The Operational Risk Awards honour excellence in op risk management, regulation and risk management service provision. Firms were invited to submit entries between February and April, with the final winners chosen using a twin-track methodology during May (see box, below).

As always, this year's awards reflect the ebb and flow of industry trends in op risk. One of those is the Basel Committee on Banking Supervision's decision to propose scrapping the advanced measurement approach – the own-models approach to op risk capital, which effectively allows banks that can model their op risk to hold smaller capital buffers.

Op risk practitioners worry about the adverse impact this could have on banks' future investment in op risk modelling. Going forward, they fear it will lead firms to place less emphasis on modelling and techniques such as scenario analysis.

But this year's Regulator of the year, the Australian Prudential Regulation Authority (Apra), has always valued op risk modelling and scenario analysis in their own right. It is keen to stress their use as tools for improving firms' understanding of op risk, and bringing the views of frontline businesspeople and op risk professionals together. This emphasis on the value of modelling has not gone unheeded by Australia's banks, some of which say they plan to continue investing to better comprehend their op risk exposures.

Other award winners also see the value of op risk modelling, despite the Basel Committee's controversial proposal. This year's Paper of the year award goes to Riaan de Jongh, Tertius de Wet, Kevin Panman and Helgard Raubenheimer – researchers at South Africa's North-West University and Stellenbosch University – who appear to have found an effective shortcut for approximating op risk capital. The technique promises eye-catching benefits, both in terms of time and computing power.

After an explosion of manipulation, mis-selling and rogue trading scandals earlier this decade, many banks have sought to renew their operational risk programmes and move towards a bigger focus on culture and conduct. This year's Bank of the year, UBS, is a prime example.

There, a $2.3 billion rogue trading loss, caused by London-based synthetic equities trader Kweku Adoboli in 2011, presaged a major overhaul of risk and compliance, says James Oates, global head of compliance and operational risk control at UBS in New York. Since then, the bank has reorganised its risk and compliance functions, devised a new firm-wide risk taxonomy, revamped its risk and control assessments, and stepped up its monitoring of employee behaviour and conduct.

While banks have always been relatively adroit when it comes to operational risk management, buy-side institutions have also grown increasingly sophisticated.

For the first time, this year's Operational Risk Awards feature the categories of Asset manager of the year and Insurer of the year. Both of our winners, New York-based asset manager AllianceBernstein and US-based insurer MassMutual, provide strong examples of op risk management in action across the broader financial services industry.

Methodology

The awards were divided into practitioner and vendor categories. Practitioner categories, comprising Bank of the Year, Asset Manager of the Year, Insurer of the Year and Regulator of the Year, were judged by a panel of Risk.net journalists who undertook extensive due diligence, including follow-up interviews with the companies involved.

Vendor categories, including awards for law firms, consultancies and technology providers, were judged by a carefully selected panel of op risk practitioners and other industry experts.

In all cases, judges considered the extent to which each entrant had demonstrated excellence and met the criteria laid out for the category or categories entered. Judges were allowed to make their final decisions based on all of the information at their disposal and not solely on the details contained in the entry.

The only exception to this twin-track process was the award for Paper of the year. This award is judged by the editorial board of the Journal of Operational Risk and has traditionally been used to recognise an outstanding contribution to the publication each year.

Cover image: Shutterstock/ToskanaINC. Awards ceremony photos: Lucy Stewart
The ability to learn from mistakes is known to be an important trait in business. It’s equally valuable when it comes to operational risk, as the experience of UBS shows.

Both during and after the global financial crisis, the Swiss bank suffered a string of risk management failures that have pushed it to improve its op risk management programme. Following $37.7 billion of write-downs stemming from US subprime mortgages, the bank came under investigation in 2008 for helping to rig Libor rates, and in 2009 it reached a $780 million settlement with US regulators relating to criminal charges that it helped clients avoid paying taxes.

But perhaps the real wake-up call came in 2011, when London-based synthetic equities trader Kweku Adoboli admitted to rogue trading that caused $2.3 billion in losses.

“It was the beginning of a new era,” says James Oates, New York-based global head of compliance and operational risk control. “No-one wanted things like that to keep happening to our firm.”

In 2012, UBS announced it would dramatically restructure its business, cutting 10,000 jobs and refocusing its investment bank on “traditional strengths” in advisory, research, equities, foreign exchange and precious metals. The same year, Sergio Ermotti, the bank’s chief executive, ordered staff to uncover and fix the root causes of its risk management failures.

Since then, UBS has reorganised its risk and compliance functions, devised a new firm-wide risk taxonomy, revamped its risk and control assessments, and stepped up its monitoring of employee behaviour and conduct. “We have remained focused on strengthening our operational risk management framework. It is a key pillar in successfully executing our strategy,” Ermotti says.

One of the most drastic changes made by the bank was to merge its operational risk and compliance functions. Begun in 2013, this process was completed at the end of last year. Oates says the aim was to leverage the respective strengths of both functions, allowing the new op risk and compliance team to take a more joined-up view of the biggest risks facing the bank.

