Intelligent solutions for quantifying Operational Risk

Overview

There is an increasingly urgent requirement for major organisations to **quantify** their operational risk in ways that can be audited, controlled, reduced or managed.

Operational risk is "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events". Legal and regulatory risks, infrastructure failures, day-to-day business risks and risks associated with outsourcing have become the motivators behind the move to proactively manage operational risk.

In addition, regulators are placing an increased emphasis on the control responsibilities of Boards of Directors and Senior Management. Directors and Senior Management need a means to ensure and demonstrate control over major operational risks across the organisation at any point in time (Basle II draft regulations on Operational Risk). For example, under Basle II Banks can benefit from a lower capital set aside if they use advanced methods, such as Bayesian Networks.

Agena specialise in building Bayesian network (causal) models of an organisation's key operational risks. Agena also provide software technology to deploy these models throughout an organisation's operating structure in the form of our web-based, operational risk management system (*AgenaRisk*).

Organisational Accidents

Major organisations can suffer catastrophic damage as a result of a single malicious or accidental event or a slow accrual of such events over time.

In recent years we have all become familiar with the large number of "organisational accidents" that have lead to financial collapse.

Organisational accidents are a product of recent times and the innovative technologies we use. These have radically altered the relationship between systems and their human elements. The major implication of this is that single individuals or small groups have the capacity to, accidentally or maliciously, bring harm or loss to a large number of people (employees, the public, shareholders) or other institutions.

Inevitably such catastrophic failures are often caused by a long-term breakdown of internal processes. Organisations might also drift and become vulnerable to *known* or previously unrecognised risks because of a change in the external environment.

Anatomy of a Vulnerable Organisation

A loss of vigilance leads to vulnerability. Vulnerability can be identified and measured via the pre-cursors of organisational accidents. Example pre-cursors might include such factors as:

- Risk analysis seen as one off exercise - no ongoing monitoring of performance;
- Confusion over who is responsible for ensuring risks are monitored;
- Audit spots problems which day-to-day monitoring fails to identify and remedy;
- Data widely collected, but fragmented and not used;
- Performance indicators not structured to monitor non-production issues;
- Root causes of accidents tend to be ignored. Incident analysis superficial.

There is of course no such thing as absolute risk free operation. Increasing resistance to danger does not mean accident free — simply reduced probability. Good organisations can get plain unlucky. Bad organisations can get lucky. In fact many lucky but unsafe organisations trade on this luck and escape accidents for long periods of time.

A risk programmes therefore need to concentrate on more than historical loss data when assessing risk; propensity to experience future losses, based on control capability, also needs to assessed.

© Agena Ltd, 2004.

Using Bayesian Networks to measure Operational Risk

Organisations can be positioned on a notional risk continuum with increasing vulnerability at one end and increasing resistance to danger at the other. The position of an organisation within this risk continuum is determined by the quality of the processes used to combat its operational threats.

Agena uses Bayesian Networks (causal models) to build an enterprise wide model of an organisation's operational vulnerabilities and risks by measuring:

- Threats to an organisation whether these be internal or external (fraud, hazardous material, technology threats etc);
- Risk control indicators from operating and control processes. Such indicators provide a measure of capability to combat internal and external threats;
- Residual vulnerabilities after the risk control capability is assessed;
- The number of loss events over time expected by size of business;
- Actual loss data (accidents and near misses) which is then used to update the residual vulnerability measure;
- Loss severity per loss event — used in combination with the number of loss events to predict the overall expected loss distribution;
- Quality of data collection processes — some losses may be unreported or kept deliberately hidden.

Our Bayesian Network models can take account of all of these risk measures to produce a unified prediction of an organisation's operational vulnerability.

In contrast historical attempts at operational risk measurement have focused on disparate and patchy approaches: E.g. scorecards; KPIs; reactive outcome measures such as those derived from loss databases and risk questionnaires.

In isolation these methods can examine only part of the complete picture and none provides a coherent basis for risk prediction.
For example, consider industry loss databases. Using data aggregated from many other organisations will tell you little about the risks your organisation is facing *now* and even less about the level of future risk. Unless you know how good the risk control processes of the organisations' that supplied the loss data were you do not know whether the data is relevant. Even if you could decide "relevance" you would still not know what the likely frequency of loss events might be. By using our Bayesian network methods we can combine locally collected loss event data with that available from industry loss databases.

Rather than disregard the status quo Agena's Bayesian Network models instead combine the information gathered from scorecards, risk loss databases and process capability information to give a unified prediction in the form of a value-at-risk (VaR) distribution or economic cost of accidents model.

Armed with Bayesian Networks you can attempt to forecast risk for *your* organisation and do so in the financial terms necessary for risk capital allocation, risk insurance or to help cost a programme of risk reduction actions.

