Implementation of the COBIT-3 Maturity Model in Royal Philips Electronics

Alfred C.E. van Gils
Philips International BV
Corporate Information Technology
Eindhoven, The Netherlands

Abstract: Philips has an ongoing Business Excellence program for all business functions, including IT. As part of this program the COBIT standard from the IT Governance Institute™ is used to do maturity (self) assessments on IT processes. The program is implemented worldwide using 10 steps including, a workshop approach, improvement management, relation to the internal control framework, organisation and communication.

Key words: IT governance, audit, COBIT, ISACA, internal control, maturity

1. ROYAL PHILIPS ELECTRONICS

Royal Philips Electronics is a global electronics company established in 1891. Headquartered in Amsterdam, The Netherlands, it has a multinational workforce of more than 225,000 and offers sales and services in 150 countries. Listed on the New York, London, Amsterdam and other stock exchanges, Philips had net income in 1999 of Euro 1.8 billion (US $1.9 billion). Divisions of Philips include Consumer Electronics, Lighting, Semiconductors, Medical Systems, Domestic Appliances & Personal Care and Components.

M. Gertz et al. (eds.), *Integrity, Internal Control and Security in Information Systems*

2. COBIT CONTROL OBJECTIVES FOR INFORMATION TECHNOLOGY

Control Objectives for Information Technology (COBIT), was originally an audit framework. It is now a comprehensive IT Governance framework, organised around 34 high-level processes and control objectives. COBIT is released by the COBIT Steering Committee and the IT Governance Institute™

COBIT recognises the following processes:

Planning and Organisation
PO1 Define a Strategic IT Plan
PO2 Define the Information Architecture
PO3 Determine Technological Direction
PO4 Define the IT Organisation and Relationships
PO5 Manage the IT Investment
PO6 Communicate Management Aims and Direction
PO7 Manage Human Resources
PO8 Ensure Compliance with External Requirements
PO9 Assess Risks
PO10 Manage Projects
PO11 Manage Quality

Acquisition and Implementation
AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI3 Acquire and Maintain Technology Infrastructure
AI4 Develop and Maintain Procedures
AI5 Install and Accredit Systems
AI6 Manage Changes

Delivery and Support
DS1 Define and Manage Service Levels
DS2 Manage Third-Party Services
DS3 Manage Performance and Capacity
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS6 Identify and Allocate Costs
DS7 Educate and Train Users
DS8 Assist and Advise Customers
DS9 Manage the Configuration

DS10 Manage Problems and Incidents
DS11 Manage Data
DS12 Manage Facilities
DS13 Manage Operations

Monitoring
M1 Monitor the Processes
M2 Assess Internal Control Adequacy
M3 Obtain Independent Assurance
M4 Provide for Independent Audit

For each of the 34 processes, COBIT specifies:
- Detailed control objectives (318 in total)
- Key goal indicators
- Key performance indicators
- Critical success factors
- Maturity models

Key to the implementation was the addition of maturity models in COBIT. The maturity model in COBIT is taken from the Software Engineering Institute's Capability Maturity Model (CMM) for Software Engineering [Pauli, M.C., Curtis, B., Chrissis, M.B. and Weber, C.V, 1993]. CMM defines the following maturity stages:

1) **Initial** The software process is characterized as ad hoc, and occasionally even chaotic. Few processes are defined, and success depends on individual effort.
2) **Repeatable** Basic project management processes are established to track cost, schedule, and functionality. The necessary process discipline is in place to repeat earlier successes on projects with similar applications.
3) **Defined.** The software process for both management and engineering activities is documented, standardized, and integrated into a standard software process for the organization. All projects use an approved, tailored version of the organization's standard software process for developing and maintaining software.
4) **Managed.** Detailed measures of the software process and product quality are collected. Both the software process and products are quantitatively understood and controlled.
5) **Optimizing.** Continuous process improvement is enabled by quantitative feedback from the process and from piloting innovative ideas and technologies.

