COBIT® 5

AN ISACA® FRAMEWORK

A Case Study Implementing COBIT® 5

MARK THOMAS

SEPTEMBER 2018

APMG International

BACKGROUND

Gain an understanding of the importance of balancing performance and conformance with a GEIT program.

Balancing performance and conformance in in an enterprise can be a daunting task. Adding up the various regulatory, compliance and conformance needs of any organization can have a major effect on enterprise performance if not governed and managed effectively.

In the country of Jordan, the Central Bank has mandated that all banks become “COBIT 5 Compliant,” which has caused a flurry of activity amongst boards and executive management across the banks throughout the country, as they move forward towards balancing organizational performance with the latest conformance requirements.

This whitepaper will explore the emerging importance of a solid Governance of Enterprise IT (GEIT) program and how leveraging the COBIT 5 framework products can greatly enhance not only compliance but can also be a positive move towards enhancing the overall governance posture as seen in Jordan.

The objectives of this whitepaper include the following:

- Gain an understanding of the importance of balancing performance and conformance with a GEIT program.
- Appreciate the value of the various COBIT and training products (Foundation, Implementation and Assessment) in the Jordanian Banking system mandate.
- Learn about the positive aspects and lessons learned of the COBIT 5 process capability assessments

CREATING VALUE

> Looking through a governance lens, it is important to understand that adopting frameworks requires a solid understanding of the business environment

Before diving into any endeavor of adopting a GEIT framework, it is important to first understand that the enterprise exists to create value for its stakeholders. Frameworks do not guarantee success but can be good practice models that can enable success. Therefore, value is created through internal and external service providers that must strive to meet the three core ingredients to creating value: realize benefits while optimizing risks and resources (figure 1 below).

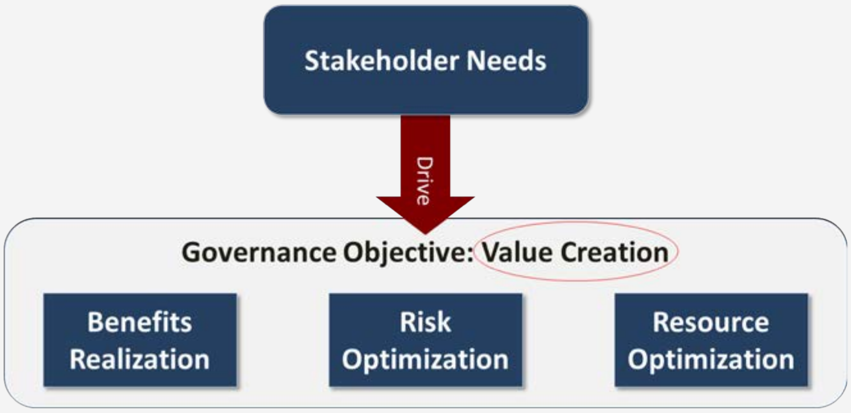


Figure 1, Value Creation Ingredients

A challenge many organizations face is not realizing that there are several governing levels and areas that must be considered when selecting the most appropriate frameworks. In today's environment, one single industry framework simply won't suffice. Looking through a governance lens, it is important to understand that adopting frameworks requires a solid understanding of the business environment as well as the value that each of these frameworks provides. Therefore, it is vital that frameworks are analyzed and adopted based on several factors, all of which should focus on one theme: create value for the enterprise. This means that IT enabled investments provide expected business benefits while optimizing resources and risks. Recognizing this is the first step towards creating a system of frameworks to support value.

STANDARDS & FRAMEWORK

> Simply understanding these levels will not automatically select the right frameworks.

There are a multitude of standards, frameworks, and bodies of knowledge out there. Consider looking at the framework ecosystem from multiple levels as illustrated in Figure 2 below. These levels provide good starting point for determining what value is created by leveraging a framework. Stakeholder needs have many drivers, but these must have a balance between performance and conformance.

At the Enterprise Governance level, the Balanced Scorecard helps measure business performance, while COSO (Committee of Sponsoring Organizations) creates a system of internal controls for conformance. This is followed by the GEIT level (Governance of Enterprise IT) where frameworks such as COBIT exist. At the Standards and Good Practices levels, frameworks can be selected based on their ability to satisfy the stakeholder needs.

