

## **The Anatomy of Business Process-specific Key Operational Risk Indicators**

The development of BP KRIs may appear deceptively straightforward. In practice, this process is by no means an easy task, as it involves a highly structured and methodical risk assessment approach. In Part Two of this article, we will explore, in greater depth, the various approaches and the intricacies in developing BP KRIs.

### **Loss-related Risk Indicators**

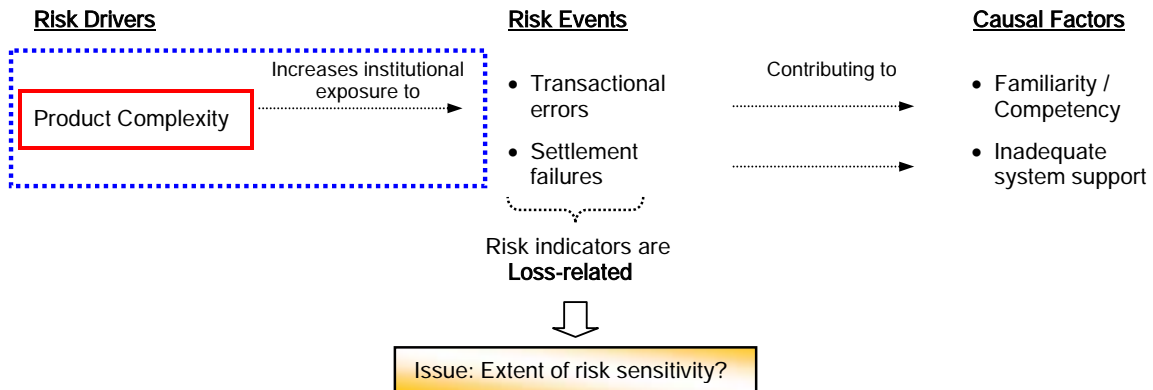
Risk indicators such as (1) Number of Transaction Errors, (2) Number of Settlement Failures, etc., are commonly applied in business functions that are operations-intensive. While data pertaining to transactional errors and settlement failures are indicative of potential operational lapses in back office settlements, “one can’t always get from A to B by way of X & Y, however.” On what basis, do we conclude that transactional errors and/or settlement failures are the ‘right’ (i.e. giving the desired risk measurement) risk indicators? By mere intuition? In the absence of a structured risk assessment methodology, an intuitive approach can be counter-productive, as we may literally end-up with a non-exhaustive listing of risk indicators. But our preconceived assumptions of risk indicators will slowly disintegrate once things are put in perspective. What happens when the risk practitioner does not give due consideration to the intertwining relationships between (i) Risk Drivers, (ii) Risk Causal Factors and (iii) Risk Events?

If the practitioner were to develop risk indicators, in isolation, without linking them to the underlying risk driver(s), the focus is likely to skew towards loss-related measurement (that is, risk indicators that measure outcomes). Generally, this approach offers ‘comfort’ to most practitioners, as the risk indicators are logically linked to some tangible, numeric outcome. Practitioners would want to track, overtime, the number of errors and/or failed transactions, as they considered proxies of inherent operational issues. Inevitably, however, the resultant risk indicators would be lagging in nature. As such, transactional errors and settlement failures are but indicators of risk events, which can be collectively categorized as Failed Transaction Processing <sup>1</sup>[Refer to Diagram 5(a)].

---

<sup>1</sup> This is one of the risk event categories, as defined by Basel.

Diagram 5(a)



While loss-related indicators provide a platform for post-mortem analysis of risk causal factors, they are not forward-looking and are lacking in risk-sensitivity. That said, practitioners should not negate the relevance of lagging indicators just because they do not achieve the desired level of 'predictiveness'. For instance, the indicator, <Number of Customer Complaints>, subject to proper investigation, may reveal underlying process deficiencies, for example, service delivery lapses.

As highlighted in Part 1 of the article, the 'predictive capability' of a risk indicator is as good as the 'accuracy' in identifying potential operational hotspots. Using the Risk & Control Self Assessment (RCSA) methodology as the platform, we will examine two variants. As we will see, notwithstanding that, the intent of the two approaches is different, both techniques rely on risk drivers (that is, sources of risks), as the focal point in risk identification.