It is not the intention of this article to give a full description on COBIT. Detailed information can be found on http://www.isaca.org.

3. COBIT IN PHILIPS

The Internal Audit department within Philips has a long-standing tradition of using COBIT and encouraging CISA® (Certified Information Systems Auditor™) certification for IT audit staff.

In addition to its extensive Internal Audit implementations, the Corporate IT Department of Philips International used the COBIT framework when participating in two company-wide initiatives. Support at Supervisory Board level was achieved by linking with the following executive programs:

1. **The BEST (Business Excellence through Speed and Teamwork) quality improvement program.**

This program has strong, visible support from senior management and is one of the five top items on the Management Agenda. As part of this program, Philips uses Balanced Scorecards and "Process Survey Tools" to measure the relative maturity of business processes within organizations. Process Survey Tools now exist for key business processes:

- Supply Chain Management
- Manufacturing Maintenance
- Manufacturing Operations
- Purchasing
- Demand Generation
- Innovate to Market

And also for some functional areas:

- Finance and Accounting
- Human Resource Management
- Information Technology

The Process Survey Tool for IT is based on the COBIT 3rd Edition. The maturity definitions from the COBIT Management Guidelines were copied and published in the format of a Process Survey Tool with only some minor formatting changes in order to align with other business functions.

2. **The Statement on Business Controls program.**

Each organizational unit within Philips issues a formal annual statement on the quality of internal controls. The process is based on controlled self-

assessment and is subject to validation by internal and external auditors. It is consolidated into the Annual Report's internal control statement and therefore has the full support of senior management. As part of this process, organizations are also asked to complete a section on IT. The IT section of the Statement on Business Controls is also based on the COBIT control objectives. In fact, completing a COBIT maturity assessment is considered sufficient basis for submitting an IT internal control statement provided that:

- The self-assessment scores are based upon sufficient supporting evidence.
- A proper action plan addresses shortcomings on all material processes scoring in or below the "Initial/Ad Hoc" range of maturity. This means that if the process performs ad hoc it is regarded as insufficient from an internal control point of view.

4. IMPLEMENTATION

The BEST program's Process Survey Tool for IT was initiated in 1999 and developed during the second and third quarters of 2000. At the beginning of the project, only the second edition of COBIT was available which did not yet include maturity models. The COBIT framework was used for the pilots, but the general ISO15504 standard (which also includes a similar maturity model), was used for establishing maturity levels.

Key to the implementation of COBIT is a workshop approach, based on self-assessments.

- The course of assessing 34 processes takes one to one and a half days;
- The process of scoring should preferably be done by a group of 6 to 8 persons;
- The group should consist of IT staff and representatives from the user community (depending on the user organisation key users, F&A representatives);
- The actual scoring should cover the following items:
  - Introduction and training into COBIT and maturity levels;
  - Scope definition (decide what to score and what not to score);
  - Scoring per process based on a self-assessment, i.e. individual scoring, discussion and consensus building;
  - Defining improvement actions and levels for the next year.
- The use of a facilitator for the process is recommended

After undergoing testing in 10 pilot workshops, the Process Survey Tool was released with two implementation paths:

- Per Product Division, where one contact person per division and/or business group was responsible for rollout
- Per region (i.e. Asia Pacific, East and West Europe, Latin America and North America), where rollout was facilitated per country

In July 2000, the 3rd edition of COBIT, which now included a fully worked out maturity model per process, was released. COBIT 3rd edition is a significant improvement.

Elements for implementing COBIT based Maturity Self Assessments

A comprehensive implementation of COBIT addresses the following 10 elements, not all of which have currently reached completion. In addition, many of the specific details are left to the discretion of different divisions, business groups and countries.

