

Volume 2/ September 2015



# CRO INSIGHTS JOURNAL

Concerns for CROs in  
a Complex Post-Crisis World





**Freddy Gielen**  
**Partner**

Freddy Gielen is a Founding Partner of Avantage Reply. Freddy has over 20 years' experience in Prudential Risk, Finance and Regulation. Prior to establishing Avantage Reply in 2004, he has worked as a consultant for systemically important institutions, The World Bank and global financial regulators. He holds a Master's degree in Finance and in Engineering. He is also a Certified Public Accountant (U.S. CPA).

---

Email: [f.gielen@reply.com](mailto:f.gielen@reply.com)

About **Avantage Reply**

Established in 2004, Avantage Reply (a member firm of Reply) is a pan-European specialised management consultancy delivering change initiatives in the areas of Compliance, Finance, Risk and treasury.

Website: [www.avantagereply.com](http://www.avantagereply.com)

**Concerns for Chief Risk Officers in a Complex Post-Crisis World**

Following the 2008 crisis, financial regulation moved from the periphery to the centre of the global economic agenda. Risk discussions were no longer confined to technocratic circles but were taken up by the financial industry as a whole, including policy makers and the general public. We saw the increasing importance of Chief Risk Officers (CROs) and recognised the need for risk management to be embedded across all levels of an organisation. In 2014, Avantage Reply launched its CRO Insights Journal to respond to these shifts.

The first edition of the CRO Insights Journal focused on the growing role of the Risk Function and how CROs' responsibilities have evolved in response to the crisis. We are now delighted to present our second edition which captures the nature of risk in an increasingly complex economic landscape.

In 2015 we are seeing the tepid beginnings of a financial recovery. However, with numerous risks persisting and new ones emerging, it is clear that we are not yet out of the woods. This remains the greatest cause for concern. The Financial Times describes risk in our time as a "global challenge that respects no boundaries."<sup>1</sup> Certainly, these risks stem in part from the interconnectedness of our technologically advanced and sometimes volatile world. Further risks have appeared as a result of regulatory and monetary policy reforms implemented in response to the crisis.

In this second edition, Avantage Reply consulted the Heads of Risk from various European banks for Belgium, France, Germany, Italy, Luxembourg, Netherlands, and the UK. We are delighted to include the perspectives of the following pre-eminent professionals:

- Joris De Backer (Board member and Executive Director) of Beobank;
- Keiran Foad (Chief Risk Officer) of Santander UK;
- Thierry Lopez (Managing Director and Head of Group Risk Management) of Banque Internationale à Luxembourg;
- Pierpaolo Montana (Chief Risk Officer) of Mediobanca; and
- Diemer Salome (Global Head of Non-Financial Risk) of Rabobank.

Together, they bring key insights and best practice solutions from their respective organisations.

The CROs shared their views on five pertinent risks and how they are being addressed. First, the CROs explored the challenges raised by the current low interest rate environment. Secondly, they observed the increasing importance of establishing a positive business culture, with an acute focus on how organisations respond to regulatory challenges and, at the same time, reduce conduct risk. Thirdly, risks raised by recent technological developments, including the threat of cybercrime, were also discussed, as were the potential pitfalls caused by third-party risk through the outsourcing and offshoring process. Finally, the CROs selected a number of emerging issues in risk management, including changes to the regulatory and legal environment, and the continual pressures placed on the Risk Function by ongoing global instability.

We hope you find the second edition of the CRO Insights Journal edifying, and we look forward to continuing the conversation with you.

**Freddy Gielen**  
Partner Avantage Reply

<sup>1</sup> 'Special Report: Managing Risk in a Globalised World', *The Financial Times*, 8 September 2015, available at <http://www.ft.com/reports/managing-risk-globalised-world>

# CONTENTS

|  |    |
|--|----|
| Will low interest rates result in a new credit bubble?                   | 4  |
| Technology risks: cyber attacks, digital transformation and social media | 8  |
| Mis-selling and business culture   | 12 |
| Third-party risks, including offshoring and outsourcing                  | 16 |
| Other risks and trends   | 20 |

# CONTRIBUTORS



**Joris De Backer** is an Executive Director at **Beobank**, where he is responsible for managing credit, financial and operational risk. Joris was previously an Executive Board member of BKCP bank. He established a new risk management board, and implemented new governance and control frameworks for both Beobank and BKCP banks. Joris has held similar roles at Artesia Banking Corporation and Landbouwkrediet bank. Joris holds a Master's degree in Applied Economics from UFSIA specialising in quantitative economics.

---



**Keiran Foad** joined **Santander** as Chief Risk Officer in April 2012. Prior to Santander, Keiran was Chief Risk Officer of Northern Rock PLC, where he was part of the executive team responsible for the sale of Northern Rock PLC to Virgin Money. Keiran also spent 25 years with Barclays, where he held numerous leadership roles within coverage, risk and change, including 2 years as Chief Credit Officer (CCO) of ABSA bank in South Africa.

---



**Thierry Lopez** is Managing Director and the Head of **Banque Internationale à Luxembourg (BIL)** Group Risk Management. He is a member of various management committees including the Commission de Surveillance du Secteur Financier (CSSF) and the ABBL (Luxembourg Bankers' Association). Thierry is currently chairman of the ABBL Banking Supervision Committee. He is the founder and board member of ALRIM (Luxembourg Association for Risk Management Professionals). Thierry is also involved in academic circles, regularly speaking at HEC-Business School of the University of Liège, the ATTF (Financial Technology Transfer Agency) and the IFBL (Luxembourg Institute of Banking Training).

---



**Pierpaolo Montana** has been a **Group Chief Risk Officer** for Mediobanca S.p.A. since June 2014. Prior to joining Mediobanca, he worked within the Risk Management departments of BNP Paribas and WestLB, specialising in quantitative methodologies for cross-asset Market and Counterparty Risks. Previously, he served for three years in the Bank of Italy's Banking Supervision Department, assisting in the implementation of Basel II for Market and Credit risk within the Italian banking system.

---



**Diemer Salome** is Global Head of Non-Financial Risk for **Rabobank**. Previously he was Head of Global Risk Advisory and Project Manager for Basel III at Rabobank. He has been Director of The Risk Management Centre and was an advisor to the Board at Bank BGZ (Poland). He was also the Head of Credit Policies & Procedures in the Netherlands for Basel II. Diemer holds a PhD in Mathematical Statistics from the University of Groningen.

