

# Auditing CMMI<sup>®</sup> Maturity and Sarbanes-Oxley Compliance

By Laurent Janssens, CISA, and Peter Leeson

With the dawn of the 21<sup>st</sup> century, a new era of corporate governance began—following the Enron and WorldCom scandals—focusing on accountability, responsibility, transparency and behaviour. The US Sarbanes-Oxley Act was created with the intent to certify that the financial statements are reliable by placing increased personal responsibility on management and ensuring that their behaviour matches the responsibilities they have accepted. As information technology (IT) supports the business processes, IT is, once again,<sup>1</sup> a major player for the survival of the organisation. IT management processes, through IT general controls (ITGC), must provide reasonable assurance that undesired events will be prevented or detected.

This article first explains at a high level how Sarbanes-Oxley was satisfied at one company. Then, it describes how a Capability Maturity Model Integration (CMMI)-based process improvement (PI) programme facilitates a Sarbanes-Oxley project and reduces its cost. It also reviews how the Sarbanes-Oxley project had positive impacts on the PI programme.

Many of the experiences in this article are based on the implementation of CMMI and Sarbanes-Oxley within the framework of a Belgian subsidiary of one of the largest European financial institutions. This financial institution is described in this article as Company X. Company X had to overcome the fact that the company was split into several sites with different languages, and people who joined the company through a succession of mergers had different priorities and different businesses (including banking and insurance). The requirement<sup>2</sup> for compliance with Sarbanes-Oxley and CMMI focused the improvement effort and allowed a better collaboration and understanding among these different units. However, before this could be accomplished, a serious effort was required to overcome the ‘not invented here’ feeling.<sup>3</sup>

## Sarbanes-Oxley Steps

The IT development department of Company X used a five-step approach for its Sarbanes-Oxley project (see **figure 1**).

1. The risk identification exercise was based on COBIT V3.2, the international framework published by the IT Governance

Institute (ITGI). This control and risk framework was used to help the Sarbanes-Oxley team members fill in a matrix of control activities to mitigate the risks. Early in the risk management exercise, the results were challenged by external auditors.

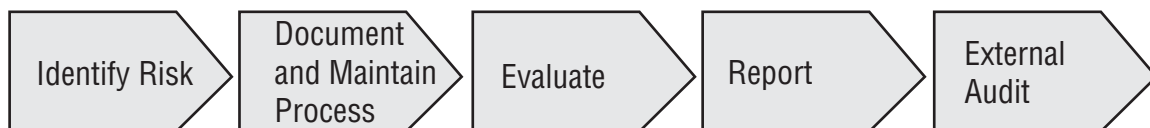
2. Based on this control matrix, a number of controls were identified as key. The key controls were clustered in management processes, and a process owner was assigned accordingly. The process owner then provided a complete description<sup>4</sup> of the control.
3. After communication of the key controls to all operational teams, their efficiency is assessed by quality assurance (QA)<sup>5</sup> through walk-throughs or compliance testing.
4. QA communicated the results of the tests to senior management; gaps were identified and remediation plans were defined and followed, with the right priority.
5. External auditors assessed the effectiveness of the controls.

This approach in five steps is iterative. The identified gaps during the evaluation process could lead to a redesign of the Sarbanes-Oxley documentation; should this be the case, the company needs to keep track of the various versions of the control description—including their validity dates—as this is important information for external auditors.

## How CMMI Helps Sarbanes-Oxley

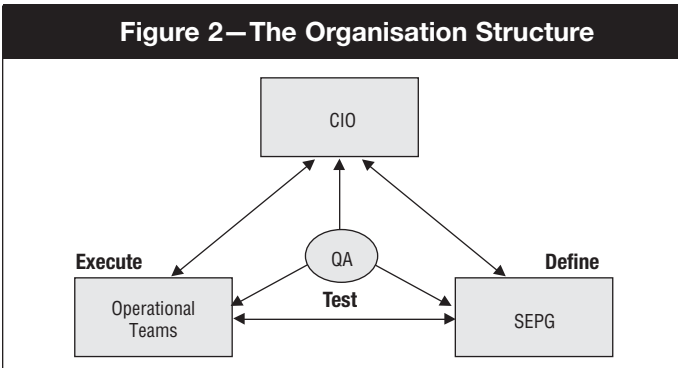
The IT development department of Company X is running a CMMI-based PI programme to improve the quality of its development. In November 2005, the company was independently appraised at CMMI maturity level 2 by a Software Engineering Institute (SEI) authorized lead appraiser. This means that project management and control processes are systematically implemented and respected throughout the IT development organisation.<sup>6</sup> Additionally, CMMI-compliant processes allowed a stabilization of customer requirements throughout the development cycle. Altran CIS,<sup>7</sup> located in Brussels, participated in both programmes. Q:PIT Ltd.,<sup>8</sup> a UK-based SEI partner, facilitated the change process.

