THE EFFECTIVENESS OF REGULATORY AND TECHNOLOGICAL MECHANISMS OF BANKING INTERNAL CONTROL: AN EXPLORATION BASED ON THE ORIGINS OF BANKS

Ludovic Kenfang Wambe *

* Faculty of Economics and Management, University of Yaounde II, Yaounde, Cameroon

Contact details: Faculty of Economics and Management, University of Yaounde II, 1365, Yaounde, Cameroon


Over the last few decades, the news about banks has been dominated by scandals that reflect a lack of inadequate internal control (IC), whereas information technology (Diard & Dufour, 2022b) and banking regulations (Dufour & Yacoub, 2021) are seen as the main tools for effective banking IC. This article aims to understand the role of regulatory measures and information technology in the effectiveness of banking IC. To achieve this, we use a qualitative approach based on the multiple-case method. The study covers six banks (African and Western) and the data is collected through semi-structured interviews with internal controllers, internal auditors, and risk managers. The verbatim technique is used for analysis. The results show that IC regulations mainly benefit Western subsidiaries from countries where regulatory standards are more advanced. However, the role of IC information technology (IT) remains unclear. Local banks need to step up investment in IT and regulations need to take account of the diversity of banks' origins. The relevance of the study lies in the need for the regulator to pay more attention to local banks, which appear to be more fragile.

Keywords: Banking, Banking Regulation, Diversity of Bank Origins, Information Technology, Internal Banking Control

Authors' individual contribution: The Author is responsible for all the contributions to the paper according to CRediT (Contributor Roles Taxonomy) standards.

Declaration of conflicting interests: The Author declares that there is no conflict of interest.

Acknowledgements: The Author is grateful to Dr. Ngoata Sylvanus for proofreading this paper.

1. INTRODUCTION

In the aftermath of the 2008 global financial crisis, voices were raised in the scientific world (Baker et al., 2017; Masciandaro et al., 2020) to describe the ineffectiveness of the internal control (IC) of banking establishments. While it was believed to be well established within the banks, the IC has continued to rise, ever since the Affaire Kerviel in 2008, with signs of great weakness. Indeed, the errors in the “trading” of the assets of the French bank Caissesd’Epargnes which occurred in 2008 led to losses of €750 million. Around the world, Coulomban and Garin (2018) in December 2017 alone accounted for some 20 banks affected by IC failures. Banks operating in African
territory do not seem immune to such problems. The news of banks operating in Cameroon, in this case, has been plagued by scandals and internal dysfunctions for more than a decade which contribute to tarnishing their image with the various stakeholders. In its activity reports for the period 2008 to 2015, the International Bank of Cameroon for Savings and Credit (Banque Internationale du Cameroun pour l’Epargne et le Crédit, BICEC) suggests a recurrence of embezzlement and fraudulent practices orchestrated by certain senior executives. Since the last embezzlement estimated in 2016 at just over FCFA 50 billion, its balance sheet has remained negative, the loss amounting to FCFA 5,253 billion in 2020. The UBA-Cameroon Bank also remains in fear of imminent bankruptcy because of the unhealthy activities observed on the accounts of many VIP customers, whose origins remain difficult to identify (Bindouga, 2021). The upsurge in banking scandals contributes to fueling the controversy over the IC systems enacted by many institutions from the 1980s. In the banking sector specifically, the ambition of such institutions to set up an adequate IC is part of the consolidation of strong and consistent performance (McNulty & Akhigbe, 2017).

