CMMI, SOX & COBIT

1 Overview

This document seeks to identify a number of ways in which a good implementation of CMMI would allow to resolve a number of Sarbannes-Oxley and CobiT requirements. This document does not claim to be exhaustive.

The usage of this document is to allow people who are responsible for defining and deploying process improvement activities to consolidate their work in such a way as to avoid redundant work. The guidance of Sarbannes-Oxley requirements and CobiT auditing recommendations should assist in defining the correct approach for the implementation of CMMI compliant processes.

This document is aimed primarily at CMMI practitioners who are seeking to implement Sarbannes-Oxley and/or CobiT practices. While the document explains some of the context and content of both of these approaches, it is based on the assumption that CMMI is known and does not clarify those practices more than necessary.

2 Context

1.0 CMMI

The CMMI is a process model that aims to offer the best quality of products and services towards the customer and user. By seeking to ensure that processes and controls are in place to identify and remove as rapidly as possible defects, it seeks to increase the level and quality of service provided.

This is a voluntary approach to quality.

1.0.0 Structure

25 process areas that cover the engineering, process management, support and project management activities of an organization.

Each process area as a number of key specific practices and goals related to achieving the results and producing the products as well as generic practices that seek to govern the process itself.

2.0.0 Implementation

The focus of the CMMI implementation is to be the business objectives and understanding the needs of the stakeholders. The CMMI focuses on engineering projects and their reporting structure.

3.0.0 Ratings[1]

The CMMI includes two levels of ratings:

The maturity level is based on the Capability Maturity Model structure and determines a number of process areas that need to be sufficiently implemented

[1] See also **Rating Differences**

, Page 4

in the organization in order to ensure the quality of the products. 5 maturity levels have been defined (1 - Initial, 2 - Managed, 3 - Defined, 4 - Quantitatively Management and 5 - Optimising)

Capability levels are based on the SECM (EIA 731) structure in which each process is rated based on its capability to deliver 6 capability levels have been defined: 0 - incomplete, 1 - performed, 2 - managed, 3 - defined, 4 - quantitatively managed, 5 - optimising.

Each level of rating, in both approaches is based on clearly defined requirements.

2.0 Sarbannes-Oxley

Sarbannes-Oxley is a series of control principles seeks to ensure that financial reporting is correct and understood by the people in charge. The approach seeks to cover and validate the processes and controls that lead to the production of financial statements.

IT is considered key in this element because of the role that played in the production and validation of the data used in the legal reports.

The Sarbannes-Oxley Act came into force in July 2002 and is a compulsory regulation of corporate governance and financial reporting for all US companies

This is a US legal requirement which serves to demonstrate firm resolve by the US Congress to improve corporate responsibility. The focus of this approach is to enforce good governance and ethical business practices.

1.0.0 Structure

A loose requirement for sufficient controls to be in place. These are covered by a number of audit requirements in the form of questions that cover the control environment, the risk assessment, the control activities, the information and communication and the monitoring activities of an organization.

From an IT point of view, Sarbannes-Oxley is interested in the controls that relate to program development, program changes, computer operations, access to programs and data. This is to be considered in relationship to the executive management and the business processes.

2.0.0 Implementation

Sarbannes-Oxley suggests that the focus of the implementation needs to be primarily on the risks and needs of the business. The controls to be put in place should be based on a clear understanding of what is needed, using the Sarbannes-Oxley documentation as a guide, not as an absolute rule. Some additional controls may be required; others may prove to be inefficient in the organizational environment.

> **Carefully consider the appropriate IT control objectives for its own circumstances**

This statement to be found on page 5 of the Sarbannes-Oxley documentation demonstrates the flexibility of the approach. The organization needs to consider what controls are required and how they should be implemented – then ensure that this is done sufficiently to achieve the related objectives.

Section 401

Disclosures in Periodic Reports

Financial statements are published by issuers are required to be accurate and presented in a manner that does not contain incorrect statements or admit to state material information. These financial statements shall also include all material off-balance sheet liabilities, obligations or transactions. The Commission was required to study and report on the extent of off-balance transactions resulting transparent reporting. The Commission is also required to determine whether generally accepted accounting principals or other regulations result in open and meaningful reporting by issuers.

Section 409

Real time issuer disclosures

Issuers are required to disclose to the public, on an urgent basis, information on material changes in their financial condition or operations. These disclosures are to be presented in terms that are easy to understand supported by trend and qualitative information of graphic presentations as appropriate.

3.0.0 Rating

There is no actual rating in Sarbannes-Oxley, this is a pass or fail approach. There is only a high-level recommendation that auditors should evaluate on a regular basis any implications related to potential changes... This should be done according to a recognized auditing standard.

3.0 COBIT

CobiT is a framework that seeks to structure the processes and controls that lead to efficient management of IT governance within an organization. The objective of CobiT is to assist in understanding and managing the links between risks, needs, controls and technical issues that an IT organization face.

The framework includes a number of elements such as a "maturity model" approach and process control and application control points; it also includes a "maturity model" approach by which the capability of each of the 34 processes can be measured.

This is an approach that is voluntarily taken by organizations to assist them in their management and control activities.

1.0.0 Structure

34 generic control objectives organized in 4 domains covering the planning and organization, the acquisition and implementation, the distribution and support, and the control activities.

