Sarbanes-Oxley, IT Governance and Enterprise Change Management

Is Your IT Organization Ready for Compliance?

An MKS White Paper
By Tim Ruzbacki
Senior Consultant
Member SEI, ACDM
Is Your IT Organization Ready for Compliance?

The Sarbanes-Oxley Act (SOA) has reset the responsibilities of organizational senior management and boards of directors, and the expectations of investors, regulators and external stakeholders. Compliance to regulatory issues is now one of the most dominant business challenges facing corporations today. As technology is now at the core of business operation, governance rigor now absolutely applies to the CIO and his/her Information Technology organization. As companies move rapidly toward SOA compliance, there are many questions that arise about the appropriate measures required to improve IT governance. Which framework to follow? What support can my vendors offer me? Are there tools and solutions available to help me?

Risk Reduction and Mitigation

One of the principle concerns facing IT departments is providing process and policies that help their organizations prepare for all business challenges. To accomplish this task, many teams choose a process methodology that satisfies all requirements while at the same time reducing the risks associated with non-compliance. Risk management includes evaluations and assessments that are often measured using IT audits. The results of the audits are designed to assess each area of the methodology to discover all potential areas of risk. Having well-defined and repeatable processes helps to mitigate risk and achieve audit compliance.

Defining COBIT

In answering the questions above, this paper focuses on one framework, COBIT, which has been developed by the IT Governance Institute as a generally applicable and accepted standard for good Information Technology (IT) security and control practices. Developed in 1996, COBIT is relatively small in size so it can be independent of any technical platforms while still maintaining a high degree of responsiveness to an organization’s business values.

COBIT provides maturity models similar to the leading process methodologies in the industry (CMM, ISO, ITIL, COSO, Six Sigma) to help control the development of IT processes. For regulatory needs today, COBIT soundly manages the gaps around business risks, corporate governance issues and other technical issues in an organization.

The rest of this paper provides management with a look at COBIT for:

- Expressing IT control practices through Maturity Models for benchmarking measurements
- Measuring outcome and performance of IT processes through Key Performance Indicators (KPI’s)
- Getting processes under control using Critical Success Factors (CSF’s)

Process Initiatives

Another business challenge combines process methodologies with Enterprise Software Change Management (ESCM) technology solutions to provide the infrastructure necessary to manage and store process workflows and to measure the results of those processes. Process-centric ESCM can be leveraged to help with Sarbanes-Oxley compliance. By using the issue management and workflow support provided by ESCM systems directly, any existing business process including all software development processes could be automated, with direct tracking and integration of all work completed, and with full audit trails. This definitely affects companies with strategic governance
initiatives, or that have to meet regulatory and auditory compliance. Some methodologies used by corporations today include:

- SEI Capability Maturity Model (CMM, CMMI)
- IT Infrastructure Library (ITIL) for service management
- ISO (International Standards Organization) 9xxx for quality management
- COBIT (Control Objectives for Information and Related Technology)

**The Sarbanes-Oxley Act**

In July of 2002, at the heels of some major US corporate accounting scandals, legislation was drafted to create new or enhanced standards for corporate accountability. Initially targeted for June of 2004, the current date for initial compliance is November 15, 2004. The act effects US public companies with a market capitalization over $75 million and the main purpose is to prevent future accounting scandals and rebuild trust of the investing public. Failure to comply to the legislation requirements results in penalties against the corporation.

**The Effect of Sarbanes-Oxley on IT**

Many of the artifacts necessary to prove SOA compliance include all the documents and work papers used to create financial reports and other publications produced for the general public. Certain sections of the act deal specifically with the internal controls a company has in place to ensure the accuracy of their data. It is even mandated that each annual report contain a separate internal report stating that management is responsible for the adequate internal control structure and that at periodic intervals that structure is assessed and modified as necessary.