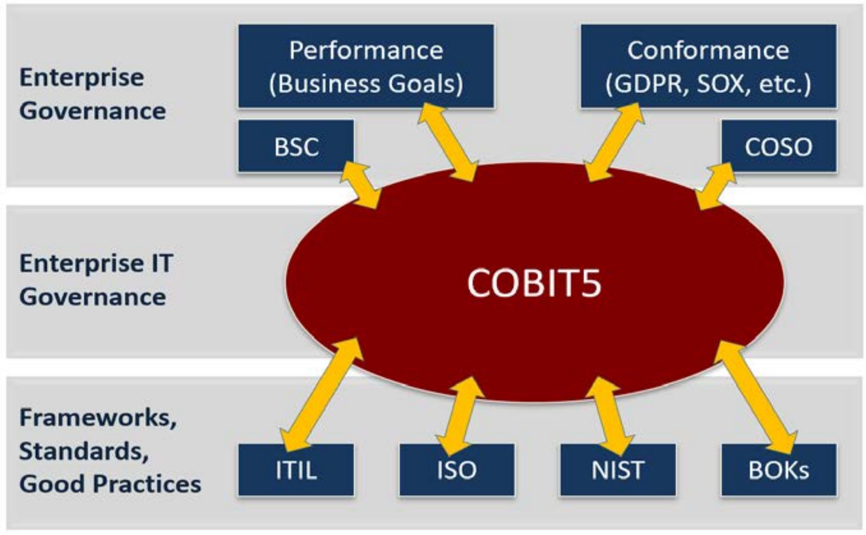

Enterprise Governance
Performance (Business Goals)
Conformance (GDPR, SOX, etc.)
BSC
COSO
Enterprise IT Governance
COBIT5
Frameworks, Standards, Good Practices
ITIL
ISO
NIST
BOKs

Figure 2, Governance Altitudes and Their Corresponding Frameworks

Simply understanding these levels will not automatically select the right frameworks. Since every enterprise sees value differently, an inventory of appropriate solutions must be conducted.

There are a few myths about frameworks that should be known before you start: First, a 'best practice' is only as good as how well it is adopted; Second, frameworks are suggestive not prescriptive; and finally, there is no such thing as a single silver bullet.

Therefore, it is no surprise that one of the top questions today regarding multiple frameworks is this: Is there framework that will help me manage all of my frameworks? The answer is simple. Yes, and it is called COBIT. This comprehensive framework is part of the ISACA product family (www.isaca.org/cobit) and assists enterprises in achieving value through the governance and management of enterprise IT. At the core of the framework are five principles, which are major inputs to how an enterprise selects, adopts and leverages other frameworks.

How does COBIT become a framework to manage frameworks? From a holistic view, the COBIT 5 enablers will not only help identify which frameworks are appropriate, but can also assist in determining the level of adoption as well. One of the powerful features of COBIT is that it references other frameworks.

Having established that COBIT 5 is a flexible framework, does it make sense to consider it a standard as well to meet a specific regulatory need? This is what is happening in Jordan now, and the results are not disappointing.

CENTRAL BANK OF JORDAN (CBJ)

The law establishing the CBJ stipulates that "the objectives of the Central Bank shall be to maintain monetary stability in the Kingdom, to ensure the convertibility of the Jordanian Dinar, and to promote the sustained growth of the Kingdom's economy in accordance with the general economic policy of the government."

CBJ is always aware of the international standards and frameworks that can benefit the financial sector in Jordan, and continually encourage the Jordanian banks to be on top of every new opportunity to create competitive advantage in the region.

Notably, the CBJ has issued many regulations in the past years for the financial sector in Jordan to comply with, including PCI standards, COBIT 5 Framework, Cyber Security Framework and recently asking the Jordanian banks for a plan to comply with GDPR. This makes the CBJ one of the pioneers and unique regulatory bodies in the region who is playing a significant role in enhancing the financial sector.

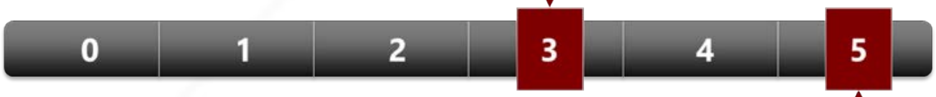
*Information from the Central Bank of Jordan Website

CENTRAL BANK REQUIREMENTS

Gain an understanding of the importance of balancing performance and conformance with a GEIT program.

The requirements for Jordanian banks, at first glance, appears very aggressive. However, once momentum gained, the results have been somewhat positive.

One requirement that has created much activity is that banks are required to implement all 37 Processes of the COBIT 5 framework targeting specific capability levels. As noted below, these processes are required to achieve a capability level 3 within 18 months of the publication of the regulation and achieve a capability level 5 within three years of the publication of the regulation.



