GRAS Newsletter 66

January 2020

What IRM Systems Get Wrong

ten provocative statements

Summary
IRM systems (formerly known as GRC systems: same thing, different label) have become a hindrance to implementing sound Operational Risk Management. From spouting long-debunked measurements (think meaningless impact/likelihood matrices and equally lame Key Risk Indicators) to a dramatic fragmentation into countless modules which flies in the face of the supposed integration in the first place, IRM systems require a drastic overhaul. This article spells out ten areas where IRM providers should improve their act if they wish to be around for much longer.

Dear reader,
A cursory glance of the IRM[1] glossies produced by the IT vendors reveals a range of colourful matrices, impressive ways to measure levels of any type of risk and a host of modules to satisfy the most demanding risk manager. Upon further examination, however, it appears that the progress of IRM systems has come to a complete stop somewhere around 2008. There are exceptions[2] but they are few. Here are ten areas where IRM systems get it wrong.

1. **The 5x5 Impact/Likelihood matrix is misleading and should be abolished**
   The infamous 5x5 matrix relies on two fundamental misconceptions. The first is that risks can be enumerated and second is that likelihood can be estimated[3] with any degree of reliability. Both concepts are ludicrous in the field of non-financial risks. Any software tool that places the Impact/Likelihood Matrix at the core of its supposed 'analysis' betrays lazy thinking. At best, the matrix can act as a conversation starter but no more. To provide a simple chart that informs the reader about non-financial risks it will be better to chart process maps with identified vulnerabilities, report actual incidents, and the status of actual outstanding actions.

2. **Risk data are unjustly presented as certainties**
   Non-financial risk is not about exact measurements but is first and foremost about understanding uncertainty. There will be no getting away from rating (or preferably ranking) risks, but the software tools used to capture information about non-financial risk must facilitate capturing information about uncertainty. That includes information that requires deep analysis of, and knowledge about the risk, rather than a singular statistic. Information such as in the table below will go a long way towards measuring non-financial risk in its proper dimensions:

Context relevance	In what context is the risk relevant
Knowledge about the risk	To what degree is the context understood
Empirical relevance	How is the risk scale empirically verified / tested
Sensitivity scale	Do large variations have small effects or vice versa
Attribution scale	How well do we understand the attributes that influence the risk

[1] In the remainder of this article, 'software tool' and IRM system will refers to any IRM / ERM / GRC IT system, such as evaluated in the *Forrester Wave GRC platforms* or Gartner's *IRM Magic Quadrant*.
[2] Notably, progress has been observed in user-friendliness, but even that is not universal. Too many IRM systems have not progressed much beyond Excel with Macros.
[3] Guessed would be a more appropriate word.

3. **Risk and controls are not two sides of the same coin**
   Some software tools get this right, but not all. Non-financial risks are ill defined at best and fraught with subjectivity as well as being innumerable. They should be taken with truckloads of salt. Controls on the other hand are at the other side of the scale. They are (or at least can be) well defined, can be linked to defined processes or process steps, may be tested, and are limited in number. A sensible course of action, therefore, would be to have controls (actual or required controls) take central stage in assessments and ratings, rather than risks.

4. **RCSA is a misleading concept**
   Risk Assessments and Control Assessments measure different things and therefore deserve separate assessments. A Control Assessment focuses on a particular process or process step, can be linked to a specific requirement (a procedural rule, a regulation or law, a policy or procedure etc), and, although the efficiency and effectiveness of controls are subjective to some degree, they are observable, objective and verifiable. Also, given that we have a limited set of controls, the Control Assessment is by definition a bounded exercise. A Risk Assessment for IRM, however, focuses on a much more vague aspect of risk: for starters, the non-financial risks of any process spans a virtual limitless universe and the assessments come down to heavy guesswork and a mix of beliefs, opinions and casuistry.

   So at the very least, IRM systems should not treat RCSA as a single task. They are two programmes here with radically different attributes, different frequencies and different purposes.

