Copyright © 2003 Information Systems Audit and Control Association. All rights reserved. www.isaca.org.

Maturity Measurement—First the Purpose, Then the Method

Erik Guldentops, CISA, CISM

A further comment on "The COBIT Maturity Model in a Vendor Evaluation Case," by Andrea Pederiva, published in *Journal*, volume 3, 2003.

Some Warnings on the Use of Maturity Level Measurement

Many people have started using COBIT's maturity models for measuring. Some are focusing too intensely on the magical numbers. When measuring IT process maturity, first and foremost be clear about the purpose of measurement, i.e., clearly understand what you need the measure for and what you will do when you have the measure. Maturity measurement is not a goal in itself, it should support, for example:

- Raising awareness
- Identifying weaknesses
- Identifying priority improvements

The measurement method that best supports the purpose should be chosen.

The most common approach of measuring maturity is a multidisciplinary group of people who—in a facilitated workshop style—debate and come to a consensus as to the enterprise's current level of maturity. The principle of not assigning a higher level when not all elements of the lower level are being applied (threshold approach) should be followed wherever possible but one should not be too stringent about it. Very often the discussion will lead to compensating factors and practices that need to be taken into account. The debate additionally will reveal the practices that are performed consistently and those that are not.

Ideally, consensus also is reached as to the level at which the enterprise should be. The agreed-upon result is then presented to management for review and ratification, and becomes input to the initiative that deals with identifying and planning improvements.

Comparison to the results of ISACA's Maturity Survey (see *Journal*, volume 6, 2002) and plotting the enterprise result onto these spider-web charts are certainly good methods and tools in support of this approach.

Table 1—Maturity Model Attributes

	Understanding and Awareness	Training and Communication	Process and Practices	Techniques and Automation	Compliance	Expertise
1	Recognition	Sporadic communication on the issues	*Ad hoc* approaches to process and practice			
2	Awareness	Communication on the overall issue and need	Similar/common processes emerge; largely intuitive	Common tools emerging	Inconsistent monitoring in isolated areas	
3	Understand need to act	Informal training supports individual initiative	Existing practices defined, standardised and documented; sharing of the better practices	Currently available techniques used; minimum practices enforced; tool set standardised	Inconsistent monitoring globally; measurement processes emerge; IT balanced scorecard ideas being adopted; occasional intuitive application of root cause analysis	Involvement of IT specialists
4	Understand full requirements	Formal training supports a managed program	Process ownership and responsibilities assigned; process sound and complete; internal best practices applied	Mature techniques applied; standard tools enforced; limited, tactical use of technology exists	IT balanced scorecards implemented in some areas with exceptions and noted by management; root cause analysis standardised	Involvement of all internal domain experts
5	Advanced forward-looking understanding	Training and communication support external best practices and use of leading-edge concepts/techniques	Best external practices applied	Sophisticated techniques deployed; extensive, optimized use of technology exists	Global application of IT balance scorecard and exceptions noted by management globally and consistently; root cause analysis consistently applied	Use of external experts and industry leaders for guidance

Table 2—Maturity Model: A "Rising Star" Chart

	Understanding and Awareness	Training and Communication	Process and Practices	Techniques and Automation	Compliance	Expertise
5	Advanced forward-looking understanding	Training and communication support external best practices and use of leading-edge concepts/techniques	Best external practices applied	Sophisticated techniques deployed; extensive, optimized use of technology exists	Global application of IT balance scorecard and exceptions noted by management globally and consistently; root cause analysis consistently applied	Use of external experts and industry leaders for guidance
4	Understand full requirements	Formal training supports a managed program	Process ownership and responsibilities assigned; process sound and complete; internal best practices applied	Mature techniques applied; standard tools enforced; limited, tactical use of technology exists	IT balanced scorecards implemented in some areas with exceptions and noted by management; root cause analysis standardised	Involvement of all internal domain experts
3	Understand need to act	Informal training supports individual initiative	Existing practices defined, standardised and documented; sharing of the better practices	Currently available techniques used; minimum practices enforced; tool set standardised.	Inconsistent monitoring globally; measurement processes emerge; IT balanced scorecard ideas being adopted; occasional intuitive application of root cause analysis	Involvement of IT specialists
2	Awareness	Communication on the overall issue and need	Similar/common processes emerge; largely intuitive	Common tools emerging	Inconsistent monitoring in isolated areas	
1	Recognition	Sporadic communication on the issues	*Ad hoc* approaches to process and practice			