***Achieve capability level 3**, Established Process, after a maximum of eighteen months from the date of publishing the regulation.*

***Achieve capability level 5**, Optimized Process, three years from the date of publishing the regulation.*

Figure 3, Process Capability Requirements

In addition to the requirement to meet specific process capability levels, the following additional requirements are noted:

- Use the 17 Enterprise Goals and 17 IT-related Goals as per the COBIT 5 Framework to create the goals cascade that drives enablers.
- Have a minimum set of policies for the governance framework.
- Have a minimum set of reports for the governance framework.
- Establish and maintain the infrastructure that supports the governance framework.
- Adopt the necessary matrices of competencies and policies of human resources management to achieve the requirements of GEIT, and to ensure that the appropriate human resources are in place.
- Adopt a code of conduct that reflects professional behavior related to the management of information and its related technology that clearly define the desired behavioral rules and consequences.

Additionally, the CBJ is requiring all banks to establish two committees for the governance and management of information and related technologies: The Committee of Governance of Information Technology, and the Directive/Steering Committee of IT.

CENTRAL BANK REQUIREMENTS

COMMITTEE OF GOVERNANCE OF INFORMATION TECHNOLOGY

- The Board shall form a committee of governance of information technology from its members, and this committee shall be formed from three members at least, and preferably include people with experience or strategic knowledge in information technology.
- The committee may hire, when necessary, and at the expense of the bank and coordination with the chairman of the Board, external experts in the field. The committee may invite any of the bank's management members to attend meetings for consultation purposes.
- The Board determines its objectives and delegates their powers, according to a charter that illustrates this, taking into consideration that the board will remain the ultimate accountable party.
- The committee shall meet on a quarterly basis at least and maintain documented records of their meetings.

DIRECTIVE/STEERING COMMITTEE OF IT

- The senior executive management shall form necessary directive committees to ensure a strategic alignment of information technology to achieve the strategic objectives of the bank and that shall be in a sustainable manner.
- Therefore, a committee named the Directive Committee of IT shall be formed and headed by the general manager and with the membership of senior executive management managers, including the head of information technology, head of risk management and head of information security.
- One of its members shall be elected to be an observer member in this committee as well as the head of internal audit, and can invite third parties to attend the meetings, when needed.
- The committee shall meet on a quarterly basis at least and maintain documented records of their meetings.

Although the requirements appear aggressive, we are seeing positive progress towards meeting these. However, this doesn't come without a few challenges.

