Too important to ignore: how banks can get a grip on operational risk

By Dr. Tom Huertas, Partner, EY EMEIA Financial Services Risk Management group

On banks’ risk dashboard, the signal for operational risk is – or should be – flashing red. Over the past ten years, losses from operational risk have soared. That has reduced earnings and depleted capital. Consequently, both investors and supervisors are demanding that banks bring this risk under control.

WHAT IS OPERATIONAL RISK?
In the dry language of the Basel Committee, operational risk is “the risk of direct or indirect loss resulting from inadequate or failed internal processes, people and systems or from external events.” This broad definition covers a myriad of non-financial risks, including conduct risk, fraud, cyber, vendor risk, privacy, unauthorised trading and information security.

Losses from operational risk have been quite significant. Over the past ten years, these have amounted to over $300 billion, stemming from a wide range of breaches in controls, conduct and security. Investors and supervisors are increasingly questioning whether banks will actually be able to retain all the earnings they initially report, or whether they will have to pay back a significant portion in fines and restitutions.

Banks’ reputations have suffered perhaps even more than their finances. In tabloid terms, operational risk has generated headlines such as:
- “Banks fined for fixing markets.”
- “Banks fined for gouging consumers.”
- “Banks fined for abetting financial crime.”
- “Hackers halt and hold up the bank.”

Figure 1. Operational risk core components
Controlling operational risk can therefore go a long way toward revitalising banks’ business models and restoring banks’ reputation.

**SUPERVISORS STRENGTHEN THEIR STICK**

Supervisors endorse these objectives and are taking steps to “nudge” banks in the right direction. The Basel Committee is proposing to alter capital requirements for operational risk. To assure consistency across banks, the proposed regime will take a single standardised approach. This has two features:

- A base requirement scaled to the size of the bank’s business. This increases as the scale of the bank increases, in a manner similar to increases in the marginal rate of tax under a progressive tax regime. The top marginal rate will be 29% of the bank’s “business indicator” (adjusted revenue).
- A multiplier that reflects the bank’s operating loss history over the past ten years relative to the size of the bank’s business. In determining the multiplier a higher weight is given to losses in excess of €100 million. If the bank has no or very low losses, the multiplier can become less than 1, so that the actual requirement for operational risk could be as low as 54% of the base requirement.

If that prospect represents the carrot, stress testing and the Supervisory Review and Evaluation Process (SREP) provide the stick. Supervisory stress tests routinely require that banks set aside capital now for the fines and settlements for which they might become liable over the stress test horizon. And, in the SREP process, supervisors assess the bank’s governance, systems and controls and may impose a surcharge on those banks whose controls are deemed to be deficient or need improvement.

In addition, supervisors have sharpened surveillance, empowered enforcement and propelled penalties to new heights. If banks are committing a breach, there is a greater probability it will be discovered; if discovered, a greater probability that the breach will result in a penalty; and a near certainty that the penalty will be high and headed higher.

**HOW SHOULD BANKS RESPOND?**

Sound risk governance provides the framework in which banks can identify, measure and mitigate operational risk. This defines the bank’s risk appetite, assigns responsibilities and develops specific plans.

A bank’s appetite for operational risk should be extremely low. A bank can have no appetite for risks that violate the law (e.g. rigging benchmarks) and it should show no tolerance to employees who do. For
Can compliance help you compete?

EY’s global financial services team can help you navigate regulation and create competitive advantage. ey.com/financial #BetterQuestions

The better the question. The better the answer. The better the world works.
other risks (e.g. cyber) the reward for taking the risk is often not apparent. There is little opportunity to charge for risks that result from lagging behind best practice. Although the bank may save cost in the near term, this could well be penny-wise and pound-foolish.

To translate this risk appetite statement into action, the bank will need to:

- Identify and understand each of the operational risks (conduct, fraud, cyber, etc.) related to customers, products, markets and businesses. This exercise includes drawing lessons learned from dealing with legacy losses as well as assessing whether gross risk can be mitigated and, if so, at what cost.
- Weigh the reward the bank is likely to achieve against the risk that will remain after mitigation. This should include a worst-case scenario and take into account the adverse consequences that a problem in one area might have upon the reputation, liquidity and capital of the bank as a whole.
- Make a leave or stay decision with respect to customers, products, markets and businesses.

If the decision is to leave, banks will need to exercise care in how they do so. Banks may face constraints in “off-boarding” customers or discontinuing products and services, particularly if such actions would adversely affect vulnerable or politically influential segments of the population. It may also be difficult to exit by selling the business. Antitrust and/or resolvability concerns may preclude selling to an in-market competitor, and many supervisors remain adverse to private equity as the owner of a bank. Consequently, banks will need to consider how they might wind down businesses they want to exit as well as how they might sell such entities.

If the decision is to stay, banks will need to ensure that losses from operational risk stay within (and ideally fall well below) the levels underlying the stay decision. Three steps deserve special emphasis:

- Make line management responsible for managing non-financial risk. Business heads are the first line of defence, and they are in the best position to identify, mitigate and manage operational risk as well as to balance this risk against reward, not only for the business as a whole, but also for the individuals working in the business (by making their compensation dependent on their adherence to effective risk management). Boards may wish to question management as to the circumstances under which future earnings could be adversely effected by current or past (“incurred but not reported”) operational risk events.
- Make the second line of defence (Risk Management and Compliance) responsible for controlling the quality of the risk management that the first line puts in place. That is the proper role for the second line. The second line’s review should not only evaluate the effectiveness of the first line’s policies and procedures but also determine whether the first line is adhering to the bank’s risk appetite. To do so the second line will need to benchmark against best practice, probe processes for weak spots, and ensure that business heads in the first line are taking prompt corrective action to nip problems in the bud.
- Equip both the first and second lines with the tools necessary to accomplish their objectives. Here, data and analytics are likely to be decisive, for they will enable banks to score products and services for operational risks and to monitor adherence of staff to policies and procedures.

