Integrating KRIs 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:

- Enabling regular review of risk trends and better visibility of technology risk and vulnerabilities
- Enabling increased accountability and improved technology risk management effectiveness
- 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, CBCP, 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.

Enjoying this article?

- Learn more about, discuss and collaborate on information security management in the Knowledge Center. *www.isaca.org/information-security-management*

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[3] 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.[4]

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:

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.

> "LINKING KRIs TO KPIs ALSO HELPS IN GETTING BUSINESS BUY-IN FOR INVESTMENT IN RISK MITIGATION MEASURES."

Figure 1 provides an overview of the roles and responsibilities of the three lines of defense, with example KRIs.

Figure 1—Three Lines of Defense and Their Roles and Responsibilities

Line of Defense	First Line of Defense	Second Line of Defense	Third Line of Defense
Organization Unit	**Lines of Business**	**Risk Function**	**Internal Audit**
Role	Risk owners/managers	Risk governance	Independent assurance
Responsibilities	• Identify and manage risk. • Assess and enhance controls. • Monitor and report the risk profile. • Comply with risk policies and frameworks.	• 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.	• Provide independent and objective assurance on the overall effectiveness of the risk governance and management. • Communicate results of the independent reviews to all stakeholders.
Example KRIs	• Percentage of incidents involving customer personal data	• Lack of succession plan for key roles	• Lack of effective reporting of key risks

The model helps in aligning risk strategy, governance, management and assurance.

Figure 2—Linking KRIs With KPIs

KRI	KPI	Implication/Business Impact
Lack of succession plan for key roles	On-time rollout of service or delivery of project	Lack of backup for identified key roles affects service continuity, leading to compliance issues and possible failure to meet service level agreements (SLAs).
Percentage of incidents involving customer personal data	Adherence to regulations, policy or processes	This indicates a failure to meet compliance obligations and might lead to scrutiny from regulators or media, which can adversely impact the reputation of the organization.
Number of services cancelled or delayed owing to security-related service downtimes	Number of security-related service downtimes	Security incidents impacting critical systems potentially cause service interruption or degradation.
Percentage of business applications/systems not supported by a backup plan	Number of business applications/systems not supported by a backup plan	Lack of data backup for business applications/systems leads to data loss and adversely affects service continuity in case of any interruption.
Number of nonconformities detected in security tests/audits remaining unresolved beyond the planned time frame	Percentage of nonconformities detected in security tests/audits, but not resolved within the time frame planned	Delay in remediating vulnerabilities detected in security tests/audits makes the organization an easy target for malicious attacks.
Number of security incidents attributed to vulnerabilities in third-party systems/employees	Inadequate third-party management	The organization's information can be exposed to risk by third parties with inadequate information security management.
Number of systems without up-to-date patches	Lack of adequate time frame for scheduled downtime of systems	Delay in patching the systems makes the organization an easy target for malicious attacks.
Lack of effective reporting of key risk	Lack of review of risk management processes	In the absence of a review of risk management processes, these processes might continue to be ineffective, resulting in nonidentification of vulnerabilities/risk.

The Need for Linking KRIs to KPIs

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

COBIT 5 for Risk and KRIs

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 KRIs, it defines KRIs, lists the parameters and criteria for KRI selection, describes the three-lines-of-defense model, lists the benefits KRIs provide to an enterprise, and outlines common challenges encountered during successful implementation of KRIs.

COBIT 5 for Risk lists some possible KRIs for different stakeholders—the chief information officer (CIO), the risk function and the chief executive officer (CEO)/board of directors (BoD). Some of these KRIs 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

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

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.

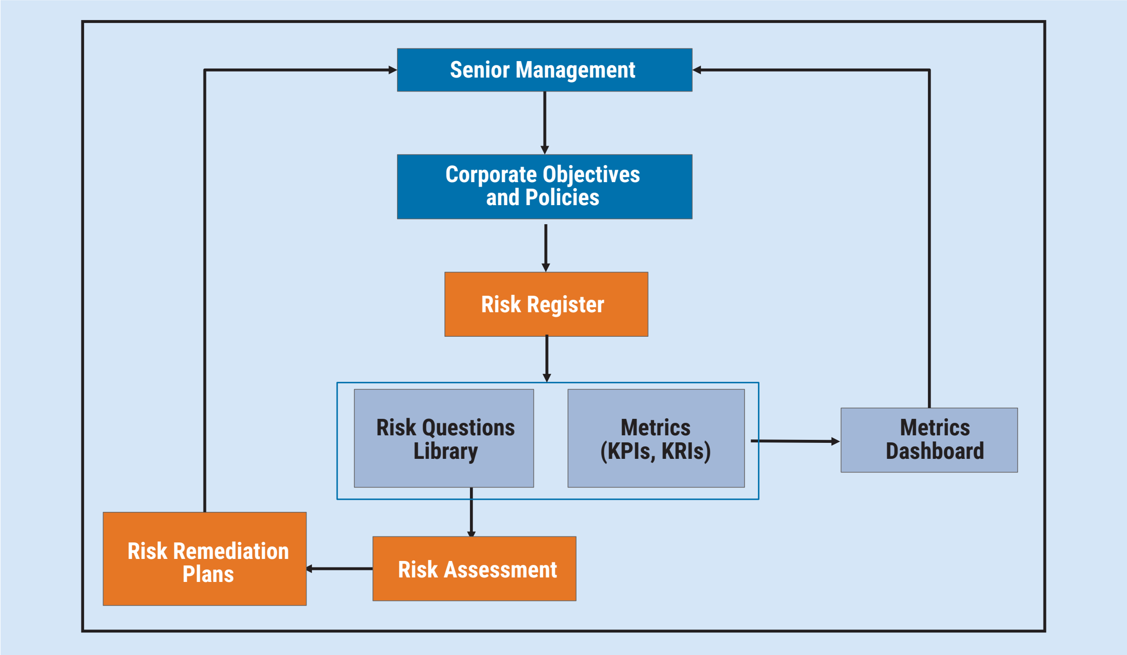
Corporate objectives and policies defined by senior management, together with other authoritative sources and standards, contribute to the development of a risk register. The risk register is used to generate risk assessment questionnaires that are used for conducting risk assessments. Risk assessment 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.[5] 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.

Figure 4—Overview of Risk Metrics Automation Workflow in a Typical GRC Solution



Endnotes

[1] For examples of operational efficiency metrics and metrics in a security balanced scorecard, see Volchkov, A.; "How to Measure Security From a Governance Perspective," *ISACA® Journal*, vol. 5, 2013, *www.isaca.org/archives*

[2] ISACA, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*

[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.*