Figure 1—Sarbanes-Oxley Steps



**The Organisation Structure**

One of the first steps of the PI programme in Company X was to define a structure with three independent departments, reporting directly to the chief information officer (CIO)<sup>9</sup> (see figure 2):



- The Software Engineering Process Group (SEPG) is responsible for the coherence of processes and their alignment with business goals and stakeholders’ needs. SEPG participates to the definition of pragmatic processes based on field experience.
- Operational teams apply the processes and the controls, and they highlight improvement opportunities based on field experiences.
- QA provides to management, operational teams and the SEPG an independent insight into the effectiveness and efficiency of the processes being used.

Through this structure, roles and responsibilities are clearly defined. The Sarbanes-Oxley controls are embedded in the IT development management processes, and their coherence is ensured in all supporting documents (process description, trainings, etc.) as part of quality checks of any process improvement initiative. Moreover, Sarbanes-Oxley testing is conducted in a professional way by QA team members as part of their ‘business as usual’ activities.

This all implies that the cost of maintenance and deployment of the Sarbanes-Oxley controls are largely part of the PI programme and that those controls are mainly institutionalized without significant additional effort.

**IT Senior Management Commitment**

Thanks to the generic practices of CMMI and the level 2 rating, the added value of improvement was really perceived: major stakeholders in the organisation, including IT senior management, were committed to providing direction through policies stating the need for the improvements and control; defining processes that support the business objectives and the corresponding embedded controls; and reviewing and discussing the way processes and controls are applied.

Due to the generic practices required by CMMI for a maturity level 2 rating, the added value of the improvement was perceived by the major stakeholders of the organisation. Policies were established by IT senior management to provide direction, state the need for improvement, and control and define how the processes are to support the business objectives. The application of the necessary corresponding embedded controls and reviews was also identified.

By clearly establishing the support of management and stakeholders in the PI programme and considering Sarbanes-Oxley as a change request—albeit an important one—for the ongoing programme, the cultural changes<sup>10</sup> required on a short delay by Sarbanes-Oxley were implemented quite smoothly. As with dynamics, it is easier to move a body that is in motion than one that is at rest, as higher energy levels are needed to compensate for the inertia. That energy had already been used to get PI started.

It is also interesting to notice that by defining the organisational structure and obtaining the commitment of IT senior management, the control environment is partly present; most of the pervasive controls—controls designed to manage and monitor the IS environment<sup>11</sup> (also called IT entity controls)—are operating efficiently thanks to CMMI.

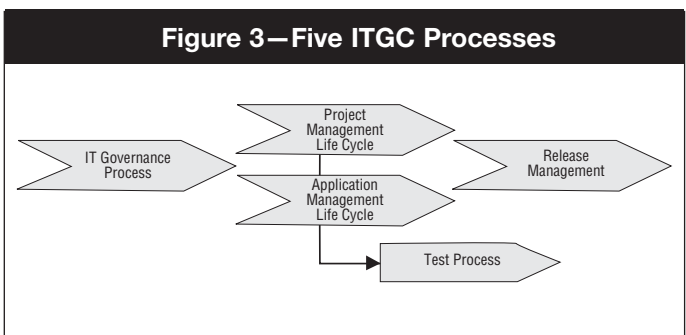
**Control Definition and Execution**

COBIT, developed by the IT Governance Institute, identifies 34 high-level control objectives, divided into four domains: Plan and Organise (PO), Acquire and Implement (AI), Deliver and Support (DS), and Monitor and Evaluate (ME).

For Company X’s IT department, the most important COBIT control objectives applied were identified as those in the PO and AI domains. These are largely covered by CMMI practice areas. As IT management processes based on CMMI practice areas are established, they are referenced in the control activities matrix and serve as an important basis for the exhaustive Sarbanes-Oxley control documentation.

