Operational risk and *control* assessment methodology

This study looks at how the risk assessment methodology is being implemented in Brazil's insurance group Grupo Asegurador BB MAPFRE as a complementary and deeper form of risk-management and control-implementation analysis. It also weighs up the pros and cons and main challenges posed by this method.

IBERÊ RANIERI
BB MAPFRE

The latest crises to hit the financial world have one standout feature that differentiates them from their forerunners: «the breakdown of trust».

The breakdown of trust in financial information and internal processes sparked off a new approach to operational risk and control assessment and ipso facto a worldwide reaction to this issue.

ILLUSTRATION STOCK

New regulations mushroomed plus new international market rules seeking to recoup confidence in internal company processes and the trustworthiness of their reports on their financial situation.

Among all the myriad concepts telling us how to implement the host of regulation frameworks and good practices, however, operational reviews are now bodying forth as the mainstay of renewed business confidence.

This article is going to look at how the risk assessment methodology is being implemented in *Grupo Asegurador BB MAPFRE* as a complementary and deeper form of risk-management and control-implementation analysis.

The article also addresses the pros and cons and main challenges of this methodology.

RISKS AND CONTROLS

It is not possible to write about this methodology without running through the basic definitions of the risk and control universe.

Every organisation is steeped in good or bad, efficient or inefficient practices. They represent the wake and bearing of its activities and are criss-crossed by the whole value chain. The resulting events of these activities almost always fall within a range of risks or opportunities. The nature of these events is determined by their impact. If the impacts destroy existing value or in some way hinder value creation they are called risks; conversely, if they create or preserve value within the organisation concerned they are called opportunities.

THE INTERNAL CONTROL SYSTEM IS DEFINED BY THE MANAGEMENT'S WHOLE SET OF POLICIES AND PROCEDURES TO ENSURE THAT RISKS INHERENT TO ITS ACTIVITY ARE KNOWN AND DEALT WITH

Corporate risk management in any organisation is driven by the board of directors, the management team and other employees. It is applied with the aim of establishing strategies to identify throughout the whole organisation those potential events capable of affecting it and then administrate those risks to keep them in line with the particular organisation's risk appetite and ensure reasonable fulfilment of its objectives.

The word «control» comes originally from the old French word *contrerole* meaning «a counter-roll or register used to verify accounts». The current Spanish dictionary, translated into English, defines it as: *monitoring, supervising or painstaking analysis with certain expectations, standards or conventions in view, etc*.[1].

Corporate risk management is an integral part of internal control. It is a process driven by the board of directors, by the management team and staff of any particular organisation, with the aim of ensuring reasonable fulfilment of its objectives: efficient and effective operations, trustworthy financial reports and law abidance[2].

The design of any organisation's internal control should enable management to tackle highly competitive and dynamic environments, the ground continually shifting under its feet with constant swings in client priorities and demands and nonstop, growth-seeking structural modifications. The existence of an internal control structure should keep nasty surprises to a minimum for upper management, helping it to maintain a course of profit maximisation and fulfilment of strategic goals.

INTERNAL CONTROL SYSTEM

The internal control system is defined by the management's whole set of policies and procedures to ensure that risks inherent to its activity are known and dealt with.

The main underlying principles of any internal control system are:

- Recognition and continual assessment of any tangible risks that might hinder the company's objectives.
- Suitable flow and availability of financial and operational information in line with market figures and events, underpinned by a secure, independently monitored information system maintained by contingency plans.
- Effective information channels to keep the importance of internal control at the forefront of all collaborators' minds and show how it is carried out at each level of the organisation.
- Ongoing monitoring by means of internal and independent auditing.
- Effective follow up by external regulators.

1 Houaiss.
2 Committee of Sponsoring Organizations of the Treadway Commission.

In sum, all risk screening and shielding is offered by the internal control system, whether these be credit risks, operational risks, market risks, liquidity risks or, in the particular case of insurers, subscription risks, which, if materialised, could affect the whole organisation.