## CONTRIBUTORS



**Bernard Colla** is a **Senior Manager** with **Avantage Reply** (Benelux and France). He is an experienced risk manager with significant expertise in asset and liability management (ALM), market risk, and stress testing. Bernard has worked in both line and change roles, with a predominant focus on the risk management function(s). Project work includes: VaR, EaR and ECAP, and IFRS change implementation. Line work includes: product control, liquidity management and front office systems. A well-rounded risk manager who has written numerous regulatory papers, Bernard recently assisted G-SIBs and D-SIBs in the preparation of their recovery plans including ECB stress tests. He is a member of the ICAAP and Recovery Plan working groups of the ABL (Luxembourg Bankers' Association).



**Tom Banens** is an accomplished **project manager and advisor who specialises in areas of work covering Governance, Risk and Compliance (GRC)**. As a former banking practitioner, Tom combines a thorough understanding of today's regulatory environment with extensive fiscal knowledge, experience and insight. Tom has a proven track record in the management of complex change programmes and regulatory waivers and in the formation of GRC assessments and institution-wide policy frameworks. Prior to joining Avantage, Tom has worked with ING, Mizuho and Dexia. He also worked as Basel Programme Manager for GE Capital with responsibilities that included credit and securities administration, Pillar 1 Reporting, Credit Risk Modelling, Operational Risk, Portfolio Management and ICAAP.



**Dario Rossa heads up Spike Reply** in the Benelux and France. Spike Reply is the Reply Group company specialising in Information Security Risk Management and Solutions. Dario has over 26 years of experience in ICT, Business-to-business e/m-commerce, information security, risk management and mobile solutions. Dario has worked for leading financial institutions including AXA, BNP Paribas, JP Morgan, KBC Bank N.V., and State Street. Dario is also a guest Professor at University of Leuven, Belgium, where he specialises in information security. He is a Certified Information System Security Professional (CISSP) and holds a Masters in Business Administration (MBA) from TRIUM (NYU, HEC Paris and LSE). He is a member of the ABL's (Luxembourg Bankers' Association) Payments Committee and the Financial IT Forum.



**Miguel Mairlot** is a **Manager** with Avantage Reply (Belgium) specialising in conduct risk and compliance functions. Miguel is a **legal and compliance expert** with over 13 years of experience in the financial sector and more than 10 years' practice as an attorney-at-law. Miguel has been a Certified Compliance Officer (FSMA) since 2012 and has worked as head of Legal & Compliance for the Bank of Tokyo and UBS. Over the years, Miguel has demonstrated a client-centered approach combined with an excellent understanding of compliance and legal risks. In addition to his role at Avantage Reply, Miguel teaches Finance Law in Brussels and is the author of a number of publications in the field of banking law and compliance.




**Rohan Wilson** is a **Senior Consultant** at **Avantage Reply**. He is a risk specialist with 8 years' financial services experience having started his career as a derivatives trader in London. He has delivered numerous risk solutions for large European banks. Rohan has worked for leading financial institutions in Belgium, Germany, Luxembourg, and the UK. Rohan read at Oxford and Nottingham Universities, and has a Masters degree in Finance from the London Business School.

# WILL LOW INTEREST RATES RESULT IN A NEW CREDIT BUBBLE?

---





**INTEREST RATES IN THE EUROZONE REMAIN AT RECORD LOWS. IN A GROWING NUMBER OF COUNTRIES, INTEREST RATES ARE NOW NEGATIVE. NEAR-ZERO INTEREST RATES MAY HAVE MADE SENSE DURING THE FINANCIAL CRISIS, BY STIMULATING A RECOVERY, BUT LOW INTEREST RATES CAN BE MORE HARMFUL THAN HELPFUL. SUCH AN ENVIRONMENT IS PRODUCING A NEW RANGE OF RISKS THAT ARE DISCUSSED BELOW.**

In March 2015, the European Central Bank (ECB) started buying €60bn of assets a month in an attempt to stimulate the European economy. This opened a new chapter in the ECB's monetary policy, creating even lower interest rates and credit spreads. Volatility ensued. In March 2015, Bunds plunged to an historic low of 0.07% yield and then in April, Bund yields rebounded 60 basis points, dragging Eurozone bond markets in their wake.

2015 has seen stronger global growth, the launch of the ECB quantitative easing programme and depressed oil prices. With this has come a global sell-off in bonds. This year has also featured the unwinding of long Bund propositions by option traders, unethical front running and a general desertion in the markets of bond buyers. All this has been accompanied by a widening of bid-offer spreads.

The ECB's quantitative easing programme is increasingly viewed with concern. One of its main objectives is to stimulate lending and investment within the Eurozone. However, an "investment paradox" has resulted.<sup>2</sup> With falling returns on assets, and confidence faltering, companies are reluctant to invest.

The quantitative easing programme has created fresh risks and challenges for banks. The Financial Times recently argued that this mass bond buying could, in fact, exacerbate "the sort of volatility it is trying to correct."<sup>3</sup>

As **Mediobanca's** CRO, **Pierpaolo Montana**, asserts, "the ECB monetary policy combined with a restrictive fiscal policy and tax policy leaves banks with massive liquidity. The system has a huge liquidity with weak demand from good quality borrowers."

<sup>2</sup> Jim Brunsden and Claire Jones, 'Drop in long-term investment hinders Eurozone recovery', The Financial Times, 9 August 2015, available at <http://www.ft.com/cms/s/0/f7c51020-3c44-11e5-bbd1-b37bc06f590c.html>

<sup>3</sup> Claire Jones, 'Draghi hands markets a gift as Eurozone growth disappoints', The Financial Times, 3 September 2015, available at <http://www.ft.com/cms/s/0/7c64c966-5256-11e5-8642-453585f2cfd.html>

# WILL LOW INTEREST RATES RESULT IN A NEW CREDIT BUBBLE?

**Thierry Lopez**, Chief Risk Officer of **Banque Internationale à Luxembourg**, describes the problems created by a low interest rate environment: “Such a [low] rate and volatile environment leads to a situation where reinvestments become a real headache and existing investments suffer from re-pricing. Clients are exiting the fixed income area, preferring to leave their cash at sight, with almost no return. That leads to an increase in banks’ liabilities.”

