

The Software Insight Tool: A Tool and Methodology for Risk Mitigation and CIO Assessments

Jerry Kastning and Jeff Herman
U.S. Army CECOM Software Engineering Center
Marilyn Ginsberg-Finner and Jim Heil
Telos Corp.

The Software Insight Tool (SIT) is a device that will guide the user in identifying and addressing software-intensive program strengths and weaknesses, as well as cost, schedule, and performance risk areas. The SIT will greatly aid management in lowering program risks and producing a product with a much greater probability of meeting the customer's requirements within cost and on schedule. The SIT is destined to become management's key guide for any risk mitigation program, both on an ongoing basis and to prepare for chief information officer (CIO) assessments and major milestone (MS) reviews. This paper describes the tool, provides background for its development, and describes how it can be used in an internal risk mitigation process, as well as in the CIO assessment process.

Mitigating Risk and Improving a Program's Health

The SIT is a vehicle that will guide the user in identifying and addressing program strengths, weaknesses, and risk areas. The SIT will improve the health of any software-intensive program throughout its life cycle — from concept exploration through development and operational support — and reduce overall program risk and total ownership costs (TOC). The key to the successful development of any system is having a sound managerial approach and asking the right questions. Acquisition program managers (PMs) now have to juggle many statutory and regulatory requirements, as well as numerous technical, performance, and cost issues, coupled with decreasing personnel and financial resources (see Figure 1).

The SIT focuses on the overall acquisition process, plans and practices, and how the acquirer and the developers structure and manage acquisition, development, and sustainment. The SIT will help PMs by providing essential insight into the health and risk of the software aspects of their program, and by providing a cost-effective risk mitigation approach across the entire set of acquisition concerns. In addition, the SIT will help the PM to prepare for the CIO assessments prior to major MS reviews.

The Army Communications-Electronics Command (CECOM) Software Engineering Center (SEC) designed and developed the SIT, in support of the Army CIO and the Army

implementation of the Clinger-Cohen Act of 1996, to address the highest risk component of most modern system development programs — the software. The vehicle's engine is a critical set of questions in the key areas associated with the acquisition, development, and support of any software-intensive program.

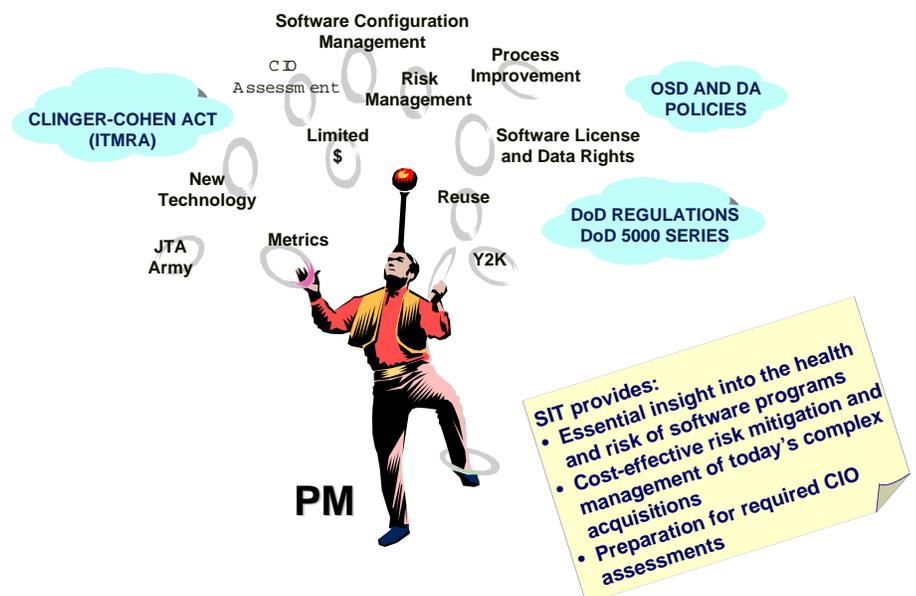
The SIT is a practical approach for risk identification when used by a PM or a software integrated product team (IPT) for ongoing or periodic internal risk mitigation reviews or preparing for major program reviews, such as CIO assessments. Using the SIT can identify cost, schedule, and performance risk areas, e.g. why program costs are increasing, why schedules are slipping, and/or where per-

formance and practices are weak. The results will yield a better managed, lower risk program and a product with a much greater probability of meeting the customer's requirements within cost and on schedule.

