Incorporate CMMI with Corporate Governance Using Enterprise Software Change Management Solutions

Tim Ruzbacki, Sr. Process Consultant
MKS Software Inc.

4th Annual CMMI Technology Conference, Denver CO
Before We Get Started...

- 15 years in process engineering and configuration management
- Helped create in-house CM system at GE Information Services
- Helped move GEIS to level 2 CMM
- Led global CMM Process Improvement effort at Ford Motor Company
- 3 years developing and directing an enterprise configuration management practice for a national consulting organization
- Frequent speaker on SCM and process improvement, including 2004 ACDM conference and 2003 & 2002 National SEPG conferences
- Reviewer / Contributor for SPIBOK (Software Process Improvement Book of Knowledge)
Agenda

- Current Governance Climate
- Relationship Between Governance and Process Improvement Frameworks
- How CMMI Compliments IT Control Objectives
- Sarbanes-Oxley Requirements & IT Control Objectives
- The Role of Enterprise Software Change Management in Supporting CMMI & IT Control Objectives
- Summary
- Q & A
Current Governance Climate

- 93% of business leaders recognize that IT is important for delivering business strategy
- 93% of organizations suffer some sort of IT operational problems
- 40% cite inadequate performance/risk management
- 80% recognize that better governance, if even through a partial solution, is needed

Governance Frameworks, Models and Regulations

- Sarbanes-Oxley
- COSO
- ITIL
- CMMI
- COBIT
- ISO
- Others

SEC Regulation
Corporate Governance
IT Governance
Governance Frameworks, Models and Regulations

- Overlap exists between quality frameworks, however, in most cases they do not conflict
- For example, IBM uses ISO 9000, CMM, ITIL, Six Sigma and homegrown quality programs simultaneously

“Quality Model Mania”, Computerworld, Gary H. Anthes, March 8, 2004
http://www.computerworld.com/printthis/2004/0,4814,90797,00.html
Governance Frameworks, Models and Regulations – CobiT (Control Objectives for Information Technology)

- **Strengths:**
  - Good checklist for IT - enables IT to address risks not explicitly addressed by other frameworks and to pass audits
  - Can work well with other quality frameworks

- **Limitations:**
  - Says what to do but not how to do it
  - Does not deal directly with software development or IT services
  - Does not provide a roadmap for continuous improvement

- **Therefore...**

“Quality Model Mania”, Computerworld, Gary H. Anthes, March 8, 2004
http://www.computerworld.com/printthis/2004/0,4814,90797,00.html
Governance Frameworks, Models and Regulations – CMMI

- **Therefore...** CMMI is the perfect complement to CobiT
- CobiT pinpoints the need for certain controls and CMMI puts them into place
- Auditors questions can often be satisfied by pointing to aspects of CMMI
  - CMMI is very detailed and geared mostly to software development
  - Focuses on continuous improvement
  - Can be used for self-assessment

“Quality Model Mania”, Computerworld, Gary H. Anthes, March 8, 2004
http://www.computerworld.com/printthis/2004/0,4814,90797,00.html
Sarbanes-Oxley Requirements

- Report to shareholders that the financial results are accurate
- Establish and document internal controls over processes and systems that produce financial statements
- Prove to auditors that the controls are in place and working as designed
- Report to shareholders that the above is the case
10 Threats to Sarbanes-Oxley Compliance

1. Lack of an enterprise-wide, executive-driven internal control management program
2. Lack of a formal enterprise risk management program
3. Inadequate controls associated with the recording of non-routine, complex, and unusual transactions
4. Ineffectively controlled post-merger integration
5. Lack of effective controls over the IT environment
6. Ineffective financial reporting and disclosure preparation process
7. Lack of formal controls over the financial closing processes
8. Lack of current, consistent, complete and documented accounting policies and procedures
9. Inability to evaluate and test controls over outsourced processes
10. Inadequate board and audit committee understanding of risk and control

* According to Deloitte – “10 Threats to Sarbanes-Oxley Compliance”
12 Key IT Control Objectives

1. Complete secure versioning & audit history of software, process, policy, and processes change
2. Developing a formal systems development methodology
3. Requirements management with user and IT approvals
4. Maintenance and versioning of project documentation
   - Systems requirement definition
5. System acquisition and change approach addressing:
   - Security risks
   - Data conversion
6. Ensuring separation of development from production activities
12 Key IT Control Objectives