## Hard to make money

**Diemer Salome**, Global Head of Non-Financial Risk at **Rabobank**, reminds us, “these [low rate] concerns force banks and CROs to focus on cost management but they may also push banks to search for yields.”

**Thierry Lopez** notes that banks can improve yields by either increasing their credit risk or by increasing investment maturities. “Basel III liquidity and capital ratios limit the first option, as riskier assets are usually illiquid and capital-consuming. The second option, nevertheless, also needs to be assessed cautiously, even with investments in ‘government paper’ from core European countries. In a scenario where rates increase, banks may indeed face capital losses on their investments. At the same time, clients’ ‘sight account’ [current account] balances are likely to decrease as clients start investing their cash. Bank funding costs may therefore increase if clients switch from current accounts to term deposits.”

**Joris De Backer**, Executive Director at **Beobank**, which has a significant consumer credit business, notes that “consumer credit which accurately prices the risk premium, means it is still possible to make money with short-term lending products.” There is much more of a business risk in long-term lending products. For example, mortgages with a flat yield curve provide limited opportunity to make money. If you take the Belgian mortgage market, it is very hard to understand how certain banks price the credit risk involved. When you see that it is possible to borrow fixed for 20 years, with a loan to value (LTV) ratio of 80% or even below, at a 2% interest rate, you have to ask yourself how the bank makes money. We’ve got a significant business risk there, in that we’ve got a mispricing of the credit risk involved in those products. Quite frankly, the business model viability and sustainability of banks underwriting this kind of long-term loan at this price is questionable.”

## A new credit bubble?

Low interest rates, combined with the search for yield by corporates and insurance companies, may create the conditions for a new credit bubble according to **Pierpaolo Montana**, Chief Risk Officer of **Mediobanca**. “Potentially we might have an accumulation of credit transactions and a credit portfolio with a risk return profile that is not acceptable. Certain financial institutions may basically extend a loan to a client at a very low interest rate because they have access to ‘free money’. That very low interest rate doesn’t take into account the actual price of the credit risk. If you think about it, this is exactly what happened with the subprime crisis. It will also lead to an increase in portfolio duration.”

*“With the current low interest rate environment possibly generating a “search for yield” through a variety of mechanisms, supervisors should be cognisant of the growth of such risk-taking behaviours and the resulting need for firms to have appropriate risk management processes.”*

Basel Committee on Banking Supervision, June 2015.

**Keiran Foad**, Chief Risk Officer of **Santander UK**, agrees: “Interest rate risk is one of my top risks. It has a huge impact on our business model. Certainly the search for yield in light of the low returns on the liquidity portfolio that we are forced to hold is an issue, especially given the increase in size of that portfolio. But I am actually more worried about the second order impacts than the first – for example, with respect to the pension liabilities that banks may have on their books.”

The Chief Risk Officers we interviewed were also concerned that quasi-infrastructure players, such as certain Global Custodians or Central Securities Depositories (CSDs) are loading their investment portfolios with longer duration and higher credit risk securities. “They’re looking for yield,” stresses **Pierpaolo Montana**. “They think whatever they buy is liquid because it’s eligible for refinancing from the central bank. That may well be the case today, but if the central banks tighten eligibility requirements, some of these securities will no longer be eligible. It is important that those Global Custodians and CSDs remain a safe haven in the industry. We cannot afford for them to take risk. We give them our assets and pension funds give them their assets to safeguard. If they are starting to invest our money, our liquidity, in portfolios that are more risky because they are looking for yield, will they continue to be a safe haven? Or are they likely to become more risky?”



## Prepared for the future

According to **Diemer Salome**, damage to reputation and reputational risk is another impact of the low interest rate environment. “Banks, rather than policy makers, are blamed in the media for low interest rates,” he says. “More than ever, banks are forced to be more transparent on their earnings model and to defend this publicly. The industry needs to regain public trust; more effort around transparent communication is key.”

Another looming risk that worries several CROs relates to the period when the ECB will shift away from quantitative easing.

“If you look at the United States, they’re trying to leave quantitative easing, but it is very, very complicated. The market does not react smoothly. Of course, I am not anticipating that the ECB will exit quantitative easing in the next 6 to 12 months. But when it happens, I think we risk to be ill-prepared as an industry to manage the impact of the shock and therefore to manage the risk,” says **Pierpaolo Montana**.

“In the US, the market as a whole reacts as a country. By contrast, in the Eurozone, exit from quantitative easing will have a different impact from country to country, because the market situation is different, the employment situation is different and the credit worthiness of each country is different. It will be difficult to predict what will happen on a European level, as well as on a national level. Clearly, I cannot believe that Germany will react in the same way as Portugal, for instance, nor Italy and Spain.”

Consumers are also prepared for higher interest rates. This raises the question of consumer affordability. “We’ve got a generation out there that has never seen high interest rates and is not prepared for a higher rate environment,” says **Keiran Foad**.

**Banks have traditionally relied on deposit funding at below capital markets rates to be profitable. (...) In addition, banks have traditionally profited from maturity transformation as the yield curve included a term premium. With market rates below zero most deposits generate losses and flat yield curve further contribute to the banking business model being exposed to the fate of the Dinosaurs.**

Jesper Berg, 'Business models at rates below zero', The Eurofi Financial Forum 2015, 9-11 September 2015.

“The question becomes: is there a new normal? Is it normal to have a mortgage at 3%? If you think about it, if rates were to go from, let’s say, 2.5% to 5%, this is double the rate”, adds **Keiran Foad**.

## Operational challenges

Low interest rates also have a practical impact on banks. **Diemer Salome** and **Keiran Foad** are both worried about the operational challenge of preparing IT infrastructure to deal with negative interest rates.

“Not all IT systems in Europe are fully prepared for zero and sub zero interest rate calculations. Reporting system’s testing is an ongoing effort,” says **Diemer Salome**.

**Thierry Lopez** argues: “In these conditions, the CRO has to ensure that these stresses are well-understood by management. He or she needs to find a subtle mix between a ‘wait-and-see’ position, which may decrease profitability in the long term, and a ‘too-permissive’ position, which may suddenly lead to significant market losses.”



**Bernard Colla, Senior Manager,**  
Advantage Reply

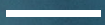
## Decrease in net interest margin

If rates remain at their current levels for an extended period, the continuous decrease in banks’ interest margins will pose a significant risk. The profitability of many banks would suffer. They would be forced to find new sources of revenue, whilst having to reduce costs. This could push them to invest in riskier assets.