Risk Mitigation Through CIO Assessments

CIO assessments are performed to satisfy the requirements of Division E of the Clinger-Cohen Act (formerly the Information Technology Reform Act [ITMRA]) [1], and to comply with the subsequent policy guidance from the Office of the Secretary of Defense (OSD) [2]. At the Department of Defense (DoD) level, its CIO is responsible for

Figure 1. How much can a PM juggle?



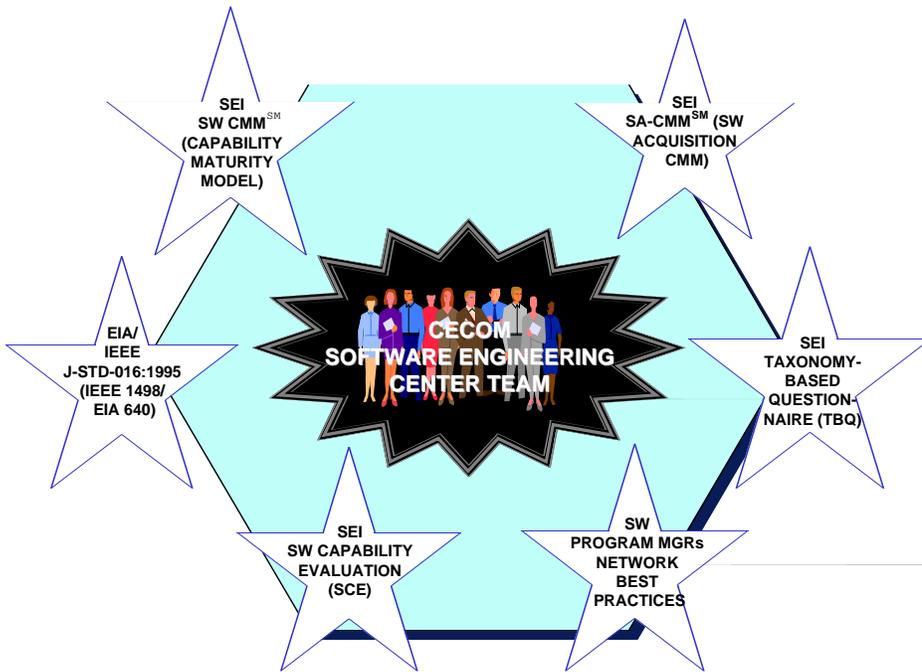


Figure 2. Sources of best practices underlying the SIT questions.

ensuring that information technology (IT) is acquired and information resources are managed within an integrated management framework, and to assess and manage the risks of DoD's IT acquisitions (including National Security Systems). Component milestone decision authorities (MDAs) and CIOs will follow similar practices for IT programs subject to their review and approval, and each service was required to provide its implementation of these requirements.

The Army implemented a formal CIO assessment process, which incorporates the Clinger-Cohen and OSD guidance into the Army's regulatory and acquisition process [3]. The Army CIO is designated to assess Army programs, and recommend to the MDA whether to continue, modify, or terminate the program. The SIT was developed to support the Army implementation, and is used to prepare for the CIO assessment.

An Expert System

The increasing complexities of system acquisition and development, coupled with shrinking resources, require not only extensive knowledge of best practices and streamlined processes, but also expert systems to help assess and satisfy the myriad program and system requirements. The SIT is a knowledge-based instrument that provides a set of questions from which

the user selects those of most importance/relevance to the current project status and issues. The SIT does not dictate a set of correct answers or actions. It facilitates identification of program risks and the subsequent planning and implementation of program improvements and risk reduction actions. The SIT is applicable whether development is in-house, by a two-party acquisition/supply agreement, by integration of existing components, by new development, or by any combination thereof.