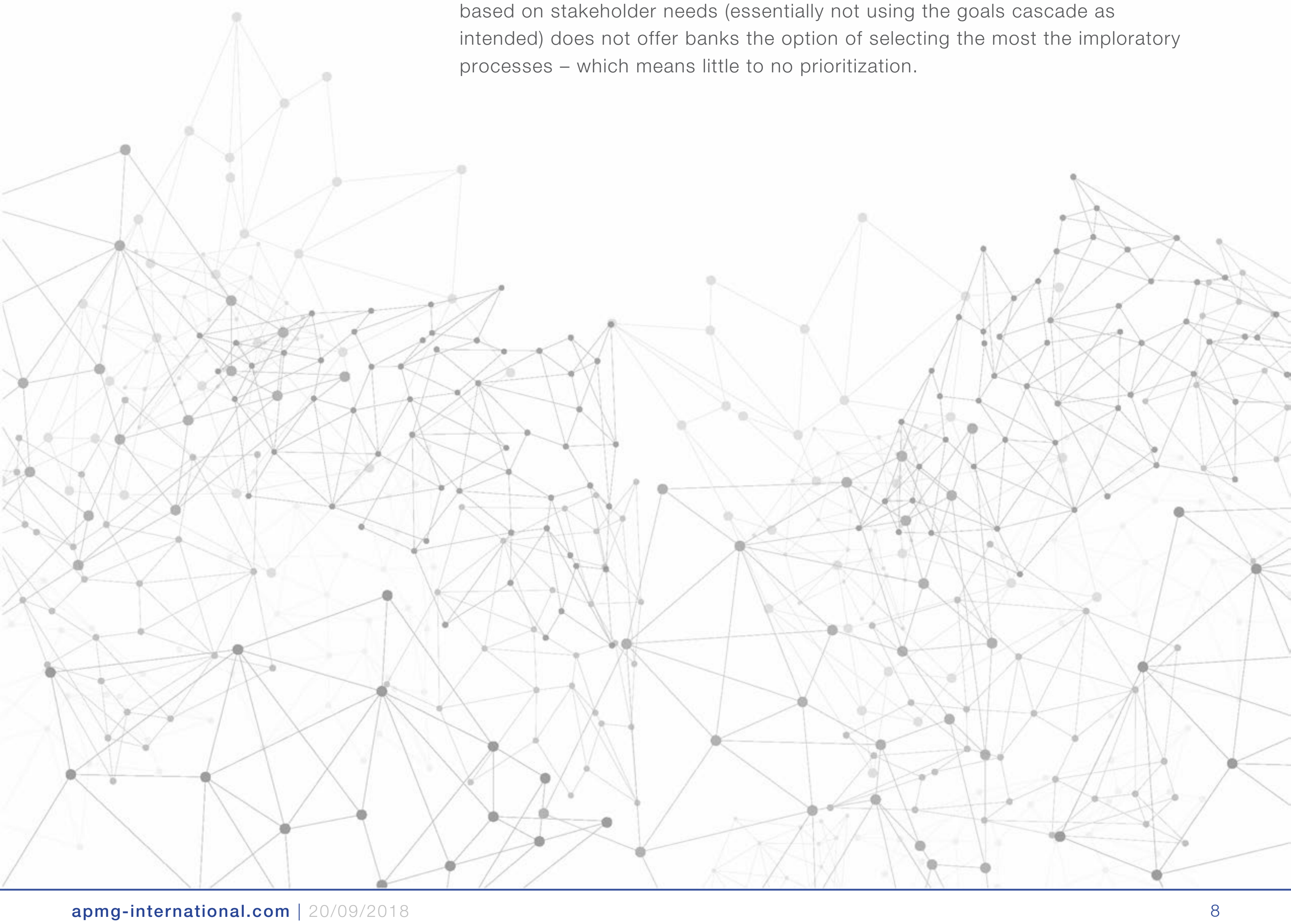
CHALLENGES

This is first time we’ve encountered COBIT 5 dictated at this level as a standard rather than a suggested framework that can be adapted based on enterprise needs. The assumption made by the CBJ was that all organizations operated similar environments, resources and levels of complexity which added a few challenges. In addition to the COBIT 5 requirement, the central bank has issued many other regulations around cloud computing, cybersecurity, and recently the adoption of the GDPR. However, understanding that the COBIT 5 framework can be leveraged as an overarching governance and management model for enterprise IT, all of these requirements can be aligned under one program to avoid redundancy.

> Gain an understanding of the importance of balancing performance and conformance with a GEIT program.

The aggressive timeline of meeting the required capability levels have been daunting. The limited time frame of 18 months to fully implement 37 processes basically means implementing two processes per month up to capability level three – fully achieved! Add to this the requirement an even higher capability level, in this case level 5, requires resources that far beyond many banks’ budgets and capabilities. This type of effort clearly requires training and expertise that often requires external assistance, and the MENA region (Middle East and North Africa) generally lacks in awareness and training provider availability in the areas of IT governance and COBIT 5.

Furthermore, by not allowing the flexibility of choosing the goals and processes based on stakeholder needs (essentially not using the goals cascade as intended) does not offer banks the option of selecting the most the imploratory processes – which means little to no prioritization.



THE PLAN AND RESULTS

Recognizing the need for industry experts in COBIT 5, a local consulting company in Amman, Jordan called ScanWave sought the direct involvement from ISACA and APMG to create a strategic plan towards assisting the banks in meeting these rigorous requirements and providing the proper accredited training.

> ScanWave sought the direct involvement from ISACA and APMG to create a strategic plan

The plan included the following key tasks:

- Provide ISO compliant process capability assessments using certified COBIT 5 Assessors.
- Provide roadmaps to meet the standard which include practices and activities required to close the gap between the current and required capability levels.
- Provide assistance to the banks in the various areas required to meet the CBJ standards.
- Build and publish a governance framework.
- Conduct frequent proper reflections, representing the current status of the progress towards the target capability levels.
- Report compliance towards each milestone.

Overall, using COBIT 5 as a standard has been successful. Aside from simply meeting the requirements, banks are finding that they have a renewed level of quality in the areas of IT Policies, Enterprise Architecture, IT Risk Management, Security, and Business Continuity to name a few.

As for the target capability levels, the following figures illustrate the growth in capability levels for all processes. The growth in process capability levels between 2017 and today are very positive. Figure 4 below indicates where two representative banks assessed – right around level one. Figure 5 represents the progress of one of these banks in 2018 which indicates a strong increase into level three.

