Achieving Capability Maturity Model Integration (CMMI) maturity level 4

Using the IBM Rational Unified Process for Compliance Management Plug-in for and other tools for compliance, risk management, and governance processes

Judith M. Myerson

February 27, 2007

Do you want to know what the missing overall stories are about CMMI? Judith M. Myerson gives an overview of the CMMI with a focus on compliance, risk and governance at each maturity level, and shows you what IBM Rational Software Solutions help achieve maturity 4. She briefly covers the hybrid approach by overlapping CMMI with Control Objectives for Information and related Technology (COBIT)

Introduction

In 'An overview of IT frameworks,' the first of the Managing Compliance series on developerWorks Rational, I talked about what IT frameworks are about and how they dictate business processes needed to meet regulatory requirements. I compared standard frameworks, including COBIT® and CMMI®, and showed how you can customize a framework.

In 'Automating COBIT business processes using IBM Rational Portfolio Manager,' the second of the series, I pointed out that COBIT is an IT governance framework that helps to ensure proper control and governance over information and the systems that create, store, and manipulate IT. COBIT provides a framework for putting controls in place to ensure you are compliant with regulations, such as the Sarbanes Oxley (SOX Act) and Basel.

CMMI (published by the Software Engineering Institute at Carnegie Mellon University in 1991) is a set of integrated models. They include software development, system engineering, and integrated product and process development, people and other initiatives on process improvement across a project, a division, or an entire organization.

In this third article of the series, I will talk about what are missing from overall stories on CMMI, how you can achieve maturity level 4 for the missing parts: compliance, risk, and governance using IBM RUP for Compliance Management Plug-in and other Rational tools. I will also briefly cover how CMMI can overlap COBIT.
Missing parts

The missing parts from the overall stories on CMMI are the processes of compliance, risk, and governance. To include these processes, the first step is to establish an overall goal on reaching the fourth maturity level of this model. Let's take a look at the goal for each process type:

- The risk management goal is to measure and control risks so that risks can be mitigated to a specified acceptable level. When new risks enter the picture, we need to update the goal to ensure these risks combined with the existing ones will stay at that specified acceptable level.
- The compliance goal is to measure and control regulatory compliance, such as SOX, so that the executives will deliver information on time and within budget. The system providing the information must have failsafe capabilities and sufficient resources. If the system does not have those capabilities, the executives will have to pay penalties for compliance violations due to lack of control, inadequate measurement techniques, software development problems, and failures due to system overloads.
- The governance goal is to manage the governance of processes and systems by which an organization operates, so that the executives can organizationally comply with the regulations on time and within budget. If there are organizational problems of complying with regulations, the executives will pay penalties for compliance violations.

CMMI overview

CMMI has five maturity stages or levels: initial process, managed process, defined process, quantitatively managed process and optimized process. All requirements for the previous stage level must be satisfied before we proceed to the next stage of the model. No maturity stages can be skipped.

You can achieve maturity stage/level 4 by using IBM® Rational® Software solutions including their Compliance Management solution. They are Rational Unified Process (RUP), to provide a configurable process framework, RUP for Compliance Management Plug-in V1.0 (Beta) to create your organization’s unique compliant development process to maintain IT systems; Rational ClearCase® working with Rational ClearQuest® to provide a change and configuration management solution; and Rational RequisitePro®, a requirements and use case management tool to address project goals. You should start managing changes and configurations at maturity level 2 and track its progress until you achieve the goal for maturity level 4.

At maturity level 1, processes are usually ad hoc and chaotic. The organization usually does not provide a stable environment. While the maturity level 1 organizations often produce products and services that work however, they frequently exceed the budget and schedule of their projects. These organizations tend to abandon processes of compliance, risks, and governance in time of crises, and are not able to repeat their past successes. Let’s take a look at the next four maturity levels, their definitions and to what extent Relational software tools can be used to achieve higher level maturity.

Level 2: Managed

Processes are characterized by projects and often reactive. The projects of the organization have ensured that requirements for compliance, risk and governance at the project level are managed
and that processes are planned, performed, measured, and controlled. The existing practices are retained during times of stress. When these practices are in place, projects are performed and managed according to their documented plans.

The standards, process descriptions, and procedures differ in each instance of the process of managing risk requirements in identifying and valuating the assets, identifying the vulnerabilities, testing the controls, determining risk impacts and implementing additional countermeasures. Likewise, they vary in each instance of the process of managing requirements for SOX compliance in planning, measuring and controlling cost and access controls, and collecting and archiving event logs. The standards, process descriptions, and procedures differ in each instance of the process of managing the requirements for SOX governance on the code of ethics for senior officers, general exemptions, and audit standards.

RUP does not provide sufficient coverage of the Supplier Agreement Management (SAM) process area and the generic goal Institutionalize a Managed Process (IMP). These tools do not implement the SAM process area and do not consider staff training in the IMP process area to meet broader organizational needs. RUP for Compliance Management Plug-in are useful in managing requirements of the compliance and governance processes, but are limited by what RUP does not cover. As shown in Figure 1, organizations can use CMMI requirements to supplement the RUP plug-in in these two areas to achieve Level 2 maturity.

Figure 1. Level 2 maturity implementation

Level 3: Defined

The organization is proactive, and has achieved all the specific and generic goals of the process areas assigned to maturity levels 2 and 3. Processes are well characterized and understood, and are described in standards, procedures, tools, and methods. The organization’s set of standard processes is established and improved over time. These standard processes are used to establish consistency among the projects across the organization. Projects establish their defined processes by tailoring the organization’s set of standard processes according to tailoring guidelines to suit a particular project or organizational unit. As a result, the processes that are performed across the organization are consistent except for the differences allowed by the tailoring guidelines.