Although the IT management processes are fully documented and available for the whole development community, process owners had to revise process documentation (with the description of the control) to satisfy Sarbanes-Oxley; these processes had to be detailed enough to ensure that they were understood, accepted and applied by operational teams. Auditors (internal and external) had other requirements for the process documentation, mainly for highlighting the key controls. This could imply an additional cost maintaining two sets of documentation, with a risk of bidirectional incoherence. By combining them, the specific CMMI and Sarbanes-Oxley requirements could become fully integrated into the internal processes and activities.<sup>12</sup>

The main objective of the Sarbanes-Oxley IT general control ‘Development and Maintenance’ at Company X is to ensure that every item put in production is under control. Based on the risk assessment, the IT development department of Company X defined 23 key controls in five processes, as shown in figure 3.



These 23 controls are common sense; there is no added complexity, just enforced management processes.

Each of these Sarbanes-Oxley controls is linked to a phase of the software development life cycle (SDLC). These controls are embedded in the milestone review checklists and, as with any other major issue in the project or application, as long as the expected result of this control is not achieved, the next phase of the project may not be started. CMMI states that the conduct of milestone reviews is part of monitoring activities and under the responsibility of the project manager. This milestone review process was institutionalised, demonstrating yet another link showing how CMMI and Sarbanes-Oxley are interrelated.

### **Sarbanes-Oxley Testing**

Sarbanes Oxley section 404 states that the organisation must provide a report on the assessment of controls over financial reporting. This implies that the controls should be evaluated independently. This was seen to be largely covered through the implementation of ongoing and continuous ‘objective evaluation’ of adherence to the processes, plans and standards by an authority that is identified within the CMMI as responsible for ‘process and product quality assurance’. As shown in the organisation structure (see **figure 2**), QA team members are ideally placed to assess the Sarbanes-Oxley controls with regard to efficient operation. Once the QA training has been adapted to include formal gathering of evidence and the job assignments have been modified, QA performs Sarbanes-Oxley testing in a business-as-usual mode.

Therefore, the overhead cost of Sarbanes-Oxley testing is kept low. However, the more challenging point is to avoid conflict situation in this QA role. On one side, QA is an improvement change facilitator, helping the teams to reach the expected maturity in the defined processes; on the other side, as a Sarbanes-Oxley tester, QA has the mandate to escalate Sarbanes-Oxley issues to senior IT management for direct action, which may lead to stopping the project until issues are addressed (the decision to stop or to accept the risk resides directly with the senior management concerned).

The change agent and the Sarbanes-Oxley compliance auditor roles are somewhat difficult to combine. However, it is understood that by assisting in planning and defining the controls, processes and activities for the project, using the latest improvements, QA has additional possibilities in helping understand why this is important and why it needs to be escalated accordingly. An intensive focus on communication and support aims to ensure that the potentially negative perception of QA by the operational teams is being addressed.

### **Positive Impacts of Sarbanes-Oxley**

Implementing a CMMI-based process improvement effort is a serious challenge, even with the full support of top management. It is not easy to implement the discipline required by the project team members to switch from a culture in which they do what appears to be correct based on today’s pressures and priorities, to a culture in which they understand, plan, document and monitor their activities, even under pressure. The requirement to comply with Sarbanes-Oxley is a

great motivator to respect the process, even in the event of an emergency.

To stabilize the requirements of a project, CMMI states that it is important to obtain commitment to the plans from stakeholders. For cultural/historical reasons, this was sometimes overlooked in Company X, with (negative) consequences as the project progressed.

Eight of the 23 Sarbanes-Oxley-defined ITGCs are related to obtaining formal approvals of stakeholders during the different phases of the project. Thanks to Sarbanes-Oxley, an important communication effort was accomplished with the business partners, making them aware that a formal sign-off is more than bureaucracy and that Sarbanes-Oxley control failure in these cases is not just the responsibility of IT.

Finally, three of the 23 Sarbanes-Oxley key controls are linked to governance practices, enforcing the management awareness of the importance of maintaining a business case.

### **Ongoing Challenges**

The following section identifies some of the challenges that are in the process of being managed or resolved at Company X. There are limitations in the way things have been implemented.

A CMMI maturity level 2 organisation focuses on project management activities, more specifically within the context of software and system engineering, and the stabilisation of the requirements and other practices. The idea behind maturity level 2 is to encourage projects and teams to deliver, in their own way and according to their own approaches, the results needed to deliver the products and the corresponding measurements and reports. Projects are not required to follow a standard approach; on the contrary, teams are encouraged to accomplish them in their own way—as long as they respect the needs and requirements laid out in organisational policy documents. Through this approach, a comparison can be made to determine what works best for the environment, customers, technology, people, etc.

