A changing world for bank analysts: new skills needed for new risks

The latest bank results season is upon us and analysts are once again dissecting banks’ quarterly earnings reports, looking for angles derived from the over or under-performance of specific business lines, or from basis-point variations of previously arrived at consensus. In analyst calls, bank CEOs and CFOs will shape their messages towards what they know analysts need and expect: commiserate over negative rates and assorted macro uncertainties, draw attention to cost cuts, address current headlines etc.

But some large stones will probably continue to be left unturned. The current dynamics reshaping the banking industry are in no way a copycat of those that led to the last financial crisis. Bank analysts will need to adjust their focus and build new skills to be able to assess the new risks. Traditional metrics may not be appropriate for the job. Alternatives like scenario analysis could help.

Changing bank risk dynamics…

Four Horsemen of Risk for the banking industry need far more analytical focus than before:

1. **Digital disruption**: the challenge to banks’ existing “analog” cultures, business models, revenue generation and cost structures posed by the fast-advancing digital ecosystem – fintechs, open platforms, artificial intelligence, cloud and digital-ledger technologies.
2. **Cyber risk**: The more the banks become parts of the digital ecosystem – for products, client relationships, transactions, operations – the more they become vulnerable to cyberattacks or cyber accidents. Moat banks now identify cyber risk as the gravest for the industry.
3. **Misconduct (including money laundering)**: This is increasingly a headline risk for banks, one which catches analysts’ and investors’ attention after the fact. The risk of bank misconduct is wider than just money laundering (which is capturing the latest headlines). It includes also terrorist financing, sanctions busting, assisting tax avoidance or evasion, product mis-selling, market abuse, etc.
4. **Climate change and environmental**: Physical and transition risks are the two areas of climate change-related risk. In addition, banks need to heed other environmental risks such as water security, air pollution, deforestation, etc. These risks are becoming increasingly central, with a growing focus from investors, other market participants, policymakers and regulators.

It is likely that future bank stresses, possibly future banking crises, will emerge from these areas. Looking at them through the wrong lenses will not help. For example, a bank with reassuring prudential metrics, a safe loan portfolio, stable funding and decent profits can pop open a money-laundering scandal. Or be the victim of a massive hack or a cyber accident (possibly due to inadequate cyber protection systems and practices). Or emerge as a major financing source to an industry harmful to the environment. By and large, these risks cannot be assessed by using the financial metrics analysts already have in their quivers. Widely accepted metrics to measure them do not yet exist.

Author

Sam Theodore
+44 (0)776 932 1043
s.theodore@scopeinsights.com

Investor Relations

Debbie Hartley
+44 203 871 2872
d.hartley@scopegroup.com

Media

André Fischer
+49 30 27891 147
a.fischer@scopegroup.com

Scope Insights

Suite 204
2 Angel Square
UK-London EC1V 1NY

Phone +44 20 3457 0444

Scope Group

Lennéstraße 5
10785 Berlin

Phone +49 30 27891 0
Fax +49 30 27891 100

www.scopegroup.com

Bloomberg: SCOP

Whenever these risks are looked at, they are in most cases linked by analysts to existing prudential or financial metrics (which are not necessarily the most appropriate); the impact on income and capital of a potential legal fine by using past examples (from different years, jurisdictions, and for different misdeeds), or of a cyberattack by using a past example of another bank in another system which was a victim of hacking.

But the harm can be massive and far more durable than the impact on a bank's bottom line in the following quarter or at year-end. And it cannot necessarily be modelled using existing financial analysis tools. A serious hack on a large bank could critically damage customer trust (even if customers do not suffer actual losses) and could challenge the bank's and even the sector's digital presence. A bank's image and business reputation can be materially hurt by conduct misdeeds (money laundering or otherwise) well beyond the legal or regulatory fine it has to pay. Equally, being slow and hesitant with new technologies and platforms can see a bank being punished with gradual erosion of market share and revenues in a way that cannot be easily captured by traditional financial metrics in a forward-looking fashion.

…make an adjustment of analytical focus unavoidable

Investors, policymakers, regulators, banks' business and individual customers (especially the younger generations) are increasingly attentive to a bank's image going beyond the P&L. A bank with a relatively clean image will not necessarily be the public's first choice (there are several other factors in the mix), but a bank with a tainted reputation stemming from the risks mentioned above will surely suffer discomfort among its constituents.

ESG factors increasingly weigh more heavily in these choices. For investors, a broader definition of ESG includes not only environmental and social aspects but misconduct and cyber risk too, as aspects of governance. Bank analysts need to adjust their focus in this direction and build new skills accordingly. Nobody in the market will want to be thought of as the dinosaur missed by the asteroid.

1. **Digital disruption risk**[1]: Bank analysts should aim to broaden their expertise beyond their home base of financial institutions and the financial sector by becoming more familiar with the digital component of other sectors such as e-commerce, mobile telecoms, or non-bank payments. Based on the assumption that sooner or later the disruption of the financial services sector in its current form will gather speed and volume, bank analysts will want to look not only at banks' attempts at pushing disruptors back. They will also aim to assess the skills, capacity and willingness of non-financial disruptors. Last, but not least, analysts will need to focus more on the related regulatory framework. In Europe, this suggests that, as important as the widely followed prudential regulations for banks are, a more in-depth assessment of the impact of non-prudential regulations such as PSD2 is essential to understand the future dynamics of the industry.