Usually the IT organization is directly responsible for management and control of the systems and technology in place to collect, store and manage the data and information contained in the company’s financial reports. But studies indicate that many IT groups are not prepared for the insurgence of activities facing their departments with SOA legislation. AMR research found that as many as 85% of companies predict that the SOA will require them to make changes to their IT infrastructure. And Gartner research found that many CIO’s are just now realizing the impact the legislation has on their operations and that:

- CIO’s must have a strategy and the resources to respond
- CIO’s have to learn what technologies will help
- CIO’s must enhance their knowledge of internal control
- CIO’s have to develop a compliance plan to specifically address IT controls

“To this end, IT professionals, especially in executive positions, need to be well-versed in internal control theory and practice to meet the requirements of the Act.”

- “A Focus on Internal Control,” ISACA

Even though the direct impact of Sarbanes-Oxley with regards to IT is on systems used for financial control, it is just a lot more efficient for most organizations to carry out a complete review of their entire IT structure. Why spend time trying to figure out what may be irrelevant when so much is at stake?

The diagram below provides a look at the various audiences involved in the overall corporate governance structure. The audiences are then linked to the particular business challenges faced at each level. Finally, links are provided into some of the solutions available to satisfy the business challenges at
each audience level. The solutions involve ESCM technology and process recognized as industry standards and best practices.

Once the need for compliance is accepted, and the CIO has determined a strategy, the course of action may become clear. The ESCM technology must be put in place if it is not there already, and the process methodologies chosen by the company must be implemented. The rest of this paper identifies the CobIT methodology and maps at a high level the various processes within the methodology to the ESCM technologies. All technologies are different, so the mapping of the processes is explained through the MKS technology solution.

**Laying out COBIT**

There are 34 processes in COBIT broken out into 4 main categories. There is one high-level control objective that relates to each of the 34 processes, and there are a total of 318 specific control objectives broken out across the 34 processes. The 34 processes are broken out into four domains:

- Planning and organization
- Acquisition and implementation
The table below identifies the 34 processes by the domains where they exist. Many of these can be mapped back to an ESCM solution and that table appears later in the paper.

<table>
<thead>
<tr>
<th>Planning and Organization</th>
<th>Acquisition and Implementation</th>
<th>Delivery and Support</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>PO1 – Define a strategic IT plan</td>
<td>AI1 – Identify automated solutions</td>
<td>DS1 – Define and manage service levels</td>
<td>M1 – Monitor the processes</td>
</tr>
<tr>
<td>PO2 – Define the information architecture</td>
<td>AI2 – Acquire and maintain application software</td>
<td>DS2 – Manage third-party services</td>
<td>M2 – Assess internal control adequacy</td>
</tr>
<tr>
<td>PO3 – Determine the technological direction</td>
<td>AI3 – Acquire and maintain technology infrastructure</td>
<td>DS3 – Manage performance and capacity</td>
<td>M3 – Obtain independent assurance</td>
</tr>
<tr>
<td>PO4 – Define the IT organization and relationships</td>
<td>AI4 – Develop and maintain procedures</td>
<td>DS4 – Ensure continuous service</td>
<td>M4 – Provide for independent audits</td>
</tr>
<tr>
<td>PO5 – Manage the IT investment</td>
<td>AI5 – Install and accredit systems</td>
<td>DS5 – Ensure systems security</td>
<td></td>
</tr>
<tr>
<td>PO6 – Communicate management aims and direction</td>
<td>AI6 – Manage changes</td>
<td>DS6 – Identify and allocate costs</td>
<td></td>
</tr>
<tr>
<td>PO7 – Manage human resources</td>
<td></td>
<td>DS7 – Educate and train users</td>
<td></td>
</tr>
<tr>
<td>PO8 – Ensure compliance with external requirements</td>
<td></td>
<td>DS8 – Assist and advise customers</td>
<td></td>
</tr>
<tr>
<td>PO9 – Assess risks</td>
<td></td>
<td>DS9 – Manage the configuration</td>
<td></td>
</tr>
<tr>
<td>PO10 – Manage projects</td>
<td></td>
<td>DS10 – Manage problems and incidents</td>
<td></td>
</tr>
<tr>
<td>PO11 – Manage quality</td>
<td></td>
<td>DS11 – Manage data</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DS12 – Manage facilities</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>DS13 – Manage operations</td>
<td></td>
</tr>
</tbody>
</table>