7. Process modeling and automation
8. Rigorous testing including user cases
9. Control over movement of applications by development personnel from test to production
   ▪ Automated approval process ensuring management review and approval of IT solutions prior to implementation
10. Post implementation review process for system modifications made in an emergency
11. Enforcement of formal policies and procedures that define system security
12. User account security parameters are in place and enforced
Process Model Selection Framework

Source: Gartner Inc., Stamford, Conn.
Benefits of CMMI & Process Maturity

- **Level 1: Performed**
  - Focus: Ad hoc process
  - Benefits: Inconsistency, rework

- **Level 2: Managed**
  - Focus: Control commitments and baselines
  - Benefits: Schedule, reduced cycle times

- **Level 3: Defined**
  - Focus: Common practices, shared experience, comparable data
  - Benefits: Cost, function, quality, productivity

- **Level 4: Quantitatively Managed**
  - Focus: Stable processes, continuous adjustments, good metrics
  - Benefits: Predictability, reuse, quality management

- **Level 5: Optimizing**
  - Focus: Continuous improvement of process and product
  - Benefits: Business control, change management

- Source: “IT Trends in Enterprise Software Development”, Gartner Consulting
CMMI Compliments IT Control Objectives

- **Level 2 KPA’s**
  - Requirements Management
  - Project Planning
  - Project Monitoring and Control
  - Supplier Agreement Management
  - Measurement and Analysis
  - Process and Product Quality Assurance
  - Configuration Management
CMMI Compliments IT Control Objectives

- **Level 3 KPA’s**
  - Requirements Development
  - Technical Solution
  - Product Integration
  - Verification
  - Validation
  - Organizational Process Focus
  - Organizational Training
  - Integrated Project Management
  - Risk Management
  - Integrated Supplier Management
  - Decision Analysis and Resolution
CMMI Compliments Control Objectives

- The following control objectives map most closely to level 2 & 3 KPAs:
  - Complete secure versioning & audit history of software, process, policy, and processes change
  - Developing a formal systems development methodology
  - Requirements management with user and IT approvals
  - Maintenance and versioning of project documentation
    - Systems requirement definition
  - Ensuring separation of development from production activities
  - Post implementation review process for system modifications made in an emergency
The Role of Enterprise SCM in Supporting CMMI & IT Control Objectives

- Enterprise SCM not only supports the CMMI KPA’s that map closely to CobiT but also supports these IT control objectives:
  - Process modeling and automation
  - Control over movement of applications by development personnel from test to production
    - Automated approval process ensuring management review and approval of IT solutions prior to implementation
The Role of Enterprise SCM in Supporting CMMI & IT Control Objectives

- Requirements Management as an extension of core SCM functionality – continuous flow through lifecycle
- Enforces and automates variety of processes – relaxed through to rigid
- Automated audit trail for all change
- Ensures releases and configurations are repeatable, secure and protected
- Ensures only planned software change is deployed to production
- Enables quick recovery of a system should errors be introduced
## Requirements Traceability & Visibility

### Overview

#### Summary
Data should be collected in multiple guided steps.

#### Category
Standard

### Status

- **Project:** ABC Tools/Savings
- **Assigned User:** Manager/Management
- **State:** Reuse
- **Privacy:** High
- **Version:** 1.1

### Details

Start: MKS Requirements 2005

### Relationships View
- **User Requirement:**
  - 1. User Requirement: Increase sales of add-on product
  - 2. Feature: Add future Values Section
  - 3. User Requirement: All materials seen by customers
  - 4. Feature: Graphics must follow corporate style guidelines
  - 5. User Requirement: Savings must be clear
  - 6. Feature: Make future values separate or clear
  - 7. User Requirement: Savings tool needs documentation

### Issue Overview
- **Project:** Form 505
- **Title:** ABC Financial
- **Created:** System Administrator
- **Modified:** System Administrator

### Fields
- History
- Relationships
- Attachments

### Example
- **Example Field:** ABC Financial
- **Example Value:** Form 505

---

*This image is a screenshot of a software interface for requirements management, demonstrating features for traceability and visibility.*
Enforce Development Lifecycle Methodology
- Model & Automate A Variety of Processes
The Role of Enterprise SCM in Supporting CMMI & IT Control Objectives

- Management visibility across the global IT organization – concise reports & metrics
- Provides for analytical quality measures – measures progress and activities over time
- Granular security model – permissions defined at the user, role and project levels
- Ensures outsourcers work on only the critical project at hand & that access to source code and intellectual property is secured at the individual, file, project levels
Process and Change Management

