Capability Maturity Models and Outsourcing: A Case for Sourcing Risk Management

By Charles McKinney, CBCP, Six Sigma Black Belt

Moving information technology (IT) functions to offshore providers is popular and controversial. With 74 percent of buyers satisfied with their outsourcing efforts and 64 percent expected to increase their use of service providers in the future, according to a 2004 DiamondCluster International survey, IT outsourcing is here to stay. Consequently, organizations need to invest in managing sourcing risk across the life cycle of their relationships with their external service providers (ESPs).

Sourcing risk refers to an organization’s exposure to its ESPs’ performing at a level below what is required and suffering consequences that could include unplanned costs, lost productivity, dissatisfied customers, brand deterioration, accounting errors, and failure to comply with laws and regulations. Recent regulatory developments heighten the need. For example, the US Sarbanes-Oxley Act’s requirements to design and maintain processes with effective internal controls extend to ESPs performing critical operations on behalf of a company.

Organizations manage sourcing risk by developing a clear understanding of their needs, designing steps to standardize and monitor vendors’ performance, and integrating these controls with their IT governance and management practices. Being proactive at the vendor selection stage is a critical success factor that determines the effectiveness of the sourcing risk management program, the value of outsourcing deals and the likelihood of unforeseen problems arising. Trends in ESPs’ adoption of capability maturity models, a popular category of best practices, provide a useful illustration—showcasing contributions that IT auditors can make and highlighting practical steps that organizations can take to be successful.

Offshoring, Software Factories and Best Practices

An immediate benefit of moving application development to an offshore ESP is lower labor costs. Outsourcing can also improve flexibility by reducing headcount and linking contractor compensation to projects with deliverables. Over the next five years, comparatively high wage inflation for IT professionals will diminish the labor cost advantage that popular offshore locations enjoy today. Furthermore, language barriers, travel costs, higher-than-planned overhead to manage outsourcing relationships and other factors can unexpectedly increase outsourcing costs.

While many ESPs use their labor cost advantage as a door opener, they tend to promote sustainable advantages associated with provisioning application development from a software factory serving a large client base. Demonstrating superior capabilities helps ESPs overcome skepticism that moving offshore is a long-term risk. Very often their marketing strategies emphasize quality, and an increasing number of ESPs are establishing internal quality management programs, basing them on best practices and assessing their internal controls with a goal of passing a critical benchmark that the marketplace will recognize and trust.

For any organization, a commitment to quality can have a positive impact beyond contributing to brand equity. GE’s adoption of Six Sigma and its contribution to top- and bottom-line performance are legendary. The Software Engineering Institute at Carnegie Mellon University (Pennsylvania, USA) reports that investment in adopting software development best practices can pay dividends. It reports that many organizations experience productivity gains of 35 percent, defect rate reductions as high as 90 percent and positive return on investment. Realizing these benefits depends on how adoption of best practices is carried out (see figure 1).

Adoption of best practices is complicated by the lack of a de facto standard. In the systems engineering realm, there are numerous models from which to choose. Best practices with significant traction include:

- **COBIT**—Familiar to IT auditors, Control Objectives for Information and related Technology (COBIT) adoption has grown rapidly since the Sarbanes-Oxley Act took effect in the US. COBIT defines 34 high-level control objectives and more than 300 detailed objectives that assist organizations with evaluating and improving the maturity of their managerial, operational and technical controls over IT assets.

  COBIT incorporates capability maturity model concepts, and IT Control Objectives for Sarbanes-Oxley, based on COBIT, was released to support compliance.

- **ITIL**—Sponsored by the UK’s Office of Government Commerce, the IT Infrastructure Library (ITIL) is a compendium of best practices for managing IT service delivery and service support. ITIL adoption is common in Europe, and many independent software vendors engage third parties to certify that their products are ITIL-compliant.

- **ISO 9000**—The International Organization of Standardization (ISO) publishes the ISO 9000 series of standards, which many organizations adopt as a basis for their internal quality management systems governing IT and non-IT functions. Organizations that comply with ISO 9000...
With a cornucopia of frameworks to choose from and pressure to deliver results quickly, adopting IT best practices can be a risky business. It can pay off with strong commitment and attention to five critical success factors: leadership, acceptance, learning, empowerment and ongoing governance.

