Re-thinking de-risking: a systems theoretical approach

<table>
<thead>
<tr>
<th>Journal:</th>
<th>Journal of Money Laundering Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manuscript ID:</td>
<td>JMLC-04-2021-0030</td>
</tr>
<tr>
<td>Manuscript Type:</td>
<td>Scholarly Article</td>
</tr>
<tr>
<td>Keywords:</td>
<td>money laundering, Niklas Luhmann, systems theory, decision, risk, danger</td>
</tr>
</tbody>
</table>

SCHOLARONE™ Manuscripts
Re-thinking de-risking: 
a systems theoretical approach

Abstract

Purpose – The paper seeks to explain the de-risking phenomenon through Luhmann’s risk/danger model and demonstrate that de-risking should be facilitated and encouraged.

Design/methodology/approach - The paper applies Luhmann’s system theory and more specifically his risk/danger model in order to describe the de-risking phenomenon and identify recommendations to address its consequences.

Findings – The paper finds that re-defining risk and the AML’s community’s understanding of it can support key stakeholders’ understanding of ML risk and the way to better address consequences of AML decisions.

Practical implications – The paper has implications for the banking and regulatory community in relation to the interpretation of de-risking. As systems aim to minimize their exposure to risk, they should not be prevented from de-risking.

Originality/Value - This paper aims to move away from a narrative description of AML phenomena and presents a theoretical foundation for the analysis of ML risk. The current response to de-risking which demonises it and aims to prevent it is deconstructed through this theoretical lens.

Keywords - money laundering, Niklas Luhmann, systems theory, decision, risk, danger

Paper type – Conceptual paper
INTRODUCTION

The domain of Anti-Money Laundering (AML) has seen a number of key transitions in relation to how the risks associated with Money Laundering (ML) have been handled. In the rules-based approach, ML-risk was managed through fixed sets of constructed indicators (Ross and Hannan, 2007). In the transition to the risk-based approach (RBA) (FATF, 2007), a more malleable and flexible path was sought, with risk sensitivity and a cluster of additional risk-related concepts being introduced to allow institutions to express their personalised and customised risks. These have allowed risk prioritisations and customisations for financial institutions and other Designated Non-Financial Businesses and Professions (DNFBPs). However, this malleability has also led to the emergence of ambiguity, with de-risking as the pinnacle of such perceived unintended consequences. Since then, de-risking in AML has been vilified and seen as a misunderstanding of the RBA, the refusal to apply it and, increasingly, the realization that the RBA may essentially imply a de-risking approach. Admittedly, some well-founded objections to de-risking included the possible push of laundered funds into alternative underground remittance systems and less-monitored routes (Ramachandran, Colin and Juden, 2018). But overall, is this attitude towards de-risking an accurate reflection of the complexities of risk? With the entanglement of the risk-based approach and de-risking, the concept of risk has come to occupy a central stage in our field. But how well do we understand risk to begin with? How can we explore AML risk and its broader fabric of interferences?

This paper aims to deconstruct the nature of risk within the domain of AML and explore how different stakeholders observe and manage ML risk, thereby impacting the risk management initiatives of each other. A greater insight into the nature of AML risk will give us the tools to a) understand the key drivers of de-risking, b) enhance risk management approaches to handle de-risking, and c) consider the systemic character of risk in the domain of ML prevention efforts. It is in this context that this paper seeks to dissolve one of the most recent contemporary myths in the domain of AML: the myth that de-risking can be, and more importantly, should be prevented. Following the review of related work in the next section, the paper takes a systems theoretical treatment of risk that is based on the work of sociologist and systems theorist, Niklas Luhmann. Based on the insights drawn from applying Luhmann’s work into Barclays bank’s handling of High-Net-Worth Individuals and an illustrative case of its de-risking of Money Services Business (MSB) Dahabshiil, the paper posits that de-risking should
not be demonised and should be viewed instead as an essential element within the broader nexus of risk-based management and governance of ML risk.

RELATED WORK

Current literature on the domain of ML risk, de-risking and risk appetite, fails to develop theoretical foundations or frameworks through which AML risk can be reflected upon. Such frameworks should not only be integrative of the challenges faced by risk practitioners across various financial institutions but should also capture the perspectives of Financial Intelligence Units or regulatory bodies. Current scholarly or industry work relating to AML is either anecdotal or descriptive on risk, with key strands revolving around ML typologies (Menz, 2019), regulation (Rose, 2019), or the wider financial and economic consequences of de-risking (Ramachandran et al, 2018). Such work is useful in informing both practitioners and academics of latest risk-related developments and in reflecting on regulators’ and obliged entities’ initiatives as well as internal processes (Naheem, 2020). However, more theoretical work is required so that we can approach the foundational conditions upon which AML risk is expressed. Without challenging the foundations of risk in AML, it is difficult to maintain an informed debate around what the future of the RBA should be.

Although there has been an increase in the ML-risk related narratives observed over the past 30 years (Hutter, 2005; Le Bouter, 2014; Wildavsky, 1979), with AML regulation following suit and becoming risk-based, ML risk and risk appetite has not been “conceptualised and analysed in much more concrete terms than in the past” (Ross and Hannan, 2007, p.113). Discussion in current academic and industry literature on the actual nature of ML risk is disappointingly sparse (Artingstall et al., 2016). Ultimately, ML risk and its key attributes need to be understood and the RBA simply does not provide the tools to achieve this.

For instance, the published FATF guidance on the RBA (FATF, 2014) mentions risk appetite just twice and does not provide guidance as to how an institution could or should articulate it. Furthermore, the FATF statement concerning ML risk appetite is not specific: “supervisors have to take steps to check that their staff are equipped to assess whether a bank’s policies, procedures and controls are appropriate in view of the risks identified through the risk assessment, and its risk appetite” (FATF, 2014, p. 15). Similarly, financial institutions’ remarks regarding ML risk appetite are vague. Financial institutions’ “risk appetite statements often
contain broad definitions of acceptable risk, such as minimal tolerance for residual Financial Crime risk” (Artingstall et al., 2016, p. 8). In addition, research on de-risking sponsored by the Financial Conduct Authority states: “we find that ML/TF risk appetite is difficult to articulate and measure, perhaps unsurprisingly. Banks are still developing this art and in particular find it difficult to ‘price’ (in broad terms) ML/TF risk” (Artingstall et al., 2016, p.23).

In summary, there exists no explicit ML risk appetite documentation nor official communication between financial institutions and regulators as to their respective risk appetites. This must be differentiated sharply from the risk-based applications of typologies where the categories of ML/TF entity-based suspicion are expressed. For example, by relying on the RBA, a financial institution would recognise the categories of ML risk that it considers as high-risk (PEPs, Cash-Based Institutions, etc) but this articulation suffers from two contingencies: a) it results in the paradox of the risk-based approach as each category requires further differentiation (Demetis, 2009) wherein we can have a Politically Exposed Person (PEP) automatically classified as high risk as per FATF recommendations but subsequently assigned a high PEP risk or a low PEP risk, ultimately undermining the ‘umbrella’ classifications of the RBA to begin with, and b) it remains unlinked to the risk appetite of the institution.