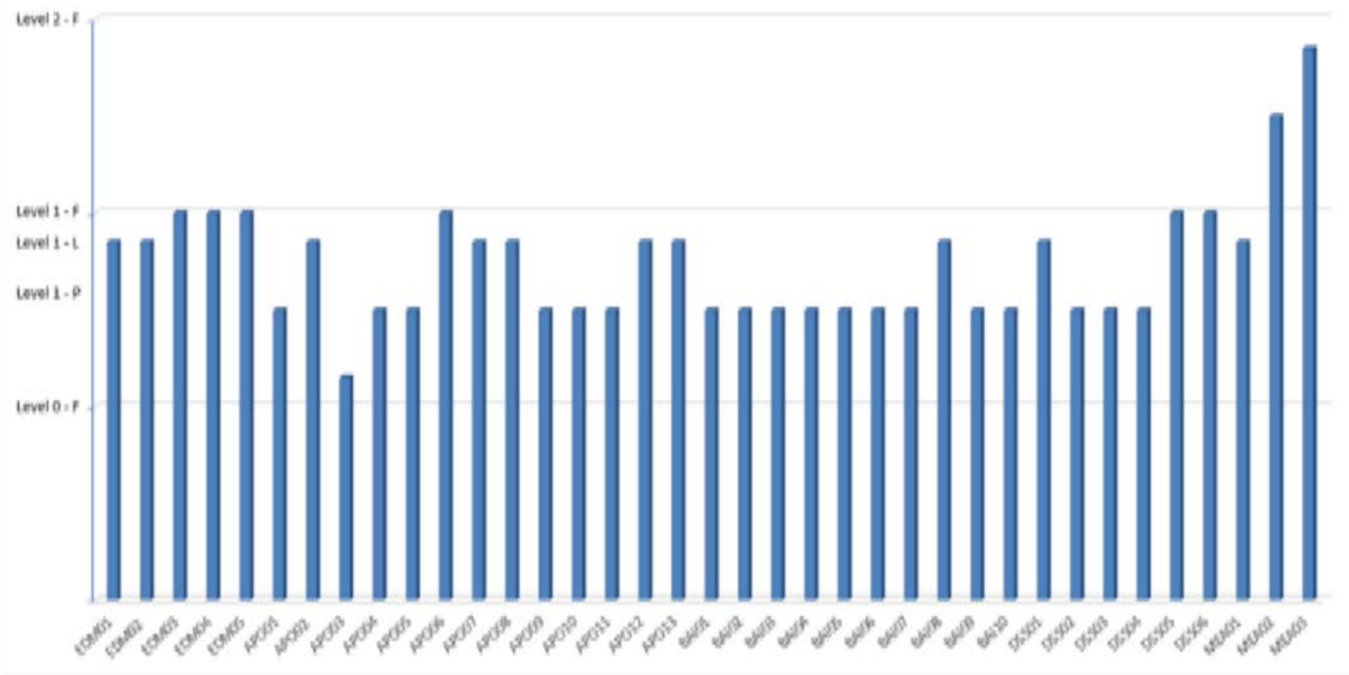


Figure 4, Representative Capability Levels in 2017

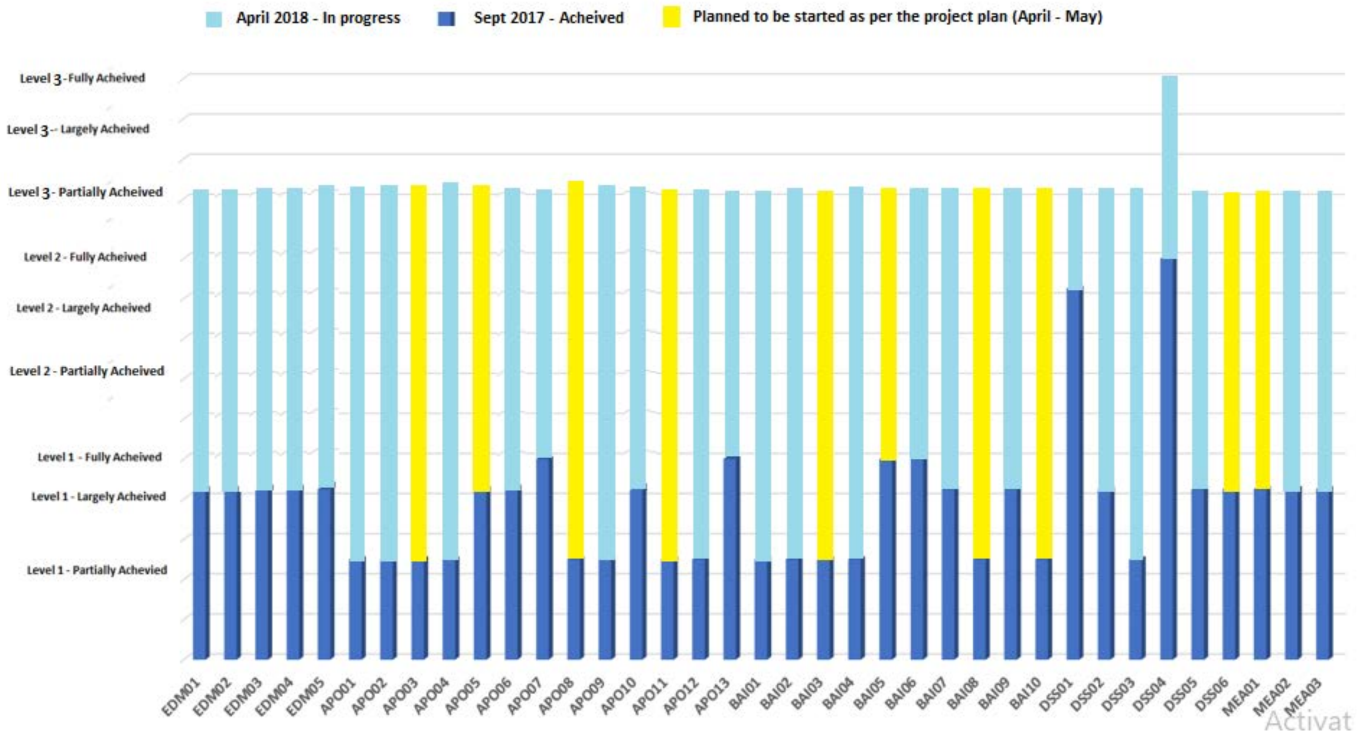


Figure 5, Sample Results for 2018

LOOKING FORWARD AND LESSONS LEARNED

> Gain an understanding of the importance of balancing performance and conformance with a GEIT program.

As expected, a primary goal is to continue to maintain the current process capability levels while working towards the target capabilities and continually improve the governance and management profiles of the banks with regards to IT. Increasing the value proposition of the IT organizations will assist in the integration with the latest regulations and requirements (cybersecurity, GDPR, etc.).

One of the predominant lessons learned is in regards to training. Although several banks are currently conducting COBIT 5 courses, the journey would have been much more efficient if training was conducted at the start of the process. In many cases, bank staff did not know the essential details of COBIT 5 during their initial assessments, which led to a cumbersome and awkward initial assessment - and had the “ah-ha” moment several months later when attending a COBIT 5 training course.

The three primary courses that will provide this value include:

- COBIT 5 Foundation
- COBIT 5 Implementation
- COBIT 5 Assessor