**Leadership**—Tone at the top sets the context for how an organization embraces best practices. Official messages, off-the-record comments, nonverbal signals, and the actions of the CEO, CFO, CIO and senior IT managers signify to middle-level IT managers, technology professionals and end users how serious they are about improving IT performance. Consistent leadership in establishing a program to improve quality, selecting best practices and aligning organizational processes with the chosen framework significantly raise the odds of success.

**Acceptance**—Leadership combined with having a compelling reason to improve IT performance facilitates organizational readiness to adopt best practices. Commitment to change by key stakeholders—IT managers, engineering staff, software development groups, infrastructure groups, user support personnel, project managers and customers impacted by IT—determines the fate of software process improvement efforts, no matter how compelling the need or elegant the solution. Successful organizations invest in change management, particularly communications, training and collecting feedback to manage expectations.

**Learning**—Organizations known for pioneering best practices recognize that continuous improvement goes beyond reaching quarterly and yearly targets. It depends on personal awareness of how individual habits affect growth and how improving performance is an inner journey beyond applying new tools and technical knowledge. Leaders foster growth through a culture of learning—investing in training programs and promoting the importance of collaborative, on-the-job education in building critical skills, attitudes and habits.

**Empowerment**—Achieving high maturity levels depends on key stakeholders being empowered to control outcomes beyond complying with policies. Too often, organizations charter process improvement teams and task IT professionals to accomplish milestones without relinquishing the authority necessary to achieve full-potential results. Many organizations that report high return on investment in adopting best practices attribute their success to finding ways to empower people by making them “process owners” without circumventing internal control.

**Ongoing governance**—The adoption of best practices can be expensive. One organization recently spent more than US $10,000 per person in its applications groups on capability maturity model implementation. The costs and the stakes require ongoing governance—oversight by an executive sponsor, coordination by a dedicated project manager, and scrutiny through performance measures that quantify costs, measure benefits and support risk management.

Source: Author

---

**Figure 1—Critical Success Factors When Adopting IT Best Practices**

With a cornucopia of frameworks to choose from and pressure to deliver results quickly, adopting IT best practices can be a risky business. It can pay off with strong commitment and attention to five critical success factors: leadership, acceptance, learning, empowerment and ongoing governance.

**Leadership**—Tone at the top sets the context for how an organization embraces best practices. Official messages, off-the-record comments, nonverbal signals, and the actions of the CEO, CFO, CIO and senior IT managers signify to middle-level IT managers, technology professionals and end users how serious they are about improving IT performance. Consistent leadership in establishing a program to improve quality, selecting best practices and aligning organizational processes with the chosen framework significantly raise the odds of success.

**Acceptance**—Leadership combined with having a compelling reason to improve IT performance facilitates organizational readiness to adopt best practices. Commitment to change by key stakeholders—IT managers, engineering staff, software development groups, infrastructure groups, user support personnel, project managers and customers impacted by IT—determines the fate of software process improvement efforts, no matter how compelling the need or elegant the solution. Successful organizations invest in change management, particularly communications, training and collecting feedback to manage expectations.

**Learning**—Organizations known for pioneering best practices recognize that continuous improvement goes beyond reaching quarterly and yearly targets. It depends on personal awareness of how individual habits affect growth and how improving performance is an inner journey beyond applying new tools and technical knowledge. Leaders foster growth through a culture of learning—investing in training programs and promoting the importance of collaborative, on-the-job education in building critical skills, attitudes and habits.

**Empowerment**—Achieving high maturity levels depends on key stakeholders being empowered to control outcomes beyond complying with policies. Too often, organizations charter process improvement teams and task IT professionals to accomplish milestones without relinquishing the authority necessary to achieve full-potential results. Many organizations that report high return on investment in adopting best practices attribute their success to finding ways to empower people by making them “process owners” without circumventing internal control.

**Ongoing governance**—The adoption of best practices can be expensive. One organization recently spent more than US $10,000 per person in its applications groups on capability maturity model implementation. The costs and the stakes require ongoing governance—oversight by an executive sponsor, coordination by a dedicated project manager, and scrutiny through performance measures that quantify costs, measure benefits and support risk management.

