

Risk

Technology Awards 2018 Winner

THE ANALYTICS BOUTIQUE
Analytics made friendly



Op risk modelling vendor of the year
Op risk scenarios product of the year



AI wide open

New technologies are bringing recognition for vendors, writes Clive Davidson

Artificial intelligence and machine learning are finding new homes in finance. Although some hedge funds and specialised teams have applied these techniques – some of which were developed in the 1950s and 60s – to market analysis and trading for a while, they are now appearing in a broader spectrum of applications.

Submissions for this year's inaugural Risk Technology Awards revealed that credit scoring, market surveillance, cyber risk detection, operational risk modelling and trade allocation are just some of the areas where the techniques are being piloted or deployed. It is still early days, and for the moment the technology is supplementing rather than replacing conventional methods, but the indications are that AI, in all its various manifestations, is going to be a game changer.

As one of our judges put it: "Wherever we look in risk technology, AI and machine learning are going to play a leading role. Anyone getting into this now will either crash and burn, or be one of the market leaders in the future."

The awards also highlighted the complexities of cyber risk, the importance of solid data management, and threw up a number of other points of interest (see box: *Other talking points from the judging process*).

At Moody's Analytics the techniques are being used to cast a wider net when analysing company default risk – for example, a pilot project is exploring the use of natural language processing

and machine learning to trawl through firms' unstructured financial statements. The raw material, typically in pdf format, would be hugely time-consuming for human analysts to read, but the project uses machines to extract relevant information and inputs it to standardised templates. The digitised information can then be run through credit scoring models and automated loan decision-making systems.

In another development project, the company is applying AI to social media to look for credit clues. "We have done tests where we have got a 20% improvement in predicting credit events, especially defaults, by applying

"Wherever we look in risk technology, AI and machine learning are going to play a leading role"

social media data to our industrial analytics,” says Stephen Tulenko, executive director for enterprise risk solutions at Moody’s Analytics. “If you can improve your credit scores, then you can save money by reserving more, or making a loan at a different price or buying a bond in a different way.”

As in many other current applications of AI to financial activities, neither the ideas nor the underlying techniques are necessarily new. What has changed is the price and performance of computer processing and data storage, which have finally reached levels that make the applications commercially viable.

“We are now at a point, especially thanks to cloud computing, where we can actually use these [AI] technologies in our day-to-day work,” says Tulenko. Previously, the infrastructure required would have been too expensive, or running the process would have taken too long

the company has concluded the information the techniques generate is supplementary to existing surveillance methods, says Cromwell Fraser, vice-president for communication compliance at Nice Actimize, which won the financial crime and market surveillance categories in the awards. “The real power comes from combining all techniques to highlight entities rather than simply events.”

The combined techniques flag possible concerns around conduct, rather than the traditional focus on specific ‘bad’ actions. They identify individuals who show anomalies or deviation in their behaviour, or who discuss certain topics that might indicate suspicious activity, and prompts their review. “Because of this new approach, made possible through these new technologies, surveillance is changing to an entity approach using combined analytics to highlight possible risk,” says Fraser. Nice

address: the risks financial institutions present to themselves, the risks they present to each other and the risks the community, as a whole, can help mitigate. The result was described by our judges as a “huge and comprehensive effort”, encompassing everything from information sharing among Swift network banks, to a new set of security controls that banks were required to attest compliance with.

To help address the threats that might lurk on its network, Swift introduced a reporting tool called Daily Validation Reports (DVR) that enables customers to verify message flows and detect unusual transaction patterns, identifying new and uncharacteristic payment relationships.

It also sought to head off attacks via another tool, called Payment Controls. This builds on the capabilities of DVR, enabling customers to define their monitoring policy, to ring-fence payment activity so it remains within that policy, and identify payment activity that could be a potential fraud risk – thereby providing protection before and after payment events.

The tool uses machine learning to identify the complex relationships and characteristic behaviours associated with payment activity, and is therefore better equipped to spot things that are unusual or suspicious. The organisation is also using other AI techniques to evolve and parameterise rules for Payment Controls. Echoing other vendors, Tony Wicks, head of screening and fraud detection at Swift, says this is just a start in terms of applying these capabilities in the industry.

“We have done tests where we have got a 20% improvement in predicting credit events, especially defaults, by applying social media data to our industrial analytics” Stephen Tulenko, Moody’s Analytics

to be useful. Now banks can take an algorithm that, in essence, may have been invented in the 1950s, and run it across a low-cost computing grid, getting an answer in seconds, he says.

Signs of crime

In market surveillance and financial crime, AI is proving to be an add-on, rather than a replacement for traditional electronic or human monitoring methods. Nevertheless, it is prompting a fundamental change in approach.

