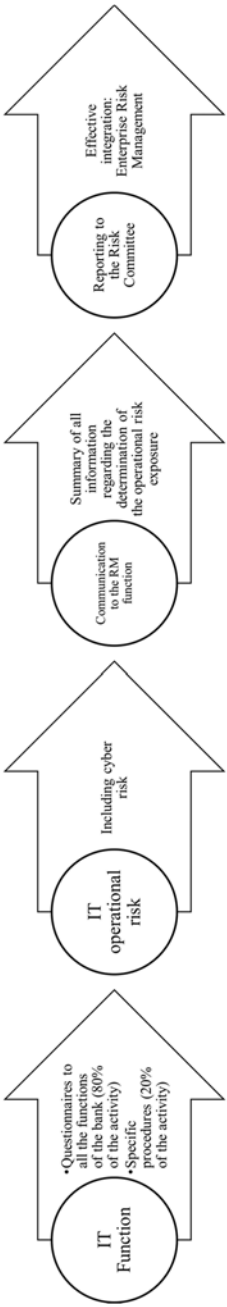
The other IT manager added:

External pressures have helped define critical areas within the bank that require prevention measures for cyber risk.

The IT Function sends self-assessment questionnaires to all the function managers and assesses the potential losses. In addition, it monitors the frequency of occurrence of operational loss and the oscillation of the loss (average mean). The IT Function considers whether to include cyber scenarios, even though the operational loss is not easily identifiable and despite the costs of supervision and communication.

Recognizing cyber threats as being correlated with various scenarios, Bank XYZ adopts both internal and external sources of analysis (ENISA – threat landscape). Figure 1 shows the phases involved in cyber risk assessment.

Figure 1 – Cyber risk management process in Bank XYZ



Source: Authors' elaboration

Integrated risk management is carried out at the board level through the Risk Committee. Every year, the IT Function prepares a report on cyber incidents for the Board of Directors and reports the data annually to the Risk Management Function. Only specific and infra-annual analyses are carried out in the case of new initiatives.

The Risk Management Function mainly deals with operational risks. It summarizes all the assessments made by other functions to determine the Risk Appetite Framework (RAF), potential losses, and capital that will be absorbed and presents this to the Risk Committee for approval. However, it is challenging to determine a model to quantify cyber risk and its reputational effects. Even in evaluating the reputational risk, cyber risk is not a separate item but falls within the whole.

The interviewees also define cyber risk as a disaster event involving Business Continuity Management. BCM is another function that is marginally involved in CRM. It was established in 2006 as part of the IT Function because most disasters mainly involve IT security. It comprises four people, including the BCM manager.

The BCM manager stated:

> Nowadays, cyber risk and the consequences of its manifestation are included among the catastrophic events.

In the case of cyberattacks, BCM only adopts disaster recovery solutions involving another information system to restore the damaged one. As a result, it is difficult to set up prevention measures, but it is also complex to identify actions to be taken once the damage has occurred. The BCM manager stated:

> Some activities, such as data backups, are useless in the case of cyberattacks because you often notice a data breach after some time, and restoring a data backup could be even more harmful.

Therefore, BCM identifies critical processes and crisis scenarios by developing contingency plans (business impact analysis) within the information systems. In addition, it tests recovery procedures, which leads to close collaboration with the IT function.

The CRM process involves another body from the third line of defense of the Bank: Internal Audit. Out of 64 people, five concentrate on IT security and only one focuses on cyber risk. Internal Audit monitors the BCM plan annually and is involved in audit inspections. As required by the regulations, the Risk Committee validates the BCM plan every three years. The control procedures are also defined every three years. Internal Audit then intervenes

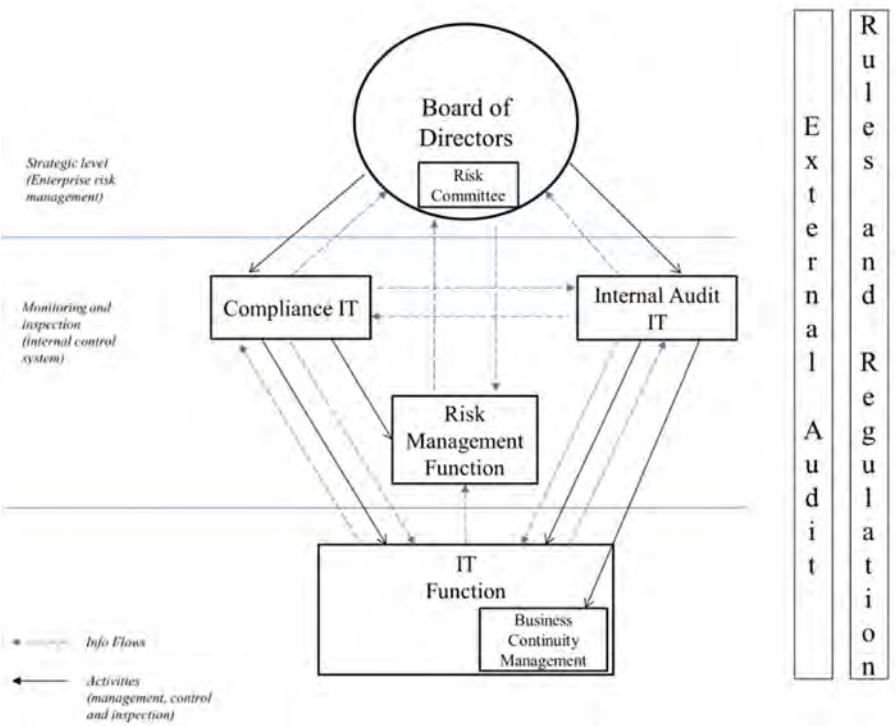
to analyze the processes and suggest, when necessary, any changes. Internal Audit also evaluates the gaps deriving from internal shortcomings and accidents.