5. **Measuring Non-Financial risk directly is a useless exercise**
   Non-Financial risks differ in fundamental ways from, e.g., Credit or Market Risk. The most obvious difference is that there in an expected reward for taking credit risk, whereas no such reward is expected from taking Non-Financial Risk. Given that risk/reward model, and the notion of being able to dial risk levels up or down at will, has given rise to highly detailed credit risk and market risk models, that take in countless pieces of information to estimate risk levels.
   Compare the sophistication of FICO scores and all the data streams that make up such scores with the casual ease with which IRM systems assume that risk levels can likewise be picked out of a hat for the limitless number of non-financial risks. This is ludicrous.

   In as far as Non-Financial Risks can be measured at all, they will need strict definitions, be taken from a well understood domain and go through painstakingly detailed modelling. I have not seen that work even attempted for, e.g., the risk of failing to carry out oversight of outsource activities or the risk of failing to carry out dual control.

   It will be more effective to focus on measuring the vulnerability of processes. This approach is regularly taken in IT assessments. Its principles can be used for Non-Financial risk measurement by looking at the quality of controls, signs of weakness in the process and understanding the vulnerabilities.

6. **Using KRI to measure Risk is not practical**
   From item 5, it follows that KRIs that focus on risk miss the point. KRIs should focus on what we manage directly, which is the quality of our processes, systems and people. Hence KRIs that measure points along a process may serve as input for both KPIs and KRIs. KRIs that are not used in operational processes are not worth reporting. A corollary of this is that IRM is greatly advanced by having a first class process design with control points, data flows and system descriptions.

   In fact, it may be argued that a decent process map is a pre-requisite for a decent KRI. Software solution purporting to assist in IRM and that do not offer decent process mapping are missing the point.

7. Events must take central stage

Events have properties which makes them much more valuable to analyse than the theoretical notion of risk. Whereas risk data is typically quite loosely defined by questionable guesses as to impact and likelihood, events are defined in the real world. They occur at a specific place and time, they involve particular systems, and they act upon given processes. Its effects can be observed, its causes may be analysed to some degree and the processes under our control may be improved in many cases.

Causal analysis is thus key for event analysis and must be supported explicitly by IRM tooling. It is, however, virtually absent in all IRM software. Causal analysis must allow for probing process design and in fact, events must be tied to elusive KRIs through evaluation and back-testing and the IRM systems should expand event data beyond the mere tabulation of losses.

8. Regulatory Change Management is a must

All banks struggle to get to grips with the myriad of rules and regulations. Analysis of rules, apportioning responsibilities, translation the rules into controls etc etc etc. are an issue that IRM software should address. RegTech is a precursor to updating the control data relevant for IRM. The AI is in fact fairly simple, and basic parsing capability will be a straight winner for any IRM supplier that manages to integrate this in their offering, not as a separate module, but fully integrated.

9. All control functions must share data

It may seem odd to put this as an element that IRM vendors get wrong, but they do. In their eagerness to sell their software, the vendors will often deal only with the Audit department, or only with an ORM department, only with a BCM function etc etc. But an IRM solution that does not set out to reach across all lines of defence is a waste of effort. Hence, adding different control functions (and that includes many first line activities) should not be an option, it should be the standard.

10. IRM cannot survive fragmentation

IRM thrives on sharing methodologies, frameworks, data and reporting. Fragmentation is the enemy of all this. Amazingly, many IRM providers have managed to create their own fragmentation by segmenting their solution into 'modules' that cover, e.g., BCM, OpRisk, Compliance, Digital Risk, Regulatory Risk, Audit etc etc etc. This is driven by sales targets rather than by methodological vision. Any IRM approach worth its salt emphasises the Integration part and seeks to avoid duplication and specialisation. Few IRM providers get this right, or even care. They should be avoided.

Conclusion

Many banks that have already adopted IRM systems are suffering from the swiss knife trauma, meaning that they have bought something with 100 features, two of which turn out to be practical and used often, one or two are used once a year and the remainder is left to rust. These banks, and indeed banks that are arriving now to the IRM party, will need to make a careful assessment of the systems on offer and not be duped into the features that may look good in a demo or a glossy brochure but are in fact not helping at all. Caveat Emptor.