2.0.0 Implementation

CobiT recommends that the IT skills and priorities be used in determining the most appropriate approach. While the framework gives clear guidance in the approach, the implementation needs to be tailored to the business.

3.0.0 Ratings

CobiT includes a rating system that includes 6 stages of reliability which are defined loosely as 0 - nonexistent, 1 - Initial/Ad hoc, 2 - repeatable but intuitive, 3 - defined process, 4 - managed and measurable, 5 - optimised.

Rating Differences

There are some significant differences between the two rating systems:

Level	CobiT	CMMI
0	Non-Existent "Complete lack of any recognizable process. The enterprise has not even recognised that there is an issue to be addressed"	Incomplete "...a process that is either not performed or partially performed. One or port of the specific goals (...) are not satisfied"
1	Initial "There is evidence that the enterprise has recognised the issues exist (...). There are no standardised processes; instead there are ad hoc approaches (...). The overall approach to management is disorganised"	Performed "A performed process is a process that satisfies the specific goals (...). It supports and enables the work needed to produce work products.
2	Repeatable "(...) similar procedures are followed by different people undertaking the same task. There is no formal training or communication (...) and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals"	Managed "[The process] is planned and executed in accordance with policy; employs skilled people who have adequate resources to produce controlled outputs; involves relevant stakeholders; is monitored, controlled and reviewed; and is evaluated for adherence to its process description."
3	Defined "Procedures have been standardised and documented, and communicated through training. It is however left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures (...) are not sophisticated but are the formalisation of existing practices."	Defined "[The process] is tailored from the organization's set of standard processes according to the organization's tailoring guidelines, and contributes work products, measures and other process improvement information (...).
4	Managed "It is possible to monitor and measure compliance (...) and take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way."	Quantitatively managed "[The process] is controlled using statistical and other quantitative techniques. Quantitative objectives are established and used as criteria in managing the process. Quality and process performance is understood in statistical terms and is managed throughout the life of the process."
5	Optimised Processes have been refined to a level of best practice, based on the results of continuous improvement (...).	Optimizing "[The process] is improved based on an understanding of common causes of variation inherent in the process. The focus (...) is on continually improving the range of process performance through both incremental and innovative improvements

The usage of similar numbering and naming principles may lead to believe that there is more similarity between the two approaches. It seems that, on examination, the CMMI is more demanding and productive at every level. The CMMI requires that training and the evaluation of adherence be performed at capability level 2; within CobiT, training is at level 3 and compliance at level 4. The CMMI requires that the process quality be under quantitative (statistical) control at capability level 4; CobiT only states that it is possible to measure compliance (this would be expected at capability level 2 in the CMMI, GP2.8 and GP2.9).

At the highest level, CobiT claims to have arrived (optimised), with the processes being at best practice; the CMMI sees this as a more ongoing process (optimizing) with quality and performance being continuously monitored and improved.

3 Sarbannes-Oxley in IT

1.0 IT Control environment

The IT control environment includes the IT governance process, monitoring and reporting. The IT governance process includes the information systems strategic plan, the IT risk management process, compliance and regulatory management,

IT policies, procedures and standards. Monitoring and reporting are required to ensure that IT is aligned with business requirements.

The IT governance structure should be designed to help ensure that IT adds value to the business and that IT risks are mitigated. This also includes an IT organization structure that supports adequate segregation of duties and promotes the achievement of the organization's objectives.

1.0.0 IT governance process

An IT governance process should be designed to help ensure that IT adds value to the business and IT risks are mitigated. Includes an organization structure that supports adequate segregation of duties and promotes achievement of objectives:

- Compliance and regulatory management
- Risk management process
- Strategic plan
- Standards
- Procedures
- IT policies

The CMMI requires that most of these features be implemented from the beginning. A number of process areas focus on ensuring that the information is based on business needs and requirements (MA Purpose statement, OPF SP1.1, OT SG1). In addition, every process area includes the requirement for the appropriate levels of policy (GP2.1), planning (GP2.2), standards and procedures (GP3.1). Finally risk management is laid out in process areas in both project management (PP SP2.2, PMC SP1.3, RSKM) and support (DAR). The systematic approach to risk is naturally covered by the continuous improvement of the processes (OPF, OPD, OPP, QPM, OID).

2.0.0 Monitoring and reporting

A monitoring and reporting process must be in place to ensure that IT is aligned with the business requirements.

This is largely covered throughout the CMMI, starting with MA, requiring that measurement and analysis are based on the management reporting needs (which should, naturally be aligned to the business needs). This information is further verified through process areas such as PPQA and PMC but also through control process areas such as DAR.

The need for the process improvement process to be aligned to business requirements is laid out from the start within the framework for process improvement (see *CMMI book* page 13: "three categories of factors that may influence your decision ... are business, culture and legacy.")

As we move to more maturity, greater focus is placed on the business needs and requirements by adding the statistical control and quality measurements based on those requirements (OPP SP1.1, QPM SP1.1).

2.0 Computer operations

These include controls over the definition, acquisition, installation, configuration, integration and maintenance of the IT infrastructure. Ongoing controls over operation address the day-to-day delivery of information services,

including service level management, management of third-party services, system availability, customer relationship management, configuration and systems management, problem and incident management, operations management scheduling and facilities management.