Source: Author

---

**An Overview of Capability Maturity Models**

Capability maturity models date back to the 1980s when the US Department of Defense contracted with Carnegie Mellon University to establish the Software Engineering Institute (SEI) as a means of improving applications developed for defense work. The Software Engineering Institute published the Capability Maturity Model for Software (CMM-SW) in 1991 and various models since then, culminating in the release of the first version of the Capability Maturity Model Integration (CMMI) framework in 2002. CMM-SW is the most popular capability maturity model today, but many organizations will transition to CMMI over the next few years because it is the standard that the Software Engineering Institute will support in the future.9

Capability maturity models support process benchmarking and continuous improvement by defining five levels of process maturity:

- **Level 1: Initial**—Application development is ad hoc or chaotic. Processes are poorly defined and undocumented. Project success is a result of individual efforts.
- **Level 2: Managed**—Projects employ basic processes to track costs, schedules and functionality with processes institutionalized across software groups. Formal adoption of techniques to measure performance has occurred and is an input to managerial activities.
- **Level 3: Defined**—Application development and other IT processes are documented, standardized and integrated organizationwide with projects always employing a version of these standard processes.
- **Level 4: Quantitatively managed**—Application development projects and processes are measured quantitatively, and managers employ statistical process control techniques to achieve and maintain high levels of quality.
- **Level 5: Optimizing**—Quantitative management tools and techniques enable continuous improvement of processes and innovation in the delivery of application development services to the business.

Each maturity level has a set of performance criteria (see...
At the highest level, there are key process areas. A key process area encompasses a broad set of internal control criteria that are critical to quality. For example, the second maturity level in CMMI and CMM-SW has key process areas for requirements management, project planning and configuration management. Each key process area has a set of goals that is specific to a type of internal control or a general characteristic of having mature processes. For example, the CMMI requirements management key process area has a specific goal for managing requirements and identifying inconsistencies with project plans and work products. A generic goal for the second maturity level to ensure processes are institutionalized as a managed process applies to requirements management and all other key process areas. Each goal has practices associated with it, and most practices further break down to subpractices and typical work products.

To stand up to a maturity level, an organization’s performance must satisfy all of the goals and key process areas of the level. This is accomplished when processes are auditable through the accumulation of project documentation, and their performance complies with each goal’s practices or equally acceptable alternative criteria. Since maturity levels build on one another, an organization wishing to stand up to the third level must comply fully with the second level, and so forth.

SEI has well-defined standards for how to assess IT processes against CMMI, CMM-SW and its other capability maturity models. For example, it published the Standard CMMI Appraisal Method for Process Improvement (SCAMPI) and the Appraisal Requirements for CMMI (ARC) for organizations employing CMMI. These guidelines define three classes of appraisals. Organizations that successfully complete a class A appraisal obtain a maturity level rating, and many of them (particularly ESPs) promote their rating as evidence of their ability to deliver high-quality software. Class B and C appraisals are less rigorous, and many organizations use them to audit projects and conduct in-flight reviews of process improvement initiatives. Figure 3 compares these three appraisal classes.

To appraise its application development processes, an organization selects projects that it will evaluate. An executive sponsor assigns a team of trained professionals to carry out the appraisal. SEI offers a robust training program to support professional development of appraisal team members, and it licenses qualified individuals to serve as authorized lead appraisal team members. Figure 3 compares these three appraisal classes.
appraisers. Lead appraisers must complete an extensive training program, meet eligibility requirements based on their experience and education, and undergo an observation where their performance leading an appraisal team is monitored. An appraisal team reviews a project by:

- Developing an appraisal method and documenting an appraisal plan, which is similar to an audit program guide
- Holding a kickoff meeting with the project team and collecting preliminary information about the project
- Gathering facts about the project by requesting and reviewing documentation, administering a questionnaire or conducting a survey, interviewing project stakeholders, and using other audit techniques, such as inspection and corroborative inquiry
- Using a common rating system and agreed-upon consensus-building procedures for the appraisal team to conclude if a project reaches the desired maturity level
- Reviewing appraisal findings and recommendations with the project team, the executive sponsor and others with a stake in the outcome
- Reporting the results to the project team and executive sponsor in the form of a final findings report with transmittal letter or in another format specified in the appraisal plan; a final findings report documents the outcome of an appraisal and provides any recommendations for improving processes

To determine if application development within a business unit, division or an entire entity stands up to a maturity level, an organization must appraise a valid, sufficient and representative set of projects. An organization’s business model, its size, a project’s value, strategic and operational risks, and how it intends to use the outcome of appraisals should influence project selection.

