Building a Maturity Model for COBIT 2019 Based on CMMI

También disponible en español
www.isaca.org/currentissue

Years ago, the COBIT® 5 Process Assessment Model (PAM) was commonly used to assess the maturity level of a COBIT® implementation. The PAM provided indicators for nine attributes and six process capability levels and was used to guide auditors and IT departments.

There is no PAM for COBIT® 2019, but Capability Maturity Model Integration (CMMI) can be used to measure capability levels and combine that information with other factors to give value to the organizational process for measuring maturity. With that information, it is possible to create custom schemas and tools.

Building the Maturity Model

COBIT® 2019 Framework: Governance and Management Objectives describes the expected capability level for each of the 1202 COBIT activities. From the score obtained for each of those activities, it is possible to determine the maturity level for the 231 practices, the 40 objectives and the five domains constituting the COBIT 2019 framework.[1] **Figure 1** gives a sample of the governance practices, example metrics, activities and expected capability levels.

A total of 1202 activities comprise the foundation for the model. Based on CMMI, COBIT has defined six capability levels as shown in **figure 2**.

Determining Capability Level

Based on the activity's capability level, the next step is to determine how to reflect the capability level for the practice. For organizations in early maturity stages, a simple average calculation for the activity values can be used to obtain the practice score or level. If an organization has a greater capacity for describing the maturity levels of their activities, then a weighted average, according to the capacity of the organization, is recommended to describe those activities.

Determining the maturity level entails using the capability level combined with other factors to get to a score that reflects not only the existence of the activities but also a holistic and integral view of the organization's processes, when combined with other metrics, to present to management. To achieve this, it is necessary to correlate the capability level with other indicators to get a better descriptive score for the processes that can give a concise approach to the organizational status. It is also necessary to create milestones beyond the CMMI generic description for each practice to identify the expected evidence for the capability level in each activity. This is especially important for creating road maps for remediation and measuring the results along the way.

The building process schema consist of five steps as illustrated in **figure 3**.

Luis Gorgona, CISA CDPSE
Is a professional with 20 years of experience in IT and cybersecurity. Gorgona served as chief information security officer for Costa Rica's Presidential House from 2006 to 2010. During that period, he was an instructor for the cybersecurity program of the Interamerican Committee Against Terrorism of the Organization of American States. From 2010 to the present, he has worked for several transnational enterprises in fields such as information security, cybersecurity and governance, risk, and compliance. In 2021, he joined the RSM Costa Rica as an IT consulting partner.

Enjoying this article?

- Read *A Risk Aware Path to Cybersecurity Resilience and Maturity. www.isaca.org/CMMI-Cyber Capability-Maturity*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

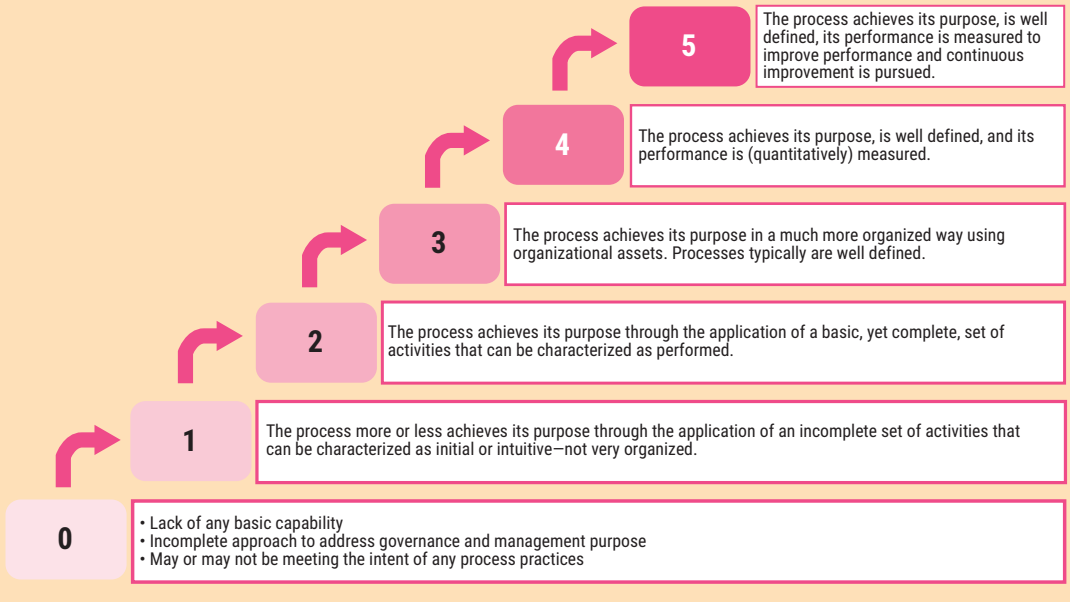
Figure 1—The Process Component

Governance Practice	Example Metrics
EDM01.02 Direct the governance system. Inform leaders on I&T governance principles and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of I&T in line with the agreed governance principles, decision-making models and authority levels. Define the information required for informed decision making.	a. Degree to which agreed-on I&T governance principles are evident in processes and practices (percentage of processes and practices traceable to principles) b. Frequency of I&T governance reporting to executive committee and board c. Number of roles, responsibilities and authorities for I&T governance that are defined, assigned and accepted by appropriate business and I&T management