Most managerial work on bank IC points to the ineffectiveness of qualitative systems (Baker et al., 2017; Flores et al., 2006) that are supposed to support quantitative control approaches. These devices find their echo in the system of governance materialized by the hierarchical organization of such companies (Lamarker & Maurer, 2019; Klein et al., 2021). However, by analyzing certain bank losses, Pakhchanyan (2016) showed that they would have been avoided if the banks had equipped themselves with more effective IC systems. The most up-to-date literature focuses mainly on banking regulation (Randriamiriana & Ouvrad, 2019; Yacoub, 2018) and information technology (IT) (Diard & Dufour, 2022b; Baker et al., 2017; Flores et al., 2006). The evocation of the regulatory system makes it possible to argue that banks evolve in a highly regulated, environment according to the theory of tetranormalization. As for the idea underlying the strengthening of the IT system, it is appropriate to include it in the logic of the theory of IT capacity. Moreover, in their study on the Affaire Kerviel, Baker et al. (2017) conclude that the Automatic Identification System (AIS)\(^1\) could have detected, if it had existed within the bank, the actions of this trader. Following these authors, Diard and Dufour (2022b) specify that biometric tools, geolocation, and video protection must be integrated into the IC process for an effective reduction in internal fraud.

By way of illustration, the Optimiso Suite software\(^2\) promotes a reliable and simplified IC (time-saving, digitized and reliable IC, automatic update without error), makes it possible to monitor fully automated controls (automatic monitoring of the progress of controls, helps employees, traceable controls) and ensures reporting (serene and rapid audit, compliance of the matrix with the auditor's requirements, rapid access to the evidence kept). Banks also need to set up comprehensive customer information systems (Customer Information System, CIS) to track and analyze malicious behaviour and customer needs (Kerviel et al., 2016), as well as production systems that enable analytical modelling of revenue tracking, risks, and patterns of use of financial products, loans, securities, hedging, and collections, etc. Using their new IT arsenal, banks are also deploying complex mathematical models to measure earnings volatility, as well as performing stress and scenario tests to detect operational and portfolio risks (Li et al., 2022). They also use IT tools for measuring Value at Risk (VaR) and Capital at Risk (CaR) to identify risk limits, as well as asset and liability management systems to detect operational and portfolio risks. These state-of-the-art IC technologies, therefore, appear fundamental for improving IC capabilities and bank management efficiency (Cheng & Qu, 2020).

While research into the IC of companies in Africa seems to be emerging (Tchuiyendem et al., 2023), scholars into the control of banks are almost non-existent. Ozili (2019) finds the problem relevant in the African context, given the weakness of the application of standards, the unreliability of sources of information, and the imperfection of the financial markets, which are the real sources of information. Added to this is the regular interference of African governments which, through their politicians, pass laws to prevent compliance with prudential standards, because they are shareholders in or affiliated to the banks. The Cameroonian state is a perfect example in that, because of its shareholding in the banks, the deputy Chief Executive Officers (CEOs) and board chairmen appointed are mainly for political reward these practices are holding back business innovation in these developing countries (Shamsub, 2023). However, those financial institutions that have applied the regulations have underperformed (Akume & Badjo, 2017). The authors justify this by the universal nature of the regulations, which do not take account of Cameroon's specific characteristics.

The foundations in the area of IT have recently been laid through doctoral research (Kenfang, 2020) which takes into account the heterogeneity of banks, including Western subsidiaries and banks from Africa or local banks. While Western subsidiaries had left the territory following the banking crisis of the 1980s, they marked their return due to the recession that occurred in developed countries following the subprime crisis (Ernst & Young [EY], 2014). Indeed, subsidiaries from countries with effective banking regulations tend to evade local regulations when they consider them unfavourable to their activities (Kouretas & Tsoumas, 2016). The COBAC R-2016/04 regulation of December 31, 2016, relating to IC in credit institutions and financial holding companies, established by the Central African Banking Commission (COBAC)\(^3\), is involved. Furthermore, supporters of the internationalization of banks postulate that advanced technological devices favour the management of subsidiaries in underdeveloped countries (Berger & DeYoung, 2006;
Detragiache et al., 2008). In other words, these ITs offer them technological advantages in the host territory (Fong, 2006; Tioumagneng et al., 2020). We then presuppose the superiority of Western subsidiaries over their local counterparts in terms of IC, also in that their presence in the host country makes management and control techniques more sophisticated (Ofori-Sasu et al., 2013; Kusi et al., 2022; Kouretab & Tsoumas, 2016). In other words, they are implementing a form of governance that enables them to excel in an emerging territory (Kusi et al., 2022).