The system software component of operations includes controls over the effective acquisition, implementation, configuration and maintenance of operating system software, database management systems, middleware software, communications software, security software and utilities that run the system and allow applications to function. System software also provides the incident tracking, system logging and monitoring functions. System software can report on uses of utilities, so that if someone accesses these powerful data-altering functions, at the least their use is recorded and reported for review.

1.0.0 IT infrastructure

The IT infrastructure in Sarbannes-Oxley includes the tools, environment and resources need to effectively perform activities related to:

- Integration
- Configuration
- Maintenance
- Installation
- Definition
- Acquisition

Most of these are covered directly in both the planning process (PP) and in the generic practices related to the processes being considered. Each process needs to ensure, from the beginning, that "adequate resources" (GP2.3) are provided to produce the results. This includes most of the elements listed. In addition to this, the configuration controls of each process and its related work products are required in order to ensure that the work is done correctly.

2.0.0 System software

If someone accesses these powerful data-altering functions, at least their use is recorded and reported for review.

- Implementation
- Effective acquisition
- Configuration
- Maintenance
- Software (Middleware, Communications, Security, Utilities)
- Database management systems

This is covered throughout the CMMI by ensuring that the process is monitored and controlled (GP2.8), objectively evaluated (GP2.9) and reviewed with management (GP2.10). In addition to this, we have the requirement that activities be continuously monitored throughout any project that could affect one of the above, through project monitoring and control (PMC) and ensuring that traces are maintained under appropriate levels of control (GP2.6).

3.0 Access to programs and data

Access controls over programs and data assume greater importance as internal and external connectivity to entity networks grows. Internal users may be halfway around the world or down the hall, and there may be thousands of external users accessing, or trying to access, entity systems. Effective access security controls can provide a reasonable level of assurance against inappropriate access and unauthorized use of systems. If well designed, they can intercept unethical hackers, malicious software and other intrusion attempts.

Adequate access control activities, such as secure passwords, Internet firewalls, data encryption and cryptographic keys, can be effective methods of preventing unauthorized access. User accounts and related access privilege controls restrict the applications or application functions only to authorized users that need them to do their jobs, supporting an appropriate division of duties. There should be frequent and timely review of the user profiles that permit or restrict access. Former or disgruntled employees can be a threat to a system, and terminated employee passwords and user IDs should be revoked immediately. By preventing unauthorized use of, and changes to, the system, an entity protects its data and program integrity.

1.0.0 Prevention of unauthorized access

Access to the data needs to be monitored and control to ensure that no unauthorized access has been committed. This includes the implementation of activities such as:

- Review of user profiles
- Passwords
- Firewalls
- Data encryption and cryptographic keys

These purely security related items are not directly referenced by the model. There is no direct relationship between the CMMI and data security.

4.0 Program development and program change

Application software development and maintenance has two principle components: the acquisition and implementation of new applications and the maintenance of existing applications.

The acquisition and implementation of new applications continue to be areas with a high degree of failure. Many implementations are considered to be outright failures, as they do not fully meet business requirements and expectations or are not implemented on time or within budget.

To reduce acquisition and implementation risks, some entities have a form of system development and quality assurance methodology. Standard software tools and IT architecture components often support this methodology. The methodology provides structure for the identification of automated solutions, system design and implementation, documentation requirements, testing, approvals, project management and oversight requirements, and project risk assessments.

Application maintenance addresses ongoing change management and the implementation of new releases of software. Appropriate controls over changes

to the system should exist to help ensure that they are made properly. There is also a need to determine the extent of testing required for the new release of a system. For example, the implementation of a major new software release may require the evaluation of the enhancements to the system, extensive testing, user retraining and the rewriting of procedures. Controls may involve required authorization of change requests, review of the changes, approvals, documentation, testing and assessment of changes on other IT components and implementation protocols. The change management process also needs to be integrated with other IT processes, including incident management, problem management, availability management and infrastructure change control.

1.0.0 Acquisition and implementation

The aspects that need to be covered are typical elements of the lifecycle

- Documentation requirements
- System development
- Architecture
- Automated solutions
- Quality assurance
- System design and implementation
- Project management and oversight
- Tooling
- Approvals
- Testing
- Project risk assessments

The control over these elements is found throughout the CMMI. The key elements to be considered within the Sarbannes-Oxley context are the manner in which security is put in place to ensure that the controls are there and are valid. Remember that the key elements of the act are to ensure that the management people know the real financial data and reports, and are ready to personally vouch for their validity. This is performed throughout the process by ensuring that the decision making is done correctly, the activities are well planned and monitored, there is an independent control of the adherence to the standards and requirements of the process, and the whole thing is regularly reviewed by higher management.

2.0.0 Maintenance

Change management, if badly handled, will open up as many risks as the creation, acquisition and implementation of new products:

- Review of changes
- Approvals
- Evaluation of enhancements
- Extensive testing
- Testing and assessment of changes on other IT components and protocols

- Re-writing of procedures
- User re-training
- Documentation
- Authorization of change requests

These are all standard activities, forming the heart of the CMMI approach. It is a reminder that maintenance activities need to be performed with the same process-based rigour as the rest. The CMMI frequently talks of projects and many believe that maintenance can be excluded as it is not a project...

