A leading Big 4 professional services firm in the Middle East was selected by a large retail bank in the region to assist in enabling IT risk management practices to deliver value to the enterprise in a cost-effective manner. The bank was facing and continues to face a growing and ever-changing IT risk landscape. Given the bank is heavily dependent on IT infrastructure and IT application systems to deliver efficient and effective banking experiences to its customers, the risk committee (RC) of the board of directors (BoD) decided that IT risk management practices of the highest order must be implemented at the bank.

The Fundamental Problems Faced

The chief risk officer (CRO) and the RC of the BoD agreed that improvement in IT risk management was required. The following areas required specific attention:

- **Fragmented IT risk management efforts**—Over the years, sections within the organization (e.g., information security function, business continuity function, IT governance function, project management office) developed their own IT risk management frameworks and their own IT risk registers. Furthermore, the enterprise risk management (ERM) function also had an enterprisewide ERM framework and facilitated enterprisewide risk self-assessment exercises that included the IT division. Needless to say, this resulted in inefficient and ineffective IT risk management. On many occasions, the variety of risk management frameworks and IT risk registers resulted in the same risk being identified, owned and monitored in different ways at the same time. The IT division employees felt overwhelmed with the number of IT risk management activities being driven by divergent functions and, ultimately, not reaching any conclusive actions or remediation plans to implement.

- **Absence of consolidated reporting**—The different risk registers at the bank could not be consolidated into one. Their structures and risk rating methodologies were completely different. Furthermore, a number of risk factors would be repeated. Consolidating all IT risk together into a single IT risk register would be extremely difficult and time-consuming to perform. As a result, the overall impression of the RC and the CRO was that IT risk management activities were unreliable and ineffective.

- **Risk culture**—The IT division and the bank as a whole did not have a risk culture. The bank was driven by a culture that encouraged and emphasized service delivery and deploying new and innovative solutions in the shortest amount of time.
The Solution

The RC of the bank and the CRO were in agreement that a structured and single approach to managing all risk related to IT should be established. A trusted and independent professional services firm was engaged to bring a fresh perspective that would help improve IT risk management at the bank. A number of approaches were discussed, and an approach was developed using leading frameworks and the Big 4 firm’s proprietary risk management methodology to address the issues faced by the bank. The discussions considered the ISACA publication *COBIT® 5 for Risk*, which comprehensively deals with the subject of IT risk management. *COBIT 5 for Risk* provides 2 perspectives on risk: the risk function perspective and the risk management perspective (figure 1).

The risk function perspective describes how to build and sustain a risk function in the enterprise by using the COBIT® 5 enablers. The risk management perspective looks at core risk governance and risk management processes and risk scenarios. This perspective describes how risk can be mitigated by using COBIT 5 enablers.

Furthermore, the *COBIT 5 for Risk* publication describes the 7 enablers for IT risk management in detail.

Source: ISACA, *COBIT® 5 for Risk*, USA, 2013

A brief introduction to the 7 enablers as described in *COBIT 5 for Risk* (figure 2) follows.

Figure 1—Two Perspectives on Risk

**Risk Function Perspective**

The risk function perspective describes how to build and sustain a risk function in the enterprise by using the COBIT 5 enablers.

**Risk Management Perspective**

The risk management perspective looks at core risk governance and risk management processes and risk scenarios. This perspective describes how risk can be mitigated by using COBIT 5 enablers.

Figure 2—COBIT 5 Enablers
Principles, Policies and Frameworks

A description of important principles related to IT risk management that should be adopted by an enterprise is provided. These principles are the foundation for the journey to build best-in-class IT risk management practices at an organization. Organizations can greatly benefit from understanding these principles and applying them in all phases of IT risk management. The principles are:

- Connect to enterprise objectives.
- Align with ERM.
- Balance cost/benefit of IT risk.
- Promote fair and open communication.
- Establish tone at the top and accountability.
- Function as part of daily activities.
- Take a consistent approach.

Guidance related to IT risk management policies is provided in terms of what should be covered in the scope of such policies and validity aspects (applicability, revalidation and distribution) to be considered in risk policies.

*COBIT 5 for Risk* provides a list of risk policies, along with their descriptions to assist professionals with a starting point to develop risk policies tailored to the organizations they serve. An entire section is provided for the IT risk management framework, which describes all the components that must be in place for effective IT risk management.