However, real efforts to invest in IT are being made by local banks to guard against scandals. This is precisely the case of the Société Commerciale de Banque-Cameroun (SCB-C), which, victim of embezzlement in 2014, is strengthening its investments in IT. This is also the case with the Gabonese Bank of International Finance (GBIF) through the “Excellence 2020” project.

The foregoing developments feed our problem on IC, which is addressed in light of the following research question: **RQ1: Do regulations and IT lead to effective banking IC?**

The objective assigned to the study is to understand how banking regulations and IT contribute to making IC effective.

The rest of this paper is structured as follows. Section 2 reviews the relevant literature. Section 3 describes the methodology that has been used to conduct empirical research. Section 4 presents the different results. Section 5 discusses those results. Section 6 concludes the study.

2. LITERATURE REVIEW

Banking regulations and IT are respectively external and internal factors of banking risk control. We situate the analysis from the perspective of the work of Buch (2003) which posits that information (via IT) and regulation are at the heart of banking activities. The combination of these two elements is, according to many authors, the guarantee of an effective banking IC. It is therefore appropriate to shed light on the notion of IC in its specificities in the bank.

2.1. Internal control: An attempt at conceptual clarification

Internal control comes from afar, from the depths of our history. The first prehistoric man who lit a fire at the entrance to his cave acted to protect himself against a risk: that of the attack of wild beasts. And, in doing so, he put in place an internal control system (Renard, 2011). Through this historical positioning, the author shows an intuitive, irrational, unorganized, imperfect IC, and above all external to individuals. The need then arises to set up a rational and reasoned IC (Renard, 2012). The first attempts to define this concept were made by French auditors and chartered accountants in the 1960s, the ambition being to guard against the risks that could taint the sincerity and regularity of the financial statements. They define it as the “set of securities contributing to the control of the company”. But it is thanks to the scandals that the question of IC is placed at the centre of research concerns. Under the impetus of the United States (US) Senator Treadway, the research milestones were laid, which led a few years later to the creation of the Committee of Sponsoring Organizations Commission (COSO). This body defines IC as a process, involving the board of directors, management and other personnel of an entity, designed to provide reasonable assurance regarding the effectiveness of operations, the reliability of financial information and compliance with applicable laws and regulations (Bertin, 2007).

According to the definition, the COSO offers a three-dimensional vision of IC. Through the cubic shape of this reference frame, it is then possible to determine, for each level of the company (subsidiary, entity, operational unit, etc.), how the five components of IC enable the achievement of the COSO objectives (control environment, risk assessment, control activities, information and communication, monitoring activities).

This reference framework is mainly used within ordinary companies, and cannot on its own be sufficient to promote understanding of the IC of the bank (Ogien, 2016), a specific company given its activities.

2.2. Bank-specific internal control

Bank IC is difficult to implement (Jardat & Boned, 2008). According to Ogien (2016), operational efficiency does not only lie in the optimization of internal management but above all in the ability of banks to control the various risks inherent in their activities. Labaki and Pallaser-Saltiel (2011) think that addressing the problem of banking IC comes down to being particularly interested in the management of operational risk. This category of risk is defined by the International Monetary Fund (IMF) (2018), as “the risk of loss resulting from an inadequacy or failure attributable to internal procedures, personnel, and systems such as information systems, or external events, including events with a low probability of occurrence but a high risk of loss” (IMF, 2018, p. 31). The main operational risk outcomes identified by Maurer (2011) include transaction errors; system or process failures; business disruption or interruption; breach of information relating to security, integrity, or confidentiality; identity forgery, hacking, and unauthorized transactions; intentional and voluntary acts and omissions; criminal trading, fraud, and theft committed by employees or outsiders; terrorist threats and attacks; as well as natural disasters. To deal with this, banks must go beyond the hierarchical organization (Burlaud, 2000) underpinned by IC governance to seek the tools and methods that can guarantee their operational efficiency (Maurer, 2011).