4 COBIT

The following section covers the requirements of the CobiT framework as included in the CobiT v4.0 (IT Governance Institute 2005). For each of the CobiT high-level controls, comments are included indicating possible interpretation, overlap and differentiation with CMMI V1.1 (Software Engineering Institute 2002). The CobiT control framework is generally seen as a valid support and guidance for the implementation of Sarbannes-Oxley.

1.0 Plan & Organise

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure should be put in place. This domain typically addresses the following management questions:

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?
- Does everyone in the organisation understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?

1.0.0 PO1 - Define a strategic IT plan

A number of aspects related to the strategy of IT are not covered by the CMMI, as the model tends to focus on the process improvement, project management and engineering aspects and less on the actual IT departmental and strategic management. However, we do find a number of points that respond to this requirement.

First of all, DAR should ensure that the strategic IT plan is based on an understanding of the needs of the business and the customers. That is further enhanced by the various organizational process areas that ensure that the organizational and business needs in terms of process, training, improvement are prioritised over the needs of the individuals and projects. All these elements underline the need for an organizational wide strategic plan that defines the long- term priorities. Other process areas and practices focus on peculiar aspects of the strategy and its implementation.

- GP2.1 - By defining the organizational expectations, management is ensuring that the strategic IT business objectives are aligned on the IT

strategy: the purpose of this practice is not just to say that CMMI requires you to plan, but explain what management expects to get out of it and ensure this is aligned.

- GP2.7 - The relevant stakeholders, internal and external are required to participate in defining the information and reporting needs. This includes the management of the data, the definition of the requirements and plans as well as the measurement and reporting requirements. This naturally includes the customers and the management.
- GP2.10 - It is expected within the CMMI framework that all processes be reviewed and understood by management on an ongoing basis. This includes the process related to controls, measurement and reporting - ensuring that the strategy is being respected.
- MA SP1.1 - The role of measurement in the management of the organization needs to be established, the purpose of measurement and analysis is to ensure that there is a measurement capability to support management information needs. This should ensure that every activity is aligned with the business objectives.
- IPM SP2.1 - Stakeholder involvement is a key component of Integrated Project Management and ensures the collaboration between the teams and stakeholders.
- IPM SP2.2 - Any disagreement with stakeholders, any key difference in realizing the objectives needs to be managed
- MA SP2.4 - Within the context of communicating and analysing the measurement results, management is expected to include the relevant stakeholders - this includes the business process users and owners. Measurements, based on the management information and reporting needs are collected, analysed and reported. The process of collecting, analysing and reporting these data are then reviewed on a regular basis with higher level management - this should include the steering committee if such a committee exists, as they are expected to be the primary requestors of reporting data.
- OPF SP1.2 - The continuous appraisal of the organization's processes (those used as well as the standards) needs to be considered in order to ensure that they correspond to the needs and requirements of the users and owners.
- PP SP2.3 - Commitment to the plans is required from all stakeholders - this includes the process owners and users.

Corporate management aspects, such as the participation in steering committees and the reporting to the CEO/CFO/CIO, are not directly referenced.

2.0.0 PO2 - Define the information architecture

The information architecture is covered in several process areas. These include project planning and project monitoring and control in which the data management plan and monitoring are referenced and required; organizational process development includes the management and architecture for process and improvement related information; configuration management includes all the aspects of ensuring the integrity of data and work products. In addition to these;

- MA SP1.2 - The measurements to be collected should be defined based on the information needed. This information needs to be classified and managed appropriately, according to the management policies.
- MA SP1.3 - The management reporting and measurement needs are well defined and established. The respect of these approaches and the assurance of the quality of data being reported are overseen by the Quality Assurance audits.
- MA GP3.2 - The process and standards used for ensuring the security and storage of the data are reviewed on a regular basis in order to cover the changing needs of the organization. This is reviewed on an on-going basis and updated appropriately.
- PMC GP2.1 - IT management has defined the information they need from the development and maintenance activities throughout the lifecycle. This includes all levels of data.

3.0.0 PO3 - Determine technological direction

The technical direction is set up first and foremost through the implementation of a process corresponding to the requirements of the "decision analysis and resolution" process area. This is reinforced through "organizational innovation and deployment" in which technological innovations are considered in relation to the needs of the organization. GP2.4 (in every process area) ensures that the people doing the work have the resources and tools they need to be able to do the work efficiently and technical solution. On a project level, the technological choices are covered by TS SP1.1.

More issues are required by the technological direction related to strategic choices and requirements based on the future of the organization - this is not covered by the CMMI but establishes the framework within which the CMMI should be working.

4.0.0 PO4 - Define the IT processes, organisation and relationship

Defining the IT processes is naturally at the heart of the CMMI. While it is specifically laid out in OPF, OPD, OPP and OID, it is the underlying principle of every element of the model.

The IT organization is not mentioned directly within the model; however the clear definition of roles, responsibilities and authority is required for every activity. Additionally, the generic practices require that the people concerned are equipped with the training and resources they need to do the work required of them.

Additional requirements of CobiT include the need of quality assurance, risk, compliance and more. These are clearly laid out in process areas such as PPQA and RSKM.

5.0.0 PO5 - Manage the IT investment

Managing the investment and the related financial aspects is, of course, critical to an organization that is seeking to respond to the requirements of the Sarbannes-Oxley act of 2002.