Regardless of industry or size, all companies need governance, and with that need comes multiple frameworks, models and standards. Using COBIT 5 to assist in integrating a holistic approach to governance while managing multiple best practices will ultimately help meet the governance goal of meeting stakeholder needs. COBIT 5 has many tools and techniques in the product architecture that can be adopted to reduce the exhaustion of managing multiple frameworks, and allow the enterprise to focus on value.

ISACA®

Trust in, and value from, information systems

Independent not-for-profit, global association
for information systems.

Owners of COBIT® 5.

www.isaca.org

APMG International

Accrediting Professionals

Global exam and accreditation institute.

Appointed by ISACA to accredit COBIT® 5 Training Providers, assuring the quality of training and certification offered.

www.apmg-international.com

SCAN WAVE

Premium provider of security solutions for business
acceleration in Jordan.

Worked with Mark Thomas/Escoute to provide COBIT® 5 training and implementation services.

www.scanwave.org | www.escoute.com

APMG GLOBAL REACH

OFFICES IN 7 COUNTRIES

- Australia
- China
- India
- UK
- Malaysia
- Netherlands
- USA

REPRESENTATIVES IN 9 COUNTRIES

- Italy
- France
- Germany
- Canada
- South Africa
- Poland
- Russia
- Spain
- Brazil

APMG International

FIND OUT MORE

☎ +44 (0) 1494 452450

✉ servicedesk@apmgroupltd.com

apmg-international.com

facebook.com/APMGinternationalLTD

linkedin.com/company/apm-group

@APMG_Inter