At the level of the Central African Economic and Monetary Community (CEMAC), COBAC through the COBAC R-2016/04 regulation provides in its article 111 that subject institutions must identify and assess the operational risk inherent in all significant products, activities, processes, and systems. This regulation organizes the IC system of banks through the provisions allowing:

- To check internal operations and procedures, measure, control, and monitor risks;
To make the conditions for collecting, processing, disseminating, and storing accounting and financial data more reliable;
To make the channels for the internal circulation of documentation and information efficient, as well as their distribution to third parties.

2.3. The theory of tetranormalization: The analysis of internal control in the light of the juxtaposition of norms

Research on the effectiveness of IC regulation, in this case, banking regulation, continues to be controversial. Created in 1974, the Basel Committee has subjected the banking sector to strong regulations which, as changes evolve, lead to increasingly complex management of the bank. These standards have intensified over the past decade, mainly due to the financial crisis. Alongside the Basel II regulations, which focus solely on banking operational risk, we see a multitude of standards. Indeed, the bank is subject to safety, quality, and environmental standards; social norms; business and technical standards; and accounting and financial standards, following the tetranormalization theory of Saval and Zardet (2005). The theory is used as a grid to analyze the internal consequences of banking regulations when they are juxtaposed (Yaouch, 2018). According to Randriamiarana (2016), the multiplication of banking standards is due to the regulator's determination to curb risks. In any case, banks gain a competitive advantage when they manage these standards well.

Internationally, the US is considered the most dynamic country in terms of banking IC regulation. After the failure of a large number of banks in the 1980s around the world, the Federal Deposit Insurance Corporation (FDIC) in 1991 passed the Federal Deposit Insurance Improvement Act (FDICIA) which required that the management of banks holding more than $500 million of assets evaluate the effectiveness of their control, financial reporting processes and that the banks' external auditors testify to the effectiveness of IC’s structure. However, internal failures occurred in the 2000s, leading to a loss of investor confidence. It was then that in 2002 the Sarbanes-Oxley (SOX) Act was enacted which imposed stricter IC measures on banks.

Several studies posit that FDICIA requirements enhance the economic viability of banks. The study by Jin et al. (2013) found that banks required to comply with this standard took less risk before the subprime crisis. They are also sheltered from many difficulties and financial problems during crises. In contrast, studies by Doyle et al. (2007) and Ashbaugh-Skaife et al. (2008) on SOX provisions have IC deficiencies. Above all, they point to a financial weakening of the banks. Cohen et al. (2008) observed a fall in bank profits after they were pegged to the SOX. In the study conducted by Randriamiarana (2016), the concept of “normative bombardment” is used by a bank manager to qualify the multitude of contradictory standards and carriers of major banking dysfunctions. This confirms the thesis of the contradiction of the standards framing the IC (Dufour & Yaouch, 2021; Yaouch, 2018). Bindouga (2021) deplores the increase in bank-related accidents due to non-compliance with this COBAC regulation. Instead of relying on banking regulations, banks should be able to rely on IT (Diard & Dufour, 2022b; Baker et al., 2017).

2.4. The theory of information technology capability: Information technology as a guarantee of effective internal control

Scholars carried out before and after the subprime financial crisis respectively by Flores et al. (2006) and Baker et al. (2017) insist on the urgency of having operational risk management IT (IT-RO). The IT capability perspective (Bharadwaj, 2000) is interesting here. This theory seeks to analyze the possible links between IT investments and organizational performance. IT capability is related to ability, the ability to mobilize and deploy IT-based resources in combination or conjunction with other resources (Bharadwaj, 2000). This capability includes tangible resources such as IT infrastructure, intangible resources such as knowledge, human resources to use and manage IT, customer orientation, and synergies between functions within the organization (Marchiori et al., 2022).