There are many relevant areas of the CMMI that seek to cover this aspect, even though the idea of IT investment is never directly mentioned. Naturally one of the main features here would be the decision process in determining how the funds and investments should be established and maintained, which should be run according to the DAR principles.

In addition to that, there is a strong emphasis throughout the project management practices that the resources and budgets need to be managed (planned, monitored and controlled) at all times. This includes the areas defined primarily in PP, PMC and RSKM, but also the approaches used in TS to determine the right technical solution to be implemented and VER and VAL when ensuring that we are achieving our objectives within the context of engineering activities.

It should be borne in mind that the engineering projects are not the only projects to be considered when implementing a process-based quality improvement programme. Creating an investment or a budget is a project and should be managed with the same care as the rest.

6.0.0 PO6 - Communicate management aims and direction

A lot of this area's details are about the communication and management of the policies. The implementation, communication and knowledge of the policies are a founding element of the CMMI-based process improvement effort. This is the main reason that the capability level 2 generic practices start with the implementation, communication and respect of a management policy, and finish with a review to ensure that the processes and practices that have been implemented correspond to management's aims and direction.

In addition to this, a number of specific practices support the need for the communication and management of the aims and direction. These include:

- MA SP1.1 - In which are laid out the management needs for information and reporting, which should naturally reinforce the aims and direction that have been set out
- PPQA SP2.1 - which ensures that any deviations at local level from the defined aims and direction are rapidly identified and corrected
- OT SP1.1 - which uses the management aims and direction to ensure that a clear training strategy is laid out is that all stakeholders have the required understanding of their roles and responsibilities (for instance those related to the implementation of the Sarbannes-Oxley act)
- OPF SP1.1 - defines the needs for improvements based on the organizational needs. These are established using measurements related to a model, but are only meaningful if they are clearly aligned to the management aims and direction.

7.0.0 PO7 - Manage IT human resources

The human resource aspect is not covered directly within the context of CMMI (it is more the objective of the "People CMM"). In particular, there is nothing within the model regarding recruitment and termination practices. However, a number of items related to the management of people are included.

- PP SP2.2 and RSKM cover the topics related the management of risks related to staffing and people, as well as the other risks that need to be managed: dependence on individuals, personnel clearance, staff retention should be included in the risks being managed both at project and at organizational level
- OT and GP2.5 ensure that the people have the competencies they need to do their job efficiently, understanding the impact of the work they do as well as supporting the roles of the people with whom they must interact.
- GP2.5 also ensures that staffing of roles is always performed based on the competencies of the personnel being used for any particular activity
- PP SP2.5 ensures that the staffing for particular projects is performed based on a clear understanding of the skills and knowledge required for the task to be accomplished
- IT SG1 pushes this a little further by ensuring that the team composition is always based on a clear understanding of how the team fits into the organization as well as the tasks that need to be completed and the skills required for those tasks.

8.0.0 P08 - Manage quality

The management of quality is possible the key raison-d'être of the CMMI. I need not go further into this point. If you are doing CMMI without understanding that you need to manage quality, you have not understood what the point of the improvement programme is.

9.0.0 PO9 - Assess and manage IT risks

While too many people are restricting the risk management activities within the CMMI to the management of project related risks, it is fairly easy to understand that the other risks (e.g. product or corporate risks) should be managed along the same lines. The implementation of a risk management strategy aims at identifying risks and reducing the amount of risks related to any task. This is well covered in the RSKM process area.

10.0.0 PO10 - Manage projects

Finally, we come to the management or projects. All the process areas within the project management category of the continuous representation are covered in this area. In addition to the management of the projects, CobiT requests that the projects be managed within the context of a programme framework. This aspect is not covered explicitly within the model; however it seems easy to understand that the management of projects needs to be done at least as well as the management of each project. That is to say that deciding on the priorities of the projects and establishing how the resources are going to be shared out is a key component of the IT governance process and should be managed with the same level of understanding of requirements, needs, resources, risks, costs, etc as each individual project.

2.0 Acquisition & Implementation

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In

addition, changes in and maintenance of existing systems are covered with this domain to make sure the solutions continue to meet business objectives. This domain typically addresses the following management questions:

- Are the new projects likely to deliver solutions that meet business needs?
- Are new projects likely to be delivered on time and within budget?
- Will the new systems work properly when implemented?
- Will changes be made without upsetting current business operations?

1.0.0 AI1 - Identify automated solutions

The need to consider alternatives and base the solution on an "effective and efficient approach" is covered directly through the Decision Analysis and Resolution and Risk Management process areas. In addition to this, we may consider

- TS SP1.1 - the requirement to consider detailed alternative solutions and make the choice based on documented selection criteria will ensure that the solution being considered is appropriate
- RD SP1.1 - Ensure that the customer's needs are really understood and fit into the solution being considered; this is balanced at the other end by
- VER SP1.3 - Ensure that there are clear procedures and criteria defined to demonstrate that the product developed corresponds to the specified requirements
- REQM SP1.1, 1.2 - Analyse all the requirements to make sure that they are clearly understood and that the customer and the development team understand and agree on what will be developed and delivered
- GP1.1 - The implementation of organizational policies throughout the organization and all process areas ensures that the solutions fit into the company needs and requirements first and correspond to the corporate needs

2.0.0 AI2 - Acquire and maintain application software

This is naturally the heart of the engineering process areas throughout the CMMI. While going through the detailed control objectives of this area, we will cover most of the practices of the engineering process areas and several support process areas.