Another risk is a sudden interest rate rise. This risk could create a “scissor effect” with a sudden decrease in asset values, combined with a sharp increase in the cost of funding. Fortunately, central banks have identified this risk. Central banks are likely to adopt a very cautious policy when they decide to increase base rates, to give financial institutions ample time to adjust. This includes adjusting the maturities of their assets and liabilities.

TECHNOLOGY RISK

# CYBER ATTACKS, DIGITAL TRANSFORMATION AND SOCIAL MEDIA





CYBER RISKS ARE ESCALATING IN THE FINANCIAL SECTOR. THREAT DETECTION, READINESS TO RESPOND TO ATTACKS, AND THE CAPACITY TO RECOVER FROM THEM, ARE NEW CHALLENGES FOR FINANCIAL INSTITUTIONS. DEFENCE IS NOT THE ONLY FOCUS, HOWEVER – BANKS ARE ALSO REQUIRED TO KEEP ABREAST OF TECHNOLOGICAL INNOVATIONS TO KEEP UP WITH CLIENTS' EXPECTATIONS. THIS CAN CREATE SIGNIFICANT BUSINESS RISK FOR A BANK IF IT FALLS BEHIND. HOW CAN CROs RESPOND TO TECHNOLOGY RISKS IN THIS FAST-MOVING AND COMPLEX ENVIRONMENT?

Cyber risk has been widely discussed in the mainstream media in recent months. Financial institutions are inevitably prime targets for cyber-criminals. In February 2015, the Kaspersky Lab revealed that a gang of cyber-criminals had infiltrated more than 100 banks across 30 countries and stolen up to one billion dollars over roughly two years.<sup>4</sup> In July 2015, RBS and Natwest were the target of a cyber attack that prevented their clients accessing their accounts online, with the Financial Times casting doubt on the ability of the banks' technology systems to meet the new demands of digital banking.<sup>5</sup> These are just a few examples of a much wider threat.

Customer behaviour is changing with the development of new technologies. Clients now expect real-time responsiveness across all products and services. As a consequence, "banks are introducing the technology enabling open and real-time systems, which in turn make them more vulnerable to hackers and cyber-criminals," says **Diemer Salome** from **Rabobank**.

At the same time, cyber-criminals are becoming increasingly sophisticated, developing more advanced tools and systems to achieve their goals.

"Hackers now invest months of time and effort in infiltrating and understanding internal bank processes," adds **Diemer Salome**.

<sup>4</sup> 'The Great Bank Robbery: Carbanak cybergang steals \$1bn from 100 financial institutions worldwide', *Kaspersky Lab*, 16 February 2015, available at <http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1bn-USD-from-100-financial-institutions-worldwide>

<sup>5</sup> Emma Dunkley, 'RBS hit by second technology glitch', *The Financial Times*, 31 July 2015, available at <http://www.ft.com/cms/s/0/d4d36a72-3789-11e5-b05b-b01debd57852.html>

# TECHNOLOGY RISK: CYBER ATTACKS, DIGITAL TRANSFORMATION AND SOCIAL MEDIA

## The human element

Far from being solely a technological issue, cybercrime also has an important human dimension. Cyber-criminals frequently use 'social engineering' to commit cyber fraud and theft. Social engineering is the manipulation and deception by human beings in the real world to obtain confidential information. This element should not be neglected in our efforts to combat cybercrime.

"Cyber attacks are consistently preceded by more and more developed social engineering," says **Thierry Lopez** of **Banque Internationale à Luxembourg**. "Therefore, the CRO certainly cannot lose sight of IT security measures that must be enhanced to protect against information system hacking, including sustained cyber attacks. On the other hand, he or she should not ignore or underestimate the human component of these attacks." It is crucial for banks to educate employees to be able to quickly identify social engineering techniques. An unusual email asking the recipient to click on a link, or a phone call to request sensitive information, for instance, must raise suspicion immediately.

"In this context," adds **Thierry Lopez**, "the CRO has an advisory role to the businesses. By putting a combination of both technical and human defence mechanisms into effect, he or she will be able to help his or her company deter or defeat ever-developing and ever-increasing cyber attacks."

Social engineering is strongly linked to identity theft. It can involve stealing someone's identity to gain access to resources or obtain credit and other benefits in that person's name. Identity theft is an area of great concern for **Beobank's Joris De Backer**: "organised crime is well equipped to steal data from clients and mimic clients' behaviour," he says. "Imagine a criminal organisation that steals data, observes a client for months, and then, at some point, calls the bank using the data collected to ask to change a phone number. A week later, they will call the bank again and give an instruction to wire money to bank account number ABC. This would obviously be followed by a call from the bank, to try to confirm that the wire transfer request is genuine. Having changed the phone number prior to that call, however, the fraudster will be able to confirm the bank transfer. That is the type of threat that we, in the banking sector, are facing. There is never a dull day!"

## The technology revolution

Technology is fast moving from the periphery to the centre of banks' business operations. Chris Skinner recently highlighted in his blog that Barclays Bank is increasingly describing itself as "a technology financial services company, not a bank with a technology division."<sup>6</sup> As **Joris De Backer** notes: "Technology is transforming banks' business models."

However, while cybercrime is one risk created by technology, business risk is another. New businesses have emerged within the payments technology sector, responding to innovation, advances in technology and customer demands. This creates an increasingly competitive environment. Telecommunication companies enter the financial ecosystem by offering new means of payment. Fintech companies influence the credit card business.

"Apple Pay, Lending Club, and other Peer to Peer Lenders, Amazon, eBay have all entered the financial sector," adds **Santander's Keiran Foad**. "There is a new paradigm out there which is eating into the profitable business segments banks have today." According to **Foad**, corporate banking is not immune to this problem. "It started with retail, but corporate banking, and soon investment banking, will be hit," he says. "So there is a significant business risk attached to technology risk. Some banks have started to respond to this by, for example, creating venture funds and investing in Fintech businesses."

## Organisational transformation

The increasing reliance on technology and their associated risks are driving significant organisational change within banks. "Information & Security Management functions, which were traditionally part of Operations or IT functions, are increasingly being integrated into the risk management cycle under a three lines of defence structure," says **Diemer Salome**. "This involves not only IT infrastructure technology protective barriers, but also risk awareness levels amongst all staff."