For risk processes, the organization is proactive in achieving the goal of risk management and decision analysis and resolution processes areas. Risk management projects can be grouped into four categories: PCs, servers, mainframes and networks, according to organization standards, procedures, and guidelines. This means projects established their defined processes of assessing and managing risks by tailoring the organization’s set of standard processes to each risk management project. For compliance processes, the organization is proactive in achieving the goal of verification, organization process focus and organizational process definition.
process areas. For governance processes, the organization is proactive in organizational focus, organizational process definition and organization environment for integration process areas.

However, the RUP does not provide sufficient coverage for Technical Solution process area needed for risk, compliance and governance processes. The RUP plug-in in managing the compliance and governance processes establishes consistency across the projects but is limited by the RUP’s coverage. As shown in Figure 2, organizations using the tools can use CMMI requirements to supplement the RUP plug-in to achieve Level 3 maturity.

**Figure 2. Level 3 maturity implementation**

![Figure 2. Level 3 maturity implementation](image)

**Level 4: Quantitatively managed**

Processes are measured and controlled. Sub-processes are selected that significantly contribute to overall organizational process performance and quantitative project management areas. These selected sub-processes are controlled using statistical and other quantitative techniques. Quantitative objectives for quality and process performance are established and used as criteria in managing processes. Quantitative objectives are based on the needs of the customer, end users, organization, and process implementers. Quality and process performance is understood in statistical terms, and is managed throughout the life of the processes.

For instance, the organization controls the selected sub-processes of compliance, risk and governance to establish quantitative objectives and use them as criteria for managing the processes. Quantitative objectives are established based on statistics from the sub-processes of risk assessment on controlling and comparing the Annual Loss Expectancy before and after implementing the countermeasures. Quantitative objectives are established for compliance and governance sub-processes on controls to eliminate penalties for violations for failure to comply with the SOX Act.

It is not known what parts of the process areas the RUP does not cover. While the RUP plug-in is useful in managing compliance from some organizational perspectives, it may be limited by what the RUP does not cover. At this level RUP does not cover staff training to meet broader organizational needs at Level 2. Therefore, as shown in Figure 3, organizations using the tools for Levels 2 and 3 can use CMMI requirements to supplement the RUP plug-in to achieve Level 4 maturity.
Achieving Capability Maturity Model Integration (CMMI) maturity level 4

Figure 3. Level 4 maturity implementation

Level 5: Optimizing the process

The focus is on process improvement. Processes are continually improved based on a quantitative understanding of the common causes of variation inherent in processes. Maturity level 5 focuses on continually improving process performance through both incremental and innovative technological improvements. Quantitative process-improvement objectives for the organization are established, continually revised to reflect changing business objectives, and used as criteria in managing process improvement. The effects of deployed process improvements are measured and evaluated against the quantitative process-improvement objectives. Both the defined processes and the organization's set of standard processes are targets of measurable improvement. Organizations must rely entirely on the CMMI requirements to supplement the RUP for Compliance Management plug-in.

Hybrid processes

You can develop a hybrid process by overlapping CMMI with COBIT. CMMI addresses 12 out of 34 COBIT processes in four domains. They are Plan and Organize (PO), Acquire and Implement (AI), Deliver and Support (DS) and Monitor and Evaluate (ME).

CMMI focuses on three PO processes: manage quality, access and manage IT risks, and manage projects. It looks at three AI processes: acquire and maintain application software, manage changes, and install and accredit solutions and changes. For the DS domain, the model addresses four processes: educate and train users, manage the configuration, manage problems, and manage data. CMMI only considers one ME process; that is, monitor and evaluate IT performance.

IT processes is one of three components of the COBIT "cube." The other two components are IT resources and information criteria (business requirements). IT resources are managed by the IT processes to achieve IT goals that respond to business requirements. It is in the business processes that CMMI dictates the way that IT resources are managed by IT processes to meet business requirements.

Conclusion

Incorporating the compliance, risk and governance processes into the CMMI requires planning ahead of time. You can achieve the goals of controlling and measuring these three processes at maturity level 4 by using the IBM RUP for Compliance Management Plug-in and supplementing them with CMMI requirements in the process areas needed for your organization. You can also achieve a hybrid approach by overlapping CMMI with COBIT.
You should communicate with a team of system administrators, business analysts, and developers on the issues of bridging the gap between technical issues, business risks, and performance compliance requirements without incurring system overloads and penalties for violations. You will find that resolving these issues makes your job much easier, especially if you are managing multiple projects and are constrained by limited resources, risks, compliance, and governance requirements. The administrators will find that resolving the issues makes their job of managing and administering the software development projects much easier.
Related topics

- Read Markus Grundmann's developerWorks article: A CMMI Maturity Level 2 assessment of RUP
- To learn more about IBM Rational Unified Process, visit the developerWorks Rational Unified Process and Rational Method Composer page.
- To learn more about IBM Rational ClearCase, visit the developerWorks Rational ClearCase page.
- To learn more about IBM Rational ClearQuest, visit the developerWorks Rational ClearQuest page.
- To learn more about IBM Rational RequisitePro, visit the developerWorks RequisitePro page.
- To learn more about CMMI, visit the Carnegie Mellon Software Engineering Institute website.

© Copyright IBM Corporation 2007
Trademarks
(www.ibm.com/developerworks/ibm/trademarks/)