Finally, the Compliance Function supports Internal Audit in monitoring compliance with laws and regulations. Two people focus in particular on IT. There is also close collaboration with the IT function.

The Risk Committee deals with the effective integration of ERM. There is a continuous information flow between functions, particularly with the internal control system.

Figure 2 shows the information and communication flows and the organizational dynamics and activities regarding the CRM process.

Figure 2 – Information flows and activities in the cyber risk management process of Bank XYZ



Source: Authors' elaboration

Figure 2 emphasizes the central role of the IT Function in this process, highlighting the direct connection with the internal audit and compliance func-

tions (respectively, the third and second lines of defense). The Risk Management Function, conversely, has a marginal role. It receives the overall IT risk assessment from the IT Function, aggregates this information with other information related to the operational risk exposure, and reports it to the Risk Committee, thus being responsible for the internal reporting process.

5.3. The role and impact of external pressures and stakeholders on the development of the CRM process in Bank XYZ

The findings in the previous section show that Bank XYZ should comply with the external rules issued by financial regulators to guide the correct approach to monitoring cyber risk. This attitude can be seen in the external pressures and the periodic controls imposed on financial institutions by governments and financial regulators.

Although the financial sector is highly regulated, the Bank itself tries not to be solely norm taking but aims to find a balance between compliance with laws and regulations and business environment contingencies. The Compliance Manager, who agreed with the Head of the IT Function, stated:

> From an internal control point of view, many improvements in processes and procedures would not have been possible without certain regulations. In addition, the board of directors' awareness has increased, internal information flows among different functions and levels have improved, and there is greater collaboration.

In this regard, CRM is seen as continuously changing to improve and adapt to external pressures due to the regulatory environment and new knowledge arising from experience in the field.

To answer RQ3, this interplay between rules and existing implemented practices cannot be considered in isolation from the relationships between financial institutions and external stakeholders, such as suppliers and customers. According to its challenging evolution, these relationships undergo continuous change and reshaping in monitoring this emerging risk.

The Head of the IT Function stated:

> Unlike many other group activities, it is not appropriate for a cyber risk strategy to be conceived in silos of internal activity. Inter-disciplinary security systems should be coordinated to standardize and implement agreed cyber security strategies for companies and their supply chain and develop it in wider networks.

Only by redefining the relationships with these additional stakeholders can a more effective and systematic approach to CRM and, more generally,

risk management process be achieved. There is, however, the problem of balancing a compliance-driven approach, which burdens the business management, especially at the commercial and branch levels, with opportunity management and risk management. Supervisory bodies are liable to encourage financial institutions to structure and implement best practices. Unfortunately, however, these tend to raise costs.

Regarding the relationships with customers (companies in particular), a profile is made only of customers of a specific size (large companies). In the qualitative section of the questionnaire, companies were asked to provide relevant information about the company and its exposure to particular risks. Cyber risk was not identified in any precise way, and, for the moment, it has no role in the lending and funding activity of the Bank.

The Head of the IT Function stated:

> The Bank would like to evaluate the customer's cyber risk exposure to decide whether to finance a certain business activity. However, at the moment, it is almost impossible partly because customers are not able to provide sufficient information to determine their overall cyber risk exposure.

However, it is possible to analyze the risk profile of bank suppliers through questionnaires.

The IT Head underlined that:

> We are particularly attentive when choosing a supplier for our services as, if they do not correctly carry out their duties in respect of security and data protection, that will have an impact on our daily activities and as a consequence on our reputation with our customers.

It is fundamental for Bank XYZ to determine the overall risk profile of suppliers because it reflects on the Bank's IT security and reputation. Thinking about the main implication of cyber risk for the Bank itself, there is a need to pay attention to internal control activities and the external dynamics that might affect the extension and quality of such procedures. The Bank is thus aware that cyber risk requires an *outside-in* approach.