Indeed, strong IT capabilities improve firm performance (Zhang et al., 2023). Carter et al. (2012) studied the IT IC of 72 listed companies (including 36 companies that suffer from weak IC and 36 that have no IC problem). They find, using ordinary least squares (OLS), that firms’ IC failures are relative to their IT capability weaknesses. Chen et al. (2014) use IT capability theory to examine the effectiveness of the IC components defined by COSO. Their results show that the use of IT enables the reduction of IC costs, the limitation of control delays, the reporting of business risks, and the reduction of the controller’s risk premium. Deng et al. (2017) studied the link between information systems and IC in Chinese companies and found that companies with weaknesses in IC have weak IT capabilities. Cao et al. (2017) studied the relationship between the level of IT investment and IC of Chinese listed companies. They find that high investment promotes more effective IC, provided that IT is aligned with corporate strategy. Specifically, they conclude that IT strengthens one of the five COSO pillars, namely internal monitoring. Abbaszadeh et al. (2019) examine the relationship between IT and IC in Iranian state-owned enterprises. The authors show that IC IT promotes administrative, financial, and accounting control, and improves risk assessment, information, and communication, as well as control and monitoring activities. Mazza and Azzali (2018) examine the effect of IT on the IC of financial reporting in Italian companies. They find that IT promotes a compliant control framework, a better delineation of control scope, and a better allocation of control activities, which reduces risks and audit fees. Diard and Dufour (2022a, 2022b) carried out work on the relationship between IT and IC in a life insurance company, which conducts its business through numerous bank branches. The first article (Diard & Dufour, 2022a) finds that IC IT is part of a rationale of efficiency (minimisation of resources based on a risk-based approach) and control effectiveness (easier detection of risk). This is achieved by setting up an Information Risk Management unit, whose role is to analyse alerts on
employees’ outgoing and incoming emails, in conjunction with IT security software for incoming emails; daily monitoring of operator traces, with automatic analysis of suspicious transactions or recipients containing risk indicators (countries, high-risk customers, employees who have already been the subject of alerts), supplemented by a daily scan of vulnerabilities in tools and mailboxes; and software for blocking peripherals on employees’ computers, making it impossible to extract data using USB keys, with alerts generated in the event of an attempt. The second study (Diard & Dufour, 2022b) shows that fraud detection is stronger when technological tools are used for control. In the banking sector, FinTech innovation promotes risk control and improves operational performance (Li et al., 2022). Obaydin et al. (2023) study the effect of artificial intelligence (AI) on the effectiveness of IC, in this case on financial reporting processes. Although AI enhances data analysis and the quality of computerised reports, it does not control or mitigate human error (e.g., malpractice).

The extent of IT tools used in bank IC is documented by Wernz (2014). But still, it would be necessary that they make it possible to detect, well in advance, potential threats to bank security (Masciandaro et al., 2020). The concern is legitimized by the idea that operational risk can also be induced by IT. According to Maurer (2011), this is due to the increasing requirement for processing and transmission speed, intensive data management, ever-increasing trading volumes, increasingly heavy security constraints, as well as than ever-decreasing response times. In other words, the risk of technological drift consubstantial with the activity of banks is likely to hinder the effectiveness of their IC.

3. RESEARCH METHODOLOGY

In this title, we justify our research strategy and sampling method, data collection process, and analysis.

3.1. Methodology approach

The issue addressed in this article finds a strong interest in light of the resurgence of banking scandals. In Cameroon, the sector is made up of six banks, including two Western subsidiaries and their local counterparts. Recent studies on these banks indicate that Western subsidiaries hold technological advantages over African banks (Tioumagneng et al., 2020; Kenfang, 2020). Moreover, they come from territories where banking standards are the most advanced. These advantages, therefore, contribute to leaning towards a technological and regulatory “imbalance” between such subsidiaries and their counterparts, which imbalance is likely to weigh on the IC of the latter. Given the scarcity of work on the IC of banks in Africa, a qualitative study finds all its relevance. The strategy of the study of multiple cases of interpretative orientation (Yin, 2009) is used to apprehend a phenomenon as complex as IC. The selection of the sample is made by reasoned choice. The sample is made up of six banks, including two Western subsidiaries out of the four in operation, and four African banks out of 15.