Finally, Bayesian models outperform classical statistical approaches in areas where lots of historical data is thin on the ground and their graphical nature means they are easier to use and more intuitive. Where data is available Bayesian methods simply learn the risk distributions from the data.

Advantages of Bayesian Networks

The Bayesian approach not only provides quantified and auditable risk assessment, it also enables integration of multiple forms of data. This includes hard financial data such as that from loss databases, as well subjective data such as "culture", "morale" and "experience of staff".

There has been an explosion of interest in Bayesian networks in recent years because they offer many advantages:

- Best method for reasoning under uncertainty;
- Computational tractability issues have been solved so Bayesian Networks can be used now on real, large-scale problems;
- Can combine diverse data, including subjective beliefs and empirical data;

© Agena Ltd, 2004.

- Can enter incomplete evidence and still obtain predictions;
- Perform powerful "what-if" analysis to test sensitivity of conclusions;
- Visual reasoning tool and a major documentation aid.

Building Bayesian Networks

Building an operational risk model for all organisations in all business sectors is clearly an impossible task. On the other hand building local models for specific businesses or sectors is equally daunting.

Agena has tackled this challenge by working on a generic operational risk modelling approach that produces local risk modules (Bayesian Networks) for specific business areas. Once created these reusable risk modules can be used throughout an organisation with minimal tailoring. This is a key benefit of using *AgenaRisk*.

Agena's approach to creating these risk modules involves exploiting the expertise and knowledge available within your organisation to a) identify the threat levels and b) assess the effectiveness of risk controls currently and in the future. This information is gathered by eliciting probability estimates for risky events and variables from groups of internal experts. The principled use of subjective information is a central component of the Bayesian approach and is fundamental to areas where completely reliable and relevant data is scarce. Also, since any prediction involves making judgements the use of Bayesian methods embrace this reality rather than simply ignore it. They help formalise what would otherwise be informal, unrepeatable and unauditable.

Example Bayesian Model of Operational Risk

The Figures on the next page show how operational risk can be modelled using Bayesian Networks.

Figure 1 shows the graphical structure of the model. The first part involves the assessment of the capability of an organisation's security controls. The effectiveness of these controls will be determined by a number of factors: resources and budgets, staff competence, management competence, technology and operating procedures. These in turn are heavily influenced by the risk culture of the organisation. An audit of the security controls capability will produce an assessment of their effectiveness but the trust you put in this audit result will depend on whether the audit is accurate. This will, in part, also depend on organisational culture.

The next part of Figure 1 shows a number of threats to the organisation: internal and external fraud, reliability of technology systems, and vulnerability to disasters e.g. terrorist threat. These are combined and the influence of the risks they present is reduced by the controls process capability.

Finally in Figure 1 this vulnerability is used to forecast of the number of operational losses that the organisation may expect to experience. As actual losses are observed theses can be used to update our estimate of vulnerability; however the extent to which the loss data can be relied upon depends on how good the loss reporting and data collection system is. In poor capability institutions financial losses can remain hidden for substantial periods of time; they may accrue on a daily basis and be realised only upon discovery.

In Figure 2 we can see the results of executing the Bayesian model for two extreme types of organisation:

- Resistant to operational threats;
- Vulnerable to operational threats.

The loss distribution curve for the resistant organisation shows a very shallow tail compared to vulnerable organisation. It is this difference in the tails of the distribution that reveals vulnerability because the expected mean losses of both distributions are similar. Bayesian methods therefore complement Extreme Value Theory (EVT) approaches to risk prediction.

© Agena Ltd, 2004.