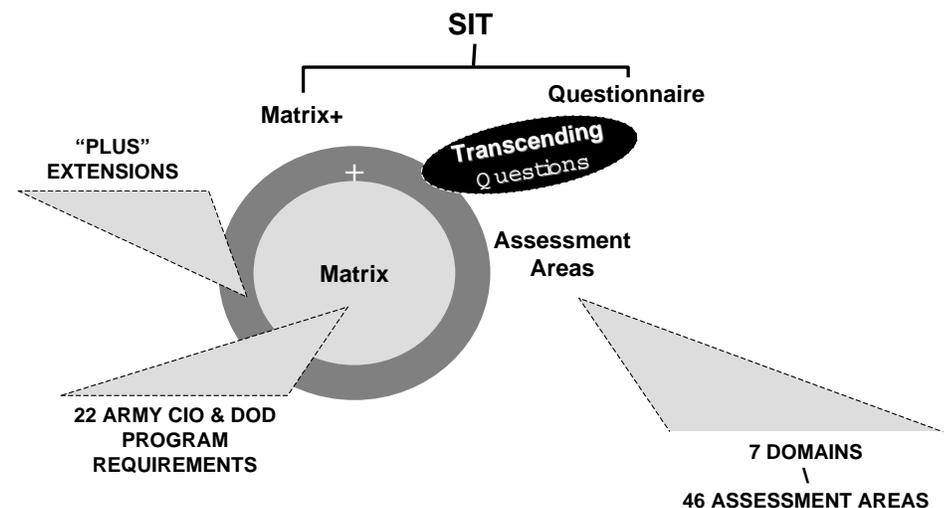
Concept of the SIT

The SIT presents a comprehensive set of questions to assist acquisition and devel-

opment management in evaluating a program against statutory and regulatory requirements (e.g. DoD 5000.2-R), as well as software acquisition best practices. DoD 5000.2-R, paragraph 4.3.5, states: "Software shall be managed and engineered using best processes and practices that are known to reduce cost, schedule, and performance risks." Use of the SIT will help accomplish the DoD 5000.2-R requirements in reducing risk and enhancing software quality [4], as well as reducing TOC. These questions can be used by Army, Air Force, and Navy System Development Offices, and federal government agencies for periodic internal program reviews to reduce software-related risk and in preparation for DoD-mandated CIO assessments or other high-level reviews.

The SIT builds on and complements well-respected sources of best practices and is intended to provide an acquirer-side perspective on plans and practices for acquisition, development, and sustainment. The major sources used for best practices are illustrated in Figure 2 [5, 6, 7, 8, 9, 10]. While there are similarities between program risk mitigation reviews and Capability-Based Assessments-Internal Process Improvement (CBA-IPs), the target is different. CBA-IPs are assessments of a developer's capabilities and maturity based on the CMMSM, while CIO assessments and program risk mitigation reviews use the SIT to assess status and risks for the entire acquisition program. The acquirer uses the SIT to assess the acquisition program, rather

Figure 3. Software insight tool structure.



- Transcending question topics:
 1. Overall life cycle approach to the software acquisition and development
 2. Compatibility with DoD goals and service enterprise-wide objectives
 3. Service-wide and joint interoperability with current and projected systems
 4. Software Quality, Safety, and Test and Evaluation
 5. Integration of the system into the projected battlefield
 6. Information assurance approach
 7. Overall life cycle software support concept (strategy)
 8. Identification of critical program risks; planning for next risk mitigation review

Figure 4. *SIT structure: Transcending question topics.*

than just the development effort. The SIT focuses on how the acquirer (the PM and his organization) plans and is progressing in ensuring a well-managed, successful program and the acquisition and support of a system that will meet the needs of the user; the CMM and the CMMI focus on a developer's process capability. The risks identified through using the SIT provide a basis for risk mitigation at all phases of an acquisition program, which may include acquisition and development process improvement. A software capability evaluation (SCE), or a software process risk evaluation (SPRE) performed by the Army, is a CBA that provides a basis for source selection by the acquirer — typically within the engineering, manufacturing/development (EMD) phase of a specific acquisition/development project. A developer uses a CBA-IPi to identify development process improvements — typically from an organizational perspective and independent of a specific development project. The SIT can be used on a periodic or ongoing basis, as well as in advance of DoD-mandated CIO assessments. An acquirer relies on a SCE in advance of source selection and may occasionally use it to take a snapshot of an ongoing development process.