1. Process for Initial Assessments
2. Process for Re-Assessments
3. Relation to Balanced Scorecards
4. Relation to SBC and Internal Control Framework
5. Communication of Action Plans
6. Consolidation of scores
7. Exchange of Best Practices
8. Process for calibration of scores
9. Scoring Directives and Guidance of Improvement Actions
10. Organisation and communication

4.1 Process for Initial Assessments

The process for doing maturity self-assessments is built upon the following elements:

- The process uses a facilitated self-assessment workshop based on COBIT 3rd edition maturity models
- The total duration is 1 - 1,5 days including introduction, training and definition of improvement actions.
- The optimal group size is 6-8 people, including one or two representatives from the user community.
- The scoring is based on consensus discussions
- A presentation and reporting standard

During the initial assessment, the definition of a set of good improvement actions is key for continuation of the program the next year. After the first

assessment round, participants are asked to select a limited number (3-5) from the 34 COBIT processes, where improvements should be focussed on the next year. The consolidated votes of the group are used to focus on a limited number of tangible improvement actions up to the next assessment round.

Improvements should balance the materiality, customer impact, cost and maturity score of a particular process. Consequently, the improvement program does not automatically have to address the lowest scoring processes in the first place. It may be more important to achieve a very high maturity score on a critical process ("Ensure Systems Security"). That however depends on the type of business, information and environment.

As a rule, processes scoring in the "Initial/Ad Hoc" range of maturity or lower, are also recommended for improvement.

4.2 Process for Re-Assessments

As a first step, an organisation needs to define the length of time to the next assessment. Experience with re-assessments in Philips is still limited and tends to use the following agenda:

- A 2-3 hour session
- The period is set to a maximum of +1 year from the initial assessment
- Setting of agreed actions and other improvements during the period
- Definition and assessment of new scores for applicable processes
- Definition of new improvement actions, scores and re-assessment period

4.3 Relation to Balanced Scorecards

The use of Balanced Score Cards for IT (BSC-IT) is starting to develop. Whenever a BSC-IT is in use, an organisation also needs to address how to include the COBIT based maturity assessments in the processes part of the scorecard. An organisation then needs to address how to include maturity targets in the BSC-IT. Examples are:

- The PST-IT done/re-assessed
- A PST action plan available
- The PST score on average X, or PST score 80% higher than Y and no score lower than Z

The relation between a maturity assessment and the BSC-IT can be directed towards a certain scoring target, or non-directive, i.e. checking whether or not the assessment took place and is properly followed-up.

4.4 Relation to the Internal Control Framework

Any implementation of COBIT should also address the relation to the organisation's formal internal control framework and auditors.

In consultation with the external auditors it was concluded that conducting a COBIT based maturity assessment is sufficient basis for submitting a control self-assessment statement to the external auditor, provided there is sufficient evidence in support of the scores.

From an internal control point of view, processes scoring in the "Initial/Ad Hoc" range of maturity or lower are not acceptable and should be addressed by (at least) defining proper follow up actions.

4.5 Communication of Action Plans

Another item in the implementation of COBIT based maturity assessments, is whether or not action plans resulting from assessments need to be communicated. If so an agreed format and communication tool has to be established.

Are action plans subsequently evaluated on their content if they exist? In practice the following variations can be found in different divisions, business groups and countries:

- Action plans are not communicated at all;
- There is a registration if an action plan has been established;
- Action plans are consolidated into an overall action plan and the content is known to all concerned.

If, as in the latter case, the content of action plans is also part of the organisation's implementation plan for COBIT, the logical consequence is to use assessment results to identify areas for improvement and guide improvement programs.

4.6 Consolidation of scores

A related issue is whether or not scores should be communicated and consolidated.

If an organisation decides to consolidate scores from self-assessments, a supporting process needs to be developed with proper tooling. Experience shows that consolidation of scores can be of some value in the sense that:

- It provides a benchmark for organisations against which scores can be evaluated, not in a precise statistical sense but more in support of a general outlook of being "in-line" within a business community.
- Consolidation of scores provides a benchmark in order to track, identify and benchmark changes over time.
- A database of scores is an efficient way of not only identifying "best practices", but also problem areas where scores drop in or below an "Initial/Ad Hoc" level of maturity.