### Cause-related risk indicators

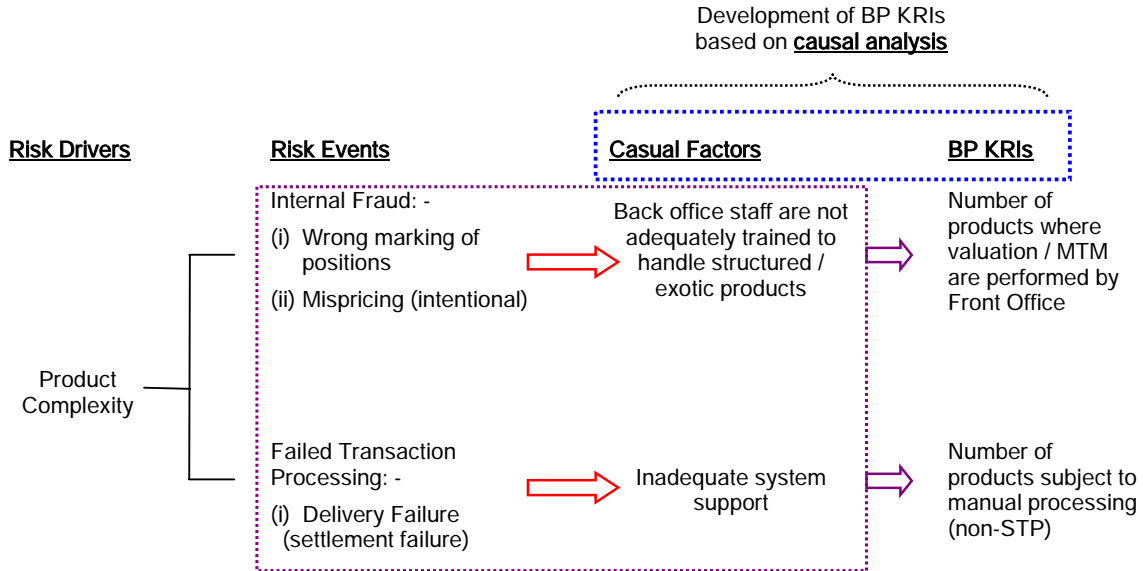
The first approach, causal risk analysis, involves a two-prong process. This approach is schematically presented in Diagram 5(b).

- Business processes risk drivers<sup>2</sup> are identified, providing the context for the derivation of applicable risk event types. In conducting risk analysis, some practitioners may concentrate solely on the risk events - risk causal relationship while giving risk drivers a miss. While there is no hard-and-fast rule, practitioners should recognize the potential pitfalls of focusing at risk events directly without the proper context.

---

<sup>2</sup> Risk Drivers are idiosyncratic to (i) different functional activities and are (ii) context-sensitive. In the smaller financial institutions, for instance, products such as LIBOR-in-arrears, inverse floaters, etc., may be deemed as complex products, whereas, in the larger institutions, these products may be deemed as 'business-as-usual'.

Diagram 5(b)