The phenomenon of de-risking is particularly illustrative of the way the RBA fails to accommodate institutions’ risk appetite as well as risk’s systemic nature. Although de-risking is the empirical manifestation of financial institutions’ appetite to risk, de-risking is currently narrowly defined as “the phenomenon of financial institutions terminating or restricting business relationships with clients or categories of clients to avoid, rather than manage, risk in line with the FATF’s risk-based approach” (FATF, 2014, para. 1). It has had unfortunate repercussions such as, for example, “reducing the flow of remittance to developing countries” (Ramachandran, et al., 2018, p. 250) and making such flows less transparent by being pushed into Hawala networks which are not easily regulated. How did we come to this position? How did the application of the risk-based approach lead to de-risking?

Although there are a number of drivers of de-risking (declining client profitability, increased compliance costs, increased regulatory and reputational risks), one of de-risking’s key drivers is the application of the RBA itself. This can be traced back to the FATF and how it has encouraged institutions to develop risk assessment tools, identify high-risk clients and
implement initiatives to mitigate high risks. Annex III of the fourth AML directive goes as far as to list correspondent banks and money transfer businesses as high-risk clients as if the category within which they belong, automatically makes them a high-risk entity. This paradox of the risk-based approach and the denial that - within each category - there is a myriad of other characteristics, attributes, proxies, that can reduce/increase the individual risk for each entity has only attenuated the problems. Behind the denial of this paradox lays the belief that risk is an objective construct which can be dissected, measured and deployed in AML. However, all the problems that institutions are experiencing when applying the RBA is proof, if needed, that risk is a subjective and an observer-relative construct. Consequently, categorisations like “money transfer businesses are high-risk clients” are both ontologically and epistemologically absurd. Alas, they are convenient for institutions that handle millions of transactions from such customers and they try to reduce their complexity en masse when needed.

The ever-increasing focus on AML and CFT within a risk-based regulatory environment has essentially developed a culture that can only aspire to de-risking (Rose, 2019). And yet, the FATF and supervisory authorities assume that de-risking is risk avoidance instead of risk governance and management. They fail to see that the majority of financial institutions that terminate certain relationships aim to reduce the complexity they face after having assessed, through the RBA, that ML risk is a composite of many elements and parameters that are interdependent. On such occasions, de-risking is a decision made by a financial institution to communicate its new risk appetite and regulate its exposure to ML risks.

The concept that de-risking is a form of risk governance and management is re-inforced by the FCA report on de-risking (Artingstall et al., 2016). This report highlights that both FATF and FCA statements on “wholesale cutting loose of entire classes of customers” (FATF, 2015) and “banks dealing generically with whole categories of customers or potential customers” (FCA, 2015) are frustrating to banks. “A bank’s decision on risk assessment may be the same whether it is undertaken on a case by case basis or wholesale basis, because the factors applied will not vary too much” (Artingstall et al., 2016, p. 19). “Risk assessments will score similar customers in similar ways. A set of similar customers will fall outside the FIs’ risk appetite and thus be exited” (Artingstall et al., 2016, p. 24). Regulators should be cognisant of this fact. Far from being a phenomenon that should be demonised and prevented at all costs, de-risking should be accepted and, as subsequently argued, facilitated and incentivised. Consequences associated with de-risking can be avoided by acknowledging the systemic nature of risk and implementing
recommendations that aim to counter-balance the impact of de-risking initiatives. Under certain circumstances, consequences like having financial access difficulties, can be detrimental to other institutions or entities as documented in current literature (Buckley and Ooi, 2014; Oxfam, 2013; Ramachandran et al., 2018). This is further explored in the following section.

Another weakness of the RBA is how it fails to capture the differences in risks faced by financial institutions and regulators and the dynamic feedback loop between those risks, again highlighting the wider issue raised by Ross and Hannan (2007) and Demetis and Angell (2007) on the “complexity of representing risk” (p. 426). Certainly, both financial institutions and regulators are required to manage and minimise ML risks through the RBA. However, while financial institutions must focus on managing regulatory risk (defined as risk of changes to regulation or misalignment of regulatory interpretation), regulators face another kind of risk, namely the risk of losing their credibility. For instance, Black and Baldwin highlight the challenges faced by regulators when applying the RBA:

“Risk-based regulators have to address a number of issues including: the risks they will identify as requiring attention; the indicators and methods they will use to assess those risks; where they will prioritise their attention and where they will not. They will also have to decide how the implementation of the risk-based framework will be managed; how it will be justified and communicated both internally and externally; how they will respond to changes and, ultimately, what level of risk or failure they are prepared to accept” (2012, p. 2).

Hence, should ML scandals arise, regulatory bodies need to be able to justify their previous and current decisions as well as actions in order to preserve their credibility. Press releases and reports issued by the Estonian and Danish regulators in the aftermath of the Danske Bank scandal, for example, certainly offer an excellent illustration of this point.

The incongruence between how the RBA implementation is expressed and how the risk appetite of a financial institution could be articulated is further illustrated by the lack of methods to quantify ML risk. Efforts to perform these tend to go through the application of the Risk Based Approach which is, right now, the only widely available method to evaluate ML risk. The RBA methodology aims to split ML risk into a set of pre-identified risk categories such as “country or geographic risk, customer risk, and product/services risk and the application of these risk categories is intended to provide a strategy for managing the potential risks” (FATF, 2007, p. 22). However, we find that this reductionist approach, while useful in observing individual risk categories, fails to identify and account for the interconnectedness
and the systemic character of risk (Ackerman, Eden, Williams and Howick, 2007). Unlike other phenomena, risk feeds off itself, generating further risk that ripples across institutions in a dynamic way. For example, as of March 2021, the impact and consequences of the decisions made by Danske Bank Estonia to onboard high-risk non-resident customers in 2007 are still being felt, despite the fact that the non-resident portfolio was closed in 2015. In late January 2020, the Danish Business Authority, Denmark’s business watchdog, announced that two Ernst and Young auditors were being brought before the Danish Disciplinary Board of Auditors for failing to meet auditing standards when providing services for Danske Bank in 2014. Similarly, a group of institutional investors are launching a EUR 358 million lawsuit against Thomas Borgen (ex-Danske CEO) for misleading investors (Monroe, 2020). In addition, the September 2020 FinCEN files leak indicates that Danske Bank Lithuania may also have weaknesses in its AML controls as well as the fact that Danske Bank had links to drug trafficking gang ‘The Brothers’ circle’, money-launderer Altaf Khanani, and was involved in mirror trading (ICIJ, 2020). Thus, six years on, the scandal continues to reverberate beyond what classical AML methods would have assessed and predicted since risk feeds off itself and cannot be ringfenced within one institution, nor jurisdiction, nor a specific point in time.