The interviews reveal the difficulty of developing a multi-perspective approach to effective "enterprise" cyber risk integration. Technology and processes are extended to critical external stakeholders, such as customers and suppliers.

In this regard, the Compliance Manager and IT Function Head stated:

> Financial companies, i.e., banks, are faced with managing cyber risk in an ever more complex environment. Of course, they have to be compliant with rules and laws, but they should also have the ability to spread and share the experience in

managing cyber risk with customers, suppliers, and other trusted third parties. This approach could be the target that would help a financial company to set an effective cyber risk management strategy in a multi-perspective approach.

Experience and expertise also play a fundamental role, as underlined in Section 5.2. Training is essential because the Bank needs to develop a cyber risk management model fitting its context and specific characteristics, effectively integrating all the Bank's internal activities and relationships with external stakeholders.

6. Discussion

The empirical evidence highlights the difficulties of identifying, assessing, and managing cyber risk as a separate risk category.

The informants are all aware of the specific characteristics of cyber risk. Still, they consider cyber risk to be a pathological aspect of IT risk deriving solely from external unauthorized data breaches. Cyber risk affects the information system and the management of personal and sensitive data due to the dimension of interconnections that it presents. Suppose we consider the three characteristics of cyber risk (i.e., vulnerability, threat, and damage). In that case, potential threats might also derive from the internal organization or misconduct enabling unauthorized access from the external environment. Vulnerability is usually linked to the organizational structure and infrastructures dealing specifically with cyber risk assessment and management. If the financial institution cannot adopt adequate procedures or activities, it is highly probable that the potential damage deriving from data breaches or cyber fraud will increase.

As such, the cyber risk rationale has an impact on the definition of patterns of actions. Accordingly, Bank XYZ cannot determine a model to measure cyber risk effectively. Moreover, the empirical analysis confirms the difficulty of standardizing the assessment and measurement of cyber risk (Ruan, 2017). Cyber risk falls within the category of risks based on sentiment and not measurement (Arena et al., 2017).

The cyber risk rationale also reflects the absence of activities improving precursor resilience, defined as the "ability to accommodate change without catastrophic failure, or a capacity to absorb shocks gracefully" (Foster, 1993:36). As BCM is part of the IT Function, its relationships with IT are close. Still, its activities mainly identify critical processes and scenarios by developing contingency plans. Therefore, the central relevance that Power

(2009) gave to this function to overcome the limits of ERM, especially in financial institutions, is not evident in this case study.

The Bank has a static risk management process based on quarterly reporting cycles on operational risk, which follows international standards and European and Italian regulations. The Risk Management Function is not involved in the cyber risk assessment or management, thus confirming the limitations and previous observations of ERM (Arena et al., 2017; Power, 2009). Instead, risk management represents the link between the operational functions and the Compliance Function and Internal Audit, mainly focusing on known risk, for which the probability of the manifestation of specific risk and its impact can be identified, assessed, and managed based on international frameworks.

Consequently, Bank XYZ has an ad hoc CRM process that is only partially integrated within the ERM of the Bank at the end of cyber risk assessment. Hence, common issues emerged with the comparative case study by Arena et al. (2017), extending the discussion on (dis)integrated risk management. Regarding the balance between robustness and plasticity, Bank XYZ had to develop specific cyber risk activities that differ from those carried out for the other known risks, like company Alpha in the study by Arena et al. (2017). Robustness in this sense prevails because the CRM process has started developing its identity within the Bank's internal control system. The predominant role of the IT Function in managing IT and cyber risks is explained by the fact that core competencies in IT and IT specialists are employed in that function. Therefore, even though standards emphasize the need to involve other functions in cyber risk assessment, including ad hoc and independent IT security functions inside the IT Function, existing practices may already be able to adapt to the regulatory environment.

The plastic component of the CRM process is also present, like in company Omega in the study by Arena et al. (2017). The need to adapt to local contingencies is crucial. Because cyber risk is not assessed as a separate risk category, cyber risk activities flow into the overall IT risk management. Specifically, at the end of the process, the comprehensive cyber risk assessment is aggregated within the general report of the Risk Management Function. Hence, Bank XYZ has strived to define specific work arrangements for cyber risk by integrating them into the existing ERM. However, the difficulties in measuring cyber risk and defining specific preventative risk mitigation activities reveal knowledge boundaries that require a discussion on task-related problems and organizational functioning. In this sense, considering the company contingencies and the interactions among the cyber risk governance bodies, the limits of ERM emerged. Therefore, integrating CRM programs

into ERM or extending the ERM system is complex (Ashby et al., 2018; Eling et al., 2021). According to Arena et al. (2017), this case study stresses the importance of developing organizational processes, tools, and internal control roles to define a stable and dynamic ensemble.