Consolidation of scores just by the figures has some limitations and drawbacks. The scope of the assessment needs to be taken into consideration when comparing scores. An assessment may have taken a very limited scope, say SAP R/3 Managed Operations, making it very difficult to compare it with a full scope assessment including legacy systems and office support.

4.7 Exchange of Best Practices

Implementing COBIT-based maturity assessments may lead to the identification of "Best Practices" in an organisation. Firstly, there needs to be at least some way of communicating scores. Then a definition of which processes qualify as a Best Practice is needed to determine whether this is the highest score available or the score above a certain value

Best practices have been identified within Philips, for almost all 34 COBIT processes based on a rule of thumb that, a score should be at least "Managed and Measurable", with some scores reaching "Optimised" levels of performance.

Following the identification of Best Practices the process for exchanging information can be addressed by means of meetings, presentations or the Intranet.

Another important consideration is the validity of scores. So far, there is no process for verification of cases that have been submitted as a Best Practice in Philips and the information is taken at face value. In a more advanced stage of implementation, audits or peer-audits may become useful tools in the actual verification and validation of best practices within an organization.

4.8 Process for calibration of scores

Since the resulting scores are based on self-assessments, a process needs to be in place to address the issue of calibrating scores, in order to ensure that assessment results present a true and fair view of the actual maturity levels.

Comparable processes within CMM [Pauli, M.C. et. al. 1993] are highly evolved into an extensive set of assessor training, curricula and audit programs, the results of which may even be published [Mark C. Paulk 2000].

Maturity definitions for COBIT processes are relatively new (July 2000) and supporting processes and applications are still far from the level of institutionalisation that has been achieved in CMM.

In practice, results from self-assessments are taken at face value. Still, there are some considerations that may result in more reliable scores:

- The first control is the assessor group composition. The recommendation is to have a balanced group comprising of IT, as well as user representatives. Involving different stakeholders in a group, results in a more balanced and reliable scoring process.
- A second control is to have a facilitator, who has experienced more than one assessment.
- A final control is to implement an audit or peer-audit process on the actual scores. Results are subject to audit as they are part of the Philips Internal Control Framework. Assessments that were combined with audits show that the assessment results did in fact provide a fair and true view, although based on a limited experience. There are some organisations that include peer-auditors in the re-assessment exercises.

4.9 Scoring Directives and Guidance of Improvement Actions

The scoring directive is optional and may be linked into the BSC-IT. It can use a very fixed format (e.g. all scores at least on a "Defined Level" of maturity) or a more open format (80% of scores at least on a "Defined Level").

Philips organisations use many different formats, from no directive at all to a very fixed quantitative target.

As stated earlier, any scoring directive should balance the materiality, customer impact, cost and maturity score of an IT process in a particular business operation.

The question then becomes, whether improvement efforts can focus beyond the level of independent self-assessments to broader improvement efforts. Typical examples in this area are ISO and ITIL implementation projects, which focus on a broad scope of IT and COBIT processes for improvement. If carried out properly, they can leverage the performance of IT processes to defined and higher levels of maturity in a single integrated effort.

4.10 Organization and communication

The final and most important implementation point is to define and set up a proper structure for communication and organization.

The introduction of COBIT Maturity Assessments in Philips is linked to a highly visible Business Excellence Program with the full support of senior managment. This has been a critical factor in the successful implementation.

Next has been the selection and development of an adequate tool for maturity self-assessment. This was done in a joint effort including representatives from Philips divisions and results were based on 10 pilot assessments.

The roll out was done per division as primary business drivers. In addition the program was also introduced worldwide as part of regional IT meetings. In some cases a facilitator provided guidance in order for participants to conduct their own workshops.