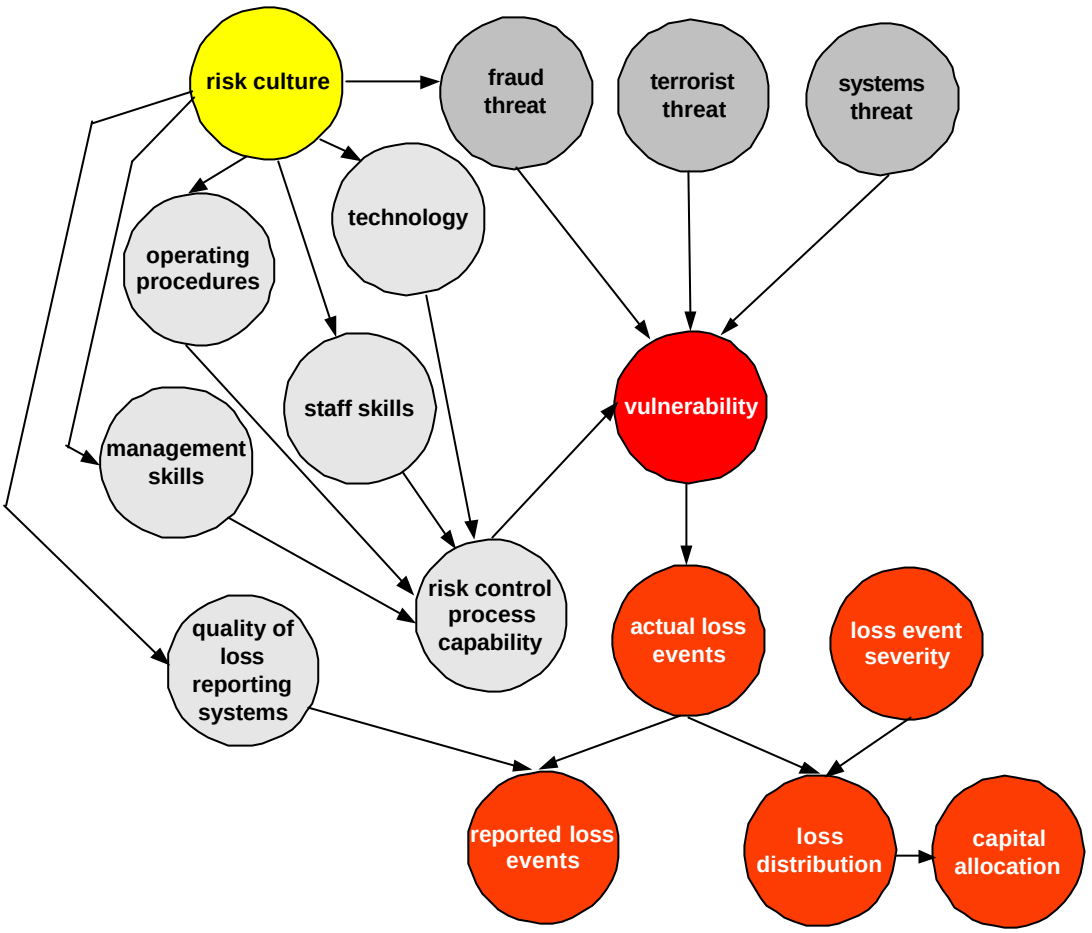

Figure 1: Fragment of Bayesian Network model for operational risk

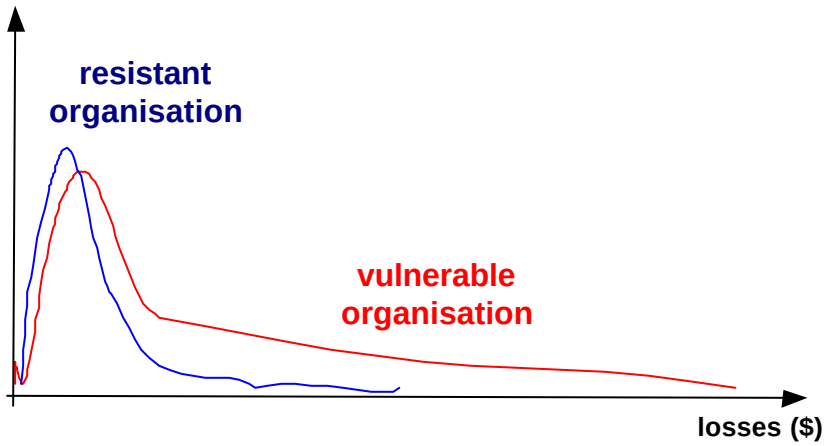

Figure 2: Predicted operational loss distribution

© Agena Ltd, 2004

AgenaRisk - an Enterprise-wide Operational Risk Management Solution

Traditional approaches to operational risk management can be expensive and inefficient because they rely on rudimentary database tools and paper documentation. The low-tech nature of such approaches hinders the sharing and dissemination of information across the organisation, limiting the value derived from the models.

To support operational risk there is a compelling requirement for an integrated approach. The chosen system needs to have the architecture to support and address ever-evolving requirements into the long-term.

Agena has developed the *AgenaRisk* platform to deliver its Bayesian technology for operational risk over a corporate intranet or the Internet.

Agena's *AgenaRisk* platform provides an integrated, corporate wide infrastructure for managing all information relevant to operational risk. Specifically, it brings together the underlying Bayesian model and all the data associated with it in such a way that it can be accessed anywhere across the organisation, with consistency and security assured. It enables staff in different locations to enter relevant information and to observe the impact of such information on the current status of operational risk.

Key *AgenaRisk* features:

- Risk prediction by business line and area;
- Risk prediction by loss event types;
- Editor to design and maintain questionnaires for assessing threats, process capability and residual vulnerabilities for all business areas;
- Editor for creating and maintaining operational risk models;
- Web-based publishing and execution of operational risk models and questionnaires for use by many users throughout an organisation;
- Integration between *AgenaRisk* incident/loss reporting system, risk questionnaire and Bayesian Models;
- Real-time email warnings when risk thresholds breached and automated generation of risk reports

© Agena Ltd, 2004