<sup>6</sup> Chris Skinner, 'More evidence of banks waking up to the digital reformation', *The Financial Services Club Blog*, 9 September 2015, available at <http://thefinanser.co.uk/fsclub/2015/09/more-evidence-of-banks-waking-up-to-the-digital-reformation.html>

CROs also have to develop new skills. “One of my concerns is that, as a CRO I have to face very sophisticated technology issues,” adds **Pierpaolo Montana**. “I need to be very aware of the technology. I need to understand what an HADOOP server is. I need to understand how technology enables the bank but also how it may be a driver of risk for the bank.”

It can also be difficult for banks today to attract the right talent. “15 years ago we, as an industry, attracted the best engineers,” **Montana** says. “Banking was what people wanted to do. Now we are followers. Now the competition to hire the brightest is harder. This is certainly slowing us down from an innovation perspective. We need to get that talent back in.”

**“93 per cent of large organisations last year suffered a security breach.”**

The Cyber Threat to Banking, British Bankers' Association, 2014, Page 3.

**“As executives regularly evaluate strategies and risks, cyber security has been elevated to the C-suite to help ensure programs and practices evolve while keeping us with new and emerging threats. The goal? To identify critical risks, help protect information and systems assets, and best respond to cyber attacks.”**

Lisa Humbert, 'Financial services firms focus on creating cyber security risk awareness', The Eurofi Financial Forum 2015, 9-11 September 2015.



**Dario Rossa, Associate Partner,**  
Spike Reply

#### **It is about how hard a cyber attack will hit the organisation**

Listing all possible cyber risks is an impossible task. Patching the systems is critical but many banks are not doing this in a timely fashion. CROs can nevertheless have a threat model in place to assess whether a threat is applicable; whether a threat could potentially exploit existing vulnerabilities; or whether a threat will materialise.

Cyber risk is not a question of when, but how hard a cyber attack will hit an organisation. CROs therefore need to understand the impact of an attack. For instance, the impact on corporate risk could be substantial and it is important to minimise associated reputational damage.

In that context, it is crucial to have all critical information assets documented, with corresponding data classification and risk assessments. Information risk dashboards, which identify and classify risks, should provide an overview of the most critical risks, mitigation plans and time lines. In the event of a cyber attack, a proper crisis management plan with communication channels should be in place and be tested at least annually.

Introducing new technologies can be very risky and disruptive to an organisation but that should not mean that financial institutions ignore technological innovations. It should mean that CROs assess the impact of introducing new technologies. To do so, it is important to have a lab environment where architects and technicians can assess whether or not technological innovations could benefit core banking activities and the banks' clients.

Whether a financial institution is in a leader or a follower position, with respect to technological innovations, depends on the maturity of the organisation and its ability to absorb the changes and risks introduced by new technologies. It doesn't mean that all banks need to be a leader in that field. Being prepared is crucial to the survival of the financial institutions of the future. In this sense, being a follower, by adopting technological innovations, could be an advantage. Not all innovations reach the level of transparency, where their usage and benefits become generally accepted.

# MIS-SELLING AND BUSINESS CULTURE

---





A NUMBER OF MIS-SELLING SCANDALS, SUCH AS OVER-SOLD PAYMENT PROTECTION INSURANCE (PPI) AND ILL-ADVISED INTEREST RATE SWAP HEDGING, HAVE BROUGHT MIS-SELLING TO THE FOREFRONT OF THE BANKING SECTOR. REGULATORS NOW EXPECT BANKS TO ADDRESS SALES MIS-MANAGEMENT AT AN ORGANISATIONAL LEVEL. FAILURE TO DO SO LEADS TO INCREASED BUSINESS RISK, INCREASED REPUTATIONAL RISK AND HEAVY FINES. WHAT CAN CROs DO TO HELP BANKS GUARD AGAINST THESE RISKS? AND HOW CAN ORGANISATIONS DEVELOP MORE COMPLIANT WORKPLACE CULTURES? THESE QUESTIONS AND MORE ARE ADDRESSED BELOW.

In the last few years, we have seen a number of banks punished for mis-selling and hit with huge fines. The Financial Times notes that some banks are still paying out huge compensation amounts for PPI nearly two decades after the products were sold. In the UK alone, the industry has set aside £26 billion to cover costs<sup>7</sup>.

While initial complaints over PPI were raised well before the financial crisis, current conditions are forcing CROs to remain vigilant against similar risks. As **Thierry Lopez** of the **Banque Internationale à Luxembourg** notes, “Very low interest rates and low growth, in addition to the increase in operational costs related to regulatory and compliance pressure, forces us to pay particular attention to fraud and mis-selling.”

#### Increased regulatory control

The European Banking Authority (EBA) adopted guidelines on Internal Governance (GL 44) in 2011. The guidelines provide a new product approval policy. This policy mandates a greater involvement, for the Risk Control function, within both the approval process and product change process.

At **Banque Internationale à Luxembourg**, “these guidelines are well-deployed as regards to new products,” says **Thierry Lopez**. “The Risk Management department is a key stakeholder in the approval process. It is thus essential for internal control functions to be increasingly involved, whether on the New Products Approval Committee or alongside it, in counteracting potential mis-selling impacts where the commercial incentivisation has not been well-calibrated.”

<sup>7</sup> Emma Dunkley, ‘UK banks not doing enough to resolve PPI scandal’, *The Financial Times*, 5 June 2015, available at <http://www.ft.com/cms/s/0/3c3fbef0-0b8d-11e5-8937-00144feabdc0.html#axzz3ll8hkLiu>

## MIS-SELLING AND BUSINESS CULTURE

Conduct risk has also emerged as a hot topic for national regulators. The risk to customers posed by banks' operational failings is now a central concern. The risk to customers posed by banks' operational failings is now a central concern – whether the customer is an institution, a municipality, an SME or an individual.

**“The scope of alleged inappropriate practices is widening, and the magnitude of previously identified detrimental practices, for example related to foreign exchange trading business, is increasing.”**

European Banking Authority, Risk Assessment of the European Banking System, June 2014.

Since 2012, the Financial Services & Markets Authority (FSMA) in Belgium has required banks to demonstrate greater levels of transparency. Banks now have a duty of care to check their clients' solvency and to provide clients with detailed information about their products. Systems were also put in place to allow consumers to easily compare offers from different banks. Overall, consumer protection has improved.