The SIT is not a tutorial or handbook on how to plan/manage a project. The SIT questions do not attempt to prescribe the correct way to do things, or prompt the user. The SIT questions are intended to ask how things are actually being done on the project (describe what you are doing) and cause management to focus on the important software/system/

program considerations/issues. Most of the SIT questions are not written to yield simple yes/no answers. The questions are open-ended and nondirective, and are designed to obtain descriptive information as a basis for achieving insight into the project status, issues, and risks. The completed responses will be meaningful to management, as well as to life cycle software engineering (LCSE) experts, and should be analyzed to identify any software-related weaknesses and risks in the program.

Structure of the SIT

Two major elements comprise the SIT: a software questionnaire and Matrix+, as illustrated in Figure 3 [11]. The Matrix+ provides an extended version of the basic Army matrix to assess a program against CIO and DoD program requirements. The questionnaire starts with a set of eight high-level transcending questions (TQs), followed by detailed questions in 46 assessment areas.

Figure 5. *SIT structure: The seven domains.*

- **Seven domains comprise the top level of the SIT Questionnaire:**
 1. SOFTWARE TECHNOLOGY
 2. SOFTWARE ACQUISITION MANAGEMENT
 3. PROGRAM MANAGEMENT
 4. SOFTWARE PROCESS
 5. SOFTWARE QUALITY
 6. TEST & EVALUATION
 7. SOFTWARE OPERATION & SUPPORT

The SIT Questionnaire — Transcending Questions

There are several questions that are of overriding importance in assessing any program. The TQs are high-level questions that should be reviewed and asked at the beginning of the risk mitigation process and should be used in summarizing key issues, risks, and actions at the end of the process. The TQs do not replace the detailed questions in the assessment areas. However, they are extremely important to the overall success of the system, from a program-wide perspective. Figure 4 provides the TQ topics.

The SIT Questionnaire — Domains and Assessment Areas

The 46 assessment areas are grouped under the seven domains listed in Figure 5. The sequence of domains and assessment areas does not imply a priority. Figure 6 provides sample SIT questions.

All MS reviews in DoD regulation 5000.2-R, "Mandatory Procedures to Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Reviews," were considered [4]. Each assessment area table has columns for each MS (0, I, II, and III), and a column for developmental program reviews labeled PR. The PR column identifies where internal program review considerations should be focused during EMD. If a question is considered relevant for a MS, a bullet is shown in the appropriate MS column(s); if the question is not considered relevant for that MS, then the column is left blank.

- DOMAIN 1: TECHNOLOGY	
- ASSESSMENT AREA 1.1: SOFTWARE REUSE, ARCHITECTURE & DOMAINS	
1.1-4: REUSE OF SPECIFIC SOFTWARE PRODUCTS (SEE AREA 2.1 COTS/GOTS) [REF. MATRIX #4]	Milestone 0 I II III PR 1 1 1 1
a. How does the program require/address identification, evaluation/test and incorporation of reusable COTS/GOTS (e.g. COE)? Is the plan satisfactory?	
c. Describe any requirements for use of specific COTS or GOTS/GFS.	
- DOMAIN 2: SOFTWARE ACQUISITION MANAGEMENT	
- ASSESSMENT AREA 2.1: COTS/GOTS BUSINESS STRATEGY	
2.1-6: UPDATES TO COTS/GOTS SOFTWARE	Milestone 0 I II III PR 1 1
a. Has a plan been developed to integrate and test updates or replacement COTS after deployment? Describe the approach. (See 7.3-2) [REF. Matrix + #4g.]	
b. Describe the process used to validate long-term supportability of the COTS/GOTS software. (See 1.1-4) [REF. Matrix + #4i.]	

Figure 6. SIT structure: Sample SIT questions.

Matrix+: An Extension to the CIO and DoD Program Requirements Matrix

Based on the Clinger-Cohen Act [1], the OSD provided guidance for its MS review requirements in the form of a matrix of high-level program requirements that were part of an OSD policy memorandum [2]. The OSD matrix addresses requirements in recent legislative reform initiatives (ITMRA, the Government Performance and Results Act [GPRA] of 1993, and the Paperwork Reduction Act [PRA] of 1995) and related DoD regulations, such as DoD 5000.2-R.