“Operational risk controllers had very good knowledge of front-to-back controls and structured approaches to assessing and reporting risk exposures,” Oates explains. “Compliance officers, on the other hand, were engaged in day-to-day business activities and decision-making.

“Last year, we reached a huge milestone, where all of the people who in 2013 had agreed in principle to the one taxonomy were now 100% aligned with it.”

James Oates, UBS

By bringing the two functions together, they have really been able to learn from each other and, more holistically, address the key conduct, compliance and operational risks.”

A crucial part of this involved rewriting the bank’s risk taxonomy. UBS now has a single, firm-wide risk taxonomy, which over the past two years has been rolled out to the entire bank. A risk taxonomy, or register of risks, categorises the principal risks firms face and typically includes definitions of risks, along with the details of relevant controls.

The move represented quite a shift, as the bank’s individual business lines, operational risk, internal audit and compliance functions all previously had their own way of describing different risks.

“Last year, we reached a huge milestone, where all of the people who in 2013 had agreed in principle to the one taxonomy were now 100% aligned with it,” says Oates. “When it comes to risk, we all now speak in the same language across the three lines of defence.”

Risk practitioners at rival banks are impressed by the firm’s efforts. “The UBS risk taxonomy is completely understandable,” says one op risk manager at a major global bank. “It explains what it is and what it is not
“We really wanted to embed the mindset that senior managers… rigorously and critically test themselves”

James Oates, UBS

[and] includes examples and buzzwords for risk managers to think about when they’re pulling it all together.”

Alongside this overhaul, UBS modified its risk assessment framework. It introduced a systematic internal control assessment, which is carried out by individual business functions every six months to assess the effectiveness of their controls, as well as an annual op risk assessment process, in which the risk management function assesses whether those controls are sufficient to keep residual risks within the firm’s appetite. Additionally, the bank developed a business risk assessment process, which allows business leads to review the effectiveness of their control environment on an annual basis and take action to remediate controls or constrain their activities.

“We really wanted to embed the mindset that senior managers across the firm rigorously and critically test themselves on whether they have the right controls for the risks they run, and proactively confirm that the controls are operating effectively,” says Oates.

The next step was to look at how issues for remediation were organised and prioritised. In the past, the bank often found itself reacting to op risk failures as they arose, or having to prioritise problems raised by regulators or external auditors – in some cases, at the cost of neglecting more important issues elsewhere. Consequently, the bank decided to consolidate its list of issues, says Oates.

With support from group-level internal audit, as well as London-based external auditors EY, a team from the op risk function led the development of a common rating scale for issues on the list. The method applies to all issues – whether they are raised by individual business lines, regulators, internal or external auditors – and comprises various scales covering reputational risk, regulatory risk, financial risk, conduct risk and technology risk. The aim is to determine the level of ‘tail risk’ associated with each issue on a scale of one to five; issues with a ranking of either four or five are considered to be high priority.

UBS has made plenty of headway on fixing these issues, too. Oates says a number of crucial remediation programmes were completed successfully last year, while the number of issues that were self-identified – as opposed to identified by regulators – grew. The bank has also seen a marked increase in the number of problems declared fixed and staying fixed.

“It’s a big step-change from our starting point,” says Oates. “And we still keep pushing on all of the business lines to further improve.”

Then there’s conduct risk. In the aftermath of previous failures, conduct risk and behaviour have become a much bigger focus for UBS as it attempts to win back the trust of shareholders and the wider public. As part of that, the bank has decided to get to grips with correlated instances of poor behaviour before they lead to bigger problems. So it has enhanced its monitoring and surveillance capabilities, investing heavily in what it calls its “employee intelligence capability”.

Having this employee intelligence capability allows UBS to look specifically at each employee and all the attributes associated with them – for example, compliance with mandatory training requirements, trading limits or external regulations. By looking at this, Oates says it is possible to discern trends or correlations in the behaviour of individuals.

“Small signals or patterns across a variety of indicators serve as an early warning sign of an individual not living the principles and behaviours of our firm,” he explains. “We can then use that as a mechanism for performance evaluations or decisions on disciplinary action.”

In general, the bank’s approach to managing conduct risk involves looking at a wide range of data, including whistleblowing reports, litigation, regulatory enquiries and operational event reviews. The bank analyses those reports to discern trends or themes, and any unusual noise receives a closer investigation.

The firm’s senior management has also championed what is known as the “speak-up maxim”. The idea is to encourage staff to speak to line managers, peers or compliance to ensure that any potential problems are flagged up. Furthermore, the bank has been working to improve its anonymous whistleblowing programme, while its performance evaluations now take account of the behaviour of individual employees.

“As a firm, we are reinforcing three key behaviours that are essential to prevent or detect the kind of incidents that occurred in the past: integrity, collaboration and challenge,” says Oates. “These attributes are all essential for a robust risk culture, and so we’ve built all three into the performance evaluations of each employee.”

Although staff performance reviews might seem somewhat removed from the day-to-day tasks of op risk managers, the hope is that embedding a positive culture will help the bank avoid another manipulation scandal or rogue trading loss.

“Championing the right culture, the right conduct, and the right compliance and control mindset is as important to the success of our function as our detective capabilities,” says Oates.