**Joris De Backer** of **Beobank** emphasises the key role banks need to play in mitigating conduct risk for consumer credit: “essentially, the regulator is interested in making sure we are selling products to people who can afford them. This affordability of the product is absolutely key,” says **De Backer**.

### Increased internal control

To meet the increasing regulatory expectation, banks are, in turn, improving their internal controls. **Santander**, for instance, has set up a robust programme to monitor sales and business practices. “We have put key risk indicators (KRI) in place, such as account closures on the first month of opening or other indicators related to the performance of the business. We make sure they are forward-looking as far as possible,” says **Keiran Foad** from **Santander UK**.

### A matter of culture

Beyond KRI programmes, the critical aspect for reducing conduct risk is establishing the appropriate culture within key bank departments. **Santander** has invested massively in a culture programme “to make sure that the first line of defence, the sales people, take sales and business practices very much into account,” says **Keiran Foad**.

**Beobank** has put a self-assessment mechanism in place to make the first line of defence accountable. “Our relationship managers,

our branch managers, all our colleagues who interact with clients must self-assess, whether they are doing things properly,” says **Joris De Backer**. “They have to attest to the second line of defence - the risk function. This includes an attestation that they stand by their behaviour. This seems to be yielding some useful results.” **Beobank** has also developed a benchmark that ensures that roughly 10% of the first line of defence personnel's time is spent on control activities. This is an interesting yardstick, and demonstrates the importance of ownership by the first line of defence, in managing risk (particularly conduct risk).

**Diemer Salome** of **Rabobank** reminds us that banks need to look beyond indicators to focus on overall organisational culture: “Managing risks based on traditional dashboard process indicators is not enough. You need to have a very good handle on culture, behaviours and attitudes. It is important internally across the organisation, but equally important on the client side in customer due diligence. We are increasingly looking into innovative approaches such as behavioural sciences and analytics to manage this risk category.”

**Mediobanca's Pierpaolo Montana** emphasises the role that incentives play for individuals in minimising conduct risk. Conduct risk management, according to **Montana**, should take both the ethical and incentive perspectives into account: “We need to understand how people make money as individuals: how they are incentivised, how bonuses are organised,” said **Montana**. “Ethical standards are very important but they only get you so far. Ethics and culture are something that the CEO and board of directors need to lead. The CRO needs to advise the business and the human resources function on adequate checks and balances to make sure people are kept under control. We need to understand how a CVA desk, a treasury function or a salesperson makes money.”

Overall, CROs stressed that effective conduct risk management requires banks to place customer care at the centre of their decision making. As emphasised by **Diemer Salome**, this can mean that banks may be required to exercise restraint, sometimes during periods of great opportunity. “The issues that can be observed in the industry around mis-selling, once again illustrate the old wisdom that the true art of risk management is to restrain the organisation in times that the market is booming and keep enforcing customer due care, even when this is not at the forefront of the mind of the client base,” he says. “It seems so simple, but in practice it is quite challenging for the risk function to achieve.”

It requires refraining from growing too much when faced with certain market opportunities and at times when there are not yet any clouds on the horizon.”





**Miguel Mairlot, Manager,**  
Avantage Reply

### Structural approach

To limit conduct risk, it is important to take into account four criteria.

First of all, the evidence – “if it’s not recorded, it didn’t happen”. It is fundamental to ensure that any electronic communication devices are fit for purpose and all communications are recorded and retained according to firm and regulatory requirements. When communicating with clients and or counterparties, it’s important to be clear, fair and not misleading, and to ensure that individuals are aware of their responsibilities and that these are understood properly.

Secondly, being able to ‘look back’ is also critical. A bank needs to be able to understand the existing inventory of products, and potential impact on the firm and its customers; from boards through to service and operational personnel. The CRO has to make sure that there’s nothing lurking in the inventory that isn’t fully understood, and that risks are thoroughly understood and mitigated on a product by product basis.

Thirdly, the ability to ‘look ahead’ is also important, and to ensure that the risk function is embedded in any new product approval process along with other critical functions. Education and training are also key. This is a great opportunity to learn from past mistakes.

Finally, I have to mention the need to ‘assess both prudential and conduct risks’. Risk officers have been historically focused on prudential risks. However, the real downfall in most cases over the past five years has been the poor way in which firms have conducted business. CROs therefore need to ensure that they are up to speed with business standards and be aware of those standards that apply to their business. Collaboration with the compliance function and other important functions are critical in understanding conduct risks and how they apply to the firm, staff, customers and most importantly, the CROs.

Engaging employees and making compliance part of a bank culture are big challenges for banks. Drawing on our ten years’ experience in compliance and conduct risk management, **Avantage Reply** has partnered with our specialist employee communications sister company, **Avvio Reply**, to offer a targeted solution. Our new publication, **‘Empowering Your Employee’**, outlines our combined experience and guidance on how banks can establish a positive conduct risk management culture in their workplace.



# THIRD PARTY RISKS, INCLUDING OFFSHORING AND OUTSOURCING

---





**THIRD-PARTY RISK, INCLUDING OFFSHORING AND OUTSOURCING, ARE GAINING INCREASING PROMINENCE WITHIN THE EUROZONE. DATA LOSS AND CONTROL BREACHES RELATED TO OUTSOURCING ARE AN INCREASING CAUSE OF CONCERN FOR BUSINESSES. WHAT ARE SOME OF THE KEY RISKS RELATED TO THIRD PARTIES? AND WHAT ARE THE KEY MEASURES THAT CHIEF RISK OFFICERS CAN USE TO MITIGATE THESE THIRD PARTY RISKS?**

While the first, second and third lines of defence buzz with activity, protected by a complex array of cyber walls, moats and ramparts, reminiscent of an elaborate French castle or a hacker's Guantanamo bay, a lonely figure toils in a dusty back room in India, harvesting your client's details on an industrial scale.

This is the stuff of nightmares in the financial services industry and represents one of the most common and grave dangers facing financial institutions today.<sup>8</sup> While outsourcing has brought cost savings, expertise and operational efficiencies, the inherent complexity of international financial institution means that management and control of these activities becomes harder and harder.