There are also four basic divisions of the framework:

- Maturity Models
- Critical Success Factors (CSF’s)
- Key Goal Indicators (KGI’s)
- Key Performance Indicators (KPI’s)

In addition to the basic framework indicated above, IT organizations designing a COBIT implementation should consider the following items:

- Primary Objectives
  - Compliance in legal, regulatory and industry issues
  - Financial reporting to investors, regulatory agencies, annual reports, etc.
  - Operations that control business processes, asset protection, security

- Control Objectives
  - Accuracy in data that is re-computed, balanced and complete
  - Authenticity of data is acknowledged and verified
  - Availability of information secure so it is not lost, erased or stolen
  - Confidentiality so that private information is not disclosed
Integrity so that information is not altered or corrupted
Timeliness so that results are expeditious and provided in the proper time period
Validity of information that can be confirmed, approved and authorized

Control Activities
- Hiring, training and supervision (oversight)
- Organizational communication and reporting structures
- Physical/logical access and authorization to all secure information
- Preventative, detective and corrective procedures and standards
- Process controls that provide sequential, balanced management
- Segregation and separation of roles and responsibilities for integrity reasons
- Systems controls and security

Tracking and Measurements
- Deficiencies are reported
- Evidence exists that internal control systems continue to function
- Internal/external information corroborate performance and events
- Physical/perpetual comparisons are made to inventory, assets, etc.
- Separate evaluations are made that measure scope and frequency information

Looking at the COBIT Maturity Models

The Maturity Model for COBIT resembles the Capability Maturity Model (CMM) for Software in many ways. While there are 5 CMM levels, COBIT recognizes the non-existence of process altogether, and begins its model at level 0. With CMM, there are 18 Key Practice Areas (KPA’s) for process development and implementation. With COBIT, there are 34 process areas broken into 4 major categories. The diagram below defines the six maturity levels for COBIT.

0) Non-existent: It seems unreasonable to think that management processes would not exist at all, but that is the definition behind this first maturity level for COBIT. What generally happens at this level, is that the organization has yet to recognize that they have a problem that needs to be solved. There is no clear direction for implementing change should any occur, and there is little understanding of the dangers and pitfalls of not having solid management processes in place. Often time the catalyst to move forward is a new regulation or piece of legislation like Sarbanes-Oxley.
1) **Initial**: The management processes are characterized as ad hoc and disorganized. Few processes are defined, and success depends on individual effort and heroics. At this level, the organization usually understands they have a problem and that they need to move forward with process improvements. The initial steps are in place but the large effort before them often requires a dedicated resource pool including outside consultants to develop and manage the necessary activities that will mature the organization. This also may help provide knowledge of tools and technology that will help an organization standardize their process improvement efforts.

2) **Repeatable**: Most management processes follow some type of regular pattern. The problem, however, is that project-by-project, team-by-team, or even individual-by-individual, they are all following something different. The fact that the organization has some process out there to follow is a start, but to mature further, the organization must begin to collect the different flavors of each process and standardize as much as possible. Otherwise, what happens is that similar tasks are being performed in a variety of ways that tend to look as though with each task performed, the wheel is created new each time. So the processes that can be repeated definitely begin to exist, but still in a much too disorganized fashion.

3) **Defined**: While the management processes at this level are well documented and communicated consistently across the organization, there are still many changes necessary to really control the processes. Standards are developed, communicated, and easily accessible to the organization, but no checks and balances are in place to manage and control the outcome. How does anyone in the organization know if the process improvement effort was successful or not? In the world of compliancy, and the organized legislation mandated by Sarbanes-Oxley, without real proof that the processes are followed and working, the effort is not complete. In level 3 the focus is that an organizational standard process set is in place for all projects to measure themselves against.