OPERATIONAL RISKS

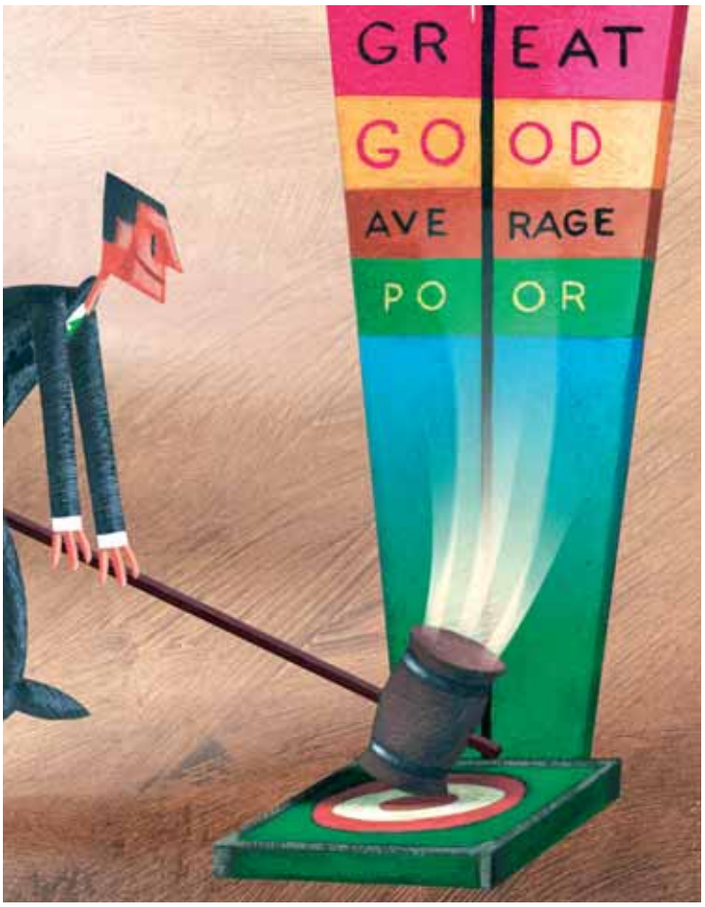
Without downplaying the other risks that at least match the importance of operational risks nowadays, this article focuses particularly on the latter.

The assessment and self-assessment method described in this article will deal exclusively with operational risks.

In early 2013 the Brazilian regulatory organisation, Private Insurance Superintendence (*Superintendencia de Seguros Privados: SUSEP*), defined operational risk as follows: *possibility of losses arising from faults, shortfalls and inadequateness of internal processes, persons and systems or from external events or frauds, including the legal risk and excluding the strategic decision-taking and company reputation risk*[3].

The methodology dealt with in this article widens this trawl to take in:

–External events
–Internal fraud
–External fraud
–Insolvency
–Process faults
–Persons
–Commercial relations
–Reinsurance
–Rating
–Systems (Information technology)



SELF-ASSESSMENT OF OPERATIONAL RISKS

Companies nowadays have opted to identify their risks by means of self-assessment. Under this way of working it is the areas themselves that are responsible for identifying the risks they run, their assessment and control.

This method, besides being fairly efficient, became in time an excellent vector of the internal control culture, especially risk assessment, involving as it does the whole organisation in its development.

[3] SUSEP, 2013.

COMPANIES NOWADAYS HAVE OPTED TO IDENTIFY THEIR RISKS BY MEANS OF SELF-ASSESSMENT

The Brazilian Banking Federation (*Federación Brasileña de Bancos: FEBRABAN*) highlights 8 of the expected results from any risk self-assessment method[4]:

1. Complete analysis of the process by those involved, identifying potential risks and assessing the control and mitigation measures.
2. Reduction or elimination of expensive or inefficient controls, creating alternative solutions and minimising risk exposure.
3. Definition and follow-up of actions to increase the efficiency of controls.
4. Assessment of existing control rules.
5. Building up a common nomenclature and understanding of risks.
6. Support in bringing the risk culture to wider notice within the organisation.
7. Establishment of suitable reporting and monitoring channels of risk exposure improvement actions.
8. Promotion of risk-management and control responsibilities within the organisation.

Some authors[5] consider that the risk self-assessment method can be conducted in three ways: interviews, meetings and self-analysis.

The method put forward in this study does not consider the first two forms, since both interviews and meetings should be conducted by a team cognisant of risk classification and identification processes.