In relation to the problems faced by the bank, this enabler can help solve the problems “fragmented IT risk management efforts” and “risk culture.”

Processes

A complete description of the core risk processes is provided in *COBIT 5 for Risk*. Core risk processes as presented in COBIT 5 are *(figure 3)*:

- EDM03 Ensure Risk Optimization
- APO12 Manage Risk

Each process is described in detail, including a process description, process goals, process governance practices, process management practices, process activities and suggested key performance indicators (KPIs) to measure performance of the process.
Furthermore, the publication also identifies and provides a description of processes that support the core risk management processes. These supporting processes are required to provide the inputs necessary to support the core IT risk management processes. The inputs that will be received from supporting processes are also described.

In relation to the problems faced by the bank, this enabler can help solve the problem “absence of consolidated reporting.”

Organizational Structures

Guidance and descriptions are provided as to what key structures/roles should be in place for IT risk management. Furthermore, these structures are presented in the “3 lines of defense” model (Figure 4) to make it easier to understand how these structures/roles should be placed in the organization.

Figure 4—Lines of Defense Against Risk
The structures/roles described include:
- ERM committee
- Enterprise risk group
- Risk function
- Audit department
- Compliance department

Supporting structures/roles related to IT risk management are also described, which include:
- BoD
- Chief executive officer (CEO)
- Chief information officer (CIO)/Chief technology officer (CTO)
- Chief information security officer (CISO)
- Business continuity manager

In relation to the problems faced by the bank, this enabler can help solve the problem “fragmented IT risk management efforts.”

Culture, Ethics and Behavior
The purpose of this enabler is to identify relevant behavior and culture elements that are required to build and sustain effective and efficient risk management in an enterprise and that contribute to establishing and maintaining a risk-aware culture at all levels of the enterprise.

The desirable behavior is categorized according to 3 levels within the enterprise:
- General (enterprisewide)
- Risk professionals
- Management

For each behavior, outcomes are described.

In relation to the problems faced by the bank, this enabler can help solve the problem “risk culture.”

Information
This enabler identifies and discusses all information items that are required to build and sustain effective and efficient risk governance and management in an enterprise.

It lists a number of information items that form risk-related information sources for the enterprise, with a definition and description of each. Items defined/described include:
- Risk profile
- Risk communication plan
- Risk report
- Risk map
- Risk appetite
- Risk tolerance
- Risk taxonomy
- Risk and control activity matrix

In relation to the problems faced by the bank, this enabler can help solve the problems “fragmented IT risk management efforts” and “absence of consolidated risk management reporting.”

**Services, Infrastructure and Application**

The purpose of this enabler is to identify and describe all services, infrastructure and applications that are required to build and sustain effective and efficient risk management at an enterprise.

Items specifically described include:
- Governance, risk and compliance (GRC) tools
- Tools for risk communication/reporting
- Incident management services

In relation to the problems faced by the bank, this enabler can help solve the problems “fragmented IT risk management efforts” and “absence of consolidated risk management reporting.”

**People, Skills and Competencies**

This enabler offers guidance on how people, skills and competencies can enable risk governance and management in the enterprise. Specific skills and competencies identified and described include:
- Risk expertise
- Organizational and business awareness
- Critical thinking
- Analytical capability

In relation to the problems faced by the bank, this enabler can help in building the required skills and capabilities that can address each of the problems faced by the bank.

**Conclusion**

The fundamental problems described herein can be solved by adopting the 7 enablers described in *COBIT 5 for Risk*. The publication will prove to be extremely useful to professionals aspiring to build effective and efficient IT risk management capabilities at their organization.

The systematic way each component of IT risk management is identified and explained helps practitioners find guidance for all matters related to IT risk management. More importantly, the publication allows IT risk management practitioners to develop consensus and acceptance from all stakeholders by referring to authoritative guidance from ISACA, which is a reputed and world-renowned body.

**Syed Salman, CISA**

Has more than 12 years of experience in IT audit and IT advisory roles. He has worked with large clients operating in the Middle East and South Asia. Salman has been involved in helping clients address issues related to IT governance, business continuity management and IT risk management. He has conducted a large number of IT audits and IT risk assessments at a variety of organizations across a number of industry segments.