COBIT 5: Taking IT Governance and Management to the Next Level

By Syed Salman, CISA

COBIT Focus | 14 November 2016

A Big 4 professional services firm in the Middle East region was selected by a leading retail bank in the region to assist in finding solutions to pressing problems related to IT governance and IT management. The bank was and continues to be heavily dependent on IT infrastructure and IT application systems to deliver an efficient and effective banking experience to its customers. Such dependence is expected to grow as the bank plans to further introduce innovative products supported by technology to a very young customer base.

The Fundamental Problems Faced

Senior management and the board of directors (BoD) agreed that further transparency was required in the management and governance of enterprise IT (GEIT). The following areas required specific attention:

- **Organization structure**—The IT division was led by the Head of IT Division (HoITD). The HoITD was the single point of contact for senior management and the BoD for all matters pertaining to enterprise IT. This included performance measurement, risk management, compliance to regulatory requirements and management/alignment of IT strategy to enterprise strategy. Furthermore, BoD involvement in IT governance was very limited and based on *ad hoc* requests.

- **Cost control**—IT expenditure had been progressively increasing over the years due to investment in advanced technologies to serve a rapidly growing customer base. However, clarity was not available on whether expenditures were incurred in an optimal manner.

- **Performance reporting**—Performance metrics reported by the HoITD to senior management were many and covered a number of aspects related to the enterprise IT. However, the metrics were not appropriately classified and organized in a manner for them to be fully understood by senior management or the BoD.

- **Risk management**—The IT division appeared to be reactive in its approach to mitigating emerging and prevailing IT risk. Senior management and BoD were unsatisfied with the attention given to establishing sound IT risk management practices.

- **Alignment to corporate strategy and goals**—Senior management and the BoD were of the opinion that a number of large initiatives that involved support from the IT division had failed to deliver the desired outcomes or had been significantly delayed due to IT division misalignment with corporate goals and the overall strategy of the entity.

The Solution

The HoITD, senior management and the BoD were in agreement that strong IT governance and management practices could enhance the ability of the HoITD to deliver higher-value IT services while optimally managing costs.
and risk. Therefore the bank took a decision to establish an IT governance division under the chief operating officer (COO) to serve as an independent body to have oversight of the enterprise of IT. The COBIT® 5 framework was adopted to serve as the guiding framework for their journey. Furthermore, a decision was made to engage a trusted and reputable professional services firm to assist in this journey. This decision was made to allow the independent professional services firm to bring with it a fresh perspective and deliver the tough recommendations that internal staff may not have been able to make on their own.

The following steps were performed:

1. **Prioritization of COBIT 5 processes**—It was understood that covering all 37 COBIT 5 processes at the same time for assessment and improvement would be very difficult to manage for the bank as it would lead to too much disruption and change all at once. Therefore, the Big 4 firm assisted the bank in prioritization of COBIT 5 processes. The Big 4 firm conducted interviews and workshops with different stakeholders inside and outside the technology group to explain what each COBIT 5 process was and to help stakeholders understand which of these processes were the most important to the bank. The Big 4 firm utilized the inputs of all stakeholders and arrived at 15 processes that were perceived to be most important. At least 1 COBIT 5 process from each domain (Evaluate, Direct and Monitor [EDM]; Align, Plan and Organize [APO]; Build, Acquire and Implement [BAI]; Deliver, Service and Support [DSS]; and Manage, Evaluate and Assess [MEA]) was selected. Therefore, a number of enterprise IT management processes and 2 enterprise IT governance processes became part of the selection.

2. **Maturity assessment using COBIT 5 self-assessment tool kit**—Using the COBIT® Process Assessment Model (PAM): Using COBIT® 5, The Big 4 firm assisted process owners to conduct a COBIT 5 maturity assessment for each of the selected/prioritized 15 processes. As per PAM, the enterprise's current maturity for each process was evaluated and assigned one of the following classifications:
   - Incomplete (level 0)
   - Performed (level 1)
   - Managed (level 2)
   - Established (level 3)
   - Predictable (level 4)
   - Optimizing (level 5)

   Clear guidance is provided in **COBIT Self-assessment Guide: Using COBIT® 5** to support practitioners in measuring the maturity of each process in scope. The published guidance allowed The Big 4 firm and the bank's management and governance professionals to reach a conclusion on the maturity of each process efficiently.

3. **Development of a road map**—As part of the project, the bank requested that The Big 4 firm develop a road map to guide the improvement of maturity of the selected 15 processes. The Big 4 firm conducted a series of workshops with process owners and stakeholders to understand their views. Such workshops helped in developing a road map tailored to the needs of the bank. The Big 4 firm used the guidelines provided in **COBIT Process Assessment Model (PAM): Using COBIT 5** to recommend the following for each of the selected processes:
   - Establish target maturity to achieve given the priorities of the entity as a whole.
   - Determine how to progress toward higher levels of maturity and what steps need to be undertaken to reach higher maturity.
   - Determine the time-line required.
   - Define interdependencies.

   The recommendations were well received by management and governance layers at the bank. All stakeholders believed that improving maturity levels of each of the selected processes would certainly help overall management and GEIT.

4. **Development of a balanced scorecard (BSC)**—COBIT 5 successfully organizes the different elements typically measured for performance reporting of enterprise IT into an easily digestible manner for non-IT professionals
to understand. In this case, Financial, Internal, Learning and Growth, and Customer areas were included. Furthermore, **COBIT® 5: Enabling Processes** suggests a large number of key performance indicators (KPIs) to measure IT management and IT governance practices. The Big 4 firm was able to utilize all this information to develop a BSC (which the bank referred to as an “integrated scorecard”) that gave senior management and governing bodies a much better and more comprehensive view of the overall performance of enterprise IT in terms which are familiar to them (Financial, Internal, Learning and Growth, Customer).

**Conclusion**

The Big 4 firm and the bank leaders found the COBIT 5 publications extremely useful to drive the discussions related to complex IT management and IT governance matters at the bank and are confident that the recommendations and solutions suggested will yield high rewards in the future.

By adopting recommendations derived from COBIT 5, the bank is well on its way to solve the fundamental problems that were identified at the start of the project in the following way:

- **Organization structure**—Operating model for the 2nd layer of defence function (IT governance division) was established to pave the way for effective and efficient oversight of enterprise IT.
- **Cost control**—Improving efficiency and effectiveness of IT governance and IT management processes
- **Performance reporting**—Measuring IT management and IT governance processes with accuracy and in a systematic manner
- **Alignment to corporate strategies and goals**—Evaluating, monitoring and directing enterprise IT in alignment with the enterprise goals and direction
- **Risk management**—Improving risk management of enterprise IT

**Syed Salman, CISA**

Has more than 12 years of experience working at professional services firms in the Middle East and South Asia. He has primarily been involved in conducting IT audits at large entities in various industry segments. In his career, Salman has had the opportunity to help a number of entities by advising them on how to solve complex problems related to IT governance, IT management and IT risk management.