In the information age, when a vulnerability (and every financial institution has them) is exploited, the efficiency and scale of the system becomes its own undoing. As thousands of hours of clerical work can be done with the push of a button, so too can tens of millions of pages of client data be shared with criminals. Ultimately, banking profits are built on trust, volume and margins. In the face of margin headwinds and relentless customer pressure to process more transactions faster for less, there is a danger of eroding precious trust by taking excessive offshoring and outsourcing risks.

"There are things we need to outsource," says **Joris De Backer** of **Beobank**. "If you take certain IT elements, for example, we're better off outsourcing them. It is absolutely key, and frankly it is a strategic risk if we don't outsource what we should."

Not all banks have the same requirements or perspectives on outsourcing.

<sup>8</sup> 'Worlds biggest data breaches hacks', *Information is beautiful*, 11 August 2015, available at <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>

# THIRD PARTY RISKS, INCLUDING OFFSHORING AND OUTSOURCING

For **Mediobanca's Pierpaolo Montana**, as the CRO of a **boutique Italian bank** with a strong reputation and tradition, "it's mainly about outsourcing the execution, never the competencies, or the problem solving."

## Loss of control

Outsourcing and offshoring pose significant risks. Controls are critical, according to **Thierry Lopez** from **Banque Internationale à Luxembourg**. "If you lose control of your outsourcing and ignore, for instance, the subcontracting cascade or non-compliance with laws and regulations, it will be exceedingly difficult to turn things around," he says. "In this situation, the consequences of what your outsourced service providers have been doing, without your knowledge, remain your company's responsibility at all times. This loss of control has every chance of materialising if your control framework is not systematically rigorous."

This situation can cause long lasting and considerable damage. The Financial Times recently reported that the fall in market value for companies hit by penalties over breaches committed by third parties can be more than 10 times that of the fine itself.<sup>9</sup>

An associated risk with outsourcing or offshoring, is that a service company becomes dominant over the primary company and sets the business agenda. "The lead should obviously remain with the business. That is, with the bank," says **Joris De Backer**. Subsidiaries of large banking groups can face significant challenges in asserting authority over third party service providers.

"Another risk is where you are a small fish in a big pond," notes **De Backer**. "Your priorities and requirements, including requirements that result from local relationships, may not be given the same degree of priority that you would have been given, had been fully in control. There is a risk that the IT outsourcing service provider, for example, takes precedence over the priorities of the business. Finding the right way to mitigate that risk is fundamental."

## Building the right framework

Creating a robust framework which defines the control structure including roles, responsibilities, accountabilities and separation of

duties is fundamental to limiting third-party risk. This includes setting up the right key performance indicators (KPI), key risk indicators (KRI), implementing proper governance, collecting information on the supplier and conducting due diligence visits.

"At **Santander**, one of the third-party outsourcing service providers did not have an appropriate Business Continuity Plan," recalls **Keiran Foad**. "The KRI prompted a red flag and we remediated the situation with the supplier." **Santander** has improved its vendor management policies, including robust risk assessment of suppliers, and an enterprise-wide programme to identify supplier side risks.

**Rabobank's Diemer Salome** highlights the importance of considering the level of quality across the entire supply chain. "Quality is only as good as the weakest link in the chain," he says. "You need to be certain that outsourcing partners are offering at least the same level of quality you want to offer your clients. This can only be done by actively measuring and managing service level agreements."

**Thierry Lopez** maintains that outsourcing partners should be managed similarly to in-house departments. This approach will help ensure the required balance of control, autonomy and quality: "The CRO needs to systematically attend follow-up meetings. He or she must treat contractors as if it were his or her own department, giving clear directions, setting precise boundaries and also allowing the required degree of autonomy. The CRO must set objectives and check whether these have been met."

According to **Joris De Backer**, outsourcing companies are not always willing to be entirely open with their clients. "The business continuity arrangements of your outsourcing service providers are sometimes a bit more complicated to assess and get a good handle on", he says. "Providers can, sometimes, be a bit reluctant to share that information with clients, for reasons that are understandable. They may not want to 'open up their kimono', and share with the wider world how they would continue to do business in the event of a natural disaster or a terrorist event, for example."

Each bank has its own way of dealing with third party risk, but as **Keiran Foad** recognises, there are no easy answers. "We try our best to tackle this," he says. "It is a complicated task and it's true that the maturity of outsourcing risk management is probably less developed than for other risk types."

<sup>9</sup> Caroline Binham, 'Companies face lasting damage after third-party misconduct', *The Financial Times*, 2 August 2015, available at <http://www.ft.com/cms/s/0/905d027a-37a9-11e5-b05b-b01debd57852.html>



***“In August 2014, the UK FCA fined an insurance firm £8.4 million for failing to treat customers fairly over the sales by outsourcing companies of accident insurance. The FCA added that inadequate business practices were “made possible by Stonebridge’s poor systems and inadequate oversight of the outsourcing companies.”***

Adapted from ‘FCA fines Stonebridge International Insurance Limited £8.4m in relation to sales of insurance policies’, FCA, 7 August 2014, available at <https://www.fca.org.uk/news/fca-fines-stonebridge-international-insurance-limited-84m>



**Rohan Wilson, Senior Consultant**  
Avantage Reply

#### **Test the fall back**

The key risks in engaging with third party suppliers are loss of control, less flexibility and compromised independence. CROs can challenge the business by performing due diligence, by insisting on real, effective and utilised management information, and by making sure they know where the work is performed and by whom.

Banks therefore need to improve their agility and their resilience, whether that means cultivating a relationship with another supplier, or by retaining skill and experience or by having multiple sites.

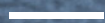
It is important to test the ‘fall back’, putting aside a full day to test resilience. Nevertheless, we have to be careful of a soft ‘fall back’, where the BAU teams surreptitiously assist the ‘fall back’ teams. The bravest option is to organise a surprise fail.

There are also ways to increase one’s independence. This includes retaining experienced staff, researching viable alternatives to changing supplier and clear management direction coming from the outsourcer to the supplier.

It is essential for the first line of defence to take responsibility for managing the third party relationship. It is also important to maintain a healthy degree of scepticism about the quantitative assessment of operational risk, as there is often a lot of ‘play’ in the numbers. As for the use of technology, it is a source of efficiency and a great facilitator, but it can also be a source of great vulnerability. How carefully is your supplier protecting your data?