This complex set of risk related elements that propagate from one institution to another, point to feedback and systemic irritations that cannot be accounted for by the current AML framework; the current deconstruction of ML risk into sub-risks using the risk-based approach, ignores the systemic nature of ML risk (Demetis and Angell, 2007). In their attempts to deconstruct risk, some obliged entities have created additional prisms through which to observe ML risk—namely, regulatory risk, reputational risk, market risk, correspondent banking risk, risk of poorly integrated IT systems, failed internal AML procedures, staff complacency and internal collusion—which have been superimposed onto the traditional categories documented in the FATF’s risk-based approach guidance. This condition is telling of risk and underscores a deep epistemological delusion whereby the conversion of risk as a subjective, sociotechnical construct is attempted into a quantifiable reality that can be acted upon. German Sociologist Niklas Luhmann describes this process as ‘scientization’. “The process of ‘scientization’ reflects a method through which humans mistakenly identify social constructions as naturally occurring phenomena” (Russell and Brabow, 2011, p. 244). Attempts to understand risk solely through a predictable, automated methodology can actually be counterproductive. For example, if a low risk customer performs a transaction to a high risk jurisdiction, the
scientization of risk scores confuses the process. The transaction may be high risk but the customer is not. In sum, in spite of its burdensome complexity, such a tool may flag cases too broadly to be useful. One instance where this can be observed is in the application of transaction monitoring software, where the scientisation of risk generates false positives (Demetis, 2019). This hinders AML efforts, creating further dangers that require internalisation.

Attempts to capture ML risk through an ever-expanding list of risk categories, evolve when knowledge about new (sub)categories of ML-risks emerges through the latest ML scandal or accumulated via AML reporting routes (e.g. FATF typology reports). Such attempts indicate that ML risk has no boundaries, travels across a multitude of environments and systems and is thus observable to fraud risk specialists, operational risk practitioners, journalists, investors, shareholders, the media, laypeople, etc. Thus, ML risk evolves through the eyes of multiple observers and environments, creating further risk and enhancing ML risk’s interconnectedness.

Given the systemic characteristics of risk and the gap in the industry’s current approach in dealing with ML, we adopt a systemic view of risk in the tradition of second order cybernetics (Von Foerster, 1981; Luhmann, 1993). By doing so, we attempt to approach the foundations of risk as a social construction and relate systemic risk to the challenges faced within the domain of AML. This theoretical approach can allow us to reflect on the structure of its propagation from one system to another and the wider consequences of risk. In order to provide a systemic framework within which to understand and analyse ML risk, a brief introduction to Luhmann’s Systems Theory is offered below with an emphasis on risk (Luhmann, 1993). The concepts described will be subsequently applied onto AML phenomena and we shall use an illustrative case from Barclays bank’s de-risking of Money Services Businesses (MSBs) in order to explain why de-risking should be accepted, facilitated and incentivised.

THEORETICAL APPROACH THROUGH LUHMANN’S RISK FRAMEWORK

Luhmann’s theoretical framework is based on a multiplicity of disciplines, including biology (Maturana and Varela, 1980), mathematics (Spencer-Brown, 1969), sociology, (Parsons, 1951) and cybernetics (Ashby, 1957; Bertalanffy, 1968; von Foerster, 1974, 1981). Indeed, “Luhmann sees the nucleus of cybernetic thought in the notion that a system whose operations are oriented on the fulfilment of certain purposes will orient its behaviour on a constant feedback from the environment and can therefore cope with a high, unknown level of
complexity” (Paetau, 2013, p. 79). Financial institutions, insofar as they are dealing with a web of ML typologies, compliance-oriented challenges, and the unavoidable ambiguities of RBA’s interpretation, face similar levels of complexity, both within their own systems, and in their respective environments. As argued by Borsch (2011), it is precisely this multidisciplinary approach within systems theory that enables Luhmann to develop a grand theory successfully. As the field of AML itself draws from different disciplines in its attempts to tackle ML, a more general theoretical approach can allow us to identify the wider transitions that occur within our field. Luhmann’s insights on risk can thus be applied to the RBA.

Following a long tradition of systems theorists, Luhmann observes the world as systems and environments. A system is distinct from its environment, and since the environment is not a system, it does not have the same capabilities as the system (Luhmann, 1995a). Furthermore, a system cannot exist without being separated from its environment. If the distinction between a system and its environment is not made, “if everything blends into everything else and no clear boundaries can be established, then no system exists” (Borsch, 2011, p. 21). Thus, for any given system, the system is “nothing but the difference to its environment” (Luhmann, 2002, p. 66).

For Luhmann, systems have their own functions and system formation is the key feature of modern society. As such, the system is Luhmann’s essential starting point and the starting point of any system’s theoretical analysis. However, the function of the system is, simply, that of differentiation (or distinction) between system and environment for the purpose of minimising the complexity of the environment. Indeed, “the social world comprises enormous complexity which social systems each, in their own way, reduce” (Borsch, 2011, p. 7).

The following diagram conceptualises the system and its environment:

![Figure 1: System, Environment and Boundary](image-url)
The difference between system and environment can only be delineated by the observing entity marking the boundaries between system and environment.

Therefore, “the definition of a system, indeed any definition for that matter, is above all an act of choice and an observer-relative act. The observer is crucial in the construction of any system” (Demetis, 2010, p. 42). Depending on what the observer is focusing on (e.g. an AML transaction monitoring system, or the system of the Egmont group), a system can be anything ranging from a human organism, society, a financial institution, or a financial intelligence unit, among countless other entities. It can be anything the observer conceives of as a system.

While the environment is more complex than the system because it has more options, variety, and degrees of freedom, the system compensates for its ‘inferiority’ by eliminating or introducing degrees of freedom. For instance, referring back to Figure 1, if the system is a financial institution and the ruling government (i.e. another system within the environment) were to announce further economic and financial sanctions against Russia, the system might decide to no longer bank with Russian nationals in order to avoid sanction breaches and regulatory fines. Now that system and environment have been introduced, risk according to Luhmann can be discussed.

To Luhmann, risk is not ontologically real but instead, it is a social construction. As he mentions:

“The already familiar discussions on risk calculations, risk perceptions, risk assessment and risk acceptance are now joined by the issue of selecting the risks to be selected or ignored. And once again, discipline specific research can reveal that this is not a matter of chance but that demonstrable social factors control the selection process” (Luhmann, 1993, p.4).

