Today, as we continue to adapt to a highly volatile environment, businesses are becoming more proactive about risk management. Nowadays, risk management is on everyone’s corporate agenda, whether a private or public organization. Special attention to risk management is paid by governments, semigovernments, stock exchanges, shareholders and regulators. After all, risk is everywhere, but, perhaps surprisingly, it is not all bad. Let us not forget that when it comes to risk, there are both threats (risk with negative consequences) and opportunities (risk with positive effects). And it is for good reason that optimizing risk is a far more valuable objective than simply striving to eliminate risk altogether.

Risk and time are opposite sides of the same coin, for if there were no tomorrow, there would be no risk. Time transforms risk, and the nature of risk is shaped by the time horizon: The future is the playing field.1

Risk assessment and risk management are integral parts of IT security at any organization, or at least they should be. One would think that, IT being critical to an organization’s operations, the risk related to IT and IT security would be covered by many different risk management frameworks, including the Committee of Sponsoring Organizations of the Treadway Commission (COSO) for enterprise risk management (ERM), the Risk Management Society’s RIMS Risk Maturity Model (RMM), Project Management Institute’s (PMI) Project Risk Management, International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27005 Information technology—Security techniques—Information security risk management and the ISO 31000 family. However, this was not the case until recently. When it comes to risk management in the IT domain and specifically the governance and management of enterprise IT, arguably, there is only one leading globally accepted and in-use business framework to employ: COBIT® 5.

Perspectives on Risk With COBIT 5

Two perspectives on how to use COBIT 5 in a risk context are shown in figure 1:

- **Risk function perspective**—Describes what is needed in an enterprise to build and sustain efficient and
effective core risk governance and management activities

- **Risk management perspective**—Describes how the core risk management process of identifying, analyzing, responding to and reporting on risk can be assisted by the COBIT 5 enablers

Organizations need to understand that COBIT 5 is an end-to-end framework that considers optimization of risk as a key value objective. COBIT 5 considers governance and management of risk as part of the overall governance and management of enterprise IT.

![Figure 1—Two Perspectives on Risk](source: ISACA, COBIT® 5 for Risk, USA, 2013. Reprinted with permission.)

There are 2 dedicated processes: one in the governance (Evaluate, Direct and Monitor [EDM]) domain and the other in the management (Align, Plan and Organize [APO]) domain, which represent Ensure Risk Optimization (EDM03) and Manage Risk (APO12), respectively. Risk management is embedded throughout the COBIT 5 framework.

The governance process (EDM03) seeks to ensure that:
- IT-related enterprise risk does not exceed risk appetite and risk tolerance.
- Risk to enterprise value that is related to IT use and its impact is identified and managed.
- The potential for compliance failures is minimized.

The management process (APO12) works to:
- Integrate the management of IT-related enterprise risk with overall ERM.
- Balance the costs and benefits of managing IT-related enterprise risk.

In addition to that, **COBIT® 5 for Risk** highlights key supporting processes from the COBIT 5 framework for the risk function. Organizations can obtain risk-specific outputs such as a risk management strategy, a risk management communication plan, and financial and budgetary requirements to respond to and mitigate risk. This can also help them to monitor risk metrics and targets and reports on noncompliance issues and root causes.

These processes include, but are not limited to:
- Ensure Governance Framework Setting and Maintenance (EDM01)
- Ensure Benefits Delivery (EDM02)
- Manage Strategy (APO02)
- Manage Budget and Costs (APO06)
- Manage Relationships (APO08)
- Monitor, Evaluate and Assess Performance and Conformance (MEA01)
- Monitor, Evaluate and Assess Compliance with External Requirements (MEA03)

**Scope of COBIT 5 for Risk**
Figure 2 shows the scope of *COBIT 5 for Risk* and how it relates to other ISACA® publications that, together with *COBIT 5 for Risk*, provide comprehensive guidance on risk governance and management over enterprise IT. It shows that *COBIT 5 for Risk*: 

- Focuses on applying the COBIT 5 enablers to risk through the risk function perspective (i.e., how to use COBIT 5)
- Enables an effective and efficient risk governance and management function
- Provides high-level guidance on how to identify, analyze and respond to risk through application of the core risk management processes in COBIT 5 and through the use of risk scenarios
- Aligns with and links to established ERM market reference sources (standards, frameworks and practical guidance) and the ERM initiatives
- Provides a link between risk scenarios and COBIT 5 enablers that can be used to mitigate risk

**An important aspect and a distinguishing feature of COBIT 5 for Risk** is that it provides 20 risk scenario categories to help organizations better mitigate risk. Those risk scenarios can be used to help guide and direct risk management activity. Unlike other frameworks and standards, the scenarios in *COBIT 5 for Risk* cover more than 100 risk types, such as employee sabotage and theft, data breaches, industrial espionage, and support for innovation.