The focus on requirements, design and development are at the heart of the engineering process areas. The control and auditability requirements are to be found within the generic practices, in particular GP2.8, GP2.9, GP2.10 and GP3.2. Additionally we have the need for configuration management (GP2.6 and CM) and acceptance and testing procedures (VER and VAL).

The CobiT emphasis placed on maintenance is not covered directly and explicitly within the CMMI.

3.0.0 AI3 - Acquire and maintain technology infrastructure

The technological infrastructure is largely covered within the generic practice GP2.3 which requires that the resources, including technical, be made available for each and every activity.

In addition to this the supplier management process areas (SAM and ISM) assure that there are appropriate procedures for the selection and management of suppliers and their products.

Specific infrastructure requirements are covered in specific process areas, such as Validation and planning.

4.0.0 AI4 - Enable operation and use

The main focus of this control is to ensure that the required knowledge of the new systems is made available where and when required. This is covered primarily in the following areas:

- OT - Focuses on providing the training needed at each and every level
- TS SP3.2 - Requires that the development of the user documentation be developed in parallel to the product development itself. The CMMI, like most engineering practices sees the documentation as an integral part of the product to be delivered to the customer
- PI SP3.4 - ensures that the finished product, after it has been appropriately evaluated and package is delivered in an orderly manner to the customer.

5.0.0 AI5 - Procure IT Resources

The IT resources in CobiT, as in CMMI, include all the required resources, including people, hardware, software and services. This is done through the selection of suppliers of those resources as well as the management of the resources internally.

Naturally, the first area where we will look is the GP2.3 in which "adequate" resources are required for each and every process in the model. In addition to that, we have planning for skills and knowledge (PP SP2.5 and IT SP2.1) as well as other resources (PP SP2.4). The usage of Decision Analysis and Resolution within the framework of supplier selection and management completes the picture.

6.0.0 AI6 - Manage changes

Change management is a key component of any development or engineering environment. In this case, we see the key elements for the change management practices within requirements management, configuration management and project monitoring and control as far as the project is concerned. In addition, we find the management of change permeates the organizational process focus and definition areas as well as the more complex organizational innovation and deployment process area.

7.0.0 AI7 - Install and accredit solutions and changes

The main concerns of this section cover the requirements for testing and release of the product. Most of the practices required are covered in the verification and validation process areas. Additionally, some of the requirements are covered by the product integration practices, particularly SP3.3 and SP3.4, which cover the delivery of a completely evaluated product.0

There are additional requirements in CobiT that are not explicitly covered by CMMI. They include the requirement to "automate the system used to monitor changes to application systems..." and the requirement for a "post-implementation review of the operational information system", which goes beyond the milestone review that we would find within PMC.

3.0 Deliver & Support

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and the operational facilities. It typically addresses the following management questions:

- Are IT services being delivered in line with business priorities?
- Are IT costs optimised?
- Is the workforce able to use the IT systems productively and safely?
- Are adequate confidentiality, integrity and availability in place?

A lot of emphasis of the CobiT in this case is placed on the security of the data and the infrastructure. The CMMI focuses more on the processes required for the creation and development of activities and does not directly reference the need for security aspects, except obliquely by mentioning that "security requirements" need to be included in the project plan, or through the risk management process area.

1.0.0 DS1 - Define and manage service levels

The requirement for good communication between the development organization and the customers and, in particular the definition of the services that will be provided is self-evident in any reasonable engineering environment. The CMMI is frequently criticized for the lack of reference to the customer and the customer needs. This is naturally covered throughout the model through the usage of the term "stakeholder".

In addition to the above a number of business requirements related activities are found throughout the model. They include the business policy requirements (SP2.1) and control (SP2.10) found in every process area, as well as key process areas such as those related to requirements (RD and REQM). The service levels are further managed through the implementation of a valid measurements and their analysis. The usage of these measurements for the identification of process needs and improvements furthers this option. This is finally strengthened by the process performance measurements and quantitative project management to ensure that the service level is maintained throughout the development cycle.

2.0.0 DS2 - Manage third-party services

The management of third-party suppliers is found in the CMMI in the "supplier agreement management" and "integrated supplier management" process areas. These two areas effectively cover the requirements of the identifying the services, categorizing them according to supplier types, maintaining formal documentation of relationships, formalizing that relationship, ensuring quality of work and transparency of communication, managing the risks and monitoring the performance of suppliers.

3.0.0 DS3 - Manage performance and capacity

The requirement to be able to manage the performance and capacity of the IT resources is clearly an implementation of the relationship between plans that is covered in the SG1 of the CMMI's Integrated Project Management process area. The requirement here however does go further.

While the CMMI does make a number of requirements in relationship to planning for resources and skills and being able to monitor the availability of those resources (particularly in PP and PMC, but also in SP2.2, SP2.3 and SP2.8), the focus of the CMMI remains on the project rather than on the long-term usage of resources and capacity. One could argue that the management of a programme along the CMMI guidelines would cover this aspect; however the requirements of CobiT would be best covered by bringing the PP and IPM process areas up to capability level 4 in the area of planning for resources and skills.