Luhmann’s work on risk operationalises a key distinction: that between risk and danger. The key difference between risk and danger is that of attribution: the difference is determined by the observer. In short, a decision maker will observe the consequence of his decision as a risk that he has decided to internalise while the non-decision maker (i.e. the affected party) will observe the consequence of someone’s decision as a danger emanating from its environment. Nevertheless, both the affected party and the decision maker observe the same phenomenon, albeit with an observer-relative sensitivity towards its interpretation in the duality between risk/danger. Thus, both risk and danger are manifestations of the same phenomenon observed by different observers. The fundamental point to consider, however, is that the distinction
between risk and danger does not hinge on certainty or safety but on attribution: risk is attributed to the system’s decisions while danger is attributed to the environment. Risk is “the possibility of future damage, exceeding all reasonable costs, that is attributed to a decision” (Luhmann, 1990, p. 225) while “danger is a possible loss considered to have been caused externally” (Luhmann, 1993, p. 22). However, from the perspective of an individual who did not make the decision or accept the associated risks, the possibility of a loss is perceived as a danger that is caused by an external force. Thus, even though a decision may be made as part of a democratic process, the possibility of loss or damage is not voluntarily accepted by all potentially affected parties through the decision making process. As Luhmann discusses:

“Decisions are always the decisions of somebody, not the decisions of everybody. Therefore the real dangers in modern society are the decisions of others. Almost all other dangers, including natural disasters, can be avoided, for instance by moving out of a region threatened by storms or earthquakes and settling elsewhere. But the danger that results from the decisions of others cannot be avoided because others are everywhere” (Luhmann, 1990, p. 226).

The 2008 financial crisis illustrates this point. Senior management and shareholders of the big financial institutions that were deemed “too big to fail” (Sorkin, 2009), perceived the possibility of a financial crisis as a risk while taxpayers perceived it, and ultimately experienced it, as a danger. However, the 2008 crisis also showed that decision-makers - such as Lehmann Brothers, Merrill Lynch or Freddie Mac and Fannie Mae - became affected parties too. The danger such financial institutions generated through their very own decision-making was so great, that their environment (i.e. governments and regulators) had to internalise it as risk. This generated further danger to the initial decision makers who therefore became victims.

Overall, on the basis of the few concepts described above (e.g. system/environment, risk/danger), we illustrate Luhmann’s risk model in figure 2. There are two separate systems (System A that makes the decision and System B that is the affected party or the victim) and describe the basic principles of the model right after with an example.
We take System A here to be a financial institution. Danger (e.g. a customer that may be actively looking to launder money or simply a high risk Politically Exposed Person (PEP) or a High Net Worth customer) originates from the environment and irritates system A. If the financial institution (i.e. System A) makes the decision to internalise the danger (e.g. accept a high-risk client which may expose the institution to ML risk and/or regulatory scrutiny) then System A will *internalise danger into risk* and reap any associated rewards (e.g. high commission rates on future transactions). Thus, once internalised, the danger becomes a risk for System A.

However, decisions made by the financial institution to internalise dangers and convert them into risks will also produce *second order dangers* which are external to the financial institution (System A) and impact other systems such as System B. For instance, an institution’s decisions to consistently onboard high risk customers may expose the jurisdiction it is based in, the wider regulatory environment and the regulator to the danger of higher exposure to ML. In figure 2, System B is the regulator who faces the danger that results from System A’s decision.

To a second order observer, the risk/danger distinction changes depending on who the first observer is (i.e. System A or B). Consequently, risk is also an observer-relative construct. In summary, decision makers generate risks and victims, who are not involved in the decision making process, face the associated dangers.
To provide an empirical illustration of Figure 2, we refer to the 2015 Barclays bank case resulting in a GBP 72 million fine. In 2011 and 2012, Barclays executed a series of transactions amounting to GBP 1.88 billion on behalf of ultrahigh-net-worth (HNW) clients that were Politically Exposed Persons (PEPs) (Financial Conduct Authority [FCA], 2015). In order to take on the clients as quickly as possible and to generate GBP 52.3 million in revenue, Barclays decided not to apply its own standard procedures, consisting in performing enhanced Customer Due Diligence (CDD) as required by the RBA. The identity of the clients was so sensitive that the bank agreed to pay them GBP 37.7 million should their names ever be revealed. In November 2015, the FCA (the UK regulator), fined Barclays GBP 72 million. At the time, the FCA made the following statement: “While we make no finding that the transaction involved financial crime, the circumstances of the transaction gave rise to a number of features which indicated a higher level of risk. This required Barclays to adhere to a higher level of due skill, care and diligence but Barclays did not follow its standard procedures” (FCA, 2015). In addition, the FCA made the following statement:

“Barclays failed to follow its own standard procedures, failed to implement any adequate alternative procedures, and failed to have sufficient regard to the JMLSG Guidance and other relevant guidance in issue during the relevant period. Barclays focused on its objective of entering into the business relationship and executing the transaction quickly and on the exceptional confidentiality restrictions in place, rather than on the importance of completing the EDD required and making a careful and considered assessment of the potential financial crime risks” (FCA, 2015, p. 22).

Ultimately, Barclays is a financial institution driven by revenue, profits and shareholder approval. The following extract from the FCA report documenting the circumstances leading to the fine, points to that direction as:

“On the basis of the EDD information available to it at that time (which, as outlined in paragraphs 4.32 to 4.47 below, was inadequate) Legal and Compliance did confirm that the appropriate level of EDD had been conducted, including that the PEPs had been properly identified, and that the Clients’ sources of wealth were legitimate. This was not compliant with Barclays’ usual procedures that required the front office to give this confirmation. In addition, Legal and Compliance did not have the benefit of the knowledge held by front office senior management about the Business Relationship and a number of relevant issues that had emerged during negotiations between the Clients and senior management” (FCA, 2015, p. 16).

The compliance subsystem could be interpreted as having had to ‘surrender’ to the greater will of the sales subsystem while the goal seeking behaviour of the entire system was oriented towards securing the deal.
In the figure below, Figure 3, we illustrate Barclays’ 2015 AML fine by applying the basic risk/danger skeleton of Figure 2. Barclays bank is represented as system A, system B can be society or the regulator for instance. System A’s decision not to apply enhanced due diligence in order to quickly onboard the HNW PEP clients, perform the GBP 1.88 billion transaction and secure GBP 52 million in revenue may result in a potential fine which is the risk that the front office has decided to internalise. The regulator is the victim who, not having been part of the decision making process, sees the onboarding of ultrahigh-net-worth clients that are PEPs and the execution of GBP 1.88 billion transaction as ML danger to its jurisdiction.