Taken together, these steps should enable banks to shift the emphasis from curing breaches to preventing them, as the following examples show.

WHOLESALE MARKETS: ARE YOU IN CONTROL?

Benchmark rigging, mis-selling and unauthorised trading incidents at major banks have created the impression in some quarters that misconduct is the norm at banks, at least in wholesale markets. That such misconduct came as a surprise to the executives responsible has prompted commentators to question whether banks have become too complex to manage and supervisors to ask executives “are you in control?”

“Yes” must be the answer that executives can demonstrate, if they are to comply with increased supervisory standards on individual accountability such as the UK senior managers regime. “Yes” must also be the answer, if the bank is to actually exhibit the “zero tolerance” for losses from failure to act with integrity or to comply with regulation. For executives to be able to answer “yes, I am in control,” banks need to:

- Review policies and procedures to assure that the bank complies with all relevant regulations in each of the jurisdictions in which it does business. Of particular importance to the question of operational risk are requirements relating to suitability, transparency, conflicts of interest, insider trading and other forms of market abuse, segregation of client assets and transaction reporting.
- Test the procedures front to back to assure that they work as intended and that they cannot be gamed, evaded or subverted, either by employees or third parties.
- Use surveillance to detect unauthorised trading and possible market abuse. Investigate potential cases promptly. Deal harshly with those who violate policy.
Some of the largest losses from operational risk have resulted from shortcomings in the design and governance of products sold to consumers. To limit such losses in the future as well as to respond to increasing supervisory scrutiny, banks are starting to score products and services. This helps banks avoid some risks entirely and to limit losses from the risks that remain.

The risk scoring approach front loads risk management. Rather than dealing with problems after they occur and then seeking the root cause, the scoring approach takes a forward look, starting with the intrinsic risk stemming from product design, target market definition and distribution strategy. In particular, it clearly profiles the risk of the product; checks that the product is suitable for the target market; determines whether disclosure is both accurate and appropriate; creates clarity of responsibility in the distribution chain and ensures that compensation reinforces effective risk management.

Arguably, these are all results that a bank should get from its product approval process. However, these processes by and large start and stop at the product introduction stage. The scoring approach not only sets an initial score; it makes sure the business keeps ongoing risk within that score. It tracks whether the bank is actually selling the product to customers within the target market as well as whether the product actually performs in accordance with the disclosure made to consumers. If such tracking reveals that the bank is veering off course, the bank cannot simply drift where profit would otherwise drive it. The bank has to revert to the original plan or make the case to amend the product’s features, target market, distribution and/or disclosure.

EMERGING RISKS: CAN YOU IDENTIFY AND MITIGATE THEM?

The shift from cure to prevention also requires the bank to identify and mitigate emerging risks. Digitisation is a case in point. This opens new ways for clients, vendors and third parties to interact with the bank. It promises greater convenience, greater choice and greater transparency, all at faster speed and lower cost.

But digitisation may also entail risk. As access becomes more open, how does the bank continue to protect privacy, safeguard assets and preserve the integrity of its systems? Or will digitisation open the door to cyber criminals and/or cyber terrorists? As reliance on vendors increases, how does the bank control the quality of the services that they...
CONCLUSION

As these examples show, operational risk is – or should be – occupying a prominent place on banks’ risk management agenda. Losses have been substantial, and future risks – both internal and external – abound. Both supervisors and investors are demanding that banks bring operational risk under control.

Banks can do so, and many banks are well on the way to doing so. The leader banks have strengthened governance, assigned responsibility to line management and improved risk management. They are identifying the operational risks inherent in their various businesses; assessing if, how and at what cost such risks can be mitigated; and evaluating whether accepting the remaining risk is consistent with their strategy. If it is not, leaders have left, either by selling the business or winding it down. Where leaders decide to stay, they are strengthening their lines of defence by appropriate investments in technology, data and analytics. They are also making supervisory exercises such as stress tests and recovery and resolution planning do double duty. The analyses not only help the bank pass the exam; they also point the way toward measures that can help mitigate operational risk.

The service company is one such measure. This pulls together into a separately capitalised subsidiary the essential services the bank will need in order to continue in operation whilst it is being resolved. In the process of planning for death, banks are taking steps to make life better: Banks are cataloguing, rationalising and renegotiating inter-affiliate service-level agreements and contracts with third party providers. The service company is also pulling disparate silos together into a single unit. This standardises procedures, allows the bank to realise economies of scale and strengthens the business case for investment in the new technology necessary to keep up in the race to bring costs down.

Despite this progress, much remains to be done. Laggards need to catch up with leaders, and leaders need to remain on the cutting edge. No small task, as technology continues to develop and the economy continues to struggle. But no small reward for those who succeed: lower losses, lower costs, better profits and a better reputation.

Dr. Tom Huertas
Partner, EY EMEIA Financial Services Risk Management group

E: THuertas@uk.ey.com
T: +44 20 7151 2556
W: ey.com/grn

About the author
Dr. Tom Huertas is a partner in the EY EMEIA Financial Services Risk Management group, and chairs the EY Global Regulatory Network. He is a former member of the Financial Services Authority’s Executive Committee. He also served as alternate chair of the European Banking Authority, as a member of the Basel Committee on Banking Supervision and as a member of the Resolution Steering Committee at the Financial Stability Board. Tom holds a PhD in Economics from the University of Chicago, and has published extensively on banking and financial issues, including his recent book “Safe to fail: how resolution will revolutionise banking” (2014).