- Define and enforce unique processes
- Requirements management
- Issue tracking
- Approvals, notifications, to-dos, escalation
- Metadata collection
- Reporting

- Flexible processes
- Understands about artifacts
- Delivers visibility

- Automates workflow
- Enforces review cycles
- Automated audit trail
### Procedures Under Version Control

<table>
<thead>
<tr>
<th>Stage</th>
<th>Description</th>
<th>Reviewed By</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Master project schedule exists, identifying Development, QA, and Documentation activities for all committed features and milestone dates. Provide all schedules to Project Manager. Create integrated project schedule and post it on the project page.</td>
<td>Development, QA, Documentation</td>
<td>YES</td>
</tr>
<tr>
<td>5</td>
<td>Risks have been identified and mitigation strategies developed. Identify risks and mitigations. Produce risk mitigation plan. Approve risk mitigation plan.</td>
<td>Development, QA, Docs</td>
<td>YES</td>
</tr>
<tr>
<td>6</td>
<td>A tracking mechanism using issue trends exists to monitor project status. Issue trend charts accessible via project page. QA defect analysis in place and accessible.</td>
<td>Project Manager, QA</td>
<td>YES</td>
</tr>
</tbody>
</table>

**Evaluation Team**

<table>
<thead>
<tr>
<th>Evaluation Team</th>
<th>Name</th>
<th>Title</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Product Management</td>
<td>Colin Doyle</td>
<td>Product Manager, PI</td>
<td>July 25, 2003</td>
</tr>
<tr>
<td>Development</td>
<td>Jeff Smith</td>
<td>V.P., R&amp;D</td>
<td>July 24, 2003</td>
</tr>
<tr>
<td>Project Management</td>
<td>Blair Ernest</td>
<td>Project Manager</td>
<td>July 24, 2003</td>
</tr>
<tr>
<td>QA</td>
<td>Phil Ruby</td>
<td>Director- Quality Assurance</td>
<td>July 25, 2003</td>
</tr>
<tr>
<td>Global Customer Care</td>
<td>Not Applicable</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Page Revision Information**

- $Author: colin $  
- $Date: 2003/07/25 14:14:00 +0000 $  
- $Revision: 1145 $  
- $Source: mohandocs/PI/Project_Management 5 $
Provide for Independent Audit
– Complete Audit Trail for Change

<table>
<thead>
<tr>
<th>Field</th>
<th>Original Value</th>
<th>New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Add impact analysis to model</td>
<td></td>
</tr>
<tr>
<td><strong>State</strong></td>
<td>Submit</td>
<td></td>
</tr>
<tr>
<td><strong>Project</strong></td>
<td>IABC Tools</td>
<td></td>
</tr>
<tr>
<td><strong>Description</strong></td>
<td>iSeries add impact analysis</td>
<td></td>
</tr>
</tbody>
</table>

**Modified by Rob Butter (devbh) on Apr 13, 2004 6:10:19 PM**

**Modified by Rob Butter (devbh) on Apr 13, 2004 6:10:47 PM**

**Assigned User**  Rob Butter (devbh)

**Modified by Rob Butter (devbh) on Apr 13, 2004 6:12:19 PM**

<table>
<thead>
<tr>
<th>Field</th>
<th>Original Value</th>
<th>New Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>State</strong></td>
<td>In Development</td>
<td></td>
</tr>
<tr>
<td><strong>Priority</strong></td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td><strong>Planned Release</strong></td>
<td>PDM 1.0</td>
<td></td>
</tr>
<tr>
<td><strong>Development Type</strong></td>
<td>Strategic</td>
<td></td>
</tr>
<tr>
<td><strong>Release Type</strong></td>
<td>Full</td>
<td></td>
</tr>
<tr>
<td><strong>Classification</strong></td>
<td>New Capability</td>
<td></td>
</tr>
<tr>
<td><strong>Release Planning</strong></td>
<td>R1</td>
<td></td>
</tr>
<tr>
<td><strong>Feature Specification</strong></td>
<td><a href="http://">Link</a></td>
<td></td>
</tr>
</tbody>
</table>

**Modified by Rob Butter (devbh) on Apr 13, 2004 6:17:09 PM**

**Modified by Rob Butter (devbh) on Apr 13, 2004 6:18:28 PM**
Software Configuration Management

- Tightly integrated to process management
- Configurations
- Versioning
- Release management
- Deployment tracking
- Change Packages
- History tracking
- Audit logs