![Figure 3: Analysis of Barclays Bank 2015 fine through Luhmann’s risk/danger model](image)

At this point, the key building blocks of Luhmann’s systems theory should be clear: When stimuli from the environment (e.g. ultra HNW PEPs that want to be onboarded) is considered by system A (i.e. Barclays bank in our case), the decision to execute a transaction is brokered through internalising the danger that HNW PEPs’ transactions may violate AML regulation and weaken the financial system. To the decision-maker (Barclays bank), the consequence of risk-taking is the reward (GBP 52 million in revenue), and the risk is receiving a financial fine (a GBP 72 million fine on this occasion). To the victim (the regulator), the danger is a breach
of regulation, a threat to the confidence in the financial system and/or a failure to adequately manage and prevent financial crime in the UK.

The relevance of Luhmann’s work on risk and the risk/danger distinction has been illustrated through Barclays Bank’s 2015 regulatory fine. To demonstrate the versatility of Luhmann’s theoretical framework for exploring and understanding the AML domain, we will now apply Luhmann’s risk/danger model to the de-risking phenomenon.

DE-RISKING, RE-RISKING AND BARCLAYS’ ILLUSTRATIVE CASE

The FCA defines de-risking as banks removing “bank accounts/services from customers or other relationships which they associate with higher money laundering risk. It has been attributed to the increasing overall cost of complying with regulatory requirements” (Artingstall et al., 2016, p. 5). The belief is that de-risking is performed in a wholesale manner with banks unwilling to truly assess the risk associated with such customers.

When considered through Luhmann’s risk/danger model, de-risking describes a phenomenon whereby financial institutions no longer wish to maintain risks in exchange for potential rewards. They therefore seek to externalise those risks they maintain internally, remove them from their own systems and feed them back into the their respective environments; in the process, they will therefore convert risk back into danger. De-risking arises for a multitude of reasons: declining client profitability, increased compliance costs, increased regulatory and reputational risks (Ramachandran, et al., 2018), but is essentially driven by the decision-making system aiming to minimise the complexity it faces. When too many decision-making systems externalise their risks, while at the same time, other systems in their respective environments are not willing to internalise the corresponding dangers then an accumulation of danger emerges in a particular category (e.g. money service businesses). In this regard, we can articulate the systemic definition of de-risking as a state of ‘suspended dangers’ that are not internalised by systems.

One side-effect of de-risking is that it may reduce visibility of such ‘suspended dangers’ and either push ML into smaller institutions that lack the resources and expertise needed to manage high-risk clients. Furthermore, it could also push ML and terrorist financing into financial mechanisms, such as alternative remittance systems, that exist outside of regulatory scrutiny.
In addition, de-risking can exclude legitimate businesses and consumers from the financial system, which can have negative effects on a country’s economic and social development. Finally, such dangers can threaten the credibility of regulators should the latter fail to address them (Grima et al., 2020; Ramachandran et al., 2018; Rose, 2019). To regulators, de-risking clearly represents a danger, as it “may drive financial transactions underground which creates financial exclusion and reduces transparency, thereby increasing money laundering and terrorist financing risks” (FATF, 2015). This concern is also expressed by the FCA which states: “we require banks to put in place and maintain policies and procedures to identify, assess and manage money-laundering risk. This requires banks to use an effective risk-based approach” (FCA, 2015). Thus, when a financial institution transforms a danger “that was formerly seen as external into processable and manageable activities” (Renn, 2004, p. 103), its decision generates (second-order) danger for entities that neither took part in the decision making process nor benefited from the decision. In this case then, such entities can be the regulators and the de-risked customers that are the victims of the de-risking process. The regulator has to handle such danger one way or another. The issue, however is that the regulator, as a system, communicates and responds through regulation. For instance, if there is a critical mass of financial institutions and banks that no longer wish to internalise dangers in exchange of potential rewards, there will be a high volume of danger that will require internalisation. The regulator will want to incentivise systems to internalise such danger and will need to do so through regulation.

In sum, by de-risking their own systems, financial institutions create irritations for regulators. However, while financial institutions can produce irritations for regulators, they cannot steer regulators’ responses to these irritations; responses are determined by the regulator itself. In the UK, for example, regulators threatened to fine financial institutions that could not provide robust rationale for de-risking activities. Systemically, such an approach essentially discourages financial institutions from externalising danger and aims to incentivise institutions to maintain risk within their systems. This approach, however, imposes a level of complexity that financial institutions will not or cannot handle. Placing obstacles to de-risking will have its own unintended consequences. The irony in this context is that essentially de-risking is the result of the application of the risk-based approach. However, if regulators attempt to prevent the application of the FATF’s recommendations, institutions may start “seeking much more specific guidance on managing high-risk relationships of the types that have led to account exit” (Artingstall et al., 2016, p. 70) possibly demanding the introduction of prescriptive
regulation in order to obtain legal safe harbour for instance. It is the management of this dynamic that is now at stake. Figure 4 below presents how the risk/danger distinction is operationalised in the context of de-risking.

In Figure 4, the top box represents danger (1). As discussed, it is believed that de-risking is a response to an increased cost of compliance, increased regulatory scrutiny, regulatory fines and liability. Because of dangers associated with certain customers judged as representing higher ML risks, the financial institution (System C) makes the decision to de-risk (2) and thus terminates its relationship with higher ML risk customers. This allows the financial institution to externalise the risk associated with managing such clients into danger at its environment (3), which in turn generates danger for entities that were not involved in the decision-making.

Figure 4: De-risking through Luhmann's risk/danger model
process (e.g. de-risked customers or the regulator). In Figure 4, we show one impacted party as the regulator (System D) that needs to internalise such phenomena that affect the wider financial system’s stability (3). De-risking is perceived by regulators as a danger that may affect consumers or create wider competition problems. Thus, if regulators object to an institution’s attempt at reducing its own complexity, they may create the danger of fines against that very financial institution, which, if levied (4), would represent a new danger (1) that the financial institution would be forced to internalise because it made the initial decision to de-risk (2). At a minimum, regulators could create new guidelines to suppress phenomena like de-risking. However, these in turn would lead to their own unintended consequences and subjected to the variable danger/risk distinctions imposed by various institutions. Ultimately, the recursive cycles between danger/risk are inescapable. The very existence of a risk-based approach presupposes a de-risking-based approach (DRBA) at the same time. Without the development and formalisation of both an RBA and a DRBA, regulators cannot steer their institutions (in the cybernetic sense) and they cannot maintain a balance between the two distinct phenomena that represent them.

Even a prescriptive rules-based approach implies that some rules are imposed instead of others. In turn, the non-inclusion of other possibilities for rules, generates dangers that can affect AML systems in different ways. Put differently, the prescription of a rules-based approach amounts to a forced prescription of the non-inclusion of other rules, with each ‘rule’ enabling a mix of danger and risk. Ironically, a rules-based approach in itself is also a form of forced de-risking.

