Mitigating operational risk is becoming a priority for banks that want to avoid penalties, reduce the likelihood of regulatory investigations and rebuild tarnished reputations. That’s prompting a step-change in the way operational risk is viewed and managed – moving away from a siloed, backward-looking approach, and towards a culture in which operational risk is managed proactively, strategically and on an organization-wide basis.
The growing importance of operational risk

Ten years ago, if you looked at a UK bank’s financial statements, you wouldn’t see a lot of ink devoted to things like conduct risk or IT risk. In those days, operational risk was a relatively minor consideration – not something to be managed, calculated and disclosed in the same manner as credit and market risk. Very few institutions made a concerted organization-wide effort to identify areas of operational risk, understand its impact, or put in proactive measures to mitigate it.

But all that has changed. Today, a bank’s ability to understand and manage operational risk is a key factor for commercial success – and the penalties for failing to manage it are growing in size and impact.

What is Operational Risk?

The Basel Committee defines operational risk as the risk of loss resulting from inadequate or failed processes, people and systems or from external events. This definition includes legal risk, but excludes strategic and reputational risk. Legal risk includes, but is not limited to, exposure to fines, penalties, or punitive damages resulting from supervisory actions, as well as private settlements.

This paper looks at four trends driving an increased focus on operational risk. It explores the dangers for financial institutions that continue to manage operational risk in a siloed, ad-hoc and backward-looking manner. And it sets out the many benefits for institutions that can manage operational risk in a strategic way – and demonstrate convincingly that they are doing so.
One of the most powerful arguments for stepping up operational risk management is the size of modern-day regulatory fines for operational failings. Between them, the twin scandals of PPI mis-selling and interest-rate rigging contributed to a massive £42bn in penalties issued by the UK’s Financial Conduct Authority between 2009 and 2014.

Commenting on a further round of misconduct fines in 2014, Tracey McDermott, then the FCA’s director of enforcement and financial crime, clearly signalled the FCA’s continuing willingness to penalize firms that fail to institute strong operational risk management: "This is not about having armies of compliance staff ticking boxes. It is about firms understanding, and managing, the risks their conduct might pose to markets. If they fail to do so they will continue to face significant regulatory and reputational costs." ¹

Other regulators have been equally firm. Following its investigation of Deutsche Bank’s role in the Libor and associated rate-rigging scandals, the German regulator BaFin found the bank’s Global Head of GFFX "specifically responsible for organizational and procedural deficits concerning IBOR submissions, together with general failures in risk management, internal monitoring and business culture," according to Forbes. ²

Small wonder, then, that senior risk practitioners agreed in December 2015 that misconduct was their second biggest operational risk concern for the coming year.³

IT risks are climbing the agenda
And misconduct isn’t the only failing of people, processes and systems to attract hefty fines in recent times. In 2015 the Prudential Regulation Authority (PRA) stunned the industry by issuing its first ever financial penalty – £14m to Royal Bank of Scotland, NatWest and Ulster Bank for a major IT systems failure that in 2012 prevented customers from accessing their accounts.

On that occasion, the PRA found the incident was caused by "the failure of the banks to have the proper controls in place to identify and manage exposure to the IT risks within their business." ⁴

Those words may have sent chills down many Chief Risk Officers’ spines, since banks are instituting ever more complex automated systems, connecting ever more devices to them, entrusting ever more sensitive data to the cloud, and outsourcing ever more systems to third parties.

Even where no fines are involved, glitches in these complex, inter-related systems can be highly damaging to the business. In August 2015, for example, BNY Mellon found itself unable to value billions of dollars of mutual and exchange-traded funds due to a failure in a valuation system run by a third party.⁵

Various facets of information systems rank high on risk practitioners’ worry lists. A survey by Risk.net revealed that IT risks, outsourcing risks and cyber-security risks rank at #8, #6 and #1 respectively on the list of top 10 operational risk concerns for 2016.

Step up operational risk management to avoid penalties
Penalties for operational failings have reached a level where they are having a material impact on firms’ profitability and ability to deliver shareholder value. There’s a clear argument for stepping up the focus on operational risk management, to the point where it becomes an integral aspect of risk management and evidence of good governance across the organization.

“Our data shows that the regulator means business. The £819 million in fines recorded for the first six months of 2015 compares to just £335 million for all of 2013.”