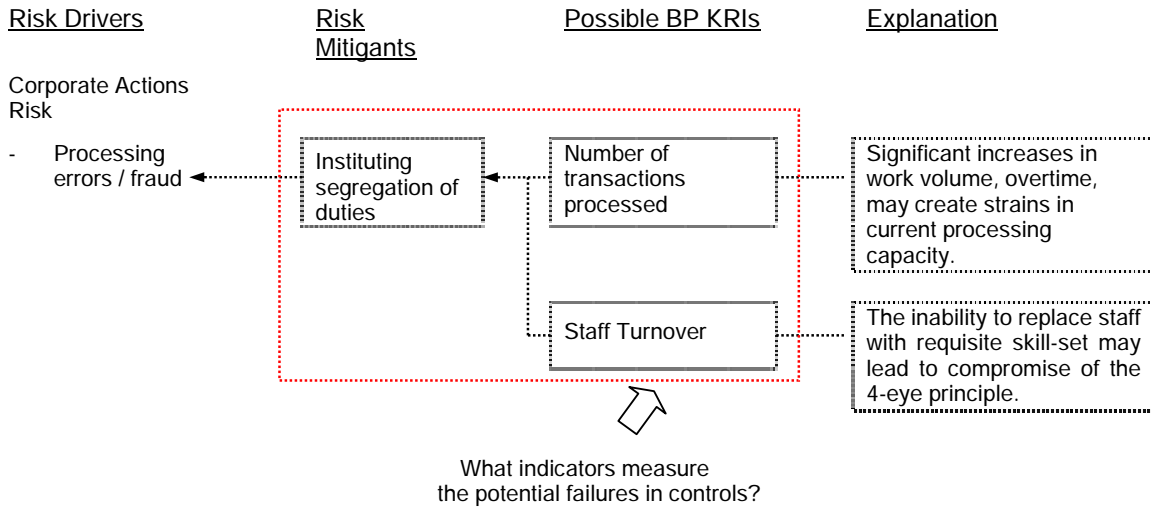


- The identified risk events are drilled down to the specific risk causal factors for the purpose of identifying leading risk indicators. Instead of measuring the number of failed settlements on a post-mortem basis, an attempt is made to 'predict' potential settlement failures. For example, indicators that tracks (1) the number of non-Straight-Through-Processed products and the (2) Volume of Processing will yield a fairly good indication of potential settlement lapses [Pointer 3 - Indicators should not be analyzed on a silo basis. The notion of a **composite risk indicator** does not refer to a singular but a set of inter-related of leading and lagging risk indicators. When these indicators are analyzed in tandem, a fuller picture unveils. Thus, be it lagging or leading, risk indicators should be complementary].

**Control Failure-related risk indicators**

Unlike the first approach that uses risk causal factors as proxy of risk events, the second technique relates the KRIs to potential failures and/or lapses in risk controls. In other words, what type of KRIs indicates control failures? We will use the example of custodian business for illustrative purposes.

**Diagram 6**



Suppose one of the dominant risk area concerns processing errors and/or frauds arising from the performance of corporate actions. As an alternative to examining the underlying contributory risk causal factors, we can explore the following: -

- “What controls are currently available to mitigate the identified risk areas?”, and
- “What type of risk indicators ‘best’ measure the potential failures in the controls?”

If you were thinking of some sophisticated risk indicators, perhaps, the results may appear somewhat disappointing. Highly complex patterns with multiple dependencies would make it difficult to understand and interpret KRIs and should be avoided. People can only manage the risks that they understand. In this case, the potential lapse in segregation of duties can be ‘predicted’ by what are commonly referred to as generic indicators, namely, (1) Transactional Volume and (2) Staff Turnover. Sounds, surprising? Some practitioners, however, fall into the complacency trap, falsely assuming that they have a good grasp of the contextual application of risk indicators [Pointer 4 - Practitioners should understand the (i) intent and (ii) functionality of each indicator i.e. clarity over what are being measured and the purpose]. Risk indicators are meaningless without a reference context.

**Risk Point Analysis**

The first two techniques represent a logical, scientific approach towards BP KRIs development. Strictly speaking, KRIs is not entirely scientific-centric. KRIs is ‘artistic’ as well. The artistic part of KRI development stemmed from two aspects. Firstly, KRIs development involved business judgement. It requires the insights of business process owners who know the idiosyncrasies, which are generally hidden from the radar-screen of seasoned risk practitioners. This epitomized the old saying, “The Devil is in the Details”. Secondly, it is forensic to the extent that the practitioner needs to know where exactly the risk issues reside. It is liken to finding the right tree amid a dense forest.

In this segment, we will briefly examine the third approach, Risk Point Analysis (“RPA”). RPA requires the practitioners to conscientiously analyze the risk entry points of business processes. Risk entry points are not limited to control deficiencies or lapses. They refer to the vulnerabilities (literal sense: the circumstances where risks arises) of any given functional process. In addition, certain types of risk indicators, in particular, fraud-related indicators, require practitioners to think out-of-the-the box. Consider this thought-provoking statement: -

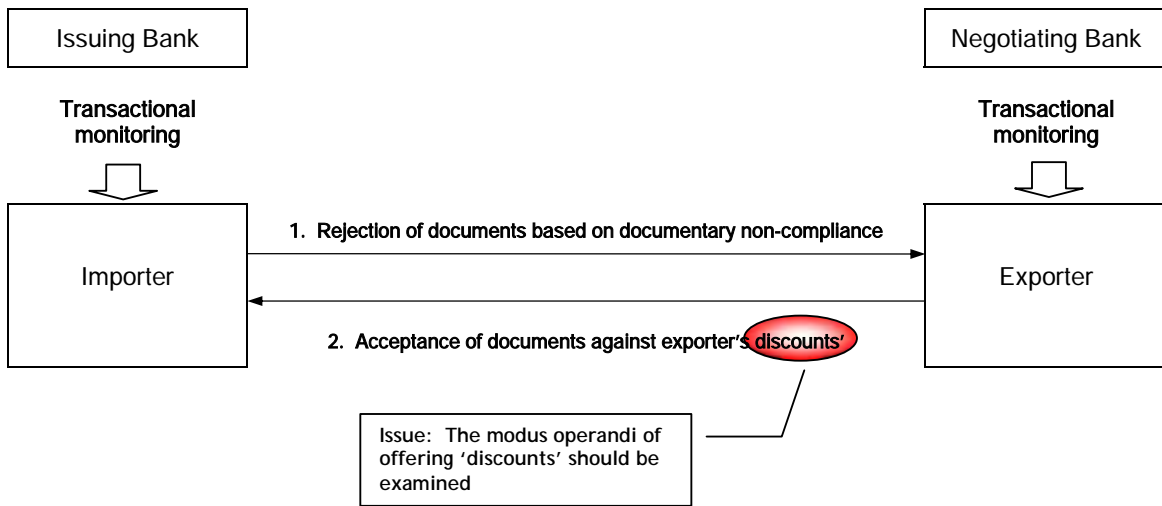
“Since something potentially risky is always happening underneath the surface, without anyone noticing it, what could it be this time?”

