BUSINESS RISK MANAGEMENT LTD

Key Risk Indicators
2 days
On-line

Day 1 - The Importance of Key Risk Indicators

The fundamentals of KRI's

- **What are KRI's?**
- **What KRI's provide**
- **Adding value to the overall ERM process**
- **Identifying any risk exposure relating to current or emerging risk trends.**
- **Determining the potential impact of risk events.**
- **The importance of Risk oversight as part of the Governance process**
- **Providing perspective through benchmarking.**
- **Predicting new scenarios — especially within high-risk areas**
- **Enabling timely and ongoing actions to minimise risk**
- **Enabling leaders and key personnel to receive alerts of potential risks in advance.**
- **How effective KRI's help in the achievement of strategic objectives**
- **Providing time to develop the appropriate and effective risk responses and action plans.**
- **Establishing objectivity within the risk management process.**
- **KRI's provide an early warning system**

Exercise 1 - The challenges of establishing KRI's

The difference between KRI's and KPI's

- **KPIs mainly focus on how well businesses are achieving their goals.**
- **KPIs identify and prioritize a company's key goals as well as monitor performance against those goals.**
- **KRIs are predictive.**
- **They assess and manage potential risks to goals.**
- **They focus on the likelihood of achieving the goals based on potential risk factors.**
- **KRIs are linked to an organization's risk posture and strategic priorities, and help identify current and emerging risks related to each key goal.**
- **KRIs also monitor risks and send an early warning when the business is at risk of not achieving its goals.**

Exercise 2 – Reviewing the KRI's

An effective method for developing KRIs

- **Types of KRI's**
  - **coincident indicators**
  - **causal indicators**
  - **control effectiveness indicators**
  - **volume indicators**
- **Analyse a risk event that has affected the organization in the past (or present)**
- **Then work backwards to pinpoint intermediate and root cause events that led to the ultimate loss or lost opportunity.**
- **Management can then use that analysis to identify information associated with the root cause event or intermediate event that might serve as a key risk indicator**
- **The goal is to develop key risk indicators that provide insight that risks may be emerging.**
- **The closer the KRI is to the ultimate root cause of the risk event, the more likely the KRI will provide management time to proactively take action to respond to the risk event.**

Exercise 3 – Select 5 key risk events and identify the root cause

Characteristics of effective KRI's

- **Easy to understand**
- **Preventative**
- **Available to all**
- **Comprehensive**
- **Reliable**
- **Comparable**
- **Measurable**
- **Risk sensitive**
- **Attributable**
- **Balanced**

Exercise 4 – Discuss the process required for effective KRI's

KRI Governance & Methodology

The successful identification and application of effective KRIs require a structured approach

- **Determining the effectiveness of the Governance process**
  - **How effective are the processes to oversee the key risks?**
  - **How is it ensured that early warnings and critical near misses are notified to those responsible for Governance?**
  - **Are the reporting mechanisms effective?**
- **Identify existing metrics.**
  - **Risk events in the business are evaluated, along with their associated controls.**
  - **Review existing metrics for each high-risk potential event.**
- **Assess gaps.**

- Evaluate the suitability and effectiveness of each of these existing metrics as leading risk indicators.
- Assess the 7 dimensions
    - Frequency
    - Trigger levels
    - Escalation criteria
    - Leading or lagging indicators
    - Ownership
    - Historical data
    - Data accuracy

Exercise 5 – Review the metrics for a key process and identify gaps and trigger points

Day 2 – Implementing the KRI process

Cause and effect risk indicators

Causes

- Number and type of causes identified in loss event or near miss data collection
- Examples

    - Staff turnover as a % of staff
    - Staff morale (collected from staff surveys)
    - Number of IT patches not implemented
    - Number of attempted IT hacking attacks
    - Number of overdue internal audit actions
    - Number of manual interventions to correct automated process failures

Effect indicators

- The indirect costs of operational loss events (e.g. lost market share, fines, etc.)
- Duration of staff absence due to health and safety incidents
- Customer satisfaction impact
- Number and duration of disruptions to processes and systems
- Number of negative press reports following a negative event
- Number of negative social media posts following a negative event

Exercise 6 – Determining the cause and effect indicators

Ensuring KRI's are identified for each business process

Food Production

- Increase in quality problems
- Rise in sustainability concerns

Strategic

- Stakeholder complaints regarding inclusion
- Trend in number of decisions subsequently challenged

Financial

- Increase in number of targets missed
- Final budget too prescriptive - staff feeling let down
- Changes to budgets during the year
- Negative trend in number and value of write-offs

Distribution

- Delivery failure increase
- Vehicle safety concerns

Customers

- Increased number of complaints
- Annual growth in number of customers being less than expectation each year

Regulatory

- Increase in regulatory breaches
- Increase in legal challenge
- Unusual trend of inspection results
- Any instance of negative feedback from an International body

HR

- Trend in numbers of positions filled from outside the organisation
- Increase in overall sickness or absenteeism levels or number of leavers

Technology

- Virus warnings
- Traffic monitoring hotspots
- Ransomware messages
- Unexpected software installs
- Reported examples of data centre access breaches/ near misses

Exercise 7 – Select a risk category and link KRI's to each risk

Cybersecurity KRI's

Key aspects

- Firewalls
- VPN
- Intrusion Detection
- Virus Scanning
- Traffic Monitoring
- Third party access
- Restriction of user access
- Encryption (SSL the most common)
- Breach of privacy or confidentiality
- Loss of data integrity
- Vandalism and Sabotage
- Domain and Password Controls
- Encryption
- Security Testing

Exercise 8 – Identification of Cyber KRI's

Developing a KRI Dashboard

- A KRI dashboard is a visual display of risk data

- By tracking KRIs over time, you can identify trends and take action to mitigate risks before they become problems
- Trend data for each KRI over time
- Threshold values for each KRI
- Links to relevant reports or tools
- Actions to reduce near misses
- Set threshold values for each KRI
- Review and update regularly

Exercise 9 – Developing a KRI dashboard

KRI tracking and trend analysis

- Once the KRIs are in place, they must be tracked regularly
- Use of data analytics is an excellent approach
  - Comparisons between systems that are not linked together
  - Fuzzy matching
  - Real time exception reporting
- Building trend analysis into the process – to ensure risk owners spot the trends
- The frequency depends on what the KRI represents.
- These should be reported to the top management and escalation procedures must be established and communicated to personnel handling these metrics.
- Not all KRIs have the same levels of escalation,
- It is imperative to follow the hierarchy of reporting and not overwhelm the management with too much information.

Exercise 10 – KRI monitoring – the ERM process

The need to engage stakeholders

- When identifying KRIs, involve all relevant stakeholders.
- Gain stakeholder buy-in so everyone is on the same page and vested in the success.
- Ensure all information about KRIs and the process are accessible to all stakeholders.
- Create a central point of contact to whom stakeholders can go to get support.
- Keep stakeholders updated in a timely manner as things change.