Self-analysis is carried out by means of questionnaires drawn up to assess control structures. These have to be filled in by the managers themselves or sometimes by the people directly responsible for the operation in question. This makes it possible to ascertain whether or not the process per se chimes in with good control practices.

Self-analysis questionnaires are ideal for gleaning information on risks and control levels in a broad, general and rapid way, providing the questionnaires are drawn up in such a way as to foster reflection by the respondent about his or her own processes.

RiskM@p

Since 2003, *Grupo Asegurador MAPFRE* has been consolidating risk management processes worldwide; it was in fact in this era that a self-analysis-questionnaire-based method was set up called RiskM@p.

The self-assessment promoted in Riskm@p is based on the following features: risk- and control-evaluation questionnaires; identification of risks and controls carried out by the management of process manuals and monitoring of action plans deriving from previous work.

Every two years *Grupo MAPFRE's* insurance and reinsurance organisations, which, in the case of Brazil is the *Grupo Asegurador BB MAPFRE*, are invited to carry out the operational risk self-assessment process and also to weigh up the effectiveness of controls and action plans drawn up. The overall purpose of this exercise is to take necessary measures for the prevention or mitigation of identified risks and improving the control environment.

[4] Leite Costa.
[5] Assad, Oliveira, Martins Ferreira, Duque Estrada Felipe y Frank, 2010.

The questionnaires, taking in all operational risk categories, are directed at managers who take a direct part in the insurers' critical processes.

MAPFRE's global sphere of action is conducive to an across-the-board awareness of critical processes; this makes it possible to work from a global base of operational risks and to standardise risk factors.

The self-same working method applied to the group's insurers is also applied to RiskM@p. Although the validation tests are conducted every two years, administrators of the tool verify globally every year the implementations that can be carried out.

The final product of the RiskM@p is risk matrices, which can then be observed through various filters, thus allowing managers to identify the most critical risks within the processes they are responsible for.

The same goes for upper management, which can use this information for strategic planning.

INDEPENDENT ASSESSMENT OF OPERATIONAL RISKS

The pros of risk self-assessment are unquestionable in terms of speed, scope and low application cost. The widespread takeup of this method by the major corporations vouches for its value and efficiency.

At least as a complement to self-assessment, however, independent assessment can by no means be ruled out.

For the purposes of this study, an independent assessment is considered to be one carried out by an external consultancy or the internal control area itself.

Independent assessments are generally led by people aware of the risk and control concepts, structures and categories. They are carried out by means of interviews and analysis of the rules, process design and internal documents that describe or show the trend of the analysed processes over time.

In comparison to self-assessment, independent assessment is more time consuming and more restricted in scope. So what are the pros of using this method?

Some natural characteristics of the human being can justify this choice:

1. There is a natural and human characteristic to downplay risks when these are analysed by the person actually responsible for the process in question. People tend to believe that certain events are much likelier to happen to others' processes than their own.
2. The sheer routine of constantly repeating the same process tends to

THE PROS OF RISK SELF-ASSESSMENT ARE UNQUESTIONABLE IN TERMS OF SPEED, SCOPE AND LOW APPLICATION COST

INDEPENDENT ASSESSMENT IS A PROCESS CARRIED OUT BY PROFESSIONALS DEALING WITH ALL ASPECTS OF RISKS AND CONTROLS ON A DAY-TO-DAY BASIS

reduce the care taken. Controls are slackened in favour of process speed or, with time, some important aspects may be skimped to engender a false complacency in the process.

3. Even deeper down in the human psyche lurks a fear that a bad self-assessment of the process you yourself are responsible for could make your line manager suspect flaws in your own management, showing you up in front of your colleagues, team or superiors.

4. Lastly, the fear that any flaw flagged up in the process might lead to an increase in your already heavy workload. For each flaw at least an action plan will have to be conceived, drawing valuable and often scarce resources away from more productive uses.

In an ideal world none of the abovementioned aspects would be tolerated within any organisation. Much as we might resist them, however, we should never forget that management is always an activity carried out by human beings and, as such, susceptible to a whole range of behavioural tics.