These discussions need to consider the institutional context of Bank XYZ (Power, 2015). According to *neo-institutional theory* (DiMaggio and Powell, 1983; Scott, 2013), the regulatory requirements of Banca d'Italia, deriving from the enactment of European directives and regulations, play a crucial role.

The rules provide a general framework but do not lay down strict or detailed provisions for the CRM process in financial institutions. This moderate flexibility allows Bank XYZ to consider its specific characteristics, dimensions, and activities. From this perspective, existing practices interpret the rules and theory moves into practice while minimizing negative impacts and maximizing positive outcomes from implementing new procedures (Robalo, 2014). Ends and means need to be seen differently: they change and are constantly adapted according to cyber environment developments and regulations.

The findings underline that Bank XYZ cannot be defined as just a *norm-taking* entity because the compliance-driven approach has improved the existing processes and procedures and increased the collaboration between functions and the Board of Directors' awareness. Rules and regulations in this context are seen as a means to improve business management and information management, which inevitably affect the risk reporting process and communication with external users (e.g., investors – see Giner et al., 2020).

Bank XYZ is also trying to improve CRM to develop a process to assess, manage, and monitor cyber risk systemically (Bodin et al., 2018; Boyson, 2014). The aim is to find a way to analyze future trends and threats (specifically the cyber risk exposure of its customers), which are continuously changing as cyberspace is constantly evolving. Cybercrime can defeat even a prepared and comprehensive rapid-response capability, and organizations will inevitably be subject to cyberattacks regardless of their best efforts to protect themselves (Crovini et al., 2018). In this regard, introducing specific activities in the event of adverse cyber threats and building internal cyber resilience will be necessary to avoid losing a competitive advantage or adapt to the changes in the surrounding environment (Eling et al., 2021). Furthermore, cyber resilience might deliver the intended business ends even in the face of adverse events, requiring a move beyond the IT system and considering behavioral perspectives (Eling et al., 2021).

CRM requires a process of knowledge acquisition and gathering (Ashby et al., 2018; Durst and Henschel, 2020; Eling et al., 2021). Even though Bank XYZ is aware of the urgent need to manage cyber risk properly, especially

in this sector, another aspect requiring improvement is the risk culture (Power, 2009). It is essential to enhance informed and reasoned decision making (Palermo et al., 2017) within the internal control system, governance bodies, and external stakeholders (e.g., investors). Education and training underpin any good information security program (Association of Certified Fraud Examiners [ACFE], 2018). However, the challenge is to balance the cost of supervision, responses, and other cyber resilience activities and the cost of cyberattacks (Bodin et al., 2018).

This case study confirms that financial companies need to develop a CRM infrastructure to improve their capacity to identify, assess, and manage cyber risk, considering the role of relationships with external stakeholders. This capacity inevitably affects the external risk reporting process (Crovini and Ossola, 2021; Crovini et al., 2022b), especially in the financial sector, and the management decision to disclose cyber risk information. Risk disclosure then potentially influences the investors' perception of the company's overall risk exposure and related evaluation (De Luca and Phan, 2019; Giner et al., 2020; Crovini et al. 2022a; Crovini et al., 2022b).

7. Conclusions

This paper presents an in-depth case study on CRM, an emerging issue in the risk management and internal control systems of financial entities. The findings of this study go some way toward answering the call made by Ashby et al. (2018) and Eling (2018) to investigate the practice and impacts of disruptive technologies and innovations on governance mechanisms and the relationships with particular categories of stakeholders, such as regulators, suppliers, and customers.

Drawing on institutional theory (DiMaggio and Powell, 1983; Scott, 2013) and the concepts of boundary objects and infrastructure (Arena et al., 2017; Power, 2015; Star, 2010), this case study highlights the crucial role of regulations in shaping the internal organizational structure of Bank XYZ. It also describes the complex relationship between the corporate aim of protecting the Bank from cyber risk and the actual capacity to model a systemic and multi-perspective CRM process. Finally, the study highlights the institutional complexity of financial institutions and the dynamics of (dis)integrated risk management with the related difficulties in balancing the robust and plastic components of a risk management system.

The research contributes to the existing knowledge on cyber risk and CRM in the following ways: (1) by shedding light on the definition of cyber risk used

in practice and the impact of such conceptualization on the definition of patterns of actions; (2) by analyzing the cyber risk objects (i.e., internal process, activities, and organizational actors involved) to manage cyber risk in a highly regulated industry; and (3) by analyzing the role and impact of external dynamics and stakeholders on the design and implementation of the CRM process.

Consequently, this study extends the debate on specific risk management practices, revealing the difficulties of developing a multi-perspective CRM process that considers interactions between organizational dynamics and the external environment.

As CRM involves all the bodies of the Bank's internal control system, the discourse on dual risk management emerges clearly (Kaplan and Mikes, 2016). Even though CRM is mainly undertaken at the operational level, other bodies (i.e., the Compliance Function and Internal Audit) provide independent scrutiny of the overall compliance with standards and laws.

