Integrating KRI s and KPIs for Effective Technology Risk Management

Performance evaluation is a key element of any management system and a good governance practice. It involves six key activities: monitoring, measurement, analysis, evaluation, internal audit and management review. Performance evaluation of an organization's risk management system ensures the risk management process remains continually relevant to the organization's business strategies and objectives. Organizations should adopt a metrics program to formally carry out performance evaluation. An effective metrics program helps in measuring security and risk management from a governance perspective.1

Simply stated, metrics are measurable indicators of performance. The two key metrics that are used are key risk indicators (KRIs) and key performance indicators (KPIs). COBIT® 5 for Risk defines KRIs as metrics capable of showing that the enterprise is, or has a high probability of being, subject to a risk that exceeds the defined risk appetite.2 They are critical to the measurement and monitoring of risk and performance optimization. These metrics help in effectively reporting the risk management performance results (risk communication) to stakeholders and enable management in taking informed risk management decisions. While KPIs focus on business performance, KRIs focus on risk management performance.

This article highlights how a risk metrics program can be used to integrate KRIs and KPIs for effective technology risk management.

Risk Metrics Program

An effective risk metrics program yields several benefits, including:

- Assisting in management review and providing decision indicators for continual improvement of technology risk management
- Providing inputs for prioritizing resource allocation decisions
- Assisting in streamlining risk communications
- Contributing to overall cost savings and increased risk management efficiency

The key steps in the risk metrics program are:

- Selection and development of metrics
- Collection of metrics data
- Analysis of metrics data
- Reporting of metrics results

Do you have something to say about this article?
Visit the Journal pages of the ISACA® website (www.isaca.org/journal), find the article and click on the Comments link to share your thoughts.

https://bit.ly/2sOsp0D

Rama Lingeswara Satyanarayana Tammineedi, CISA, CRISC, CBGP, CISSP, MBCI, PMP
Is a consultant to various industries in the area of cyberresilience, covering information security governance, information security policy and procedures, security assessments, operational and information risk management, business continuity management, IT disaster recovery planning, ISO/IEC 27001 implementation, data privacy, and ITIL assessment. He has more than 30 years of IT experience in diverse organizations—business and technology—that enables him to deliver client-focused services and value as a cybersecurity consultant.
1. The first line of defense is the management teams of individual lines of business (LoBs), who are responsible for identifying and managing the risk inherent in the products, services, processes and systems within their LoBs.

2. The second line of defense is an independent corporate risk function, responsible for designing the risk management framework; defining roles and responsibilities; and providing oversight, support, monitoring and reporting.

3. The third line of defense is the internal audit function and is responsible for an independent review of the organization’s risk management controls, processes and systems.

The set of risk metrics selected for initial implementation should be based on the organization’s current risk management maturity level and should contribute to improvement of high-priority risk management focus areas. The metrics should also cover various categories of stakeholders in the organization. The collection and analysis of metrics data and reporting of metrics results can be automated (see the section of this article titled “Automation—The Role of GRC Tools in a Metrics Program”). The three-lines-of-defense model is suggested to establish risk ownership and ensure accountability.

**Risk Ownership and the Three-Lines-of-Defense Model Against Risk**

Business managers tend to think that technology risk is owned and managed by IT or the risk function within the organization. COBIT 5 for Risk defines IT risk as business risk, specifically, the business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise.

The three-lines-of-defense model can be used as a primary means to structure the roles and responsibilities for risk-related decision-making and control to achieve effective risk governance, management and assurance:

**Figure 1**

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Unit</td>
<td>Lines of Business</td>
<td>Risk Function</td>
<td>Internal Audit</td>
</tr>
<tr>
<td>Role</td>
<td>Risk owners/managers</td>
<td>Risk governance</td>
<td>Independent assurance</td>
</tr>
<tr>
<td>Responsibilities</td>
<td>• Identify and manage risk. • Assess and enhance controls. • Monitor and report the risk profile. • Comply with risk policies and frameworks.</td>
<td>• Assist in determining risk strategies, policies and structures for managing risk. • Provide risk management frameworks. • Define roles and responsibilities. • Provide oversight, support, monitoring and reporting.</td>
<td>• Provide independent and objective assurance on the overall effectiveness of the risk governance and management. • Communicate results of the independent reviews to all stakeholders.</td>
</tr>
<tr>
<td>Example KRI</td>
<td>• Percentage of incidents involving customer personal data</td>
<td>• Lack of succession plan for key roles</td>
<td>• Lack of effective reporting of key risks</td>
</tr>
</tbody>
</table>

The model helps in aligning risk strategy, governance, management and assurance.
The Need for Linking KRI s to KPIs

Linking KRI s to KPIs enables business managers to appreciate the relationship between risk and business performance, and relevance of KRI s to the organization’s business objectives and risk appetite. This helps in cross-functional collaboration and embedding risk considerations into business decisions. Linking KRI s to KPIs also helps in getting business buy-in for investment in risk mitigation measures. Figure 2 shows some examples of KRI s linked to KPIs and the business impact of the KRI s.