Maintaining heterogeneity is relevant in that the activities of Western subsidiaries are mainly driven by regulations and IT (Buch, 2003). The sample is limited due to the opacity of the banking sector. In any case, it fulfills the Hiday Rispol (2002) criterion which requires in a multiple case strategy several cases varying from 2 to 6.

Intervention research is another interesting method for studying this issue. It involves long-term immersion in banks (around 1–2 years) to understand the different types of fraud that exist, the means used to control them, the control process, the players involved, the frequency of control, and the different results of the control. This is the method used by Diard and Dufour (2022b). This was done on a single case of a life insurance company, the one-year intervention contract having been signed between the company and the researchers. Unfortunately, access to the bank for long-term searches is still difficult to achieve.

3.2. The measuring instrument, the data collection, and analysis

The data for the study are primarily, collected during 2021. The interviewees consisted of six: two internal controllers, one internal auditor, and three risk management managers of banks established in the cities of Yaoundé and Douala (Table 1). For reasons of anonymity, we use the codes ICBSi (Internal Controller of the Subsidiary), ICABj (Internal Controller of the African Bank Subsidiary), IASBi (Internal Auditor of the Subsidiary), HRMABj (Head of Risk Management the African Bank). These cities were chosen because they house most of the banks’ headquarters. The qualitative approach followed by the study leads a fortiori to the interview guide as an instrument for collecting data. The interviews carried out last an average of 49 minutes and take place in the offices of the various managers.

<table>
<thead>
<tr>
<th>Table 1. Summary of managers interviewed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Banks</strong></td>
</tr>
<tr>
<td>Western subsidiaries</td>
</tr>
<tr>
<td>African banks</td>
</tr>
<tr>
<td><strong>Total</strong></td>
</tr>
</tbody>
</table>

Data are analyzed manually. The manual analysis consisted of studying the ideas of the participants, the words they use (lexical analysis), and the meaning they give to them (analysis of enunciation). It made it possible to classify the interview guide by theme. Thus, the speeches of the actors interviewed were transcribed, which made it possible to constitute verbatim around the obtained topics.

4. RESULTS

The results obtained show a substantial contribution of regulations to the effectiveness of IC. As for the role of IT, it is still difficult to understand, even if it should be noted that it is at the heart of the activities of all banks.
4.1. Banking regulations favourable to internal control

Bank subsidiaries are in phase with IC regulations that prevail within the banking sector in the CEMAC zone. It allows them to claim a better IC.

4.1.1. The effectiveness of internal control banking regulations within banks

Whether we are on the side of subsidiaries or local banks, there is no doubt that the COBAC R-2016/04 regulation has effectively come into force. The speeches of internal controllers, internal auditors, and risk management managers interviewed confirm this. They affirm that:

“Yes, the banking regulation obliges us to set up an IC. This is the COBAC regulation through the 2001 regulation on IC and the most recent, which is that of 2016. That of 2016, for example, organizes IC in terms of risk and performance” (ICSB, personal communication, November 2, 2021);

“Yes, there is a regulation that governs the implementation of IC, namely the COBAC R-2016/04 regulation” (ICAB, personal communication, November 3, 2021); “Of course, the COBAC is very strict on this. This is precisely the COBAC R-2016/04 regulation relating to the IC of credit institutions and financial holding companies” (IAB, personal communication, November 6, 2021); “There is a whole set of regulations on IC and risk. The new 2016 COBAC regulation also requires us to have an internal control system” (HRMAB, personal communication, November 25, 2021).