Independent assessment frees the process manager from these knee-jerk reactions. It is also a process carried out by professionals dealing with all aspects of risks and controls on a day-to-day basis. Assessing risks and controls is the proper remit of these team members rather than a complementary responsibility of the manager, who will no doubt spend 90% or more of his or her concentration on his or her day-to-day activities.

On the downside, the greater depth of the independent analysis is more time-consuming and resource-intensive. For this reason the best use of independent assessment may be in very specific and one-off cases to flesh out the self-assessment activities and results.

BB MAPFRE OPERATIONAL RISK ASSESSMENT METHOD

Driven by all the abovementioned challenges, *Grupo Asegurador BB MAPFRE* developed its own methodology for assessing operational risks as a complement to the tried and tested Riskm@p self-assessment process.

To develop this methodology no direct observation was made of the existing self-assessment method. Since

both are based on international standards, it was in fact possible to build up strong synergy between them.

The BB MAPFRE operational risks assessment method comprises a pre-analysis phase and then another 11 stages, to be described below[6]:

Pre-Analysis. The main aim of this phase is to train up and drill the team that is going to carry out the assessment processes. During a period of time that varies according to the process involved, the team begins the work of establishing standards, designing processes, policies, regulations, legislation, inspection notes, information on impacts and processes resulting from the business continuity plan (BCP), among other items. All this could be considered as a warm-up phase.

Stage 1. Identification of Risks and Controls. This stage involves mapping out the whole process, if this has not been previously designed, or validation if the process is already up and running. This phase also includes identification of the risks in their pure form, free of controls, weighing up whether the risks exist or not. By internal definition, the area responsible for assessing internal controls does not carry out the process design; it is therefore necessary to bring in the support of the area of processes that in this particular moment are acting as one of the main providers of the operational risks and controls team, thereby mapping out the processes that are to be validated by means of the ARIS tool[7].

Risk are identified in terms of a strict categorisation based on international rules to ensure maximum systemisation.

Stage 2. Assessment of the Pure Risk and Drawing up the Risk Matrix. On the basis of the information gleaned in the pre-analysis and the risks identified in Stage 1, the specialist internal control team begins the work of vetting information and assessing the pure risk for drawing up the pure risk matrix. Twenty three types of risks are assessed for each process activity.

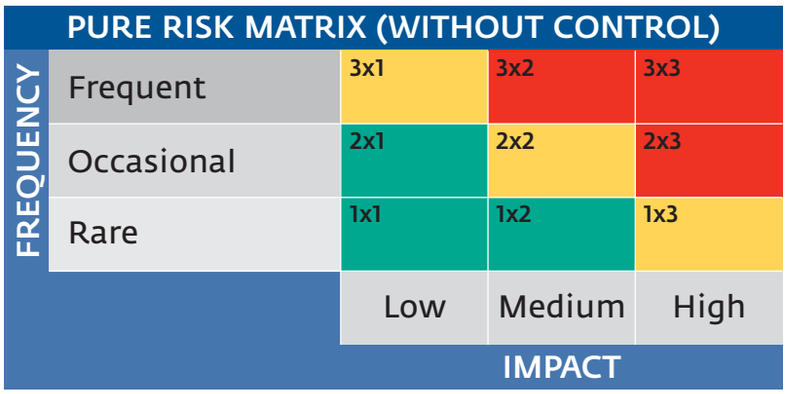
The pure risk matrix is created on the basis of frequency and impact. Frequency is represented on a scale of 1 to 3; the value 1 means «Rare» for a period of over 6 months and 3 means «Frequently» for a period of 1 to 30 days. The impact is also represented on a 1-to-3 scale, in which 1 is considered to be a low value and 3 a high value.

It should be pointed out here that impact is not established from a financial perspective. Impact in this method is observed from the point of view of the activity's ultimate objective. This means that even activities that prima facie produce no financial impact could have an associated risk, classified as high if the manifestation of this particular risk could hamper achievement of the activity's ultimate goal. As already pointed out, process activities create some sort of value within a corporate structure; if manifestation of the risk hinders the activity, this also represents an obstacle to value creation.

