The COBIT Maturity Model in a Vendor Evaluation Case

By Andrea Pederiva

The maturity model provided by the COBIT Management Guidelines for the 34 COBIT IT processes is becoming an increasingly popular tool to manage the timeless issue of balancing risk and control in a cost-effective manner. Control Objectives for Information and related Technology (COBIT) is published by the IT Governance Institute (ITGI) and Information Systems Audit and Control Foundation (ISACF).

The COBIT Maturity Model is an IT governance tool used to measure how well developed the management processes are with respect to internal controls. The maturity model allows an organization to grade itself from nonexistent (0) to optimized (5). Such capability can be exploited by auditors to help management fulfill its IT governance responsibilities, i.e., exercise effective responsibility over the use of IT just like any other part of the business.

A fundamental feature of the maturity model is that it allows an organization to measure as-is maturity levels, and define to-be maturity levels as well as gaps to fill. As a result, an organization can discover practical improvements to the system of internal controls of IT. However, maturity levels are not a goal, but rather they are a means to evaluate the adequacy of the internal controls with respect to company business objectives.

In volume 6, 2002, of the Information Systems Control Journal, the article “Control and Governance Maturity Survey: Establishing a Reference Benchmark and a Self-assessment Tool,” by Erik Guldentops, CISA, CISM, Wim Van Grembergen, Ph.D., and Steven De Haes, discusses the results of the 2002 ISACA survey on the maturity level of 15 COBIT IT processes. According to the article, survey target processes were selected a year prior by interviewing a group of 20 IT and senior experts.

The ISACA survey results can be used as a reference benchmark and a self-assessment tool. The results of the survey cover a broad range of countries, industries and size groups, making them useful for numerous companies worldwide.

In an engagement experience, this author participated on a team that used the COBIT Maturity Model to benchmark four possible vendors, and then compared its results to the ISACA survey results. The process undertaken, as well as the lessons learned and the results, is discussed in the remainder of this article.

Main Issues and Lessons Learned

At the beginning of this benchmarking effort, there were two main issues:

• The need for a criterion to choose the processes to benchmark
• The need for a method to measure the vendor’s maturity level with respect to the COBIT Maturity Model

The processes to benchmark were chosen by scoring the COBIT IT processes on a risk-importance basis, from the point of view of a potential customer. This task followed a logic similar to the one in the risk assessment form of the COBIT Implementation Tool Set.

The definition of a method to measure the maturity level required more effort, in part, because the desire was for a method precise and efficient enough to allow for interaction with potential vendors. A questionnaire and a ranking system were developed to compute the maturity level from the questionnaire results. While the approach was not unusual, there were a few new ideas used that proved to be valuable. (These new ideas subsequently have been tested by other AIEA colleagues.)

The method used is not strictly incremental and, therefore, does not satisfy the COBIT Maturity Model’s incremental criterion—to check “a posteriori.”

However, the method proved to be strong, with respect to the objective of benchmarking the four organizations under examination, and the results were logical given the knowledge collected on the organizations during the benchmarking effort. Moreover, it appears that the method can be further developed to build a strictly incremental approach.

Finally, if combined with different methods, the comparison between the benchmarking results and the ISACA survey results provided a basis for an overall discussion on the distribution of the “strongest” and “weakest” areas.

Benchmarking Results

Figure 1 displays the results of the benchmarking effort as compared with the 2002 ISACA survey results. The four organizations were essentially software makers with an independent consultancy branch; hence, the benchmark values refer to the ISACA 2002 survey results related to the Europe, Middle East and Africa (EMEA) small IT service providers. The ISACA value was computed as the weighted mean of the respondents’ distribution on the six possible maturity levels (0 - 5).

The benchmarking results reveal that three of the four companies are aligned between themselves and the ISACA sample with the exception of a few processes. However, one company
almost always has a maturity level far below the other companies. The results can be better understood with the following facts:

- CO4 was the only participant in the benchmark that was not ISO9000-certified.
- The respondents are IT vendors with consultancy branches; hence, IT processes (including AI4 Install and Accredit Systems) are their core processes.
- The processes in which the ISACA sample has a score lower than the benchmarking sample appear to be the typical core processes of an application systems developer and vendor. This suggests a possibly different composition between the benchmarking sample and the ISACA sample for the EMEA small IT service providers.
- CO3 is the IT subsidiary of a publicly owned group with strong quality and organizational culture—in part, due to its defense-related experiences.

**Benchmark Method**

The method used in the benchmark is based on a questionnaire derived from the COBIT Maturity Model, and it relies on a “scenario” concept—i.e., every maturity level is considered to be a scenario. A maturity level scenario includes the description of the organization and the internal controls of a company satisfying the requirements of a specific maturity level.

The questionnaire is intended to capture the compliance of an IT organization under investigation to the diverse scenarios describing each maturity level. Based on the questionnaire results, an algorithm computes a “compliance” vector that describes the compliance of the organization to every scenario. Then, it uses the vector to compute the maturity level as a weighted average of the organization’s compliance with respect to each scenario.

**The Questionnaire**

To arrange the questionnaire, the maturity level descriptions of the COBIT Maturity Model were studied. It was concluded that the descriptions of the maturity levels could be viewed as sets of “atomic” statements. Each maturity level description is a statement that can be either true or false, or either partially true or partially false. The examination resulted in the realization that a compliance value could be computed for the maturity level by collecting and then combining a compliance value for each statement.