4.1.2. Regulations considered favourable to the control of operational risks

The new COBAC regulation of 2016 insists on the implementation of a control system that makes it possible to control the risks. These are precisely the conclusions of Jin et al. (2013). The main speeches obtained from the various players in the banks studied testify to the role of regulatory packages in controlling operational risks in these terms: “After the organization of internal control, it is necessary to map risks to detect the most likely to occur. The IC system makes it possible to control risks” (ICSB, personal communication, November 2, 2021); “I would say yes, we may have moved away from the regulations of the 2000s to those of 2016. This change in regulations promotes better internal control” (ICAB, personal communication, November 3, 2021);

“The COBAC R2016/04 regulation aims to optimize the internal control system of credit institutions with innovations in terms of the creation of new level 2 control units, namely the permanent control of operations, the control of compliance, accounting control and risk management. The regulations also give a right of scrutiny to the deliberative body” (HRMAB, personal communication, November 16, 2021);

“The new regulations drawn up by COBAC are full of a set of principles in terms of internal control and risk. The purpose of these regulations is to promote better internal control” (HRMAB, personal communication, November 10, 2021).

4.1.3. Requiring evolution to adapt to the context

Some shortcomings of the regulations on the IC appear from the speeches responding to three of the six executives. Their verbatim illustrate that:

“The problem with the COBAC regulation is that it is modelled on the Western model which still does not take into account the realities and the environment in which African banks operate, particularly local banks. However, this regulation promotes better internal control even if it does not hold” (ICSB, personal communication, November 2, 2021);

“The regulator must clarify the roles of internal control actors, especially in terms of skills, because for me, the roles are at the same skill level. Furthermore, I believe that the UEMOA framework is an example to follow in this direction” (ICAB, personal communication, November 3, 2021);

“I think that at this level the regulator should be more precise about the internal control procedures because they are not well defined” (HRMAB, personal communication, November 10, 2021). The standards decreed only by the executives of African banks make it possible to consolidate the idea that Western subsidiaries enjoy a regulatory framework in phase with that applied in the country of origin. The standards that prevail in these territories are mainly inspired by the Basel rules from which the COBAC regulations are developed.

4.2. A mixed effect of information technology on the effectiveness of internal control

If IT is of undeniable utility for banks, this utility does not seem to be observed in IC. They are indeed used in day-to-day banking operations, without there being any question of a specific CI technology in the sense of Flores et al. (2006) or Baker et al. (2017). This importance is reflected in these terms: “They are very useful as survey and evaluation tools” (ICSB, personal communication, November 2, 2021);

“We must try to appropriate ICTs so that our activity is increasing[ better]” (IAB, personal communication, November 6, 2021); and “ICTs come more as a support in the management of operations” (ICAB, personal communication, November 3, 2021);

“Be automated to minimize possible risks at checkout level” (HRMAB, personal communication, November 25, 2021); “It enables risk to be managed at the level of the collection aspect” (HRMAB, personal communication, November 16, 2021); “In risk management, the bank depends on ICT” (HRMAB, personal communication, November 10, 2021).

However, the results support Maurer’s (2011) thesis that banks’ IT is likely to promote operational risks. This is illustrated by the following remarks collected from the risk managers of local banks:

“I want to say yes that ICTs carry risk but here everything will depend on the type of risk” (ICAB, personal communication, November 3, 2021); “They constitute a risk for the management of operations” (IAB, personal communication, November 6, 2021);

“ICTs carry computer risk, they are risky and we are in an environment where technology is scary” (ICAB, personal communication, November 3, 2021); “ICTs are mixed because their control is divine” (HRMAB, personal communication, November 23, 2021); “Ifs are complex, they are very mixed, they bring other
5. DISCUSSIONS