Naturally, the QA team, which needs to ‘test the controls’, would have an easier job finding the appropriate artifacts and evidence required if everyone did things the same way. The sharing and standardisation of identified and measured best practices is the focus of CMMI maturity level 3 (which Company X hopes to achieve by 2008<sup>13</sup>) and should further reduce the cost of Sarbanes-Oxley compliance.

Sarbanes-Oxley testing seeks to ensure that controls are operating efficiently. For example, the Act ensures that the test plan is signed off by the right business representative, but does not guarantee the quality of this test plan in terms of effectiveness, completeness, etc. Sarbanes-Oxley is there to limit the risks but not to improve the quality of the process or the product. That is the main difference with a PI programme, where quality should be embedded not only in a way of working but also as a kind of philosophy: one does not produce quality because one is told to, but because the culture encourages one to think of placing quality first. However, Sarbanes-Oxley compliance is accomplished because it is required!

CMMI does not offer formal certification (such as the certification for ISO 9000). While a CMMI appraisal's 'validity' is limited to three years, there is no requirement to perform a new appraisal or to maintain the results achieved previously. The model is there to support ongoing, continuous improvement, not as a guarantee of levels of quality. Sarbanes-Oxley, on the other hand, requires that audits be performed on a yearly basis, and the level of quality achieved is a continuous requirement to be respected at all times, even the week after the audit and even during the holidays. Organisations must remain Sarbanes-Oxley-compliant from the first of January until the end of December.

For its improvement programme, Company X defined a road map laying out in time the different initiatives by focusing on the benefits to be achieved. This includes a number of improvements related to the business needs and priorities, focusing first on known areas of 'lesser strength', then on overall consistency in the processes, then collaboration and communication between teams (internal and external), and finally on known weaknesses<sup>14</sup> and continuous improvement.

These successive improvements and changes can seriously impact the results of the Sarbanes-Oxley compliance and corresponding controls. As a consequence, each new or improved process needs to go through a double Sarbanes-Oxley control. When the PI staff members wish to start up a PI project, a first review is performed by the Sarbanes-Oxley compliancy specialist. This specialist reviews the PI project's summary and determines whether there is no impact, a potential impact, a known large impact or a known small impact. The following are the decisions that can be made:

- This probably has no impact; go ahead with the change without Sarbanes-Oxley expertise.
- This may have an impact and any products, processes and templates should be reviewed and approved before they are put into production.
- This probably has an impact and the Sarbanes-Oxley compliance specialist should directly participate on the team that is researching and documenting the change.

Even if the Sarbanes-Oxley compliance specialist decides not to participate in the approach, all staff members have been trained on the importance and principles of Sarbanes-Oxley and will be on the lookout for the any potential risks, which are then identified and reported for review.

## Conclusions

Following the first year that Company X was required to undergo the complete Sarbanes-Oxley exercise, the results of the first audit were encouraging. The understanding that has been provided by the PI programme has allowed determining the need for improvement and planning the path for the improvement in all aspects of the development and management processes. The sharing of practices and lessons learned throughout the organisation has enabled the company to significantly decrease the cost of the activities, increase productivity and reduce the time wasted. In the same manner, the cost of Sarbanes-Oxley compliance has also been significantly reduced through the systematic implementation of processes and related controls.

The Sarbanes-Oxley Act is now a fact of life that cannot be avoided. IT is one of the areas most impacted due to the cross-organisational nature of its activities. However, this is probably not the end of the story. A number of questions remain open: Does Sarbanes-Oxley manage what is arguably the biggest risk toward recreating the Enron-style scandal it was created to avoid? Are the Sarbanes-Oxley gaps identified within what IT considers 'material weaknesses'? The future will probably reveal the answers; however, history indicates that the biggest frauds happen at the board level.

It is not yet clear whether the Sarbanes-Oxley Act will really avoid this. What is known is that the implementation of best practices for project management and engineering does facilitate the implementation of legal controls and constraints of this type. The authors believe that if CMMI helped improve the processes and controls on a day-to-day basis, which in turn facilitated the compliance of these new constraints, it would probably work again should they change the rules in the future.