What we also need to highlight is that the financial institution (system C) and the regulator (system D) are located in one another’s environment. Decisions in system C generate dangers that may be internalised as risks in system D. System D then responds to the risk by creating new dangers for system C, which may, in turn, decide to internalise these dangers as risks and may then respond by making new decisions perceived as dangers by system D, so on and so forth. Thus, the risk/danger distinction is self-referential and reproduces itself at every step of the decision-making chain. As Demetis (2010) explains, “risk cannot therefore be specified or pointed out simply because it is categorised, even when the perception of risk is communicated; its re-genesis will transcend any system that attempts to manipulate it” (p. 113).

Now that de-risking has been described through Luhmann’s risk/danger model, we explore this phenomenon further by looking at how the victim or affected party does not necessarily have
to accept its role of victim and how under such circumstances, re-risking arises. This is explored through the Barclays bank vs. Dahabshiil case, which we will now discuss.

BARCLAYS VS DAHABSHIIL ILLUSTRATIVE CASE

In May 2013, Barclays bank announced it would close approximately 250 accounts belonging to Money Service Businesses (ACAMS, 2013). The rationale was that “some of them, including some remittance companies, did not have the necessary systems in place to spot criminal activity with the degree of confidence required by Barclays’ regulatory environment” (Tran, 2013a). The response to such a decision was met with controversy with charities explaining that remittance companies “provide a lifeline for 40% of the Somali population” (Tran, 2013b) representing USD 1.2bn annually, more than the country’s annual international aid (UN Food and Agriculture Organization). As Dahabshiil stated:

“It is important to remember that we are not just a business. We provide a lifeline service to Somalia and other African countries. We enable Somalis to help themselves, by sending money to every corner of the Somali territories to enable relatives and friends to buy food, medicine and to pay for education. Remittances are also used for investment in business start-ups and property – remittances are helping Somalis get the country back onto its feet after two decades of war” (Dahabshiil, press release, 23 February 2017).

Barclays Bank, however, explained in a statement that it had “made a legitimate decision to exit these businesses based upon the well-known risks of money laundering and terrorist financing in the money service business sector” (Moore, 2013). Essentially, Barclays bank’s decision was driven by exposure to financial crime risk. Yet, Dahabshiil’s solicitors issued a high court application seeking to prevent Barclays from closing its accounts. They claimed that:

“by giving them notice of its intention to withdraw banking services from their businesses Barclays has acted (or is threatening to act) unlawfully, because (put shortly) Barclays is alleged to be in a dominant position in the market for the provision of banking services to money service businesses, either generally or in relation to the particular sector in which the relevant claimant operates, and by ceasing to provide such services without objective justification Barclays would be abusing its dominant position contrary to Article 102 of the Treaty on the Functioning of the European Union (“TFEU”) and the Chapter II prohibition in the Competition Act 1998” (Dahabshiil & others v Barclays Bank Plc, 2013).
In October 2013, the court granted an injunction preserving business relationships between Dahabshiil and Barclays until the full trial took place and awarded Dahabshiil the costs of seeking the injunction.

To understand this case through Luhmann’s risk/danger model, we now consider Figure 5. System E represents Barclays, which has previously on-boarded MSBs (identified as being high-risk by the FATF) and internalised the risk presented by this customer base. More specifically, on-boarding MSBs as clients is a risk that was accepted by the banking institution and, as decision maker, the institution implemented adequate mitigating tools for managing this risk. Now system E has decided to de-risk, which entails the financial institution to unbank MSBs because of a new climate of close regulatory scrutiny, for instance, thus lowering financial crime risk tolerance for this sector.

Barclays (system E) terminates this relationship to comply with its obligation to apply the risk-based approach. Dahabshiil (system F), affected by Barclays’ decision, takes Barclays to court and obtains an injunction against Barclays, preventing it from terminating their relationship. Through this process, Dahabshiil internalised the danger posed by Barclays’ de-risking decision by means of taking Barclays to court. This internalisation turned that danger into risk, more specifically, the risk of having the court judging in favour of Barclays bank. However, the court’s decision allowed Dahabshiil (system F) to refuse system E’s de-risking. By taking Barclays to court, system F rejected Barclays’ de-risking decision and prevented it from being able to externalize its financial crime risk. This is described in Figure 5 with the process “Refuse de-risking” → “Second-order de-risking within F”. Furthermore, the decision to reject Barclays’ de-risking attempt impacted Barclays itself. Barclays was taken to court and was impacted by such events, financially of course and reputationally. This is shown in Figure 5 by the arrow between the “second-order de-risking within F” box and the “Second-order danger” box, which then leads to the “Danger” box affecting System E. This case illustrates the repurposing of system F danger into system E danger.

The key takeaway, however, is the fact that Dahabshiil was unwilling to internalise the danger of being de-risked and by taking Barclays to court, it rejected the level of complexity that would have come with being unbanked.
Now that we have discussed the Dahabshiil vs Barclays case, we delineate three distinct possibilities in how the decision making process of System F could react to system E’s de-risking decision:

**Scenario 1: Accepting De-risking**

System F represents an MSB that now faces a decision in relation to handling the danger generated by system’s E decision. The MSB could decide to accept the signalling from system E and implement processes to establish and maintain the existing relationship with system E, or it could secure a relationship with another financial institution. System F may thus decide to improve its own risk management system to address the banking sector’s risk aversion to regulatory scrutiny. More specifically, system F may decide to implement better procedures for account monitoring, develop KYC policies, audit Customer Due Diligence processes, and/or strengthen risk management systems. In this scenario, system F assumes the role of decision maker and internalises the danger generated by system E (through risk externalisation). Under such circumstances, re-risking occurs. This is represented in figure 5 with the process “Subsequent decision of risk externalisation: De-risking” → “Danger” →
“Accept de-risking” $\Rightarrow$ “Re-risking within F”.

Implication for de-risking: Under scenario 1, system E successfully de-risks and system F, through its own decision-making, is not a victim who faces danger. Instead, system F re-risks its own system.

Scenario 2: Rejecting de-risking

Another scenario illustrated by Figure 5 is the possibility that system F rejects system E’s de-risking, refusing to internalise the risk that system E has externalised through de-risking. In such a case, system F does not re-risk its own system, and similar to what we observed in the Dahabshiil vs Barclays case, through its own decision-making, system F transfers the danger generated by system E into the environment.

Implication for de-risking: Under scenario 2, danger re-enters the environment because system F makes the decision not to internalise it as risk (as observed in Figure 4, step 4). System E may be able to de-risk successfully if system F transfers the danger into the environment, without it impacting system E. However, if system E becomes the victim of system F’s decision, system E will be unable to de-risk successfully thus impacting its ability to manage risk and sustain its systems and controls as per its risk appetite.

Scenario 3: Enduring de-risking

The final scenario illustrated in Figure 5 is that in which system F does not make any decisions and remains victim of the consequences of system E’s de-risking initiatives.

