Analysing business processes

A good understanding of how a business works is the fundamental prerequisite for operational risk analysis. Johan Palm describes the rationale for, and implementation of, the Swedish National Debt Office's bottom-up business process analysis

Risk analysis is an important instrument for gaining control over risks. According to security standard BS 7799[1], such analysis is one of the three key factors[2] in achieving good security organisation. Most other international regulations and standards also advocate risk analysis, and most countries have national regulations that prescribe it. Nevertheless, there is seldom a methodological, standardised approach to how such analysis should be carried out and, consequently, the practice varies widely. Generally speaking, there are three different approaches[3]:

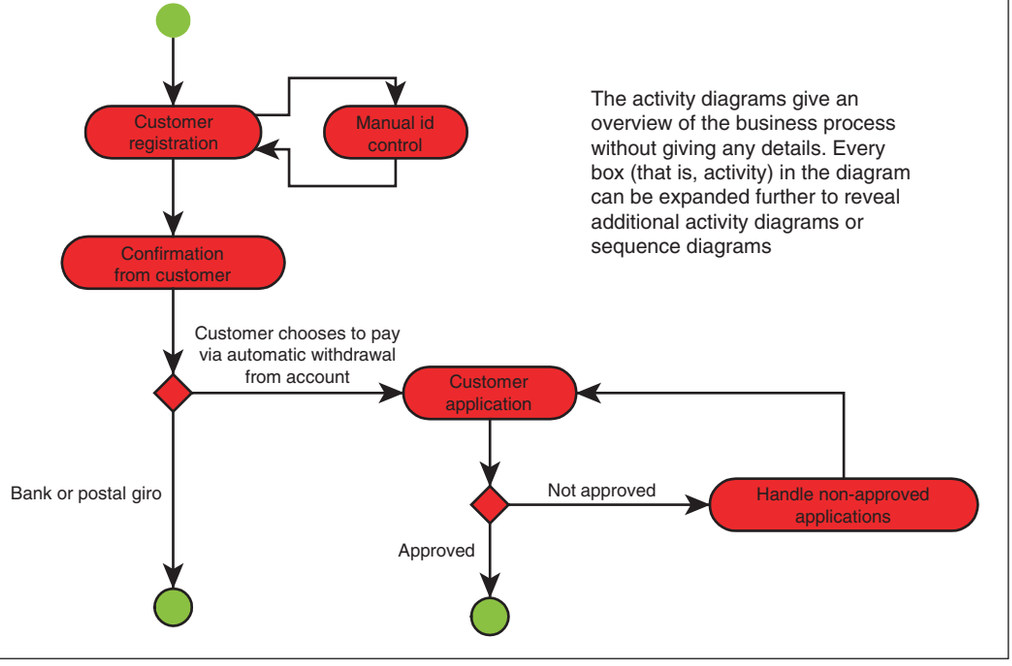
- Risk analysis can be a part of the audit or risk control process, where an internal or external auditor reviews an undertaking. The audit industry is increasingly process-oriented, as can be seen below.
- Within an organisation, the different departments can carry out subjective risk analysis through self-assessment. This is often performed by means of seminars in which the relevant staff can consider different scenarios.
- Risk analysis can also be based on checklists drawn up within or outside the organisation. These lists can either be designed to compare different evaluation criteria among the different departments within the same organisation, or be generic, and try to address phenomena that are often problematic within an organisation. In the latter, self-assessment can be used to evaluate how well the organisation complies with information security standards, such as BS 7799.

For all the above methods, commercial companies have developed products to assist in the evaluation. These companies include, of course, some auditing firms. These products might focus on deployment of scenarios, supply more or less specific checklists, or combinations of both. Very often there is the option to self-assess compliance with a security standard, and to formulate in-house security requirements. The product wrapping also differs between company products. Sometimes the assessment process is bundled with services from the companies' own consultants, while at other times the assessment products are stand-alone systems that the customer can use freely.[4]

The method proposed below differs from traditional methods in certain key areas. It can be characterised as a bottom-up approach in which, by means of a structured procedure, the central work processes are revised and administrative and other shortcomings identified. The method was developed as part of a project at the Swedish National Debt Office. The project started in 2001 and most of the work processes at the different debt office departments have now been analysed and documented with the aid of this method.