- Visual diff/merge
- Parallel development
- Geographically distributed development

- Manages all artifacts
- Controls versions
- Controls configurations
Enforceable Review Process
Securely Deploy Change into Production

Change Requests

Build & Deploy

Generate C.P. List

Apply C.P.’s

Retrieve Source

Build

Archive Built Objects

Copy to Target

Prepare on Target

Install on Target

SIT

UAT

PROD
Management Dashboard – Provides Concise Reports & Metrics
Analytical Quality Measures

Critical Items Report - Submitted in Last 7 Days

<table>
<thead>
<tr>
<th>ID</th>
<th>Modified Date</th>
<th>Summary</th>
<th>State</th>
<th>Assigned User</th>
<th>Prior</th>
</tr>
</thead>
<tbody>
<tr>
<td>54</td>
<td>18/03/2004</td>
<td>Grammar error in the amortization calculator</td>
<td>In Development</td>
<td>David Martin (SMARTy)</td>
<td>Critical</td>
</tr>
<tr>
<td>32</td>
<td>29/04/2003</td>
<td>Need to formalize the software project planning process</td>
<td>In Progress</td>
<td>project_manager project_manager</td>
<td>Critical</td>
</tr>
</tbody>
</table>

Group Total: Project = Stock

<table>
<thead>
<tr>
<th>ID</th>
<th>Modified Date</th>
<th>Summary</th>
<th>State</th>
<th>Assigned User</th>
<th>Prior</th>
</tr>
</thead>
<tbody>
<tr>
<td>30</td>
<td>09/04/2003</td>
<td>Develop QA audit policies/procedures for requirements management activities</td>
<td>In Progress</td>
<td>qa_manager qa_manager</td>
<td>High</td>
</tr>
</tbody>
</table>

Group Total: Project = Product Delivery Model (PDM)

Defect Trend Rate

The amortization calculator:
- Investigate developer developer Critical
  - Short Term Defect
  - Submit

Group Total: Project = Amortization
Ensure Systems Security With Enterprise-Level Security Model

- Provides granular security
  - Define permissions at the user, role, or project levels
- Dynamic Groups (role-based permissions)
  - Provides administrators a high degree of flexibility by defining user permissions (i.e. Project Manager) according to the project they are working on
Manage Supplier & Third Party Services - Outsourced Development Control

States only visible to Development Manager:
- Submit
- Investigate
- Reject
- Defer
- Cancel

States only visible to offshore developers or consultants:
- In Development
- Development Done
- Code Review Done
- Add to Build
- Failed QA
- Verified

States only visible to local development group:
- Built
Sarbanes-Oxley, CMMI & Enterprise SCM

**Audience**
- CEO
- CFO
- CIO
- VP IT
- VP Operations
- VP Development
- Project Leads

**Business Challenge**
- **Regulatory Compliance**
  - Management visibility into IT
  - Audit compliance
  - Risk minimization
- **CMM/CMMI and Audit Performance**
  - Traceability, audit trails
  - Automated, repeatable and enforcable process
  - Security
- **Project Execution**
  - Coordination, control, integration

**Solution**
- Policies and procedures on IT governance
- Management reporting
- Integrated process management, reporting & process change control
- Process-centric software configuration management
Analyst Recommendations

“Process-centric software configuration management (SCM) can be leveraged to help with Sarbanes-Oxley compliance. By using the issue management and workflow support provided by SCM systems directly, any existing business process (not necessarily a software development process) can be automated, with direct tracking of all work completed, workflow integration with human beings, and full audit trails...

...Companies with a strategic governance initiative, or those companies that have to meet regulatory and auditory compliance that goes beyond financial reporting into their very development processes, should investigate process-centric SCM for the reasons given above.”

- Uttam Narsu, Principal Analyst, Forrester Research
Enterprise SCM Can Help…

- Define, model, enforce and automate processes from requirements capture through to deployment
- Provide full audit trails
- Allow global development teams to collaborate in real-time
- Providing tight security for offshore and outsourced work
- Give management visibility into global development activity with a Management Dashboard that provides clear and concise reporting

... to more quickly achieve higher levels of CMMI and satisfy IT control objectives thus improving IT and Corporate Governance
Q & A

Tim Ruzbacki
Ph: 1-800-633-1235 ext. 5117
truzbacki@mks.com