4.0.0 DS4 - Ensure continuous service

The continuity and contingency requirements of CobiT could be covered by an implementation of risk management in which the risks of disruption and disaster are properly covered; however the topics of security and continuity are not covered within the CMMI, except obliquely through ensuring that resources are provided, etc.

5.0.0 DS5 - Ensure systems security

As with DS4, the security requirements of CobiT could be covered by an implementation of risk management, however the topics of security and continuity are not covered within the CMMI, except obliquely through ensuring that resources are provided, etc. Certain aspects of these requirements should be covered in the data management plan (PP SP2.3).

- MA SP1.3 - The data collection and storage procedures are designed to ensure the security of the data.
- MA SP2.3 - The storage of the data and the results prevent the updates or changes that are contrary to the appropriate security levels.
- OPD SP1.4 - The organization's measurement repository is designed to ensure that data regarding the processes and security aspects are protected from ill-advised access.
- GP2.1 - Stringent policies ensure that the security is understood and communicated to all the relevant stakeholders. The policy is the basis for the design of processes and procedures for the manipulation and protection of data.
- GP2.10 - Management regularly reviews the security processes at all levels to ensure that they correspond to the policies and security requirements.
- PP SP2.3 - The data management plan in each project will ensure that the data collected and managed is protected appropriately.
- PMC SP1.4 - The management and monitoring of the data being collected and consolidated is done throughout all activities.

6.0.0 DS6 - Identify and allocate costs

The management of the IT costs and the allocation of the resources appropriately are done through a good implementation of the process area "decision analysis and resolution". Also, there is coverage of the allocation of the costs through the budget management practices (PP SP1.4 and SP2.1). Again, the CMMI's focus remains at the project level, while the CobiT focus is at the organizational level. Both areas overlap but address different things.

7.0.0 DS7 - Educate and train users

The identification and delivery of training needs for the users, as for the organization are largely covered by the process area relative to organizational training. It should be noted that the organizational training process area does not specifically address the needs of the users by opposition to the needs of the project team members. However, it should be understood that the training needs of the users are requirements that need to be managed and allocated as with all other requirements. The documentation is developed and delivered in parallel to the product (TS SP3.2) and the training courses that need to be developed and delivered are done according to the processes defined within OT SP1.4 and OT SP2.1.

8.0.0 DS8 - Manage service desk and incidents

The management of a service desk and incidents is not explicitly covered in the CMMI, however, there are detailed explanations regarding the need for management of change and understanding the customer needs. The requirements management process area does cover some aspects of this control.

9.0.0 DS9 - Manage the configuration

The CMMI has a significant number of requirements regarding configuration management. The requirement within the CMMI focuses on ensuring the consistency of data across the life of the product - this is covered both in the configuration management process area and the related generic practice (GP2.6). As is usual within CMMI, the manner in which this is performed is not considered.

CobiT is slightly more demanding, requiring more than just the results and requiring that a single central repository be established which includes "hardware, application software, middleware, parameters, documentation, procedures and tools for operating, accessing and using the systems and services."

10.0.0 DS10 - Manage problems

The identification, management and resolution is naturally a key element throughout the CMMI, it is one of the guiding factors in project planning and monitoring and control.

In addition to this,

- CAR - Causal Analysis and Resolution ensures that regular problems (common causes of variation) are analysed systematically with a view of continuous improvement.

- DAR - Decision Analysis and Resolution ensures that decisions are made based on a reasoned selection between alternatives. This should ensure that decisions that are questionable can be reviewed and justified before problems are generated.
- PPQA - Quality Assurance has a key role in which they are required to identify problems early and rapidly by a continuous review of the approaches and processes that are being used throughout the organization. They are then in charge of ensuring that the problem is resolved as efficiently as possible, escalating the issues to the management level as appropriate.

11.0.0 DS11 - Manage data

Within CMMI data management is referenced directly in three process areas: project planning, project monitoring and control, configuration management. In addition to that, there are some practices that reference the obligation to understand the needs of the organization and the risks related to the management of the data as well as other aspects. MA SP2.3 references more particularly the storage needs for measurements so as to ensure that they are available and protected appropriately.

Again, the CobiT's requirements for security and backup aspects are not covered explicitly within the CMMI but are only referenced or alluded to in various subpractices.

12.0.0 DS12 - Manage the physical environment

Once again, we are in a context that is not covered by the CMMI. The physical environment is specifically identified as something to be considered in the context of each process area under GP2.3 which requires the provision of appropriate resources. In addition, there is some reference to the physical environment in the project planning and monitoring process areas. A clearer reference is included in RSKM SP1.1 where it is mentioned as a potential source of risks.

13.0.0 DS13 - Manage operations

This control references procedures, scheduling, monitoring and management of documents and hardware. Most of the requirements here will be covered by most of the CMMI. In fact, the answer to this area is probably one of the key *raison d'être* of the CMMI as a whole. The area covers most of the maturity level 2 requirements in terms of management of people and projects as well as configuration management.

4.0 Monitor & Evaluate

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and providing governance. It typically addresses the following management questions:

- Is IT's performance measured to detect problems before it is too late?

- Does management ensure that internal controls are effective and efficient?
- Can IT performance be linked back to business goals?
- Are risk, control, compliance and performance measured and reported?

1.0.0 ME1 - Monitor and evaluate IT performance

The monitoring and evaluation of performance is identified as a critical practice is many places throughout the CMMI.