GRUPO ASEGURADOR BB MAPFRE DEVELOPED ITS OWN METHODOLOGY FOR ASSESSING OPERATIONAL RISKS AS A COMPLEMENT TO THE TRIED AND TESTED RISKM@P SELF-ASSESSMENT PROCESS

6 Controles, 2013.

7 ARIS (Architecture of Integrated Information Systems) is an integrated Company modelling approach. It offers process analysis methods and comes up with a holistic view of the design, management, workflow and application-implementation process. (Architecture of Integrated Information Systems, 2013)



THE BB MAPFRE OPERATIONAL RISKS ASSESSMENT METHOD COMPRISES A PRE-ANALYSIS AND ANOTHER 11 STAGES

Stage 3. Walkthrough. Stage 2 onwards represents the start of the control assessment and verification process, Stage 3 being the only stage in the process that is optional. It consists of monitoring execution of the control and its activities and is conditional upon the quality of information obtained in previous stages. Should it be established that the material obtained up to that time is insufficient for coming to any conclusion on the existence or quality of the controls, there would then be a need for monitoring of their execution directly in the area affected or responsible.

Another characteristic of this stage is that it can be carried out concurrently with Stage 4, since the need of a *walkthrough* may also crop up during the collection of information and control testing.

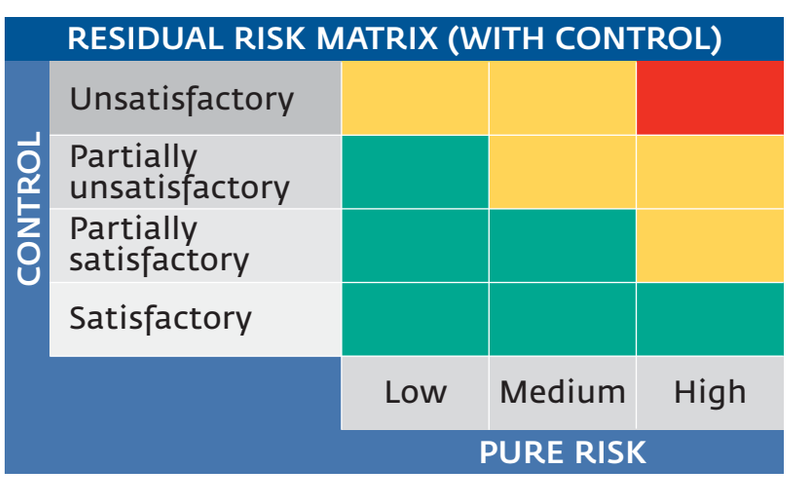
Stage 4. Control Testing and Assessment. In this stage, as in Stage 2, the work concentrates on the objectives in view. The base of Stage 2 is the objective of the activity; in this stage it is the objective of the control.

The test to be carried out is defined in terms of an analysis of the objective of the existing control.

As in previous stages, score-based criteria were again established here to assess the control test. In this case the scoring scale runs from 1 to 4, in which 1 means «Unsatisfactory» and 4 means «Satisfactory».

It is deemed to be «Unsatisfactory» when there is seen to be no control or if the internal control specialists lack the wherewithal for carrying out the tests. «Satisfactory» means the existing control has been tested and no error has come to light.

Stage 5. Residual Risk Matrix. The residual risk matrix combines pure risk and control, combined in factors of 1 to 3 for the risk (low, medium and high) and 1 to 4 for the controls (unsatisfactory, partially unsatisfactory, partially satisfactory and satisfactory).



The result of this stage is the risk matrix for the analysed process.

Stage 6. Recommendation or Suggestion of Improvements. Once the matrix has been obtained and the position of the risk in the quadrant, the control team then initiates the process of describing the recommendations and suggestions of improvements.

Here again the independence of this model comes into its own. The recommendations will help managers to direct efforts by means of action plans in the most objective and efficient way possible, minimising the unnecessary expenditure of resources.

Stage 7. Drawing up the Final Result. The final result involves compiling all the information obtained in the 6 earlier stages and communicating the opinion and comments on the findings to those responsible for the process. This knowledge is transmitted in a presentation, which is the objective of Stage 8.

Stage 8. Presentation and Action Plan. The various points are vetted in a final meeting with those responsible for the process. Any doubts and differences of opinion that may crop up are dealt with in this meeting, enabling managers to propose with more security an action plan to mitigate or eliminate those risks.