Nice Actimize has invested heavily in AI and machine learning, with the techniques playing a key role in its fraud, anti-money laundering and trading compliance detection products. In fraud, the company uses machine learning on data to discover patterns and develop models, while in anti-money laundering, machine learning and AI are used to segment groups and optimise rules and models, as well as to create predictive suspicious activity scores. In trading compliance, machine learning is used to segment population groups, discover unusual patterns of communication or behaviour in trading and to proactively identify patterns of crime and non-compliance.

While the use of the techniques is “exciting”,

Actimize is now offering tools to its customers to build their own machine learning models.

The success of these early deployments and the results coming out of pilot projects suggests AI is crossing through an inflection point on its development curve, says Tulenko at Moody’s Analytics.

The result could be that firms start looking for more creative ways to use it – and one area that needs all the help intelligent technology can offer is cyber risk and security.

The alarm that surged through the industry following the Bangladesh Bank cyber heist in early 2016 was felt acutely at Swift. The attackers had exploited the organisation’s network to carry fraudulent messages and facilitate massive illegal funds transfers. Although Swift’s network and core messaging services were not themselves compromised, it suddenly became clear that not only were the banks themselves vulnerable, but the electronic interconnectedness on which they relied to do business compounded their exposure. How Swift responded would be critical for the industry as well as for its own future.

The organisation identified three areas to

The problem with people

Despite all the developments in AI and machine learning, operational risk still relies heavily on human judgement. But human judgement is notoriously subject to biases, and these biases can pose a significant threat to the quality of scenario analysis for risk evaluations, says Rafael Cavestany Sanz-Briz, founder and chief executive officer of The Analytics Boutique, which won two categories: op risk modelling vendor and op risk scenarios product of the year.

Herding, authority bias, fear of looking uninformed, or lack of involvement are among the factors that can influence the quality of scenario analysis. So can the design of the scenario questionnaires, their delivery method, the data available and the interaction of evaluators in workshops. The Analytics Boutique’s Structured Scenario Analysis

Risk Technology Awards 2018

platform helps mitigate these biases by separating the scenario process into scenario identification and voting phases, with experts answering individually rather than in workshops and 'seed questions' embedded in the questionnaire to evaluate the level of expertise of participants.

This approach is designed to counteract biases – such as those of herding and authority – by requiring answers from individual evaluators rather than group answers, says Cavestany. Participants who might be quiet in groups are given equal opportunity to contribute. “The most vocal or domineering participants do not necessarily possess the most expertise. [The approach] also increases the involvement of experts [because they] know they are being evaluated and that their answers are individually tracked,” he says. And more weight is given to participants who demonstrate better predictive skills in their response to the seed questions, thereby improving the overall result, claims Cavestany.

On top of data

Another thread running through the awards is the need for robust, flexible and sophisticated



Stephen Tulenko, Moody's Analytics

data management as the foundation of any major risk application. Vendors across many categories highlighted it as a critical factor in their systems, but it came into sharpest focus where business and regulatory requirements converge, such as in credit modelling, stress

testing and regulatory capital calculation and reporting.

“In the stress-testing world – and for regulatory reporting generally – regulators and risk managers got on the same page in terms of thinking carefully about data and data structures

OTHER TALKING POINTS FROM THE JUDGING PROCESS

■ The fact that the regulatory reporting system category got far and away the most pitches – with almost 20 candidates – hints at how much time and attention is being consumed by proliferating reporting obligations. It was a closely fought contest, with many of the vendors offering broad and deep functionality backed by substantial effort devoted to tracking and interpreting the evolving regulatory requirements.

In the end, the judges chose Wolters Kluwer because of its up-to-date and comprehensive global coverage, recently improved data handling and positive client testimonials, especially from mid-tier institutions. The company also notably won a deal against strong competition to provide ABN Amro with regulatory reporting. The bank said Wolters Kluwer's software would help “ensure increased data granularity and transparent data lineage” – critical requirements in today's onerous compliance regimes.

■ Murex winning the enterprise risk management system category is indicative of a trend among vendors that have extended their capabilities into risk management after starting out with a front-office or

transaction lifecycle focus. It makes sense. These firms may have existing pricing, trade capture and data management functionality, which are a good foundation for a broader tilt at risk management.

Murex's MX.3 platform now offers modules for credit, market and liquidity risk, as well as margining and limit management. It incorporates calculators for the various derivatives valuation adjustments, as well as market risk regulations – the Fundamental Review of the Trading Book, standardised approach for counterparty credit risk and derivatives margining regime.