4) **Managed**: Once communication and documentation are under control, management processes are then monitored and measured for adherence to the guidelines. One of the keys to success is the technology or the tool set used to help monitor and measure the various aspects of the processes. ESCM tools are among the most useful for providing the information and results necessary at level 4. The logic behind change and configuration management ties in completely with an organization’s ability to map process workflows and run reports against the milestones at each state within the workflow. There are a limited number of robust ESCM tools in the market, but companies affected by regulatory audits and Sarbanes-Oxley must consider the investment in this technology to satisfy all aspects of the external regulations.

5) **Optimized**: The best practices of the organization and of the industry are now followed and automated to insure compliance and to provide the necessary audit trails. Through a continued process improvement effort, the processes have been refined and automated to reflect positive changes in many areas within the organization. Definitely, the audit trails are in place and proof that an organization is in compliancy with regulations and other corporate governance issues is readily available. Improvements in automated tool solutions and technologies further the cause for complete COBIT process maturity.

**The Critical Success Factors**

- A regulation and audit committee is formed to oversee all audit and compliance activities
- Control practices are defined to prevent internal oversight breakdowns
- IT governance activities are integrated into the enterprise governance process and leadership behaviors
- IT governance focuses on enterprise goals, strategic initiatives and technology resources
- IT governance activities are defined with a clear purpose documented and implemented that are based on enterprise needs
Management practices are implemented to increase efficient and optimal use of resources and increase the effectiveness of IT processes.

Organizational practices are established to enable:
- Sound oversight
- Controlled environments
- Risk assessments
- Standards
- There is integration and smooth interoperability of the more complex IT processes such as configuration and change management.

The Key Goal Indicators:
- Adherence to laws, regulations, industry standards and contractual commitments
- Appropriately integrated and standardized business processes
- Availability of appropriate bandwidth, computing power and IT delivery mechanisms
- Benchmarking comparisons of IT governance maturity
- Creation of new service delivery channels
- Enhanced performance and cost management
- Improved return on major IT investments
- Improved time to market
- Increased quality, innovation and risk management
- Meeting on time and on budget requirements and expectations of the customer
- Reaching new and satisfying existing customers
- Transparency on risk taking and adherence to the organizational risk profile

The Key Performance Indicators:
- Increased availability of knowledge and information for managing the enterprise
- Increased linkage between IT and enterprise governance
- Increased number of IT action plans for process improvement initiatives
- Increased satisfaction of stakeholders (survey and number of complaints)
- Increased utilization of IT infrastructure
- Improved cost efficiency of IT processes (cost vs. deliverables)
- Improved performance as measured by IT balanced scorecards
- Improved staff productivity (number of deliverables) and morale (survey)

The table and chart below show the breakdown of the 34 process areas and how they apply to the different internal organizations responsible for them. Note the number of processes either managed or controlled by the ESCM team from IT and IS. The items shaded red are very critical since they are both managed and controlled by the same group. Yellow shows only the items managed by a group, and green covers those items only controlled by group. Please note the abundance of red and green in the IT/IS column where the ESCM team resides. Also note that ESCM never manages only a single item. If it affects ESCM at all it affects it at a control level at the minimum.
**COBIT Process** | **Executives** | **Finance** | **IT/IS**

**Planning and Organization**

PO1 – Define a strategic IT plan | Manage | | Control
PO2 – Define the information architecture | | Manage/Control | Manage/Control
PO3 – Determine the technological direction | Manage | | Control
PO4 – Define the IT organization and relationships | | Manage/Control | Manage/Control
PO5 – Manage the IT investment | Manage | | Control
PO6 – Communicate management aims and direction | Manage | Control | Control
PO7 – Manage human resources | Manage/Control | | Manage/Control
PO8 – Ensure compliance with external requirements | Manage | Control | Control
PO9 – Assess risks | Manage | Control | Control
PO10 – Manage projects | | Control | Manage/Control
PO11 – Manage quality | | Manage/Control | Manage/Control