Especially in companies belonging to a critical infrastructure sector, the overall approach to cyber risk needs to evolve. Promoting a cyber risk culture is essential to enhance informed and reasoned decision making, both inside and outside the organization, considering regulators, investors, and auditors. This evolution might consider shifting to cyber resilience practices that reflect the changing nature of cyber risk and allow financial institutions to be better prepared or recover promptly from cyberattacks. In this way, the CRM process would integrate existing risk management practices involving identifying, analyzing, treating, and communicating known risks (Eling et al., 2021).

This study also has many practical implications. Regulators, public institutions, and governments need to adopt a joint strategy against cyber threats and enhance information sharing. Sharing experience and practices would also be helpful to strengthen the effectiveness of cyber risk controls by improving management control systems and developing appropriate techniques to measure the economic, financial, organizational, and reputational impacts of cyber risk. Moreover, accountants and risk managers have a vast professional opportunity to integrate the CRM process into management control systems effectively. Companies need specialists with skills in management control as well as information security. Specialists would also support and improve the activity of the Board of Directors at the strategic level. Finally, there are significant implications regarding the necessity to link the internal control system and the external risk reporting process (Crovini et al., 2022a; Crovini et al., 2022b; Allini and Manes-Rossi, 2014; Aureli and Salvatori, 2013; De Luca and Phan, 2019). An integrated CRM process has the crucial role of facilitating the identification of cyber risk as a critical aspect that should be communicated to ex-

ternal users (e.g., investors, auditors, and regulators) to allow them to make informed decisions. Hence, this study strengthens the importance of having an appropriate internal CRM process as a necessary step to ensure the effectiveness of a mandatory risk reporting process.

However, this case study presents certain limitations. First, the intrinsic limitation is that Bank XYZ did not permit the study to disclose or make any explicit reference to aspects considered sensitive. In addition, cyber risk became an issue for Bank XYZ only a couple of years before the data collection, and the modeling of the CRM process was undergoing a profound rethink. However, that allows future research to further the analysis and consider the evolution and change of this process.

Regarding future research opportunities, researchers could focus on other cases, thus comparing CRM processes implemented in different contexts. Interactions between financial institutions and other external stakeholders can be analyzed to monitor the possible impacts of newly amended tools to promote cyber risk awareness (e.g., insurance policies). Moreover, it would be interesting to study the cyber "calculative culture" (Mikes, 2011) by considering cyber risk as an autonomous risk category to be quantified reliably with first-order measures or by applying risk *envisionment* practices. Finally, it would be interesting to analyze the link between ERM and external risk reporting in greater depth to determine whether there is any positive or negative impact on the quality of risk information disclosed in annual reports. Focusing on external risk reporting would be beneficial to assess the value relevance of risk information.

References

Ahrens T. and Chapman C. S. (2006), Doing qualitative field research in management accounting: Positioning data to contribute to theory, *Accounting, Organizations and Society*, 31, pp. 819-841. doi: 10.1016/j.aos.2006.03.007.

Alali M., Almogren A., Hassan M. M., Rassan I. A. L. and Bhuiyan M. Z. A. (2018), Improving risk assessment model of cyber security using fuzzy logic inference system, *Computers and Security*, 74, pp. 323-339. doi: 10.1016/j.cose.2017.09.011.

Alali M. and Almogren A. (2017), Fuzzy logic methodology for cyber security risk mitigation approach, *Journal of Networking Technology*, 8(3), pp. 83-90.

Aldasoro I., Gambacorta L., Giudici P. and Leach T. (2020a*), Operational and Cyber Risks in the Financial Sector*. (Basel – Switzerland: Bank for International Settlements).

Aldasoro I., Gambacorta L., Giudici P. and Leach T. (2020b), *The Drivers of Cyber Risk*. (Basel – Switzerland: Bank for International Settlements). -- Available at: https://www.bis.org/publ/work865.pdf.

Allini A. and Manes-Rossi F. (2014), Do corporate governance characteristics affect non-financial risk disclosure in government-owned companies? The Italian experience, *Financial Reporting*, 1, pp. 5-31. doi: 10.3280/FR2014-001001.

Ammirato S., Sofo F., Felicetti A. M. and Raso C. (2019), The potential of IoT in redesigning the bank branch protection system: An Italian case study, *Business Process Management Journal*, 25(7), pp. 1441-1473. doi: 10.1108/BPMJ-04-2018-0099.

Arena M., Arnaboldi M. and Palermo T. (2017), The dynamics of (dis)integrated risk management: A comparative field study, *Accounting, Organizations and Society*, 62, pp. 65-81. doi: 10.1016/j.aos.2017.08.006.