Another very pragmatic approach adopted by some is to decompose the maturity descriptions into a number of statements to which management can provide their level of agreement (e.g., "a lot," "largely," "somewhat," "marginally" or "not at all"). Andrea Pederiva's article in volume 3 of the *Journal* provides an excellent example of that and also illustrates another purpose where maturity measurement is beneficial—product, service or vendor selection. Refinement can consist of adapting the simple statements to the organisation's environment and issues, and even of adding weights of importance to each statement, as Pederiva showed. A more advanced approach would then use the control objectives and critical success factors of CobiT to add statements to appropriate maturity levels. Then, it is up to the user to include a simple but consistent measurement method that efficiently supports the purpose of the measurement.

It is not easy, however, to obtain, based on the maturity levels, a nice continuous measurement of the "goodness" of the IT control environment. One reason for this is that the maturity levels—while primarily measuring ***how*** IT processes are controlled—also mix in some of the ***what***, i.e., the control practices. Another reason is that certain attributes—as illustrated by the maturity attribute table provide in the CobiT *Management Guidelines* (see **table 1**)—are not measured in all levels. For example, one practice can be addressed increasingly in levels 2 and 3 and then not at all in level 4. As a result, the score at level 4 may suddenly drop because an attribute is no longer measured on the assumption that it has been taken care of at a lower level.

When breaking the maturity levels into more measurable elements, one also has to be careful of the qualifiers when assigning values to the elements, for example:

- Level 2—There is limited stakeholder involvement: completely agree.
- Level 3—There is complete stakeholder involvement: largely agree.

This would imply a higher score at level 2 than at level 3 because of the qualifiers—"limited" and "complete." While it is the intention to look for higher degrees of compliance when going up maturity levels, it may appear strange when looking at the component "stakeholder involvement" that the score obtained is reduced. The cause is the use of increasingly stronger qualifiers. An extreme case in point is the negative statements in levels 0 and 1. For example, if one is not careful and simply applies the compliance scores to all measurable elements, one would get a high score for a negative statement and the score would become lower as one improves.

A different method, focusing only on the ***how*** and thereby overcoming some of the above issues, consists of using the matrix of attributes as documented in CobiT's *Management Guidelines* and scoring for each attribute per process—where one is and where one wants to be (through checklist or workshop). This facilitates the identification of major trends (e.g., lack of awareness and insufficient policies). **Table 2** illustrates how the matrix itself can become the as-is and to-be recording and reporting tool, in the form of a "rising star" diagram.

Maturity levels are not a goal in themselves but a means to a business objective. Therefore, think about the purpose first, then choose the method. Then use it consistently, being aware of its strengths and weaknesses, and being clear of the action that needs to be taken when certain results are achieved. Once the results are obtained, they must be analysed carefully, as the method may be the cause of strange outcomes.

Erik Guldentops, CISA, CISM
is advisor to the IT Governance Institute, professor at the post-graduate Institute of the University of Antwerp and former director of security at SWIFT.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association*, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. Information Systems Control Journal does not attest to the originality of authors' content.

© Copyright 2003 by Information Systems Audit and Control Association Inc., formerly the EDP Auditors Association. All rights reserved. ISCA™ Information Systems Control Association™

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by the Information Systems Audit and Control Association Inc., for a flat fee of US $2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org