**Acquisition and Implementation**

AI1 – Identify automated solutions | | Control | Manage/Control
AI2 – Acquire and maintain application software | Manage | Control | Manage/Control
AI3 – Acquire and maintain technology infrastructure | Manage | Control | Manage/Control
AI4 – Develop and maintain procedures | | Manage/Control | Manage/Control
AI5 – Install and accredit systems | Manage | | Manage/Control
AI6 – Manage changes | | Manage/Control | Manage/Control

**Delivery and Support**

DS1 – Define and manage service levels | Manage/Control | | Manage/Control
DS2 – Manage third-party services | Manage/Control | | Manage/Control
DS3 – Manage performance and capacity | Manage/Control | Control | Manage/Control
DS4 – Ensure continuous service | Manage/Control | Control | Control
DS5 – Ensure systems security | | Manage/Control | Manage/Control
DS6 – Identify and allocate costs | Manage | Control | Manage/Control
DS7 – Educate and train users | Manage/Control | | Manage/Control
DS8 – Assist and advise customers | Manage/Control | | Manage/Control
DS9 – Manage the configuration | | Manage/Control | Manage/Control
DS10 – Manage problems and incidents | | Manage/Control | Manage/Control
DS11 – Manage data | Control | | Manage/Control
DS12 – Manage facilities | Manage/Control | Control | Control
DS13 – Manage operations | Manage/Control | Control | Control

**Monitoring**

M1 – Monitor the processes | Control | | Manage/Control
M2 – Assess internal control adequacy | Manage | Control | Manage/Control
M3 – Obtain independent assurance | Manage | Control | Manage/Control
M4 – Provide for independent audits | Manage | Control | Manage/Control

**MKS ESCM Solution**

There are very few ESCM solutions available in the market. They have to be able to satisfy the laundry list of requirements below. Also, they have to be able to satisfy expectations of external auditors who are going to ask for proof that processes are secure and manageable. Auditors also want to know that ESCM technology can provide an organization the ability to recreate points in time that demonstrate reliable processes and the data extracted at points along those processes.

So what must the ESCM technology solution provide? Like the MKS solution, it must:

- Be backed by a service-oriented organization tuned to customer responsiveness
- Deliver process control but not at the expense of agility
- Enable IT organizations to seize control of global development activities
- Have low administration burden and support costs
• Provide next generation, enterprise-based architecture and capabilities at a low total cost of ownership (TCO)
• Quickly ramp to productivity and efficiency challenges
• Span multiple platforms, teams and tool environments

Illustration of a Document Process Workflow

What does it all mean and how does it help the CFO?

Sarbanes-Oxley auditors will ask a lot of questions, but two basic questions will be: What is your standard operating procedure (SOP)? And, Who authenticated that the SOP was followed? The burden of proof will be on the CFO since Sarbanes-Oxley is concentrating on financial reporting procedures. So knowing that there was technology in place that provided the ESCM security like the MKS solution gives the CFO the confidence to answer those questions with accuracy and authority. The solution made it possible for:

• All corporate policies and templates to reside under version and change control
• All customer commitments being tracked and reported
• Assurance that everyone is aware of all commitments and approvals have been given
• Online access to status updates
• Secure and reliable system management
• Traceable and auditable reporting on all corporate policies and templates
Even with certifications, such as CMM, CMMI or ITIL, companies still should consider the COBIT methodology when preparing for their SOA audit. The expectation of a good set of SOP’s and a willingness to provide work in progress with action plans for all deviations to internal governance standards must be satisfied. (IT organizations that manage and control the vital ESCM processes necessary to securely and accurately satisfy the regulatory requirements must be in place.)

**Sources of Information**

- [http://www.itgi.org/](http://www.itgi.org/)
- [http://www.sox-online.com/coso_cobit.html](http://www.sox-online.com/coso_cobit.html)
- [http://www.isaca.org](http://www.isaca.org)
- [http://www.sarbanes-oxley.com](http://www.sarbanes-oxley.com)
- [http://www.cfo-direct.com](http://www.cfo-direct.com)
- [http://www.itgovernance.org](http://www.itgovernance.org)
- [http://www.auditnet.org/docs/CMbp.pdf](http://www.auditnet.org/docs/CMbp.pdf)