While recognising the breadth and quality of Murex's risk abilities, one of the judges remarked that the “scope of an enterprise risk platform is on the cusp of being redefined”. Risk and finance are being driven together as senior managers seek more holistic views of exposures and opportunities, underscored by new accounting standards such as IFRS 9 and CECL. As a result, institutions will be looking for near real-time support for their business decision making that takes into account the regulations and their own risk/reward strategies. This implies enormous challenges

in terms of modelling, stress testing, data management and performance. The next few years will reveal which of today's enterprise risk platform vendors have the right technological foundations, plus the will and the skill, to rise to the challenges, or whether it is an opportunity for a new entrants.

■ Submissions for the best vendor for systems support and implementation were noteworthy for the extensive and rigorous services they described and the passion with which they argued their case. With increasingly complex systems spanning more business processes, vendors are finding they can no longer simply deliver software and walk away. Some vendors are having to scramble to bring their support up to scratch, while others have been looking to play the long game by establishing technology partnerships with their clients.

The winner in the category, Sageworks, stands out for the way in which it has made responsive, high-quality support integral to its corporate culture – an attitude that “exudes from every interaction between company and client”, as one judge put it.

in the wake of the financial crisis,” says Tulenko of Moody’s Analytics. The revelation during the crisis that banks had no idea of their exposures to each other and could not calculate them in anything approaching a timely manner sent a shock wave through the industry.

“Regulators and risk managers all came to the conclusion that we need get data straight in order to understand what is going on – and that means straight whether you are in finance, risk, credit or accounting departments,” says Tulenko. Stress testing – the regulators’ chosen mechanism for driving up the resilience of the financial system – is forcing a convergence among departments in thinking strategically about data, with the goal of a “single source of truth” for business and reporting, says Tulenko.

And institutions cannot just pay lip service to data integrity, says Alexander Tsigutkin, chief executive officer of AxiomSL, which won the IFRS 9 enterprise solution of the year and regulatory capital calculation product of the year categories. Global standards such as the Basel Committee on Banking Supervision’s standard



Alexander Tsigutkin, AxiomSL

stress-testing data require banks not only to strengthen their risk data aggregation capabilities and risk reporting practices, but also be accountable for their datasets. “Bank executives responsible for submitting reports and attesting to the numbers and positions need to trust their

“Bank executives responsible for submitting reports and attesting to the numbers and positions need to trust their governance process in order to confidently sign off those reports” Alexander Tsigutkin, AxiomSL

239, Europe’s new General Data Protection Regulation and the US Federal Reserve’s rule that chief financial officers must validate their

governance process in order to confidently sign off those reports [knowing] that the numbers and positions are correct,” says Tsigutkin.

The new accounting standards, IFRS 9 and the US equivalent, the Financial Accounting Standards Board’s current expected credit loss (CECL) accounting standard, are driving home these points. The economic assessments of credit risk that these standards require are significantly more complex than any previous regulation, says Tsigutkin.

“IFRS 9 and CECL compliance require much more data over a longer history, with more granularity and precision [than before],” he says. The data and IT infrastructure they require to complete the numerous reporting templates will effectively support almost any regulatory need. Furthermore, the specific analytical facilities required for IFRS 9 and CECL, such as the ability to drill down to all source data, are so powerful and useful that banks are beginning to leverage them for risk-informed economic decision making, he says.

The challenge of data is often characterised as the three Vs: volume (big data), velocity (need for real-time or near real-time monitoring and analysis, and frequent reporting) and veracity (verifiable accuracy). As one of our judges pointed out, to these must now be added volatility, visualisation, value and variety – including unstructured data such as text, social media, weather reports, satellite and other images, and the output of the ‘internet of things’. As the awards demonstrate, AI and machine learning are already enabling these other data forms to enter the orbit of the industry’s analytics, initially for identifying risks, but there is no less potential for them to identify opportunities too. ■

ABOUT THE AWARDS

The Risk Technology Awards were presented in London on June 12, alongside our longer-running awards for operational risk practitioners.

The winners were selected by a panel of 11 technology users, analysts and *Risk.net* editors.

Interested parties were invited to submit a pitch document by March 28, addressing three questions: how the firm meets the industry’s needs in the relevant category, what differentiates it from other vendors, and how its product or service had changed in the previous 12 months. Client testimonials were encouraged, but were not compulsory.

These documents were shared with the judges, who were asked to rank each shortlisted firm. The

panel met on May 22 to compare notes and discuss the most closely contested awards.

Categories in which the judges could not agree on a winner – or in which the panel was not convinced by the quality of the pitches – were dropped from the awards.