### Capability Maturity Model Adoption Trends

SEI tracks capability maturity model adoption through its membership. For example, it requires lead appraisers to report information about the appraisals they conduct. Using these data, SEI publishes annual profiles of CMM-SW and CMMI adoption. These profiles tabulate capability maturity model adoption by region, industry, company size and other variables. Capability maturity models were initially popular with government organizations and defense contractors. During the 1990s, organizations in many industries began using them, resulting in cross-industry adoption today.14

In 2002, 42 percent of organizations using capability maturity models were non-US companies, and between the late 1990s and 2003, the number of non-US firms reporting successful appraisals at maturity levels four and five grew at twice the rate of US firms, according to SEI data.15 India-based ESPs were early adopters of CMM-SW to differentiate themselves in the marketplace. Since the 1990s, government and industry groups in China, Hong Kong, Malaysia, the Philippines and other countries vying for ESP marketshare have actively sponsored professional organizations, conferences and training events to raise awareness of capability maturity models. Adoption of capability maturity models and commitment to obtaining maturity level four and five ratings are on the rise as a result, and also because firms in these countries want to develop credibility with Fortune 1000 buyers and overcome a perception that India-based ESPs have superior capabilities.

When outsourcing application development outside of the US, a minority of companies inquire about ESPs’ use of capability maturity models and maturity level assessments, according to Gartner Group.16 Those that do often fall into critical customer segments, and many offshoring pioneers on the buy side require ESPs to have a high maturity level rating. A recent CIO magazine article reported that many financial services firms refuse to do business with ESPs that are not at maturity level five.17 Some government agencies are setting strict standards, too. The US Department of Defense routinely uses maturity level three as a cutoff for contracting opportunities, and recently proposed legislation that would make maturity level three certification a requirement for certain types of firms doing business with the federal government.18

### Digging Deeper Into Appraisals

Asking ESPs about their adoption of best practices and the results of their capability maturity model appraisals is a useful way to learn about potential service providers’ approaches to quality. Organizations ought to be skeptical, however, when relying on capability maturity model ratings because of ambiguity about standards for the professional independence of appraisers and professional oversight of appraisals used to communicate assurance to the marketplace.

In addition to employing strict criteria when licensing lead appraisers (including a nascent, promising code of conduct), SEI requires organizations completing appraisals to report the results and provide information that will assist in reviewing the outcome for irregularities. CMMI strengthens these requirements over CMM-SW. Nevertheless, lead appraisers licensed by SEI are not subject to black-and-white standards for professional independence covering:

- **Independence from management**—Standards such as ARC and SCAMPI encourage appraisal teams to act independently and objectively in their duties. However, SEI has not released and publicized criteria mandating technical and managerial independence of appraisal teams. Many organizations conduct their own assessments and self-report the outcomes of appraisals. One company, whose identity is being kept anonymous, promoted a business unit’s CMM-SW maturity level four rating and published a letter from the organization’s lead appraiser on its web site. The letter described how appraisals within the business unit were conducted, disclosed which projects were reviewed and concluded that a maturity level four rating was warranted based on the results. Curiously, the letter did not have any corporate letterhead. Only by reading the e-mail address of the lead appraiser did it become evident that he/she was an employee of the company.
- **Independence as an attesting entity**—Self-reporting achievement of performance benchmarks is a popular marketing tactic. In the context of using reported information to rely on a third party’s internal controls, organizational independence of the entity providing an opinion about the organization having its internal controls evaluated is a critical success factor. Standards for conducting appraisals do not clearly address situations when independence as an attesting entity is necessary—such as when an organization might
promote its maturity level rating on its web site in the same way it would provide a link to information about its Systrust® seal. The lack of standards is exacerbated by the absence of a strong oversight body to enforce professional ethics in the use of capability maturity models as an assurance tool.