Activities	Capability Level
1. Communicate governance of I&T principles and agree with executive management on the way to establish informed and committed leadership.	2
2. Establish or delegate the establishment of governance structures, processes and practices in line with agreed-on design principles.	
3. Establish an I&T governance board (or equivalent) at the board level. This board should ensure that governance of information and technology, as part of enterprise governance, is adequately addressed; advise on strategic direction; and determine prioritization of I&T-enabled investment programs in line with the enterprise's business strategy and priorities.	
4. Allocate responsibility, authority and accountability for I&T decisions in line with agreed-on governance design principles, decision-making models and delegation.	3
5. Ensure that communication and reporting mechanisms provide those responsible for oversight and decision making with appropriate information.	
6. Direct that staff follow relevant guidelines for ethical and professional behavior and ensure that consequences of noncompliance are known and enforced.	
7. Direct the establishment of a reward system to promote desirable cultural change.	

Source: ISACA, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, *https://www.isaca.org/resources/cobit*

Figure 2—Capability Levels for Processes



Source: ISACA®, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, *https://www.isaca.org/resources/cobit*

All information should be integrated into a tool that allows an assessment of the organization and creates the proper reporting in a language that top-level management can understand and sponsor.

Once all the information is integrated into the tool, the evaluation scorecard should look similar to **Figure 4.**

Figure 3—Maturity Model Building Process

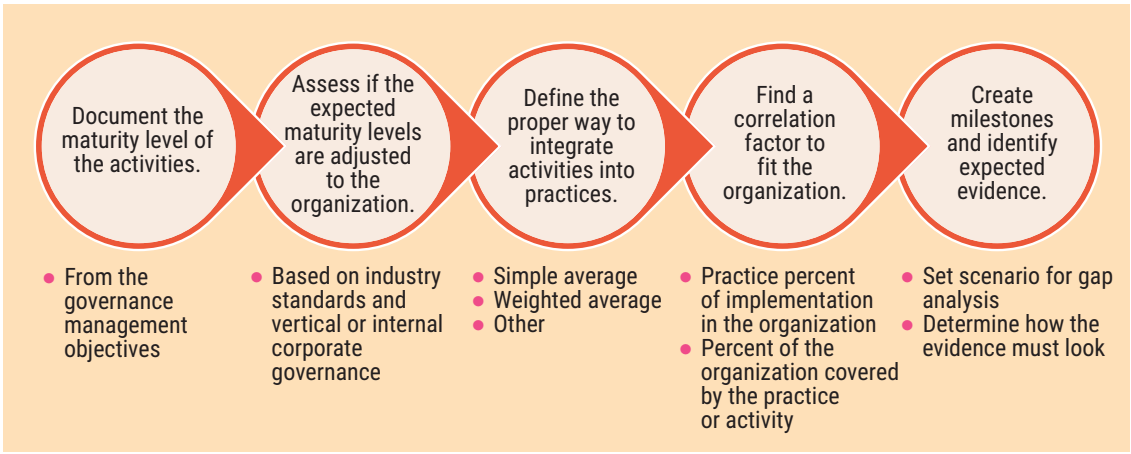


Figure 4—Activity Maturity Evaluation Scorecard

Practice ID	EDM01.01	
Practice Name	Evaluate the governance system.	
Practice Description	Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements and evaluate the current and future design of governance of enterprise I&T.	
Activities	Analyze and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence governance design.	
Nonexistent	There is no activity in place.	0
Performed Process	The activity is existent.	1
Managed	The activity is approved and in place.	2
Established	The activity is approved and in place and communicated.	3
Predictable	The activity is approved and in place and communicated. Metrics are in place to measure the activity.	4
Optimizing	The activity is approved and in place and communicated. Metrics are in place to measure the activity. Results from the metrics are used to improve the process.	5
Capability Level	1	
Expected	2	

Conclusion

Maturity models are becoming the common language used by organizations to understand the current state of their COBIT implementations. They also serve as guides to create gap analysis and road maps for improvement. Every organization is different, so different roads can achieve the desired result for different organizations, verticals, industries or regions.

Author's Note

The author wishes to thank Mariela Varela and Raúl Rivera from the ISACA® Costa Rica Chapter for their review of this model and their suggestions for improvement.

Endnotes

1 ISACA®, *COBIT® 2019 Framework: Governance and Management Objectives*, USA, 2018, *https://www.isaca.org/resources/cobit*

> "MATURITY MODELS ARE BECOMING THE COMMON LANGUAGE USED BY ORGANIZATIONS TO UNDERSTAND THE CURRENT STATE OF THEIR COBIT IMPLEMENTATIONS."