Ashby S., Buck T., Nöth-Zahn S. and Peisl T. (2018), Emerging IT risks: Insights from German banking, *Geneva Papers on Risk and Insurance – Issues and Practice*, 43(2), pp. 180-207.

Association of Certified Fraud Examiners (ACFE) (2018), Report to the Nation: Occupational Fraud and Abuse. (ACFE). -- available at: https://legacy.acfe.com/report-to-the-nations/.

Aureli S. and Salvatori F. (2013), Investigation of risk management and risk disclosure practices of Italian listed local utilities, *Financial Reporting*, 1, pp. 121-167. doi: 10.3280/FR2013-001006.

Banca d'Italia, Circolare 285/2013 Disposizioni di vigilanza per le banche – First part, Tit. IV, Chap. 4, section V. -- available at: https://www.bancaditalia.it/compiti/vigilanza/normativa/archivio-norme/circolari/c285/?dotcache=refresh.

Barley S. R. and Tolbert P. S. (1997), Institutionalization and structuration: Studying the links between action and institution, *Organization Studies*, 18(1), pp. 93-117. doi: 10.1177/017084069701800106.

Bodin L. D., Gordon L. A., Loeb M. P. and Wang A. (2018), Cybersecurity insurance and risk-sharing, *Journal of Accounting and Public Policy*, 37(6), pp. 527-544. doi: 10.1016/j.jaccpubpol.2018.10.004.

Bojanc R. and Jerman-Blažič B. (2008), An economic modelling approach to information security risk management, *International Journal of Information Management*, 28(5), pp. 413-422. doi: 10.1016/j.ijinfomgt.2008.02.002.

Boyson S. (2014), Cyber supply chain risk management: Revolutionizing the strategic control of critical IT systems, *Technovation*, 34(7), pp. 342-353. doi: 10.1016/j.technovation.2014.02.001.

Brender N. and Markov I. (2013), Risk perception and risk management in cloud computing: Results from a case study of Swiss companies, *International Journal of Information Management*, 33(5), pp. 726-733. doi: 10.1016/j.ijinfomgt.2013.05.004.

Bromley P. and Powell W. W. (2012), From smoke and mirrors to walking the talk: Decoupling in the contemporary world, *Academy of Management Annals*, 6, pp. 483-530.

Caldarelli A., Fiondella C., Maffei M. and Zagaria C. (2016), Managing risk in credit cooperative banks: Lessons from a case study, *Management Accounting Research*, 32, pp. 1-15. doi: 10.1016/j.mar.2015.10.002.

Carlile P. R. (2002), A pragmatic view of knowledge and boundaries: Boundary objects in new product development, *Organization Science*, 13(4), pp. 355-457. doi: 10.1287/ORSC.13.4.442.2953.

Carlile P. R. (2004), Transferring, translating, and transforming: An integrative framework for managing knowledge across boundaries, *Organization Science*, 15(5), pp. 555-568. doi: 10.1287/ORSC.1040.0094.

Crovini C., Giunta F., Nielsen C. and Simoni L. (2022a), Do companies disclose relevant information about intangibles? Insights from business model reporting and risk reporting, ICAS-EFRAG. -- Available at: https://www.icas.com/__data/assets/pdf_file/0008/610892/Insights_Intangibles_Report_Final.pdf.

Crovini C., Schaper S. and Simoni L. (2022b), Dynamic accountability and the role of risk reporting during a global pandemic, *Accounting, Auditing and Accountability Journal*, 35(1), 169-185. doi: 10.1108/AAAJ-08-2020-4793.

Crovini C. and Ossola G. (2021), Is risk reporting a possible link between financial and management accounting in private firms?, *Financial Reporting*, 1, pp. 29-60. doi: 10.3280/fr2021-001002.

Crovini C. (2019), *Risk Management in Small and Medium Enterprises* (Oxon, UK: Routledge).

Crovini C., Ossola G. and Marchini P. L. (2018), Cyber risk: The new enemy for risk management in the age of globalisation, *Management Control*, 2, pp. 135-155.

De Luca F. and Phan H.-T.-P. (2019), Informativeness assessment of risk and risk-management disclosure in corporate reporting: An empirical analysis of Italian large listed firms, *Financial Reporting*, 2, pp. 9-41. doi: 10.3280/FR2019-002002.

Dillard J. F., Rigsby J. T. and Goodman C. (2004), The making and remaking of organization context: Duality and the institutionalization process, *Accounting, Auditing and Accountability Journal*, 17(4), pp. 506-542. doi: 10.1108/09513570410554542.

DiMaggio P. J. and Powell W. W. (1983), The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields, *American Sociological Review*, 48(2), pp. 147-160.

Durst S. and Henschel T. (2020), Knowledge risk management – State of research, in S. Durst and T. Henschel (Eds.), *Knowledge Risk Management. From Theory to Praxis*, pp. 3-10 (Springer Nature). Doi: 10.1007/978-3-030-35121-2_1.