## References

- Balty, Yves; European SEPG presentation: Surfing the SOX Wave Thanks to CMMI, 2006, [www.espi.org](http://www.espi.org)
- IT Governance Institute, *Control Objectives for Information and related Technologies (COBIT)*, 1998-2007, [www.itgi.org](http://www.itgi.org)
- SEI and Carnegie Mellon University, CMMI, [www.sei.cmu.edu/CMMI](http://www.sei.cmu.edu/CMMI)
- IT Governance Institute, *IT Control Objectives for Sarbanes-Oxley*, 2004, [www.isaca.org/sox](http://www.isaca.org/sox)
- Leeson, Peter; 'CMMI, SOX & COBIT', 2006, [www.qpit.ltd.uk/LinkedDocuments/CMMI-SOX-COBIT 40.pdf](http://www.qpit.ltd.uk/LinkedDocuments/CMMI-SOX-COBIT%2040.pdf)
- Steward, Thomas A.; 'Fair Business Is as Fair Business Does', *Harvard Business Review*, October 2006, p. 14

## Endnotes

- <sup>1</sup> As it was previously with the e-commerce revolution, the introduction of the Euro, the year 2000 and others in the past few years
- <sup>2</sup> Sarbanes-Oxley is a legal requirement. CMMI was an internal requirement from the head office.
- <sup>3</sup> Personal experience shows that this attitude is very common, particularly in multinational environments, where there is frequently a feeling that anything coming from the mother company is wrong, before it is analysed or considered; it may be grudgingly accepted later.
- <sup>4</sup> Who performs the control, frequency of the control, etc.
- <sup>5</sup> QA in this context is taken in the CMMI sense of the word: assuring proactively the quality of the products and services delivered to the customer by ensuring that the right processes, practices, standards and controls are implemented and performed from the start. This is more than just reviewing or testing the products after the fact.
- <sup>6</sup> An interesting byproduct of the PI programme was the reduced learning curve required by the project managers to complete their PMP certification.
- <sup>7</sup> [www.Altran.com](http://www.Altran.com)
- <sup>8</sup> [www.qpit.ltd.uk](http://www.qpit.ltd.uk)

<sup>9</sup> The CIO is responsible for setting the policies that determine the organisational objectives and strategies. These are then used to prioritise projects (including change management) and guide the controls and activities throughout the organisation.

<sup>10</sup> Sarbanes-Oxley demands that people take personal responsibility for the quality of their own work, by understanding the impact and commitment that are linked to their role. This is directly reflected in the high-level punishments that could be related to a lack of respect of the controls in place. Many organisations, including the one the authors were working with (at the beginning), seem to be largely composed of people who are ‘only doing their job’ and are willing to sign off on documents if someone else signed off previously. Blame is frequently more common than responsibility.

<sup>11</sup> This definition is extracted from the glossary at [www.isaca.org](http://www.isaca.org).

<sup>12</sup> Nevertheless, external auditors require an executive summary; hence the process needs to be defined with different ‘layers’.

<sup>13</sup> The time to move up another level is longer than in most organisations mainly because of the size of the IT department and the variance between the staffing. This company has grown largely through acquisitions and mergers, combining a number of different cultures, products, legacy systems and locations and working on a daily basis in three languages.

<sup>14</sup> This sequence may appear surprising. In fact, the areas of ‘lesser strength’ are those that were identified as generally good, with the right approach in place; however, it was not being performed consistently. These are areas where improvements can be rapidly implemented, correcting minor deviations from the desired approach and rapidly gaining the benefits of the improvement. The weaknesses were areas in which new approaches needed to be researched, analysed, defined, trained, etc.; these were placed at the second level so as not to lose the improvement momentum, but take the time to properly plan and staff these more complex approaches.

<sup>15</sup> CIS stands for Consulting and Information Service

### **Laurent Janssens, CISA**

is a senior consultant at Altran CIS<sup>15</sup> in Belgium, where he leads the IT governance practice. He has 12 years of experience in the IT management and IT audit world. Among his experience, Laurent co-ordinated all Sarbanes-Oxley testing-related matters at the IT department of a leading financial organisation. He can be reached at [ljanssens@altran-cis.be](mailto:ljanssens@altran-cis.be).

### **Peter Leeson**

is a CMMI Appraiser and an instructor and visiting scientist with the Software Engineering Institute (Carnegie Mellon University, Pittsburgh, Pennsylvania, USA). He assisted with the implementation of CMMI-compliant processes that satisfy and facilitate the business objectives within the organisation being considered. He can be reached at [peter@qpit.ltd.uk](mailto:peter@qpit.ltd.uk).

*Information Systems Control Journal* is published by ISACA. Membership in the association, a voluntary organization serving IT governance professionals, 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 ISACA 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 2007 by ISACA. All rights reserved.

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 ISACA, 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](http://www.isaca.org)