The behavior of ESPs in general is not being questioned, but the temptation of some firms to cut corners or misrepresent their capabilities cannot be dismissed, since pressure to expedite the certification process and reduce compliance costs can take a toll. Very often, for example, it takes seven years to institutionalize maturity level five application development processes. A Class A CMMI appraisal typically costs about US $70,000 per line of business, according to the Robert Francis Group. These shortcomings and pressures point out the risk of relying on maturity level ratings as a form of assurance and the importance of investing in due diligence during vendor selection.

A Life Cycle Approach to Managing Sourcing Risks

Many organizations treat due diligence as a one-time activity to be conducted when engaging an ESP for the first time. Others—particularly large companies with a portfolio of outsourced projects and functions—employ a life-cycle-based process that integrates due diligence with other vendor selection, performance monitoring and risk management activities. Leading life cycle approaches have four stages: vendor selection, vendor evaluation, performance measures implementation and ongoing performance monitoring.

Figure 4—Capability Maturity Model Representations

The continuous representation is used to improve the capability levels of select processes. For instance, CMMI breaks the key process areas at all maturity levels into four domains: engineering, project management, process management and support. Organizations adopting a continuous representation can improve their capability level in one or more domains. The continuous representation of CMMI gives organizations the flexibility to focus on particular areas, instead of striving for a maturity level rating.

Many organizations opt for a staged representation because it facilitates broad control of processes. ESPs that promote their CMMI maturity level rating should be appraising with the staged representation. The table below compares the two representations in CMMI.

<table>
<thead>
<tr>
<th>Comparison of CMMI Representations</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Staged Representation</strong></td>
</tr>
<tr>
<td>Organizations follow a predefined path to improve and benchmark their processes.</td>
</tr>
<tr>
<td>There is a history of use with case studies and data demonstrating return on investment.</td>
</tr>
<tr>
<td>Organizations can achieve a maturity level by completing one or more class A appraisals.</td>
</tr>
<tr>
<td>This representation is similar to CMM-SW and often used to migrate to CMMI from CMM-SW.</td>
</tr>
<tr>
<td>A maturity level rating summarizes process improvement results.</td>
</tr>
</tbody>
</table>
conducted and which projects are reviewed a condition of bidding. Organizational requirements and deal characteristics should dictate the choice of methods, including the level of effort invested in following up on information provided by ESPs in the vendor evaluation phase.

Vendor evaluation encompasses the activities that lead to selection of an ESP. Various laws, regulations and industry customs constrain how companies evaluate prospective vendors. For example, in Europe it is common to use an invitation-to-tender process. Government entities in the US have controls to ensure fair and open competition, and many other industries are subject to procurement regulations as well as purchasing policy enhancements that are necessary for effective internal control. It is common to use a request for proposal (RFP) to gather information from prospective ESPs that will be used to evaluate them, select a winner and award a contract after negotiations are concluded. An RFP gives ESPs instructions for submitting a proposal that describes their business model, services, corporate size, locations, human resources, organizational structure, management practices, technical methodologies and experience serving other firms.

Organizations spend a significant amount of time reviewing proposals, following up on information that is provided and recommending finalists to senior management decision makers. Vendor evaluation activities should employ criteria from the vendor selection strategy and use a common set of templates. Often, organizations use a quantitative scoring algorithm to compare proposals and select finalists that will be evaluated in depth. The time spent validating maturity level ratings should correspond to the importance of this factor in the decision-making equation. Techniques that work well are reviewing final findings reports and other documentation about appraisals, inquiring about quality of work with client references, and possibly assigning an internal team or independent third party to conduct a formal due diligence review of finalists’ application development practices and facilities. If a formal review is warranted, integrating capability maturity model criteria into the due diligence audit program guide is one way to validate ESPs’ reported maturity level and benchmark their capabilities.

Negotiating and executing a contract with a well-crafted service level agreement is a foundation for ensuring ongoing quality from an ESP, as long as there is attention to monitoring performance in a constructive, rational way. Best practice organizations implement performance measures as part of service level agreements with their ESPs. These key performance indicators ideally cover financial performance, project efficiency, defect rates, requirements traceability and other dimensions that are critical to quality. Instituting performance measures offers several advantages, such as relating performance to IT strategies, providing visibility to total outsourcing costs and establishing triggers to facilitate timely escalation of risks to the attention of key stakeholders. Performance measurement data can also assist in allocating quality assurance and internal audit resources dedicated to reviewing projects outsourced to ESPs.