Based on this concept, the maturity level descriptions were split into separate statements, and all statements in the maturity level descriptions were separate in the questionnaire.

Figure 2 displays an example of how the questionnaire statements were derived for the maturity model of process PO10 Managing Projects.

**Figure 2—Questionnaire Construction for PO10 Managing Projects (maturity levels 0 and part of 1)**

<table>
<thead>
<tr>
<th>Maturity Level Description</th>
<th>Questionnaire Statements</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Nonexistent</td>
<td>• The organization does not use project management techniques.</td>
</tr>
<tr>
<td></td>
<td>• The organization does not consider business impacts associated with project mismanagement and development project failures.</td>
</tr>
<tr>
<td>1 Initial/Ad hoc</td>
<td>• The organization is generally aware of the need for projects to be structured and it is aware of the risks of poorly managed projects. The use of project management techniques and approaches within IT is a decision left to individual IT managers. Projects are generally poorly defined.</td>
</tr>
</tbody>
</table>

To obtain a compliance value for each statement, the following question was asked: “With respect to your organization, how much do you agree with the following statements?” Four possible answers—not at all, a little, quite a lot or completely—were provided.

The answers were mapped to the following compliance values—0, 0.33, 0.66, 1 (figure 3).

**Figure 3—Compliance Level Numeric Values**

<table>
<thead>
<tr>
<th>Agreement with Statement</th>
<th>Compliance Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not at all</td>
<td>0</td>
</tr>
<tr>
<td>A little</td>
<td>0.33</td>
</tr>
<tr>
<td>Quite a lot</td>
<td>0.66</td>
</tr>
<tr>
<td>Completely</td>
<td>1</td>
</tr>
</tbody>
</table>

**The Algorithm**

When the questionnaire is complete, each maturity level will have a set of statements, each with its own compliance value of 0, 0.33, 0.66 or 1. For example, figure 4 shows the fully compiled questionnaire for the level 3 maturity model of
The compliance value for the scenario can be computed as the average of the compliance level of the statements. In the case of maturity level 3, it is equal to 8.63/11 = 0.78.

Working in the same way on the other maturity levels, one can compute a compliance value for all the maturity levels form 0 to 5. Figure 5 provides an example of the possible results of this computation.

Finally, the maturity level summary for the process was computed by combining the normalized compliance values for each maturity level as shown in figure 7.

**Lessons Learned**

Because of its construction criteria, the questionnaire is aligned completely with the maturity model and fairly detailed with respect to the maturity requirements. This has proven to be useful to support subsequent discussions aimed at identifying the key points that were enabling or preventing the organization to reach a given maturity level.

The experience also suggested that to exploit the benefits of the maturity level paradigm, it appears useful to allow a company to grade itself in the full range from 0 to 5 rather than having to choose a position in the coarse grid (0, 1, 2, ... 5).

As a suggestion, in performing a benchmarking effort, first discuss the maturity requirements without showing the maturity level in which the questions belong. This will reduce any bias by the respondents that can be present when they know the effects of the answers on the final result.

Further work must be done to assemble a strictly incremental approach to the measurement of the maturity level, as required by the COBIT Maturity Model. However, for comparison purposes, the method presented here proved to be efficient, providing strong results and facilitating the subsequent discussions on the use of the COBIT Maturity Model as an effective management tool.
To make the method applicable beyond comparison, as with planning improvements (as-is, to-be, gap analysis), it must manage partial compliance at lower levels. That is not an issue in the method presented here, but for improvements one wants to see consistency at the lower levels before evaluating the contributions at the higher levels.

Summary

The COBIT Management Guidelines do not suggest any special methodology to measure the maturity level of the IT processes, and many approaches can be followed. However, to use the COBIT Maturity Model as an effective management tool, companies must develop an efficient methodology to measure the maturity level of their IT processes. The results of a benchmarking effort based on the COBIT Maturity Model and the method used to measure a maturity level for the IT processes have been presented. Although the method is not strictly incremental, as required by the Maturity Model, it proved to be an efficient tool to measure the maturity level for comparison purposes. It also provided ideas that can be developed and used to build a strictly incremental method.

Endnotes


2 Associazione Italiana IS Auditors (AIEA), is the Milan ISACA chapter, in Italy.

3 COBIT Management Guidelines, IT Governance Institute and Information Systems Audit and Control Foundation, 2000, p. 100

4 For example, one has to check “a posteriori” if a company in which the method is rating, for example, 3.5 really satisfies all the conditions to meet the maturity level 3.

5 This author has recently engaged in another benchmarking effort involving some 20 small Italian banks. This effort involves a strictly incremental approach.

6 Staff is greater than 150 people, but less than 1,500 people.

7 When the descriptions were split into distinct statements, some statements partially lost their context and became less understandable; for this reason, some statements were modified for the sake of clarity to avoid ambiguities.

8 It was discovered that equivalent questions and a set of possible answers could be used. For example, after some discussion, the following question was chosen: “How do you rank the following statements in the range true, partially true, not completely false, false?” Some alternatives were discussed, and the one described was chosen.

Andrea Pederiva
is a manager at Deloitte & Touche in Treviso, Italy. He has developed vast experience in the field of management and control of information systems with specific reference to the development and the assurance of internal controls for IT organizations. He has experience in privacy, IT auditing, quality management, IT security, project management and project risk management.