Indeed, a good KRI should flag anomalies and/or activities that may not be immediately obvious. This is a daunting task, however. Let us look at two examples:

- (i) Over a span of 2 days, the Credit Card Service Center of a certain bank receives 30 calls requesting card replacements and re-routing of replaced cards to new addresses. Could such a trend signify something unusual? A sudden increase in the change of customers’ static data might be an early indication of credit card identity theft or perhaps a major card scam [Pointer 5 - Risks must be capable of being tracked].
- (ii) Letters of credits issued (on behalf of a certain client) were never economically utilized by the purported beneficiaries but expire on maturity. Client’s explanation being, “No documents would be submitted, as transactions will be settled outside L/C terms”. This unusual practice may suggest potential abuse of the bank’s L/Cs.

To illustrate the conceptual application of RPA, we will use the example of trade financing operations. Diagram 7 depicts the negotiation of documents by the importer’s bank (i.e. Issuing Bank) upon receipt of the same from the exporter’s bank (i.e. the Negotiating Bank). On advice that the documents are non-compliant, the Importer confirmed to the Issuing Bank that he will not accept the documents. For certain types of commodities where prices tended to fluctuate on a month-on-month basis, the desire to reject documents on the basis of discrepancies can be fairly high especially if the Importer feels that he should not be paying a higher price than what the market is currently offering. The Importer may propose an offer - acceptance of documents is contingent on the Exporter’s willingness to accede, say a 30% discount on the L/C amount. Desperate to close the deal and avoid unnecessary charges, the Exporter agrees to the arrangement. Prima facie, this appears like a typical business-as-usual, rejection-and-acceptance of discrepancies. But can this signify something more ‘devious’ than what it is?

Diagram 7



Perhaps, we could take a step back and asked, “Is it possible for the exporter to create deliberate discrepancies?” The creation of discrepant documents would give the importer a ‘legitimate’ opportunity to open-up a ‘dialogue’ with the exporter on the acceptance of the documents and inevitably, the exporter agrees to accept discounts on the shipment. And contrary to the conventional practice of deducting from the L/C proceeds, the exporter agrees to remit the discounted sum to the importer instead. The flow of monies from the exporter to the importer is ‘legitimized’ in the ordinary course of L/C negotiation. But could this be symptom of laundering?

**Validation of KRIs**

Generally, while the validity of KRIs should be back-tested against actual loss experiences, there are practical issues, however. Firstly, how much data is needed to achieve statistical significance? Secondly, not all risk indicators can be validity empirically. Using the earlier example of the trade financing operations - (1) Do we have a sufficiently large number of similar loss reporting? (2) Does it mean that, in the absence of documented data, the associated risk indicators that are designed to track laundering / corporate mal-practices are therefore not valid? The ‘predictiveness’ of risk indicators should not be solely measured against actual occurrence. This reminds us of the hypothetical textbook example of a Corporate Treasurer who faces a zero-sum game in deciding whether to assume a hedge strategy or not. If the market experiences a downturn, he would probably received compliments from the Board of Directors for having foresight and safeguarding the firm’s value. Conversely, if the market conditions are favourable, how would the Treasurer justify for the costs of hedging and therefore, reduced profit margins?

## Conclusion

Defining KRIs does sound simple; perhaps, straightforward, in the eyes of practitioners? But we will probably find that the architectural design of a holistic set of BP KRIs will grow in complexity, as we delve beyond the surface level. KRIs cannot be developed overnight; 'clinical' trails and errors are but a necessity. In short, do not give up on KRIs as a risk management technique.