After performance measures are implemented, performance monitoring becomes an ongoing activity. Typically, an ESP reports performance data in compliance with its service level agreement, and an organization has staff responsible for monitoring ESP performance, reporting metrics to senior management, responding to issues and supporting the resolution of problems. Some organizations—even especially organizations with a strategic dependence on their ESPs, a large portfolio of outsourced application development projects or both—budget for a number of project reviews each year to gain added assurance that processes are operating at the desired maturity level. The mix of activities to monitor performance becomes the repeatable process for sustaining the benefits of due diligence and ensuring the reliability of ESPs’ performance for as long as application development is outsourced.

**Lessons Learned for IT Auditors**

IT auditors can play a unique and valuable role in educating application development stakeholders about best practices and promoting the benefits of sourcing risk management when outsourcing is on the management agenda. In particular, IT auditors can add value by:

- Serving as an objective, independent risk advisor to audit stakeholders and senior management (e.g., members of the IT steering committee)
- Working through internal audit processes and with IT managers to help ensure that outsourcing plans are sensitive to risks inherent in outsourcing and mitigated through a sound vendor selection strategy, due diligence and ongoing performance monitoring
- Performing independent verification and validation of the vendor selection strategy that will guide the process of choosing an ESP and the criteria for relying on maturity level ratings disclosed by potential service providers in their proposals
- Participating in the vendor evaluation process in a way that provides assurance to key stakeholders that due diligence is well executed, controlled and comprehensive, and the overall vendor selection process is disciplined
- Factoring outsourced application development functions and projects into the annual risk assessment and audit plan that guides IT audit activities
- Reviewing and providing feedback on performance measures and processes to monitor ESP performance, so that sourcing risk management continues to be effective
- Integrating capability maturity models into the IT audit methods used to review projects and processes

Even more than any other group of IT professionals, IT auditors have a unique perspective on the importance of process discipline, the value of best practices and the need for professional skepticism when ESPs market compliance with best practices as evidence of their ability to deliver high-quality services. Speaking generally, the role of the IT audit function is critical to quality, and its value will grow in the future as enterprises come to depend more on technology while being subject to stricter requirements for internal control, quality and cost-effectiveness.
Endnotes

2 Harry, Mikel; Richard Schroeder; Six Sigma: The Breakthrough Management Strategy Revolutionizing the World's Top Corporations, New York, Doubleday, 2000
4 IT Governance Institute, COBIT 3rd Edition, 2000
5 van Bon, Jan; IT Service Management: An Introduction Based on ITIL, Amsterdam, The Netherlands, Van Haren Publishing, April 2005
7 Op. cit., Harry, Mikel; et al.
9 For more information about Software Engineering Institute’s decision to sunset CMM-SW and support CMMI, see www.sei.cmu.edu/cmmi/adoption/sunset.html (accessed 2 January 2005).
10 Op. cit., SEI
11 Ibid.
15 Ibid.
16 Jester, Rolf; Partha Iyungar; Dion Wiggins; “CMM in Asia/Pacific: Rapidly Changing Competitive Environment,” Gartner Group, June 2003
17 Koch, Christopher; “Bursting the CMM Hype,” CIO Magazine, 1 March 2004, p. 48-54
18 Ibid.
20 Bowles, Adrian; “Metrics for Application Development: Building the Right Systems Right Can’t be Left to Chance,” Robert Francis Group, January 2003

Charles McKinney, CBCP, Six Sigma Black Belt
is senior manager with SecureIT Consulting Group. He formerly was a senior manager at KPMG LLP in the firm’s risk advisory services practice. He leads teams that deliver IT audit and advisory services to public sector, nonprofit and financial services clients. He has expertise in planning IT strategies, designing IT architectures, reviewing information systems and IT projects, and improving cost-effectiveness and quality within the IT function. For the last three years, McKinney has focused on helping CIOs adopt IT governance, Six Sigma, capability maturity models and other best practices to improve IT performance.