The risk analysis is focused on the management of operational risks. For credit risk, market risk and other risks associated with business, there are tried and tested methods – both quantitative and qualitative – for evaluation. Operational risks are defined in the proposal from the Bank for International Settlements (BIS) as "the risk of loss resulting from inadequate or failed internal processes, people

1. Activity diagram



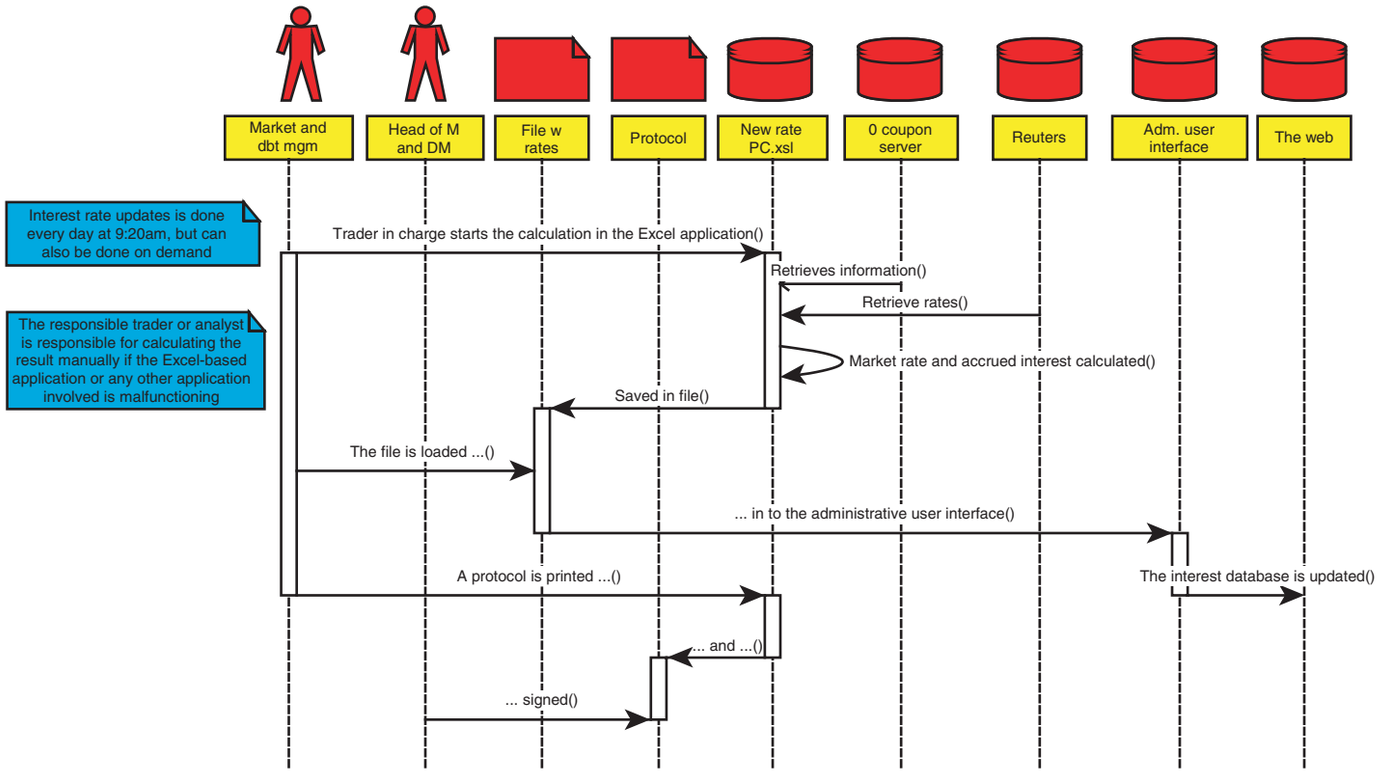
[1] *British Standard 7799 sets out the requirements for an information security management system. It helps identify, manage and minimise the range of threats to which information is regularly subjected. See also ISO/IEC 17799, Code of practice for information security management*