Implication for de-risking: System F is the victim that now needs to find other systems (i.e. other financial institutions) that will accept to onboard it as customer. When viewed collectively, the frameworks and scenarios we present above can serve as a blueprint for introducing a de-risking based approach (DRBA).

OVERVIEW AND RECOMMENDATIONS

De-risking is essentially the contagion effect of risk assessments. This point is re-enforced by the FCA’s sponsored report on de-risking that highlights FATF and FCA statements on “wholesale cutting loose of entire classes of customers” (FATF, 2015) and on “banks dealing
generically with whole categories of customers or potential customers” (FCA, 2015). The FATF has essentially designated whole categories of customers and sectors as high-risk. It ultimately flags the probability of ML risks unto entire classes of customers. Why is then de-risking stigmatised when it is the mirror-image of the FATF’s process? In fact, de-risking is a naturally occurring phenomenon which follows the risk assessment and hence the decision making process dictated by the FATF. Regulators are essentially denouncing the fact that too many institutions are abiding by the FATF’s guidance.

This is frustrating to banks because “a bank’s decision on risk assessment may be the same whether it is undertaken on a case by case basis or wholesale basis, because the factors applied will not vary too much” (Artingstall et al., 2016, p. 19). “Risk assessments will score similar customers in similar ways. Thus a set of similar customers will fall outside the Financial Institutions’ risk appetite and thus be exited” (Artingstall et al., 2016, p. 24).

Furthermore, the cost of compliance is high, there is a lack of confidence in the regulator and fear of misinterpretations of regulatory expectations. Financial institutions simply do not feel that they have the support from the regulator. The FCA sponsored report on de-risking states:

“Many of the banks we have spoken to have indicated that, although they take a RBA to each client relationship, they are not just building in the actual risk of a client (or its customers) acting in a damaging way—they are also building in their assessment of how the appropriate regulators, or financial institutions higher up the ‘food chain’ (who are almost seen to be acting in a quasi-regulatory capacity), will assess their approach. Essentially there is a certain amount of second-guessing going on. In today’s environment, the vast majority of these assessments will fall on the side of caution” (Artingstall et al., 2016, p. 40).

Hence de-risking also reflects financial institutions’ lack of confidence in the regulator and uncertainties in relation to regulatory expectations. In addition, de-risking concerns private sector responses to irritations from its environment (such as the regulator), communicating a willingness to forfeit a region or a sector to signal good faith based on ML scandals. This is what Deutsche Bank did when it “broke off its relationship as a correspondent bank for US dollars with Danske in Estonia in September 2015 because of concerns over non-resident customers” (Milne, 2018). Similarly, Danske Bank announced in 2018 that “it would scale down its business in the Baltic countries to focus on the Nordic markets” (Reuters, 2018).

Such an exit is, of course, not the result of a simple fear of misinterpreting regulatory expectations; rather it is a move that demonstrates Danske Bank’s understanding of regulatory
expectations. On such occasions, de-risking is a decision made by a financial institution to communicate its new risk appetite and regulate the system’s exposure to regulatory scrutiny of course, as well as to ML risks.

“Many of the banks we have spoken to have indicated that, although they take a RBA to each client relationship, they are not just building in the actual risk of a client (or its customers) acting in a damaging way—they are also building in their assessment of how the appropriate regulators, or financial institutions higher up the ‘food chain’ (who are almost seen to be acting in a quasi-regulatory capacity), will assess their approach. Essentially there is a certain amount of second-guessing going on. In today’s environment, the vast majority of these assessments will fall on the side of caution” (Artingstall et al., 2016, p. 40).

Although de-risking is perceived by the regulator as danger from its environment, it is the result of irritations triggered by the regulator itself, which in turn affect its own environment. As such, the regulator needs to be mindful that ML risk and regulatory risk feed off one another and affect financial institutions’ perception and understanding of risk. Another element that needs to be raised is the fact that de-risking is to be expected since organisations seek to minimise their exposure to risks that sit outside their appetite. Yet, if too many organisations de-risk at the same time, externalising their risk into danger, there may be a critical mass of victims (as per Luhmann’s risk/danger model) facing such danger. This is a phenomenon observed in the USA where a World Bank survey (2014) identified that 80% of MSBs were struggling with account opening. Under such circumstances, we prescribe encouraging and incentivising re-risking.

De-risking initiatives observed amongst financial institutions are strategies for the latter to minimise their systems’ exposure to risk and externalise ML and regulatory risk. The regulator may respond to a new ML danger by introducing a new regulation for MSBs for example. The risk for such a new regulation may be the deployment of additional supervisory resources to ensure compliance. As we have seen, the danger to financial institutions may be uncertainty with regards to the regulator’s expectations resulting into the institution’s de-risking of MSBs. In addition, since de-risking aims to minimise exposure, it should not be prevented as it involves imposing a complexity that the system is not willing to handle. However, on the other hand, de-risked customers such as MSBs are in turn encouraged to reject their role of victim (as per Luhmann’s risk/danger model) and the danger they face once de-risked. Inevitably, the financial institution’s de-risking may result into second order danger such as MSBs seeking services from institutions that do not have the bandwidth or level of sophistication to deal with
high ML risk clients such as MSBs, thus exposing the jurisdiction to additional ML danger. Similarly, we note that regulators object to de-risking when too many decision-making systems reduce their complexity and convert their risk back to danger while other systems do not or cannot internalise such danger.

To prevent too many decision makers from de-risking at the same time and ensure that victims have the ability to become decision-makers, the regulator needs to consider its actions through Luhmann’s risk/danger theory. Essentially, the regulator has the following approaches to address de-risking:

- Provide means for victims to internalise or reject danger;
- Provide means for decision-makers to maintain danger internalisation;
- Increase decision makers’ ability to internalise danger;
- Decrease the danger within the environment;

In light of the above points, we are proposing that the regulator should act as a router steering the transition from de-risking to re-risking and vice versa. Formalising the options we deconstruct above into a De-Risking Based Approach (DRBA) and introducing a coherent set of recommendations for managing de-risking when it occurs can allow a better distribution between risks and their (institutional) handlers.

Tension between regulating de-risking versus banning de-risking has been observed but ultimately, the regulator needs to facilitate systems’ ability to either internalise or reject danger while also incentivising decision-makers to either internalise danger or maintain danger internalisation. As such, the regulator should create mechanisms to facilitate danger rejection as observed with Dahabshiil. Similarly, to encourage danger internalisation, the regulator should provide support and/or training with the development of robust Know Your Customer (KYC) and CDD for victims and decision-makers. In addition, more time can be provided to other systems/institutions within the environment to decide whether they wish to internalise danger and absorb systemic de-risking when it occurs. Regulators should increase the minimum notice period between decision to de-risk and actual customer exit and provide a mechanism, platform, or information system for swift onboarding to other institutions. An information system for brokering KYC-interoperability and supporting the transferability of onboarding documentation between institutions could support such efforts to regulate de-risking. Furthermore, to limit the regulatory uncertainty, the regulator should aim to provide
for customisations of its de-risking based approach for categories most affected by de-risking (Correspondent Banking Relationships, Non Profit Organisations, Fintechs, MSBs). Finally, to facilitate decision makers’ ability to internalise danger, the regulator should provide further guidance and support for categories that represent a greater source of risk to financial institutions. It should develop and sign-off a risk appetite evaluation tool and methodology to validate financial institutions’ risk appetite and ensure decision makers’ risk appetite is aligned to that of the regulator.