Durst S., Bruns G. and Henschel T. (2018), The management of knowledge risks: What do we really know?, in *Global Business Expansion: Concepts, Methodologies, Tools, and Applications*, pp. 258-269 (IGI Global). Doi: 10.4018/978-1-5225-5481-3.CH013.

Eaton T., Grenier J. H. and Layman D. (2019), Accounting and cybersecurity risk management, *Current Issues in Auditing*, 13(2), pp. 1-9. doi: 10.2308/ciia-52419.

Eisenhardt K. M. (1989), Building theories from case study research, *Academy of Management Review*, 14(4), pp. 532-550. doi: 10.2307/258557.

Eling M. (2018), Cyber risk and cyber risk insurance: Status quo and future research, *Geneva Papers on Risk and Insurance: Issues and Practice*, 43(2), pp. 175-179. doi: 10.1057/s41288-018-0083-6.

Eling M., McShane M. and Nguyen T. (2021), Cyber risk management: History and future research directions, *Risk Management and Insurance Review*, 24(1), pp. 93-125. doi: 10.1111/rmir.12169.

European Banking Authority (EBA (2017), Final Report Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation process (SREP). -- Available at: https://www.eba.europa.eu/documents/10180/1841624/Final+Guidelines+on+ICT+Risk+Assessment+under+SREP+%28EBA-GL-2017-05%29.pdf/ef88884a-2f04-48a1-8208-3b8c85b2f69a.

European Union (EU) (2016), Directive 2016/1148 Concerning Measures for a High Common Level of Security of Network and Information Systems across the Union. -- Available at: https://eur-lex.europa.eu/legal-ontent/EN/TXT/PDF/?uri=CELEX:32016L1148&from=IT.

Financial Services Authority (2006), *Business Continuity Management Practice Guide* (Financial Services Authority).

Foster H. (1993), Resilience theory and system evaluation, in *Verification and Validation of Complex Systems: Human Factors*, pp. 35-60 (NATO ASI S. Springer US).

Giner B., Allini A. and Zampella A. (2020), The value relevance of risk disclosure: An analysis of the banking sector, *Accounting in Europe*, 17(2), pp. 129-157. doi: 10.1080/17449480.2020.1730921.

Giovannoni E., Quarchioni S. and Riccaboni A. (2016), The role of "roles" in risk management change: The case of an Italian bank, *European Accounting Review*, 25(1), pp. 109-129. doi: 10.1080/09638180.2014.990475.

Gordon L. A., Loeb M. P., Sohail T., Tseng C. Y. and Zhou L. (2008), Cybersecurity, capital allocations and management control systems, *European Accounting Review*, 17(2), pp. 215-241. doi: 10.1080/09638180701819972.

Institute of Risk Management (IRM) (2014), *Cyber Risk. Resources for Practitioners*. doi: 10.4018/978-1-5225-0808-3.ch014.

ISACA (2012), COBIT 5 for Information Security. -- Available at: https://www.isaca.org/resources/cobit.

ISO/IEC (2018), Information Security Risk Management. -- Available at: https://www.iso.org/standard/75281.html.

Italian Ministry of Defence (2019), Documento Programmatico Pluriennale per la Difesa per il triennio 2019-2021. -- Available at: https://www.difesa.it/Content/Documents/Documento_Programmatico_Pluriennale_(DPP)_2019_2021_digit.pdf.

Kaplan R. S. and Mikes A. (2016), Risk Management – The Revealing Hand, pp. 16-102. -- Available at: http://www.hbs.edu/faculty/Publication Files/16-102_397b963b-1a8b-4dcf-942f-e45acc8c9e96.pdf.

Law Decree 81/2021 – Regolamento in materia di notifiche degli incidenti aventi impatto su reti, sistemi informativi e servizi informatici di cui all'articolo 1, comma 2, lettera b), del decreto-legge 21 settembre 2019, n. 105, convertito, con modificazioni, dalla legge 18 novembre 2019, n. 133, e di misure volte a garantire elevati livelli di sicurezza. -- available at: https://www.gazzettaufficiale.it/eli/id/2021/06/11/21G00089/sg.

Lim C. Y., Woods M., Humphrey C. and Seow J. L. (2017), The paradoxes of risk management in the banking sector, *British Accounting Review*, 49(1), pp. 75-90. doi: 10.1016/j.bar.2016.09.002.

Mikes A. (2009), Risk management and calculative cultures, *Management Accounting Research*, 20(1), pp. 18-40. doi: 10.1016/J.MAR.2008.10.005.

Mikes A. (2011), From counting risk to making risk count: Boundary-work in risk management, Accounting, *Organizations and Society*, 36, pp. 226-245. doi: 10.1016/j.aos.2011.03.002.