[2] *The others are legal, statutory, regulatory and contractual requirements, and the particular principles, objectives and requirements for information processing that an organisation has developed*

[3] *See also Philippe Jorion, 2001, Value at risk, second edition, McGraw Hill, New York, page 452*

[4] *See, for example,* www.dfs.se/products/sbaeng/check/

2. Sequence diagram



The sequence diagram gives a detailed account of a so-called 'use case', which is essentially one process of the business. It shows how the different actors interact. It is also possible to visualise alternative workflows. For pedagogical reasons, it is often a good idea to use graphical elements for the different types of actors, in this case organisational units, documents, systems and databases. Notice that the project is focused on the administrative work and workflows. Calculations and research are often treated as 'black boxes'

and systems or from external events".[5] The BIS has also said it is uncertain how operational risks should be estimated and that no accepted methods have yet been developed. Nevertheless, the BIS has recently separated operational risks from other risks, and financial institutions will soon have to fulfil a separate capital accord for these risks. The fact that these types of risk require their own capital accord can be seen as a sign of their growing importance.

Operational risk management capacity has been improved, despite the fact that methods of measurement and evaluation still, in many respects, lag behind corresponding methods in the evaluation of credit risk and market risk. Furthermore, there is insufficient access to historical data concerning operational risks.[6] The BIS has therefore deemed it necessary to make several methods available to settle the capital accord. The simplest method is to measure gross revenue and use this to determine the capital accord. In the most complicated method – internal measurement – the banks need to have developed a considerable ability to measure different risk factors. Risk analysis should, in addition to the management of incidents, dovetail with such a concept when risk factors are to be measured and evaluated.

Business process analysis

A prerequisite for risk analysis is a good, detailed picture of how the business operates and who is involved. This is achieved through business process analysis, which provides a verbal and graphical account of the business. The analysis should be carried out separately, in order to provide the basis for the risk analysis. Nevertheless, the analysis can have several goals. Business modelling creates an abstraction and a common description of the current business. Parties not involved in the risk analysis can also use the results of the modelling. Examples of such parties could, for example, include company and agency management, handling officers, IT department system developers, consultants and auditors. All the above have different reasons for requiring an overview of how the business is run and organised.

A useful way to perform the business analysis project is to separate the notation used for the modelling and the project model used to run the project. In the projects carried out at the Debt Office, we used a modern project management model based on an iterative and incremental procedure, with a pre-established work plan. The work plan consists of milestones (increments) and every increment can be performed several times (iterations) to ensure quality.

The basic structure of the notation comes from the business process re-engineering area. However, while business process re-engineering focuses on how the business processes should work and how they should be organised, the business process analysis is content with describing how the business actually operates. Through the descriptions and diagrams that the process analysis pro-

[5] *See Basel Committee on Banking Supervision, September 2001, Working Paper on the Regulatory Treatment of Operational Risk, page 2*
[6] *See Basel Committee on Banking Supervision, January 2001, Consultative Document, The New Capital Accord, page 94+*

duces, it is possible to follow the business processes independently of the different departments, divisions and other organisational units within the business analysed. The analysis can thus be defined as authentically process oriented. At the Debt Office, we used the unified modelling language standard (UML) for the visualisation. UML was adopted as the standard in 1997, and was immediately used to focus on systems development. In recent years, it has been introduced – with great success – as a standard for business process analysis.[7] The purpose of creating graphical demonstrations, for example diagrams, is to visualise how the business operates in certain areas, that is, which aspects of the business need to be emphasised and which can be left out. A graphical illustration makes it possible to create a background for discussion and throws up ambiguities and contradictions. The graphics stay on display all the time and when the concepts, structures and work processes are discussed, it is clear how they have been contemplated thus far. This makes the models easier to develop and more sophisticated, and it is also easier to communicate the content of the models with other interested parties (see figures 1 and 2).