COBIT 5 for Risk and KRI s

COBIT 5 for Risk is a COBIT® 5 professional guide that discusses IT-related risk and provides detailed and practical guidance for risk professionals. Specific to KRI s, it defines KRI s, lists the parameters and criteria for KRI selection, describes the three-lines-of-defense model, lists the benefits KRI s provide to an enterprise, and outlines common challenges encountered during successful implementation of KRI s.

COBIT 5 for Risk lists some possible KRI s for different stakeholders—the chief information officer (CIO), the risk function and the chief executive officer (CEO)/board of directors (BoD). Some of these KRI s are shown in figure 3.

Automation—The Role of GRC Tools in a Metrics Program

A governance, risk and compliance (GRC) risk management solution provides an organization with a consolidated view of its risk. The solution allows for risk assessment and gives authorized personnel
Figure 3—Example KRIs From COBIT 5 for Risk

<table>
<thead>
<tr>
<th>Event Category</th>
<th>CIO</th>
<th>Risk Function</th>
<th>CEO/BoD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Investments/project decision-related events</td>
<td>• Percent of projects on time, on budget</td>
<td>• Percent of IT projects, reviewed and signed off on by quality assurance (QA); that meet target quality goals and objectives</td>
<td>• Percent of IT investments exceeding or meeting the predefined business benefit</td>
</tr>
<tr>
<td></td>
<td>• Number and type of deviations from technology infrastructure plan</td>
<td>• Percent of projects with benefit defined up-front</td>
<td>• Percentage of IT expenditures that have direct traceability to the business strategy</td>
</tr>
<tr>
<td>Business involvement-related events</td>
<td>• Degree of approval of business owners of the IT strategic/tactical plans</td>
<td>• Frequency of meetings with enterprise leadership involvement where IT’s contribution to value is discussed</td>
<td>• Frequency of CIO reporting to or attending executive board meetings at which IT’s contribution to enterprise goals is discussed</td>
</tr>
<tr>
<td>Security</td>
<td>• Percent of users who do not comply with password standards</td>
<td>• Number and type of suspected and actual access violations</td>
<td>• Number of (security) incidents with business impact</td>
</tr>
<tr>
<td>Involuntary staff act: destruction</td>
<td>• Number of service levels impacted by operational incidents</td>
<td>• Number of incidents caused by deficient user and operational documentation and training</td>
<td>• Cost of IT noncompliance, including settlements and fines</td>
</tr>
<tr>
<td></td>
<td>• Percent of IT staff who complete annual IT training plan</td>
<td>• Number of business-critical processes relying on IT not covered by IT continuity plan</td>
<td>• Number of noncompliance issues reported to the board or causing public comment or embarrassment</td>
</tr>
</tbody>
</table>

Source: Adapted from ISACA, COBIT 5 for Risk (Figure 70: Example KRIs), USA, 2013. Reprinted with permission.

the ability to assign metrics to risk, collect changes in the organization’s risk profile, and monitor risk and metrics against targets and tolerance thresholds.

Corporate objectives and policies defined by senior management, together with other authoritative sources and standards, contribute to the development of a risk register. The risk register is used to generate risk assessment questionnaires that are used for conducting risk assessments. Risk assessment results drive the development and implementation of risk remediation or mitigation plans. These plans, as well as the outcomes, are communicated to senior management.

Corporate objectives and the risk register are used to develop the metrics—KPIs and KRIs, respectively. The metrics dashboard or results are communicated to senior management on a regular basis. Figure 4 provides an overview of a risk metrics automation workflow in a typical GRC solution.

Conclusion

Risk communication is a key element of the risk management process. Communication and consultation with stakeholders are important as they make judgments about risk based on their perceptions of risk. An effective risk metrics program brings objectivity into stakeholders’ risk perception by providing a shared language to measure the effectiveness of security and risk mitigation measures within the organization. Integration of KRIs with KPIs helps in strengthening organizations’ risk culture by enabling business managers to recognize the business benefits of effective technology risk management.
For a detailed description of the three-lines-of-defense model and its role within the enterprise’s wider governance framework, see COBIT® 5 for Risk.

Op cit ISACA

For a detailed description of the importance of communication and consultation in risk management, see International Organization for Standardization, ISO 31000:2018, Risk management—Guidelines.

Endnotes


3 For a detailed description of the three-lines-of-defense model and its role within the enterprise’s wider governance framework, see COBIT® 5 for Risk.

4 Op cit ISACA

5 For a detailed description of the importance of communication and consultation in risk management, see International Organization for Standardization, ISO 31000:2018, Risk management—Guidelines.