Mukhopadhyay A., Chatterjee S. and Saha D. (2013), *Cyber-risk decision models: To insure IT or not?*, *Decision Support Systems*, 56, pp. 11-26.

National Association of Insurance Commissioners (NAIC) (2018), Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement. -- available at: https://www.naic.org/documents/cmte_ex_ittf_180921_cyber_supplement_report_2018.pdf.

National Institute of Standards and Technology (NIST) (2018), *Cybersecurity Framework*. -- available at: https://www.nist.gov/cyberframework.

Öğüt H. and Menon N. (2005), Cyber insurance and IT security investment: Impact of interdependent risk, in *Fourth Workshop on the Economics of Information Security (WEIS)*. (Harvard).

Öğüt H., Raghunathan S. and Menon N. (2011), Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection, *Risk Analysis*, 31(3), pp. 497-512. doi: 10.1111/j.1539-6924.2010.01478.x.

Otley D. and Berry A. J. (1994), Case study research in management accounting and control, *Management Accounting Research*, 5(1), pp. 45-65. doi: 10.1006/MARE.1994.1004.

Palermo T., Power M. and Ashby S. (2017), Navigating institutional complexity: The production of risk culture in the financial sector, *Journal of Management Studies*, 54(2), pp. 154-181. doi: 10.1111/joms.12241.

Pérez-Cornejo C., Delgado-García E. de and Quevedo-Puente J. B. (2019), How to manage corporate reputation? The effect of enterprise risk management systems and audit committees on corporate reputation, *European Management Journal*, 37(4), pp. 505-515. doi: 10.1016/j.emj.2019.01.005.

Poon M. (2009), From new deal institutions to capital markets: Commercial consumer risk scores and the making of subprime mortgage finance, *Accounting, Organizations and Society*, 34(5), pp. 654-674. doi: 10.1016/J.AOS.2009.02.003.

Power M. (2004), The risk management of everything, *Journal of Risk Finance*, 5(3), pp. 58-65. doi: 10.1108/eb023001.

Power M. (2009), The risk management of nothing, *Accounting, Organizations and Society*, 34(6-7), pp. 849-855. doi: 10.1016/j.aos.2009.06.001.

Power M. (2015), How accounting begins: Object formation and the accretion of infrastructure, *Accounting, Organizations and Society*, 47, pp. 43-55. doi: 10.1016/J.AOS.2015.10.005.

PricewaterhouseCoopers (PwC) (2018), Global Economic Crime and Fraud Survey 2018. -- available at: https://www.pwc.com/gx/en/news-room/docs/pwc-global-economic-crime-survey-report.pdf.

Robalo R. (2014), Explanations for the gap between management accounting rules and routines: An institutional approach, *Revista de Contabilidad*, 17(1), pp. 88-97. doi: 10.1016/j.rcsar.2014.03.002.

Ruan K. (2017), Introducing cybernomics: A unifying economic framework for measuring cyber risk, *Computers & Security*, 65, pp. 77-89. doi: 10.1016/j.cose.2016.10.009.

Saldaña J. (2012), *The Coding Manual for Qualitative Researchers* (2nd ed.). (Los Angeles: SAGE).

Scapens R. W. (1990), Researching management accounting practice: The role of case study methods, *British Accounting Review*, 22(3), pp. 259-281. doi: 10.1016/0890-8389(90)90008-6.

Scott R. W. (2013), *Institutions and Organizations. Ideas, Interests, and Identities* (4th ed.). (SAGE Publications, Inc.). -- https://uk.sagepub.com/en-gb/eur/institutions-and-organizations/book237665.

Star S. L. (1999), The ethnography of infrastructure, *American Behavioural Scientist*, 43(3), pp. 377-391. doi: 10.1177/00027649921955326.

Star S. L. (2010), This is not a boundary object: Reflections on the origin of a concept, *Science, Technology, & Human Values*, 35(5), pp. 601-617. doi: 10.1177/0162243910377624.

Tsang H. W. C. and Lee W. B. (2020), An integrated research methodology to identify and assess knowledge risk in a corporation with application to a financial institution, in S. Durst and T. Henschel (Eds.), *Knowledge Risk Management*, pp. 135-158 (Springer). Doi: 10.1007/978-3-030-35121-2_9.

Appendix A: Meetings and interviewees

Meeting	Interviewees	Duration *(minutes per person)*
July 2018	IT Manager	90
November 2018	2 members of the IT Function team	90
December 2018	Business Continuity Manager	30
March 2019	Responsible for Compliance Function	30
May 2019	Chief of Internal Audit	60
June 2019	Chief Risk Officer (CRO)	60
September 2019	IT Manager	60
October 2019	1 member of the IT Function team	60
January 2020	IT Function Manager	90
January 2020	Business Continuity Manager	90
January 2020	Responsible for Compliance Function	90
January 2020	Responsible for Internal Audit	60
January 2020	Chief Risk Officer (CRO)	45