It is up to each organization to decide how to use these scenarios to build its own information risk management processes.

A few suggestions and practical tips as a starting point follow:

- Identify overall enterprise objectives and perform an analysis of the most relevant IT risk scenarios impacting the enterprise objectives.
- Link the IT risk scenarios with the real business risk.
- Once the scenarios are identified and linked, perform risk analysis by assessing frequency and impact. Also identify the risk factors.
- Once risk analysis and risk factors are performed and identified, use them further for risk aggregation, risk response and mitigation.

**COBIT 5 for Risk** Alignment With Other Standards and Frameworks

*COBIT 5 for Risk*—much like COBIT 5 itself—is an umbrella framework for the governance and
management of risk. To better understand this umbrella position, one needs to understand the positioning of COBIT 5 for Risk against the following IT risk-related standards.

ISO 31000:2009—Risk Management
COBIT 5 for Risk addresses all ISO 31000 principles through the COBIT 5 for Risk principles and enablers. Also, the process as defined in ISO 31000 is fully covered by the different processes and practices of the COBIT 5 for Risk process model. COBIT 5 for Risk, however, provides more extensive guidance and includes areas not covered by ISO 31000, such as IT risk governance and management.

The process as defined in ISO/IEC 27005 is fully covered by the different processes and practices of the COBIT 5 for Risk process model. The COBIT 5 for Risk model provides more extensive guidance and includes areas not covered by ISO/IEC 27005, such as risk governance and reacting to events. The fundamental difference between the two frameworks is that COBIT 5 for Risk addresses a comprehensive number of categories of IT risk, whereas ISO/IEC 27005 focuses specifically on information security risk.

COSO ERM—Integrated Framework
COBIT 5 for Risk addresses all 8 components defined in COSO ERM and, for some components, extends the coverage of COSO ERM to the specifics of IT use in the enterprise. Although COBIT 5 for Risk focuses less on control, it provides linkages to management practices in the COBIT 5 framework. The essentials for both control and general risk management, as defined in COSO ERM, are present in COBIT 5 for Risk, either through the principles themselves, the framework’s conceptual design, the process model or the additional guidance provided in the framework.

Applying COBIT 5 for Risk
A few practical tips for leveraging the guidance in COBIT 5 for Risk in an organization follow:

- Encourage executive management to demonstrate support for the risk management program.
- Identify the key organizational structures/roles that are required to build and sustain effective and efficient risk governance and risk management in the organization. COBIT 5 for Risk helps organizations to identify such roles by providing a specific description/definition of each role and structure. This helps organizations to establish their lines of defense for risk management.
- Risk management must be embedded in the normal process and form part of the daily management practice.
- Establish a risk-aware culture among all employees at all levels.
- Influence the behavior and culture of the organization through constant communication; the enforcement of organizational rules, regulations incentives and rewards; and raising awareness about risk and risk management and the role of people in it.
- Identify and develop metrics to serve as key risk indicators (KRIs) to describe and track indicators of that risk.

Final Words
COBIT 5 for Risk has been available for quite some time now, but still, organizations consider it more of a management and operations framework and set of guidelines while neglecting a major chunk of the framework, for the obvious reason that organizations fear the consequences (both in terms of cost and time) if risk management fails. They also fear to communicate the risk to top management and, therefore, they perform risk management as part of either operational activities or because of the requirement of certain specific standards such as ISO 27001. COBIT 5 does talk about management and operations processes, but at the same time, it covers corporate governance and enterprise IT processes and activities as well and, most importantly, risk management. COBIT 5 for Risk currently is the most powerful and the only framework that covers risk related to IT and not just information security.

Hafiz Sheikh Adnan Ahmed, CGEIT, COBIT 5 Assessor, ISO 20000 LA, ISO 27001 LA, ISO 27032 Lead Cybersecurity Manager ISO 38500 Lead IT Corporate Governance Manager, Lean Six Sigma Green Belt
Is a motivated achiever with more than 11 years of significant, progressive experience in the IT field, focusing on information security, IT governance, ISO standards implementation and compliance, IT service management, risk management, software project management, and process improvement. Ahmed is a board member of ISACA United Arab Emirates Chapter and a Professional Evaluation and Certification Board certified trainer. He is the recipient of the 2017 Middle East Security Award in the category of Rising Stars in Security and Risk and the 2016 Security Advisor Middle East award in the category of Personal Contribution to IT Security. He can be reached at adnan.gcu@gmail.com.

Endnotes