The following table lists key actions the regulator could implement to address de-risking systemically:

<table>
<thead>
<tr>
<th>Theory</th>
<th>Recommendations</th>
<th>Outcome(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Facilitate victims’ ability to internalise or reject danger.</td>
<td>1) Create frameworks or mechanisms to facilitate danger rejection as performed by Dahabshiil (e.g. the use of courts and leveraging laws and regulation).</td>
<td>Financial institutions are incentivised to keep danger internalised and continue to manage the business relationship. &lt;br&gt; FIs identify which complexity they can face: dealing with potential victims’ danger rejection or the potential ML risk they represent. &lt;br&gt; FIs may end up facing more complexity than their systems and controls can handle to avoid litigation.</td>
</tr>
<tr>
<td></td>
<td>2) Provide support and/or training with the development of robust KYC/CDD for victims and decision-makers.</td>
<td>De-risked customers have stronger internal processes which may increase their costs but ensures ongoing access to banking services. &lt;br&gt; In turn, the banking industry develops greater confidence in its high risk customers’ internal AML processes.</td>
</tr>
<tr>
<td></td>
<td>3) Increase the notice period between decision to de-risk and actual customer exit and provide a mechanism, platform, or information system for swift onboarding to other institutions.</td>
<td>Provides time for victims to identify the next course of actions and enables other systems within the environment to decide whether they can internalise such newly generated danger.</td>
</tr>
<tr>
<td>Incentivise decision-makers</td>
<td>4) Customise de-risking proposals</td>
<td>The regulator regains a certain level of responsibility temporarily and hence liability</td>
</tr>
<tr>
<td>Recommendation</td>
<td>Description</td>
<td></td>
</tr>
<tr>
<td>----------------</td>
<td>-------------</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Maintain danger internalisation.</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Decrease the danger within the environment.</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>(Correspondent Banking Relationships, Non Profit Organisations, Fintech, MSBs).</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Provide further guidance and support for categories that represent a greater source of risk to financial institutions.</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Develop and sign-off a risk appetite evaluation tool and methodology to validate financial institutions’ risk appetite and ensure decision makers’ risk appetite is aligned to that of the regulator.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Oversee and sign-off FIs’ RBA.</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Introduce guidance on a De-Risking Based Approach (DRBA) that formalises the management and handling of de-risking.</td>
<td></td>
</tr>
</tbody>
</table>

By formalising their risk appetites, financial institutions may decide to unbank categories of customers in what the regulator may qualify as a wholesale manner. While this may create an initial de-risking wave, it will increase the transparency of the jurisdiction’s overall risk appetite, facilitate information flow and as such increase decision-makers’ confidence in the regulator, remove uncertainty, thus increasing decision makers’ ability to internalise danger and facilitating re-risking across the financial system.

Develop a set of flexible measures to assess countries and FIs’ appetite and/or tolerance to ML risk more effectively and apply measures proportionate to the level of appetite and/or tolerance in order for FIs to focus their DRBA more effectively.

Develop specific guidance and support for de-risking scenarios with case studies for both decision-makers and victims (as per Luhmann’s risk/danger model) as per recommendations 1 to 5.

Table 1: Recommendations to address de-risking
Figure 6 summarises the recommendations documented in Table 1 and articulates the De-Risking Based Approach.

CONCLUSION

The relevance of Luhmann’s work on risk and the risk/danger model has been illustrated through Barclays Bank’s 2015 regulatory fine, the de-risking phenomenon, and Dahabshiil vs. Barclays Bank, thus demonstrating the versatility of Luhmann’s theoretical framework for exploring and understanding the AML domain. In light of Luhmann’s risk/danger model, we argue that de-risking should not be prevented nor discouraged. It needs to be managed carefully through the introduction of a de-risking based approach (DRBA). Organisations need to have the ability to de-risk in order to minimise their level of complexity and align it to the robustness of their internal systems and controls. Victims have the possibility to reject danger or to internalise it as a risk which, too, can subsequently be de-risked. Through the de-risking process, a system signals that a particular risk is being externalised and converted back into a danger that other systems can internalise as a risk or face as a danger. Accordingly, regulators should leverage the dynamic between risk and danger and implement measures to support victims of de-risking by enabling the latter to either reject or delay the danger of de-risking. In
addition, regulators must manage the level of complexity faced by the risk-takers (i.e. the decision makers) once they feel that their systems can no longer handle a certain risk threshold; in this context, regulators should minimise the regulatory ambiguity and uncertainty which financial institutions perceive as regulatory risk. This can be achieved through accepting greater liability and developing greater transparency with regards to financial institutions’ and regulators’ ML risk appetite.
Bibliography:


Communications & Organisation, 45, pp. 33-48.

Industrial Crisis Quarterly, 4, pp. 223–231.


money laundering risk in UK financial services’, Journal of Money Laundering Control, 

Monroe, B. (2020) Ousted Danske bank CEO faces nearly $400 million lawsuit tied to 
historic money laundering scandal, acfcs, 28 February [Online] Available at: 
https://www.acfcs.org/ousted-danske-bank-ceo-faces-nearly-400-million-lawsuit-tied-to-
historic-money-laundering-scandal/.

Moore, E. (2013) Africa money transfer service wins injunction against Barclays, The 
Financial Times, 5 November [Online] Available at: https://www.ft.com/content/6f1a76f8-
4618-11e3-9487-00144feabdc0 [Accessed 22/03/2021].

of Money Laundering Control, 23(1), pp. 26–37. Available at: 

Oxfam (2013) Oxfam reacts to Barclays last minute extension to Somali remittance closures 
(30 September). Available online: https://oxfamapps.org/media/press_release/2013-09-
barclays-eleventh-hour-extension-response/ [Accessed 7/02/2021].

75-103.

102–114.

and Terrorism Financing Law, Volume 1. Cham: Springer International Publishing AG.

Rose, K. J. (2019) ‘The problem of regulating the easy way out – EU money laundering 


Wildavsky, A. (1979) Views: No Risk Is the Highest Risk of All: A leading political scientist postulates that an overcautious attitude toward new technological developments may paralyze scientific endeavour and end up leaving us less safe than we were before. *American Scientist*, 67(1), pp. 32-37.