Mary Stevens, Manager of Regulatory Analysis, Wolters Kluwer Financial Services

---

¹ Financial Conduct Authority, FCA fines five banks £1.1 billion for FX failings and announces industry-wide remediation programme, 12 November 2014
³ Risk.net, Top 10 Operational Risks for 2016, December 2015
⁴ Bank of England, Prudential Regulation Authority fines Royal Bank of Scotland, NatWest Bank and Ulster Bank £14 million for IT failures, November 2014
⁵ Financial Times, BNY Mellon close to resolving software glitch, 31 August 2015
Trend #2: Growing emphasis on personal accountability

If the scale of recent fines wasn’t enough to drive this message home to CROs and CCOs, the developments of the 7th March 2016 ought to be.

That day saw the introduction of the Senior Managers Regime (SMR) and Certification Regime (CR); a dual-pronged effort on the part of the financial industry regulators to instil a stronger culture of operational accountability at the most senior levels in UK banks.

Echoing the 2002 US Sarbanes-Oxley Act, introduced in the wake of the Enron scandal, the SMR makes senior executives and non-executives personally responsible for strategic decision-making across the organization. If an operational failure occurs and senior management cannot prove they took reasonable steps to prevent it, they may be personally fined or even banned from the industry.

The Certification Regime, meanwhile, extends that level of accountability to “other staff who could pose a risk of significant harm to the firm or any of its customers”. Everyone who falls under these regimes is obliged to abide by the regulators’ Conduct Rules, which “aim to hold individuals working at all levels in banking to appropriate standards of conduct.”

Co-operative hints at what’s to come

The Co-operative Bank’s experience hints at what may be in store under the SMR and CR. In 2015, the bank’s former CEO and its former head of corporate and business banking were both personally fined and banned from the industry, following widespread failures of governance at the bank.

If an operational failure occurs and senior management cannot prove they took reasonable steps to prevent it, they may be personally fined or even banned from the industry.
Issuing the penalties, PRA chief executive Andrew Bailey made the link between poor governance at individual banks and the stability of the financial sector as a whole. “Banks that are not well governed have the potential to pose a threat to UK financial stability,” he said. “The actions of Mr. Tootell and Mr. Anderson posed an unacceptable threat to the safety and soundness of the Coop Bank, which is why we have decided a prohibition is appropriate in these cases. This action makes clear that there are serious consequences for senior individuals who fall short of the PRA’s expectations.”

**Senior executives must have a robust review of risk exposure**

Under the Senior Managers’ Regime, ignorance of what’s going on in the organization is no longer any defense. That makes it essential for senior executives to have a robust and accurate view of the organization’s operational risk exposure, and of the controls in place to prevent incidents occurring.

Moreover, it requires senior executives to testify that adequate controls are in place and are adhered to, and that a strong culture of governance is present throughout the organization. If an institution does not have a holistic way of managing operational risk, senior management will find it a challenge to personally attest to the existence of a robust risk management framework across the organization – and even more of a challenge to demonstrate to regulators and auditors that such controls are in place and working.

---

6. Financial Conduct Authority, FCA publishes final rules to make those in the banking sector more accountable, 7 July 2015

Trend #3: The growing complexity of modern banking operations

Modern banks are eye-wateringly complex beasts. They operate across borders, offering a diversified array of services. They run their operations on an ever-increasing number of IT systems and deliver service through multiple electronic channels. They answer to numerous regulators in numerous jurisdictions, and must keep pace and comply with hundreds of different global, regional and local rules – some of them potentially conflicting.

On top of this, most banks grow by merger and acquisition, creating a tangled mass of processes, cultures and operating models. It’s a landscape that’s fraught with gaps, silos, broken links, duplications and oversights, all of which create chinks in which operational risk can lurk.

And if that risk is only assessed at the level of individual departments, branches or operating entities, it means nobody is in a position to provide or analyze the bigger picture. Who will notice that a failure in a third-party data center in the Philippines could bring trading to a standstill in London? Or that a customer onboarding process used in a Peruvian subsidiary falls foul of anti-money-laundering rules that the parent entity must comply with?

If a bank doesn’t have the full picture of its operational risk exposure across all of these fragmented operations, it has no hope of understanding and mitigating against the impact of IT failures, or of identifying and preventing potential instances of misconduct.