While research on IC in the African context focuses on the governance system at work (Tchuiendem et al., 2023), banks are called upon to comply with IC regulations and invest in IT. It is in this logic that it is possible to consider regulations and IT as important tools for banking IC. While the proliferation of CI standards is at the root of banking malfunctions, the banks sampled find them conducive to risk management. Above all, the study reveals subsidiaries that comply with sub-regional IC regulations. The comparative study makes sense insofar as the institutional distance of foreign subsidiaries from the parent company is supposed to make their IC difficult (Lamarque, 2017). The distance is likely to be particularly great between the head office and subsidiaries operating in poor countries (Detragiache et al., 2008). However, the study shows that the host countries’ banking regulations are a vector for the good internal management of subsidiaries, in the sense of (Kouretas & Tsoumas, 2016). Conversely, the complaints voiced by African bank executives about standards modelled on Western models provide an opportunity to recall that they are also echoed in the work of Akume and Annicet (2017). These results contradict many other studies that believe that the regulatory context in Africa is unfavourable to subsidiaries of Western banks (Ofori-Sasu et al., 2023; Ozili, 2019).

The technological aspect is also interesting given the abuses that are mainly reported within local banks. It is of definite use to all banks, even if it is not obvious to employees that it is at the heart of operational risk management. Indeed, most respondents refer to ATMs when asked to name an operational risk management technology within their bank. The justification certainly lies in the increasing complexity of banking IT (Ahouantchédé, 2015) or in the existence of a plethora of operational risks (Maurer, 2011) which, to be mastered, requires the development of dynamic capabilities, articulating sensing, seizing and transforming (Teece et al., 1997). However, the study was unable to confirm the technological advantages of subsidiaries in terms of IC. In any case, they confirm that they are more effective than national banks in developing countries (Berger, 2007).

To better understand bank IC, Diard and Dufour (2022b) recommend knowing who controls, what the control processes are, and when the control takes place. Knowing what is controlled and the attitude of the controller towards the areas controlled.

The study makes a theoretical contribution to the work of Baker et al. (2017) and Diard and Dufour (2022a, 2022b) on fraud management, particularly in regulated sectors such as financial services, which are considered to be more exposed to this risk. In addition, most research uses the resource-based view (RBV) to study the technological aspect of an organizational environment. This research seeks to show that banks need to consider that mastering IT is a continuous learning process. According to the theory of dynamic capabilities, they must develop their skills as technologies evolve and become more complex. The regulator should follow the banks in their process of compliance with the regulations, and give them time (Ofori-Sasu et al., 2023) because so far, the regulations do not allow financial institutions to perform well (Akume & Annicet, 2017).

6. CONCLUSION

The objective of the article was to investigate the contribution of regulation and IT to the effectiveness of IC in banks. The interest in such a study was justified by multiple factors, including repeated banking scandals, the diversity of origins of banks, and the scarcity of debate in the African context. The results obtained from the investigations give a place of choice to banking regulation. According to the actors, the regulation erected by the COBAC in 2016 is of great use, even if it needs to be adjusted. ITs, on the other hand, were mixed on concerns specific to IC.

The results of our study make it possible to invite all banks to increase their compliance with IC regulations. Following the studies cited at length in this article, we recommend that they invest in IT from IC to protect themselves from possible losses linked to the occurrence of operational risks. These include lawful and appropriate technologies (Diard & Dufour, 2022b). It is also an opportunity to challenge regulators on the urgency of “adapting” the standards formerly launched by Avom (2015), without this being done as “catching up with the Western model”. In this logic, they should tackle the definition of the skills of each of the actors of the IC.

There are many limitations to this research. Firstly, the sample could have been extended if the banking sector had been more open to the research. It should be noted that there are 17 banks in the banking sector. It would have been more interesting to work on all the banks. Secondly, an intervention research approach with an immersion at the time when the IC took place would have allowed us to experience the reality of IC in a banking environment. Finally, it would also have been relevant to understand the resources mobilized for each type of control (detective or preventive, for example). These are the shortcomings that could help future research. We could also examine whether it is possible to build an IC approach that suits banks according to their origins.

REFERENCES


Kenfwa, W. L. (2020). L’efficacité du système d’information organisationnel de la banque au Cameroun [The effectiveness of the organizational information system of the bank in Cameroon] [Doctoral dissertation, Université de Yaoundé II].


