Risk assessment has become an integral part of today's organization as business operations are expanding and being diversified, resulting in increased risk exposure. In addition, the tightening of regulatory bodies across the globe has resulted in the emergence of assurance functions such as operational risk management, information security, internal audit, internal control and compliance. Each of these functions stresses the importance of risk assessment within the organization and performs independent comprehensive exercises within the specific domain.¹

Generally, there is room for debate about integration among all assurance functions and the use of an integrated risk assessment program (IRAP). Most standards have mapping documents available that show control overlaps among various standards and best practices, but they are rarely followed and adopted by the assurance functions of organizations.² ³ ⁴

The question arises: Is the integration of assurance functions really a need?

Generally, professionals working in compliance, audit, risk management or information security departments face the following issues that give rise to the need for an integrated risk management program:

• Risk assessments performed by assurance professionals are specific to their respective domain and do not give a holistic risk profile of the organization, which results in the presence of unmitigated and undetected threats.

• Often, assurance functions need different departments to nominate representatives for their correspondence and coordination. Typically, a department can assign the responsibility to a single resource. The efforts of the nominee multiply as each assurance function forms its respective teams within the organization. The individual often ends up performing similar tasks, such as self-assessments, statistics reporting and call-tree updating, for different groups, resulting in duplication of effort and repetitive and redundant activities.

• Management often misinterprets observations that are common across different reviews and audit reports because of the difference in severity level and recommendation. As a result, these observations are inappropriately treated and reappear.

• The different audits and review exercises of the assurance functions often frustrate the auditee because of the constant information gathering and response requirements associated with these activities and performed in short intervals of time.

• The auditee sometimes provides different resolution and target dates for observations that are similar to those reported by different assurance functions in their audit or review reports.

Keeping these issues in mind, organizations could start considering integration of assurance functions by identifying the overlapping and redundant activities. Examples of areas of common interest include:

• Obtaining nomination for departmentwide coordinators

• Conducting awareness sessions

• Obtaining departmentwide asset inventory

• Identifying business processes

• Identifying internal and regulatory requirements

• Performing business impact analysis

• Assessing risk

• Investigating incidents

• Reporting to management

The assurance functions should synchronize and align with common activities with respect to their scope, objective and methodology. This would allow for the development of an IRAP. For risk assessment, international standards are used to ensure that best practices and controls are used to mitigate risk associated with systems, services and processes. An illustration of integrating two departments is depicted in the following figures, where one department uses ISO 27001:2005 and the other Basel II.⁵

Syed Fahd Azam, CISA, is assistant vice president of information security at Meezan Bank Limited, Pakistan. He manages information security and compliance at the enterprise levels. He is involved in developing policies, performing audits and conducting awareness sessions. Azam has five years of experience in the field of IT governance. He can be reached at fahd.azam@gmail.com.
Figure 1 identifies the steps to carry out risk assessment of different departments through integrated self-assessment.

<table>
<thead>
<tr>
<th>Figure 1—Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basel II and ISO Control Mapping</td>
</tr>
<tr>
<td>Identify Business Criticality</td>
</tr>
<tr>
<td>Identify Likelihood</td>
</tr>
<tr>
<td>Identify Impact</td>
</tr>
<tr>
<td>Calculate Risk</td>
</tr>
</tbody>
</table>

** Calculate Risk  
Risk = Criticality * Likelihood * Impact

Figure 2 specifies the factors for assigning the values for criticality, likelihood and impact.

Figure 3 is a demonstration of an IRAP.

The risk assessment integration could benefit the organization in the following ways:

- **A holistic risk management approach**—Effective coordination among assurance functions enables each function to understand the key risk areas of the organization. This, in turn, results in mitigation of risk based on consensus. Each assurance function evaluates risk with respect to its domain and views risk collectively to give an aggregated mitigation.

- **Synchronized risk assessment efforts**—The departments can strengthen each other by providing assistance through knowledge and resource sharing. This could include performing joint risk assessment exercises for areas of common interest or sharing materials such as risk assessment reports and audit programs. This can reduce redundant engagement of resources and improve synergy across assurance functions.

- **Maximum risk treatment**—When risk is analyzed from various perspectives, the likelihood of gaps within the mitigated control is greatly reduced. Maximum risk treatment results in minimal residual value, which can be accepted easily by the organization.

- **Standardized control across the enterprise**—The mapping of international standards and best practices to identify controls enables the assurance functions to develop a control baseline that could be implemented across the organization.

<table>
<thead>
<tr>
<th>Assign Criticality Weight Age to Department</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Category</strong></td>
</tr>
<tr>
<td>Core business function</td>
</tr>
<tr>
<td>Support function</td>
</tr>
<tr>
<td>Advisory function</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Determine Likelihood and Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
</tr>
<tr>
<td>Number of preventive controls is low</td>
</tr>
<tr>
<td>Number of preventive controls is medium</td>
</tr>
<tr>
<td>Number of preventive controls is high</td>
</tr>
</tbody>
</table>
**Low-cost and enterprisewide coverage**—The cost of carrying out continuous risk can be lowered if self-assessment is performed against the joint control baseline. This reduces the number of redundant activities and man-hours of different assurance functions.

**Comprehensive and consistent risk reporting**—The coordination among assurance functions results in identification of risk factors that might have gone unnoticed. Also, evaluation of risk from different perspectives helps in assigning appropriate priority with respect to impact on business area or service.

**Follow-up and control resolution convenience**—If similar or repetitive controls from various assurance functions are grouped together, their resolution by the auditee becomes simpler since he/she will have fewer observations and target dates to meet. It becomes easier even for the compliance department, as it will not have to follow up on controls separately.6, 7

**CONCLUSION**

The assurance functions in organizations should be closely associated with each function’s activities and risk findings, and mechanisms should be in place to keep abreast of these activities and risk findings. Based on overlapping activities, the functions should devise assessment strategies to work on potentially high-risk areas. Upon mutual consensus, it is critical to synchronize and align areas of engagement with the intent to strengthen the organization’s controls and improve risk posture.

---

**ENDNOTES**