Judging panel

Sid Dash, research director, Chartis Research

Clive Davidson, contributor, *Risk.net*

Ian Green, CEO, eCo Financial Technology

Günther Helbok, head of operational risk and reputational risk, head of credit risk model validation, UniCredit Bank Austria

Brad Novak, managing director, chief technology officer for the investment bank, Barclays

John D’Onofrio, chief technology officer, Citigroup

Caroline Philippe, head of operational risk, oversight and cyber security for Europe, the Middle East and Africa, Societe Generale Corporate & Investment Banking

Matthew Sandoe, risk UK chief of staff, BNP Paribas

Jeff Simmons, managing director, head of enterprise risk management, risk management division for Europe, the Middle East and Africa, Bank of Tokyo-Mitsubishi UFJ

Hugh Stewart, research director, Chartis Research
Duncan Wood, editor-in-chief, *Risk.net*

Risk
Technology
Awards
2018 Winner

THE ANALYTICS BOUTIQUE
Analytics made friendly

The Analytics Boutique

Op risk modelling vendor of the year
Op risk scenarios product of the year



Rafael Cavestany Sanz-Briz,
founder and chief executive officer,
The Analytics Boutique

The Analytics Boutique (TAB) offers a comprehensive suite of operational risk models, as well as a scenario analysis platform and model validation tools.

OpCapital Analytics provides institutions with all the operational risk modelling functionality they need to gain a deep understanding of their exposures and potential losses. The software supports the modelling and integration of four key data elements – internal loss data, external loss data, scenario analysis, and business and environmental internal control factors – to create an estimate of economic and regulatory capital requirements and to forecast loss under stress scenarios.

In December 2017, TAB introduced Structured Scenario Analysis (SSA), a web platform that manages risk scenario analysis for capital modelling and risk mitigation. SSA provides flexible questionnaires for scenario planning where potential risk scenarios can be identified, voted on and ranked by a panel of experts. Institutions can customise the questionnaires to specific scenarios, with a variety of question types, such as open or closed, as well as various formats for loss estimates. Support data, case studies or other information to help experts with loss estimates can be included. Seed questions, where the answer is known only to the scenario administration team, can be embedded into questionnaires to gauge experts' skills in evaluating uncertain risk and thus weight their answers accordingly. SSA also includes a number of techniques to mitigate cognitive biases in the experts' risk evaluations such as group thinking and deferring to authority.

SSA manages the workflow of the scenario evaluation process, scheduling workshops and individual questionnaires. The scenario administrator can enter SSA, view any expert questionnaire at any time and take further action, such as requesting more detail or calling additional meetings.

A causal factor model calculates a transparent cross-scenario correlation matrix from the experts' answers. User-friendly web-based analytics enable experts to calculate loss distribution and capital estimates given loss estimates. The experts can visualise the impact on risks of introducing mitigation plans, controls or insurance, and calculate the net present value (NPV) of such actions for justifying the required investment.

Judges' comments

"TAB has extensive operational risk modelling functionality, many users and a good reputation"

"TAB offers detailed, comprehensive and advanced functionality"

"TAB has a clear product proposition with many users and good references from the market"

To reduce correlation matrix size and Monte Carlo simulation demands for large institutions with multiple business units, SSA supports a stepped aggregation process, where scenarios can be first aggregated by risk type to get the total risk of a business unit or legal entity, then by group of entities to obtain their total risk and, finally, by all groups of entities to obtain a single loss distribution for the institution. The number of aggregation steps is flexible and almost unlimited. Five major institutions are already using SSA, with three more testing it.

OpCapital Analytics and SSA include modules for exhaustive model validation with functions such as one-click model replication, audit trail, modelling journal and parameter sensitivity analysis. Regulatory approval reports including all information required by an external analyst to replicate the model can be generated by a single click.

To ensure users are in full control of the modelling process, and to avoid its software being perceived as a 'black box', TAB publishes its modelling methods extensively. With the same philosophy in mind, the company – unusually – also opens its source code to its users.

Rafael Cavestany Sanz-Briz, founder and chief executive officer of TAB says: "SSA is a web-based platform that collects and manages risk scenario analysis for capital modelling and risk mitigation, maximising results quality and process efficiency. It provides full workflow, with on-the-fly user-friendly modelling and Monte Carlo simulation permitting the monetisation of risk estimates, rather than traditional traffic-light maps. With monetised risk estimates, SSA calculates the NPV of the introduction of mitigation plans and insurance policies directly linking risk measurement with risk management. SSA permits the calculation of rigorous and stable capital requirements, reflecting calculated cross-scenario robust correlations. Finally, SSA is designed to mitigate cognitive biases implicit in judgement-based risk evaluations." ■