2. **Cyber risk**[2]: The area of cybersecurity is arcane, difficult to penetrate in the absence of the right professional background. And, in general, the career choice of cybersecurity experts is not to analyse financial institutions for the benefit of investors. Also due to the fully understandable reluctance of bank cybersecurity experts to share critical details with outside parties like analysts and investors it is very likely that a comprehensive view of the cyber protection architecture of a bank will not be assessable from the outside. Nevertheless, a basic knowledge of key cyber risk aspects – a bank's external network protection, internal vulnerability to cybercrime (phishing, malware, targeted social engineering) – will help. Similarly, the ability to assess the quality and reliability of outside vendors (including cloud and DLT providers) should prove useful to the bank analyst.

[1] For details see the respective Wide Angle report at https://www.scoperatings.com/ScopeRatingsApi/api/downloadstudy?id=9c5057d1-81e0-4f3d-997a-0eb1a0006e1b
[2] For details see the respective Wide Angle report at https://www.scoperatings.com/ScopeRatingsApi/api/downloadstudy?id=c094f63a-1ee5-45b9-86b2-46f33ed732a2

3. **Misconduct risk (including money laundering)**[3]: Again, proper understanding of non-prudential financial regulation related to misconduct is essential. In general, misconduct risk is supervised differently from prudential risk, and by a different set of supervisors. In the UK it is the FCA (vs. the Bank of England for prudential). In the euro area, it is the national competent authorities (vs. the SSM for prudential). With respect to money laundering, the EU's latest Anti-Money Laundering Directive (AML5) is quite comprehensive, and its forthcoming version (AML6) will be even more so. But there is still visible daylight between the regulations themselves and the way they are implemented on the ground at the national level for the banks. Analysts will need to become more familiar with these discrepancies and their risks. In this way, they will not be prone to overshooting on the latest headlines (not all money laundering rumours are true) and may be able to detect negative scenarios before they become public.

4. **Climate change and environmental risks**[4]: A good starting point for bank analysts is to get familiarised in detail with the climate change-related bank supervisory recommendations of the central banks' Network for Greening the Financial System (NGFS) and the main climate-related disclosure recommendations of the FSB-established Task Force on Climate-related Financial Disclosure (TCFD). Equally, CDP's (formerly Carbon Disclosure Project) scores of public companies' climate and environmental-related disclosure – which includes banks – can help analysts understand a new and essential reporting area which is not within the traditional financial-statement bailiwick of existing bank assessment. The latest scores were published in June. Overall, to look properly at climate change and environmental challenges for banks, analysts will need to broaden their knowledge horizon into related scientific concepts, ethical aspects, and understanding other industry sectors such as energy (fossil fuels vs. renewables), power generation, manufacturing, utilities, etc.

Metrics vs. scenario analysis

Not all risks related to financial institutions can be modelled or have specific metrics associated with them. As the crisis made painfully clear, some of the major ones fit this description. But not having a tested measurement metric does not mean the respective risk can be passed over. One alternative is scenario analysis including 'what if' narratives. They may look less scientific than precise ratios and percentages (many of which will be proven wrong in due course anyway) but they could offer a quasi-realistic depiction of some of these risks.

For example, when trying to anticipate money-laundering events, the analyst can look at the geographical and business-activity reach of the respective bank. An active presence in markets more prone to criminal activities where the rule of law is more timid or in activities likely to attract money-laundering– such as private banking and wealth management – will likely present a higher risk than in the case of a retail and consumer bank mostly present in its home market in Western Europe. Against this heightened risk propensity, the analyst can assess the track record of the respective jurisdiction's supervisors and of the bank itself with respect to, say, money-laundering risk.

In most cases, negative scenario outcomes will never materialise, but that is not a reason to avoid proceeding with the analysis.

Similarly, by assessing the dynamics of competition in cyberspace – fintechs, neobanks, digital open platforms, other banks which are more digitally advanced – the analyst may be able to approximate the vulnerability of a specific bank facing market share and revenue erosion due to external digital disruption.

Scenario analysis for a specific bank is more difficult and speculative with respect to climate and environmental change, due to the very long timeframes attached to these. Nevertheless, as disclosure improves every year, this type of analysis should become more reliable and relevant.

---

[3] For details see the respective Wide Angle report at
https://www.scoperatings.com/ScopeRatingsApi/api/downloadstudy?id=a28df08e-9772-4c43-9062-fb3163dd352d
[4] For details see the respective Wide Angle report at
https://www.scoperatings.com/ScopeRatingsApi/api/downloadstudy?id=61e73d35-1d50-4e7e-95ea-fc2323e31eb4

About Scope Insights GmbH

Scope Insights provides independent credit research and commentary to help market participants understand and navigate the complex cross-currents at play in international financial markets. Scope Insights' content is not rating-related and is not produced by Scope Ratings' analysts. In addition to independent opinions and comments, it includes relative-value analyses and comparisons to help investors make better credit decisions relating to debt issued by financial institutions, non-financial corporates, and public-sector entities, with an initial focus on Europe.

Scope Insights GmbH

Lennéstraße 5
D-10785 Berlin

Phone +49 30 27891 0
Fax +49 30 27891 100

Disclaimer