In very specific cases, risks cannot be mitigated or eliminated. This will be manifested by the manager, thus recording his or her opinion that the risk must be assumed and that no action should be taken in the first instance.

Stage 9. Validation of the Action Plan. The managers, within a previously agreed deadline, have to present an action plan to mitigate or eliminate the risks. This action plan is again analysed by the internal control specialist team, checking whether the plan is realisable and, if so, in which timeframe.

It may be the case that some plans are initially linked to group projects, some of which might overrun the time period during which risk exposure can reasonably be tolerated. When this happens, the person responsible for the process has to seek an alternative form of control with the aim of minimising risk exposure until such time as the plan is definitively implemented.

Stage 10. Gearing the Action Plans towards Conformity. Within this methodology the other major collaborating provider besides the process area is the conformity area. In this model, once the revised plans have been approved they are sent to the conformity area, which then has to monitor the implementation stages and flag any possible deviations or deadline overruns.

THE ACTION PLAN DESTINED TO MITIGATE OR ELIMINATE THOSE RISKS SHOULD BE ANALYSED BY THE INTERNAL CONTROL SPECIALIST TEAM

WORKING AT THE SAME TIME WITH THE SELF-ASSESSMENT METHOD AND WITH THE INDEPENDENT ASSESSMENT HAS PROVEN TO BE AN EXTREMELY ENRICHING EXPERIENCE

Stage 11. Process Area Feedback. Should it come to light at any moment during the work that the process flow does not tally with initial representations, this information is then transmitted to the process area for it to make the due alterations.

CONCLUSION

The methodology developed by *Grupo Asegurador BB MAPFRE* does not aim to override the self-assessment method. Quite on the contrary, both methodologies can feed off each other, thus ensuring that one-off points that might otherwise have been overlooked are properly dealt with.

Working with two models has proven to be an extremely enriching experience. Self-assessment, with its wide-ranging vision, identifies the points that the manager considers to represent significant risks. Independent assessment rounds this out by studying at much greater depth the points already analysed during the self-assessment process to identify new flaws that can then be dealt with more objectively, drawing up action plans more clearly focused on risk elimination and thus minimising wastage of resources.

It goes without saying that from here on in the whole organisation comes out winning on the strength of the wide-ranging vision of the one method and the more detailed study of the other.

In a financial world beset by crises of confidence, an awareness of the risks that companies are exposed to undoubtedly makes shareholders and other stakeholders feel more confident while also boosting the security of corporate processes.

BIBLIOGRAPHY

—*Architecture of Integrated Information Systems* (2013, 09 23). Retrieved 12 27, 2013, from Wikipedia: http://en.wikipedia.org/wiki/Architecture_of_Integrated_Information_Systems

—Assad, A., Oliveira, A. A., Martins Ferreira, E. S., Duque Estrada Felipe, E. y Frank, W. (2010). *Controles internos*. Rio de Janeiro: Escola Superior Nacional de Seguros (FUNENSEG).

—Commitee of Sponsoring Organizations of the Treadway Comission. (n.d.). *COSO Gerenciamento de Riscos Corporativos - Estrutura Integrada*. Commitee of Sponsoring Organizations of the Treadway Comission & PWC. PWC.

—Controles, G. E. (2013). *Metodologia de Riscos e Controles*. São Paulo.

—Houaiss. (n.d.). Retrieved from Dicionário Houaiss: http://houaiss.uol.com.br/

—Leite Costa, M. J. (n.d.). *Gestão de Seguros*. Fundação Getúlio Vargas.

—SUSEP, S. d. (2013, 01 30). Resolución CNSP 283 - 2013. *Resolución CNSP 283 - 2013*. Rio de Janeiro, RJ, Brasil: SUSEP.

Acknowledgements

Marta González Álvarez, of Area de Controle de MAPFRE España; Luiz Gustavo Braz Lage, Director de Control Interno; Alencar Rodrigues Ferreira, Director General de Control Interno y Riesgos; Vera Lucia Ribeiro, Analista Senior de Control Interno, y Elaine Ferreira, Coordinadora de Riesgos Operacionales del Grupo Segurador BB MAPFRE.