Communication and organisation is embedded in each division and business unit with varying degrees of formality and institutionalisation. In addition there are regional programs where synergy requires a concerted effort.

5. CONCLUSION

Using COBIT to establish organizational capabilities on a maturity level, gives a clear indication of where improvement is possible and how to achieve it.

The experience in Philips includes more than 100 assessments worldwide, in a mixture of organizations and cultures.

One feature of COBIT is that it is flexible and allows users to customise applications. Philips developed its approach based on internal group workshops including presentations, training and scoring material.

COBIT has a number of outstanding benefits, in particular:

- It is an open standard;
- The documentation is clear and understandable;
- The professional organization; the IT Governance Institute™ is leading the development of COBIT by using a broad range of international references (e.g. ISO standards);
- COBIT is part of a larger program; it is kept up to date, more detailed information is available, plus there are translations, training programs and the related CISA certification;
- COBIT version 3 brings together three extremely rich methodologies in one framework, namely:
  1. The 34 COBIT processes, along with key performance indicators, key goal indicators, critical success factors and control objectives;
  2. The Business Balanced Scorecard for IT and
  3. The maturity model derived from the Capability Maturity Model for Software Engineering.

In addition, generally applied frameworks for auditing such as COSO, Control Self Assessment and quality frameworks based on ISO are well integrated in the COBIT methodology.

Some other points with respect to using COBIT for maturity assessments are:

- The language used in COBIT assumes a certain background, affinity and fluency which is not available in all (IT) groups. COBIT has a strong focus on internal control and may not be perceived as self-explanatory as is required for doing self-assessments. It may be required to establish COBIT "champions" and/or training programs to increase the level of familiarisation.

- Implementing COBIT needs to explicitly address application context. It is important to do a scope definition (what applications, processes, functions and business processes will be assessed). The maturity model also assumes a certain size of IT operations and typically only applies to operations of a certain critical mass.
- Finally, there are huge cultural differences in self-assessment scoring. Without being specific, some cultures take written documentation as law while others have a much more pragmatic and lenient attitude towards COBIT. There is also cultural diversity in the degree of openness in group sessions and affects of the particularities of group composition. There is no simple answer to any of these contextual factors.

The Philips rollout per product division and region is ongoing, and concrete activities include providing ongoing support for COBIT 3rd Edition-based assessment workshops

The rollout itself will focus on institutionalising and grounding the ten steps into the organisation.

After the rollout, Philips will focus on:

- Assessing actual outcomes of the process (based on key goal indicators and maturity levels);
- Identifying problem areas (for IT processes with low maturity scores);
- Defining best practices ('defined process' maturity level and higher);
- Improving management processes and actions;
- Benchmarking score.

6. REFERENCES

Information Systems Audit and Control Association & IT Governance Institute. **COBIT. Control Objectives for Information Technology.** 3rd Edition. Rolling Meadows, IL. ISBN 1-893209-13-X. http://www.isaca.org/

Kaplan, R. S., and Norton, D. **The Balanced Scorecard: Measures that Drive Performance.** Harvard Business Review 70, no. 1 (January-February 1992): 71-79.

Mark C. Paulk, Dennis Goldenson, and David M. White, "**The 1999 Survey of High Maturity Organizations,**" Software Engineering Institute, Carnegie Mellon University, CMU/SEI-2000-SR-002, February 2000.

National Commission on Fraudulent Financial Reporting; COSO Treadway Commission. **Report of the National Commission on Fraudulent Financial Reporting.** COSO, October 1987. http://www.coso.org/.

Pauli, M.C., Curtis, B., Chrissis, M.B. and Weber, C.V. **Capability Maturity Model for Software, Version 1.1.** Technical Report, CMU/SEI-93-TR-024 ESC-TR-93-177 February 1993. http://www.sei.cmu.edu/cmm/