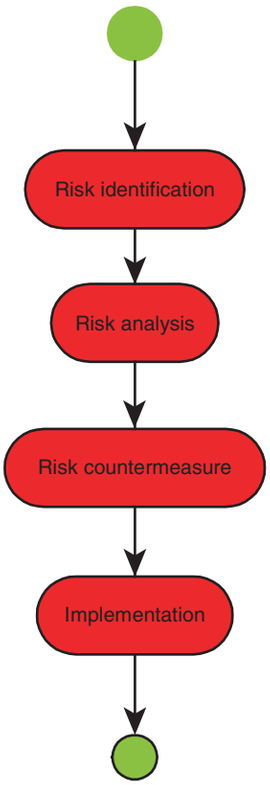
Risk analysis

The goal of risk analysis is to eliminate or at least reduce and control risk. This improvement can be achieved through changes in routines, systems and the organisation. Risk awareness is also enhanced and risks that were previously hidden or of which the organisation was ignorant or only subconsciously aware can be revealed and managed.

It is a good idea to separate the project management model from the material result in the same manner as in the business process analysis project. The risk analysis project is shown in figure 3.

Risk identification means that relevant risks in the business processes are revealed. The diagrams presented in the project described above form the basis for the analysis. An ordinary business process (for example, an interest rate saving product in a bank) can consist of approximately 50 diagrams. It is also a good idea to try to categorise the type of risk under discussion – for example, operational risk due to inadequate duality, market risk due to lack of control or consideration of the opponent's rating, etc. In the risk analysis that follows, the security requirements and risks are estimated and quantified. If the risks are assessed to be severe and relevant enough to be addressed, a risk counter measurement plan is drafted. The risk counter measurement plan is finally implemented.

3. Risk management and process



To assist in the work, several word processing templates have been developed. The templates make it possible to provide quality assurance for the analysis by, for example, using a uniform procedure during the different stages of the analysis. It is very easy to shift focus unintentionally in a scenario-based risk analysis – of which this is, to a certain extent, an example – without the help of such templates. Sometimes the focus is on user rights in the relevant IT systems, and at other times on organisational shortcomings or the lack of duality in handling payment routines. The focus can shift depending on how the diagrams are designed, on highly topical issues at the office, or on the inspiration of the project group performing the analysis. Consistent procedure is used to ensure that important issues or problems are addressed during the risk analysis.

A well-documented and generic procedure also makes it easier for new staff to familiarise themselves with the risk analysis method. Moreover, the risk analysis can thus continue unimpeded when new staff are brought on board.

Finally, the method makes it possible to get risk analysis results that are comparable over time. A risk analysis carried out one or two years from now can be compared with a previous risk analysis.

The method proposed stands out somewhat from traditional methods in as much as staff from analysed departments do not necessarily have to be involved in risk identification. At the Debt Office, the risk control department performs this identification. Since, however, risk counter measures and risk management require organisational changes and changes to working procedures, the project must have some organisational weight and it must have the clear backing of management. It is also important to be clear that while the project carries out the risk analysis, any change is implemented by the business units.

Summary

The method presented consists of two separate areas: business process analysis and risk analysis. Each area has its own project management model and its own material model of analysis. Business process analysis and risk analysis have been performed over the years and the models proposed in themselves contain little that is new. On the contrary, most larger firms have their own models for this, and consultants from external companies very often have their own preferred methods. It is not possible in this short article to show how the models are designed in detail.

One of the underlying purposes of the proposed method is to minimise the work that the staff of the business area have to put into the analysis. Otherwise the process and risk analysis are often given such low priority that the job either never gets done, or its quality is too poor to be useful. The Debt Office has had some measure of success with the proposed method.

The originality of this approach lies in the clear connection between business process analysis and risk analysis and the bottom-up model proposed. At the Debt Office we have developed a comprehensive implementation model, and this soon provided us with high-quality documentation for the whole enterprise and for the risks identified. ■

Johan Palm is information security manager at the Swedish National Debt Office

[7] *H-E Eriksson and M Penker, 2000, Business Modelling with UML – Business Patterns at Work, John Wiley & Sons, page xv and following pages*