Finally, we have to be careful of the less obvious risky lines of business and consider the dynamics of the outsourcing arrangements in a crisis. We need to ask the question: who else uses our ‘fall back’?

# OTHER RISKS AND TRENDS



**INTEREST RATES, TECHNOLOGY AND CYBERCRIME, MIS-SELLING AND BUSINESS CULTURE, OUTSOURCING AND OFFSHORING ARE AMONG THE MAIN RISK WORRYING CHIEF RISK OFFICERS; BUT THERE ARE OTHER RISKS WHICH WARRANT CONSIDERATION.**

Change to the legal and regulatory environment within which banks operate is a big concern for CROs. **Keiran Foad** of **Santander UK** says that with regulatory pressures increasing and legal obligations tightening, “some stakeholders have a tendency to take a backward looking view on what has happened in the past, imposing a view from the present onto old events”.

A consequence of an intense period of regulatory change is administrative overload. “An element of proportionality is needed to manage the increased regulatory requirements for documentation and transparency,” says **Diemer Salome**, Head of Risk Advisory and Support Financial Markets of **Rabobank International**. “We need detailed and demonstrable accountability without it becoming an undue administrative burden and a continuing focus for the management team.”

Non-Financial risk management is also becoming increasingly important for organisations such as **Rabobank** – the bank is now strongly focused on compliance, IT risk, data privacy and business continuity. This is partly in response to regulatory pressures. “These risk categories are often covered jointly in the first line of defence functions and integration of risk management increases its effectiveness in that first line,” says **Diemer Salome**. “At the same time, we are moving away from adding increasing numbers of process controls. Instead, we are investing in risk profiling, managed in a balanced way, by considering attitudes and behavioural controls.”

On a broader level, market instability is generating new challenges in risk management and a sense of unease for CROs.

“What worries me most is the global market generally,” says **Joris De Backer** of **Beobank**. “When I see what has just happened in Greece, when I see what recently happened in China, with the market tanking by more than 30%, when I see what the ECB and the Fed have on their balance sheets, where do we stand? And how will it end?”



**Tom Banens, Senior Manager,**  
Avantage Reply

**The data and risk systems conundrum**

Information technology (IT) systems can be a significant source of risk. The increasing pace of regulatory change is making it even more important for risk management to focus on IT issues. New developments including FRTB, SA-CCR, BCBS 239 and stress testing exercises require greater data granularity and quality. These requirements are leading to extensive risk system change programmes, with objectives of increasing the traceability and quality of data, and the speed and robustness of calculations.

To business users, an IT system can seem like a mysterious black box. Understanding the complex process by which output results are produced is a difficult challenge. The new “principles for effective risk data aggregation and risk reporting” (also known as “BCBS 239”), emphasises defining, gathering, and processing data. This includes sorting, merging and breaking down data sets.

BCBS 239 requires wide-ranging IT changes. This provides an opportunity to update or rebuild out-dated legacy systems. Systems which have often outgrown their original purpose. An opportunity to radically redesign and/or simplify a complex architecture.

Automating manual processes and automating reconciliations will also improve efficiency. However, these changes present challenges and risks in managing data and business structure. The recognition of these important responsibilities has led to the emergence of new roles, such as the position of Chief Data Officer.

The opportunities are great, and so are the challenges.

# CONTACTS

## Avantage Reply (Amsterdam)

The Atrium | Strawinskylaan 3051  
1077 ZX Amsterdam  
Netherlands  
Tel: +31 (0) 20 301 2123  
E-mail: [avantage@reply.com](mailto:avantage@reply.com)

---

## Avantage Reply (Brussels)

5, rue du Congrès/Congresstraat  
1000 Brussels  
Belgium  
Tel: +32 (0) 2 88 00 32 0  
E-mail: [avantage@reply.com](mailto:avantage@reply.com)

---

## Avantage Reply (London)

38 Grosvenor Gardens London  
SW1W 0EB  
United Kingdom  
Tel: +44 (0) 207 730 6000  
E-mail: [avantage@reply.com](mailto:avantage@reply.com)

---

## Avantage Reply (Luxembourg)

46A, avenue J.F. Kennedy  
1855 Luxembourg  
Luxembourg  
Tel: +352 26 00 52 64  
E-mail: [avantage@reply.com](mailto:avantage@reply.com)

---

## Avantage Reply (Milan)

Via Castellanza, 11  
20151 Milano  
Italy  
Tel: +39 02 535761  
E-mail: [avantage@reply.it](mailto:avantage@reply.it)

---

## Avantage Reply (Paris)

5, rue des Colonnnes 75002  
Paris  
France  
Tel: +33 (0) 1 71 24 12 25  
E-mail: [avantage@reply.com](mailto:avantage@reply.com)

## Avantage Reply (Rome)

V.le Regina Margherita, 8  
00198 Roma  
Italy  
Tel: +39 06 844341  
E-mail: [avantage@reply.it](mailto:avantage@reply.it)

---

## Avantage Reply (Turin)

Via Cardinale Massaia, 83  
10147 Torino  
Italy  
Tel: +39 011 29101  
E-mail: [avantage@reply.it](mailto:avantage@reply.it)

---

## Xuccess Reply (Berlin)

Mauerstrasse 79  
10117 Berlin  
Germany  
Tel: +49 (30) 443 232-80  
E-mails: [xuccess@reply.de](mailto:xuccess@reply.de)

---

## Xuccess Reply (Frankfurt)

Hahnstrasse 68-70  
60528 Frankfurt am Main  
Germany  
Tel: +49 (0) 69 669 643-25  
E-mail: [xuccess@reply.de](mailto:xuccess@reply.de)

---

## Xuccess Reply (Hamburg)

Brook 1  
20457 Hamburg  
Germany  
Tel: +49 (40) 890 0988-0  
E-mail: [xuccess@reply.de](mailto:xuccess@reply.de)

---

## Xuccess Reply (Munich)

Arnulfstrasse 27  
80335 München  
Germany  
Tel: +49 (0) 89 - 411142-0  
E-mail: [xuccess@reply.de](mailto:xuccess@reply.de)





Editor disclaimer: The information and views set out in this journal are those of the authors and do not necessarily reflect the official opinion of Avantage Reply. Avantage Reply does not guarantee the accuracy of the data included in this journal. Neither Avantage Reply nor any person acting on its behalf may be held responsible for the use which may be made of the information contained therein.