MA focuses naturally on identifying the needs in terms of measurements, monitoring and control of processes and practices at the organization level. This is identified as one of the most important process areas and is recommended as a key starting point for any quality improvement programme.

- GP2.8 covers the need to measure and monitor the performance within each process area.
- OPF SP1.1 discusses the need to identify the organizational need for improvement based on an understanding of its objectives and the strengths and weaknesses of the current processes and practices
- OEI SP2.3 further requires a measurement of the improvements as they are rolled out.

Naturally, all these areas are directly related to the need for appropriate corrective (CMMI) or remedial (CobiT) actions.

2.0.0 ME2 - Monitor and evaluate internal control

This control talks primarily about "controlling the controls". Controls are one of the key aspects of the CMMI and typically one of those that create most resistance when they are being implemented within a low maturity organization.

- PPQA ensures that each process and implementation is continuously controlled through an independent quality assurance authority who seeks to ensure that the practices and processes deployed and used focus on quality and quality improvement as defined by management
- GP2.9 and GP2.10 ensure that each process as implemented is reviewed by both the quality assurance and management to ensure that the focus remains on the business needs and the improvement of quality
- CM, MA, OPP, QPM and others ensure that there is ongoing control of the practices and processes as they are being performed
- TS and PI, in collaboration with VER and VAL, ensure that the appropriate levels of controls are carried out throughout the engineering process.

3.0.0 ME3 - Ensure regulatory compliance

This control focuses on the need to have appropriate levels of reviews and audits to ensure that all the required regulations, standards and laws have been respected. The identification of regulations that need to be respected is naturally a key part of requirements definition and identifying the organization needs within OPF, OT, MA and others. In addition to that, the respect of the those regulatory needs, once defined, are part of the work to be performed by the

quality assurance team, which includes the identification of deviations, the communication to appropriate levels of management and ensuring the corrective actions are carried out appropriately.

4.0.0 ME4 - Provide IT governance

If IT governance is not directly referenced with the CMMI, all the related detailed controls are referenced. This include

- Establishing a framework for governance by working with the board and establishing an infrastructure of policies (GP2.1), responsibility and authority (GP2.4), controls (GP2.9, GP2.10, PPQA)
- Ensuring that the activities are in line with the needs of the organization (OPF, OT, OEI)
- Communicating throughout the organization (IPM), particularly with management (GP2.10)
- Establishing value based programmes (MA, OPP, QPM)
- Resource management (GP2.3, OT)
- Risk management (RSKM)
- Performance measurement (MA, OPP, QPM, GP2,8)
- Independent assurance (PPQA, GP2,9)

5 Conclusion

The main requirement of Sarbannes-Oxley is the assurance that management is aware of the real situation and has enough controls in place to be able to demonstrate that they are completely open and above-board in their reporting. Top management takes personal responsibility, under menace of sever penalties, to ensure that the data they are reporting is completely accurate. In order to do this, they need to pay particular attention to the aspects of the IT services. Most of the reports that are generated are being done today through highly complex software-based systems that may mask or falsify data (perhaps unwittingly) through defects in the design, development, parameterization and implementation of the accounting and management software.

The CobiT approach sets out a number of objectives from a management point of view that allows understanding who is responsible and what they should be doing in various stages of the IT activities. These include a description of the controls' objectives as well as a more detailed description of what each control should be considering; management guidelines describing who should be responsible for ensuring that a number of activities are performed; goals, and indicators to be achieved at business level, process level and IT level; ratings as to how the capability progresses. All these are defined at a reasonably simple level.

This approach based on measurement, processes and controls means that a serious culture change has to be implemented in many organization to ensure that the change is implemented within the mentality of the people rather than only through the force of a "police state".

The CMMI approach focuses on achieving results from a business point of view through a continuous improvement trajectory. By implementing a process improvement programme that is based on an understanding of what the people are really doing and helping them to share the best practices, you can instil a culture in which activities such as management reviews, configuration management, quality assurance and audits are seen as a normal part of the improvement culture.

By having the defined processes in place and the controls that the CMMI recommends, you can achieve the level of communication and stability within an organization that makes the additional steps required for a Sarbannes-Oxley approach or the implementation of CobiT style controls a lot faster and easier.

This report may give the feeling that a number of CMMI requirements cover multiple aspects of the CobiT model. This is largely due to the difference in emphasis and grouping of the practices. If this report had been centred on CMMI and referenced the corresponding CobiT approaches, the results would be very different.

Achieving CMMI Maturity Level 3 does not mean you are Sarbannes-Oxley compliant; Sarbannes-Oxley is an accounting and financial reporting requirement and will not be satisfied by having your engineering processes in order. However the context will make it easier to demonstrate that the controls are in place and ready.

Achieving CMMI levels does not correspond to achieving CobiT levels. Generally the CMMI is more demanding that CobiT, however there remain aspects in each of the models that is not found in the other.

Being Sarbannes-Oxley compliant does not mean you have achieved CMMI Maturity Level 2 or whatever. Again, they look at different aspects of your business.

As can be seen in the detail of this report, there appears to be a lot of overlap between the two standards, even though they aim at different aspects of understanding and controlling the quality and reliability of the work being carried out. It is not recommended that a reasonable organization consider one standard as significantly superior and therefore ignore the other. They both ensure a quality improvement approach that is measurable and useful.