Experiences banks should be keen to avoid No bank would want to repeat HSBC’s experience in 2012, where inadequate AML controls in its Mexican subsidiary led to a $1.2bn fine, or Deutsche Bank’s experience in 2015, where insufficient compliance procedures in its overseas offices led to a $258m fine for flouting US sanctions laws. Penalties like these not only materially affect financial performance, but also have a serious impact on the bank’s reputation, at a time when banks must do all they can to restore their good name (see next section). A preventative and organization-wide approach to operational risk management can go a long way towards preventing incidents like this from occurring.
Trend #4: The incentive to rebuild reputations

The financial crisis and subsequent bailout, combined with PPI mis-selling, rate-rigging and other scandals, have substantially damaged the reputation not just of individual banks, but of the industry as a whole.

The response from regulators – on both sides of the Atlantic – has been to clamp down hard on the entire sector; introducing rafts of new rules, bumping up penalties, stepping up investigations, and demanding convincing evidence of watertight governance.

It’s reached a point where banks are struggling to cope with the compliance burden. News stories tell of staff coming in every weekend to implement new processes and run regulators’ stress tests. There are so many rules that even knowing which ones are currently in force, and which have been superseded, can be a full-time job. It can be difficult – and risky – to make a decision on the right approach to take in situations where different jurisdictions overlap and their rules appear to differ.

Banks complain that the burden of regulation, and the size of the capital buffers they are obliged to allocate, are seriously affecting their ability to conduct business, operate profitably and deliver shareholder value.

From their corner, politicians and regulators have argued that they can’t loosen their grip until the industry cleans up its act. And there are signs that this may be starting to happen. The volume of fines meted out by the FCA in 2015, for example, was down on the previous year, which many have interpreted as a thawing of hostility towards the sector.

The message seems to be that if banks tighten their controls, and assume greater responsibility for ensuring wrongdoing does not happen, the severity of penalties and capital demands may abate. That’s a strong incentive for banks to evaluate their current approach to operational risk management, and put in place a robust, organization-wide framework that will not only prevent failures from occurring, but will provide adequate evidence to regulators and auditors that appropriate controls are in place.

What it means for risk officers

For senior risk executives in the banking sector, there’s only one real conclusion to be drawn from these four inter-related trends. It’s no longer commercially viable, or wise from a reputational point of view, to leave operational risk management to individual teams or departments, where it’s managed in silos and often only noticed and reported after an incident occurs.

It’s no longer commercially viable to leave operational risk management to individual teams or departments, where it’s managed in silos and often only noticed and reported after an incident occurs.
Operational Risk in the Spotlight – Four Trends Making Operational Risk a Top Priority for Banks

A centralized and standardized approach to operational risk management also reduces the effort involved in manually collating loss data from across the organization; a process that is often subject to human error as multiple spreadsheets are collected and the data manually collated.

Stronger financial performance
With the scale of some fines now having a material impact on profitability, it stands to reason that financial performance will be stronger if the bank can avoid penalties for operational failures. A more robust approach to operational risk is also likely to prevent failures from happening in the first place, thus avoiding any commercial losses that might stem from, for example, a major IT systems breakdown. And an ability to demonstrate strong governance that actively prevents operational failings from occurring is likely to boost regulators’, customers’ and shareholders’ confidence in the bank, with a subsequent positive impact on performance.

That means being able to analyze and manage operational risk as part of the overall risk portfolio. It means understanding how one type of operational risk impinges upon another (e.g. how IT risk and conduct risk intertwine). It means having controls in place across the organization to prevent operational failures from happening – and to ensure appropriate and timely action is taken when they do. And it means senior management being personally accountable for ensuring adequate governance and controls are in place.

If these things don’t happen, the business will not only run the risk of losses and reputational damage, but it will also attract more regulatory scrutiny and potentially be subjected to increased capital allocations, fines and penalties.

What’s in it for banks?
Tightening up operational risk management isn’t just about avoiding unpleasant outcomes. Any institution that takes a robust approach to managing operational risk stands to benefit in three distinct ways.

Improved governance and compliance
As banks grapple with a multitude of ever-changing regulations, a standardized approach to risk management across the organization can help to identify requirements and manage them in a comprehensive way. That can drastically improve compliance – avoiding, for example, scenarios in which subsidiaries fail to observe the stringent rules set down by regulators governing the parent entity.

A centralized and standardized approach to operational risk management also reduces the effort involved in manually collating loss data from across the organization; a process that is often subject to human error as multiple spreadsheets are collected and the data manually collated.

Greater operational efficiency
Much of operational risk management today is fraught with inefficiency; with multiple systems, approaches and individuals dedicated to monitoring, managing and reporting on operational risk, usually on a departmental level. With the right processes in place banks can significantly streamline operational risk management and reduce the administrative workload associated with it – leading to more efficiency and accuracy of organizational information and smoother workflow.

Instead, operational risk management must be woven into the fabric of governance across the entire business.

A standardized approach – that is fully documented and demonstrable – also makes it faster and easier to comply with regulators’ demands for evidence that adequate controls are in place, reducing the chances of a disruptive regulatory investigation. And a robust framework for operational risk management also enables the bank to identify areas of concern and proactively intervene to prevent incidents from occurring; thus avoiding potential fines, losses and disruption.

What’s in it for banks?
Tightening up operational risk management isn’t just about avoiding unpleasant outcomes. Any institution that takes a robust approach to managing operational risk stands to benefit in three distinct ways.

Improved governance and compliance
As banks grapple with a multitude of ever-changing regulations, a standardized approach to risk management across the organization can help to identify requirements and manage them in a comprehensive way. That can drastically improve compliance – avoiding, for example, scenarios in which subsidiaries fail to observe the stringent rules set down by regulators governing the parent entity.

A centralized and standardized approach to operational risk management also reduces the effort involved in manually collating loss data from across the organization; a process that is often subject to human error as multiple spreadsheets are collected and the data manually collated.

Greater operational efficiency
Much of operational risk management today is fraught with inefficiency; with multiple systems, approaches and individuals dedicated to monitoring, managing and reporting on operational risk, usually on a departmental level. With the right processes in place banks can significantly streamline operational risk management and reduce the administrative workload associated with it – leading to more efficiency and accuracy of organizational information and smoother workflow.

That means being able to analyze and manage operational risk as part of the overall risk portfolio. It means understanding how one type of operational risk impinges upon another (e.g. how IT risk and conduct risk intertwine). It means having controls in place across the organization to prevent operational failures from happening – and to ensure appropriate and timely action is taken when they do. And it means senior management being personally accountable for ensuring adequate governance and controls are in place.

If these things don’t happen, the business will not only run the risk of losses and reputational damage, but it will also attract more regulatory scrutiny and potentially be subjected to increased capital allocations, fines and penalties.

What’s in it for banks?
Tightening up operational risk management isn’t just about avoiding unpleasant outcomes. Any institution that takes a robust approach to managing operational risk stands to benefit in three distinct ways.

Improved governance and compliance
As banks grapple with a multitude of ever-changing regulations, a standardized approach to risk management across the organization can help to identify requirements and manage them in a comprehensive way. That can drastically improve compliance – avoiding, for example, scenarios in which subsidiaries fail to observe the stringent rules set down by regulators governing the parent entity.
Conclusion

The four trends outlined in this document send a clear message to senior risk practitioners. It’s no longer acceptable or desirable to leave the management of individual types of operational risk to individual departments. Rather, there must be a systematic way of understanding, managing, analyzing and mitigating operational risk across the organization.

Without that systematic approach, banks will not be able to institute appropriate controls to prevent operational failures from occurring, and will not be able to demonstrate to regulators, customers and employees that strong governance is in place across the business.

Conversely, institutions that successfully embed operational risk management within a robust governance framework will reap benefits ranging from easier compliance and reporting to a stronger financial performance.
About Wolters Kluwer Financial Services

Whether complying with regulatory requirements or managing financial transactions, addressing a single key risk, or working toward a holistic enterprise risk management strategy, Wolters Kluwer Financial Services works with customers worldwide to help them successfully navigate regulatory complexity, optimize risk and financial performance, and manage data to support critical decisions. Wolters Kluwer Financial Services provides risk management, compliance, finance and audit solutions that help financial organizations improve efficiency and effectiveness across their enterprise. With more than 30 offices in 20 countries, our prominent brands include: AppOne®, AuthenticWeb™, Bankers Systems®, Capital Changes, CASH Suite™, GainsKeeper®, NILS®, OneSumX®, TeamMate®, Uniform Forms™, VMP® Mortgage Solutions and Wiz®.

Wolters Kluwer Financial Services is part of Wolters Kluwer, which had 2014 annual revenues of €3.7 billion ($4.9 billion), employs 19,000 employees worldwide, and maintains operations in over 40 countries across Europe, North America, Asia Pacific, and Latin America. Wolters Kluwer is headquartered in Alphen aan den Rijn, the Netherlands. Its shares are quoted on Euronext Amsterdam (WKL) and are included in the AEX and Euronext 100 indices.

Please visit www.wolterskluwerfs.com for more information.