The Army implemented this OSD guidance policy in the Army Policy Memorandum, "Chief Information Officer (CIO) and DoD Program Assessment Requirements," dated Nov. 14, 1997 [3]. The Army matrix, containing 22 specific CIO and DoD program requirements, was attached. This basic Army matrix was updated in 1998 and is available in Department of the Army (DA) Pamphlet (PAM) 70-3, "Army Acquisition Procedures" (Appendix XIII, "Chief Information Officer Assessment Requirements") [12] and is contained within the Matrix+ portion of the SIT Web pages at www.sed.monmouth.army.mil/sit. With regard to the program requirements in the Army matrix, DA PAM 70-3 (Appendix XIII) states that "Program managers will use these criteria on a continuing basis to evaluate their programs and will incorporate them into their acquisition processes, procedures,

and documents." (The phrase "these criteria" refers to the 22 program requirements found in the Army matrix.) The Army CIO will assess all Army Acquisition Category (ACAT) I and II programs using the Army matrix. All significant ACAT III and IV programs — with information technology expenditures of \$2 million or more in a single year, or with a total life cycle cost of \$30 million or more — will be evaluated by the appropriate organizations designated responsible for the CIO function at the Major Commands; these programs also will use the criteria in the Army matrix.

The 22 specific program requirements in the Army matrix are at a high level and take an overall program view (see Figure 7 for a list of the 22 program requirements). The Army matrix also has several detailed questions supporting each program requirement, with many of the

questions relevant to software issues. Many of these detailed questions were taken from the SIT questionnaire. The Matrix+, as available in the SIT, is identical in content to the basic Army matrix, except that it provides additional (clearly identified) detailed questions based on selected SIT questions, and provides linked cross-references to the relevant SIT questions and assessment areas. Figure 8 provides sample Matrix+ questions. Note that a "+" in the "milestones" block under MS II and III indicates that there are additional software concerns that also should be addressed, based on some of the additional detailed questions in Matrix+.

Internal Risk Mitigation Reviews

The SIT should be used periodically by PMs and their software IPTs to conduct internal reviews of a development/acquisition program to keep the project in good health, reduce the level of program risk, and to be ready for a CIO assessment. Figure 9 depicts the internal SIT risk mitigation process.

Utilizing the SIT for internal risk mitigation reviews on a regular basis will help ensure program success, in that software and program risks will be identified and managed in an ongoing and consistent manner. Internal risk mitigation reviews also will facilitate preparation for the required CIO assessments (the CIO assessments are based on the program requirements in the Matrix+ found in the SIT).

Figure 7. Program requirement areas (Matrix+).

1. CORE MISSION	12. PERFORMANCE MEASUREMENTS
2. OUTSOURCING	13. FULL FUNDING
3. BPR*/BENCHMARKING	14. INCREMENTAL (PHASED STRATEGY)
4. COTS SOLUTIONS	15. CONTRACT RISK MANAGEMENT
5. RETURN ON INVESTMENT	16. COMPETITION
6. STRATEGIC GOALS	17. EARNED VALUE
7. TECHNOLOGY	18. SOFTWARE SUPPORT ANALYSIS
8. YEAR 2000	19. SAFETY, QUALITY, and TESTING
9. STANDARDS/FLEXIBILITY	20. SOFTWARE PROCESS IMPROVEMENT
10. OPEN SYSTEMS	21. INFORMATION ASSURANCE
11. OPERATIONAL TEST and EVALUATION	22. ELECTRONIC COMMERCE
*BUSINESS PROCESS REENGINEERING	

CIO and DoD Program Requirements						
Program Requirement (Short Title)	Source of Requirement*		Milestone			
	Statutory	Regulatory	0	I	II	III
Does it maximize use of COTS technology? (COTS solution)	Sec. 5122(b) (3), Sec. 5201; 10 USC2377; FASA Sec8104	Parts 2.3, 3.3.2; FAR Part 12	1	1	:	:
a. To what extent are (will) GOTS/COTS hardware and software (be) used? (See 2.1-1a, 2.1-1b) (1) Is there a plan for identification, evaluation, & incorporation of reusable COTS/GOTS (requirements, designs, SW development plans, data element descriptions, test plans, test data, etc.)? (See 1.1-4) (2) Does the program require reuse of specific COTS/GOTS (e.g., Common Operating Environment)? (See 1.1-4) b. What desired capabilities are not available in COTS and how critical are they? (See 2.1-4) c. What needs or restrictions could preclude use of COTS? (See 2.1-2e) : g. Has a plan been developed to integrate updates or replacement COTS after deployment? (See 2.1-6a, 7.3-1) h. What is the approach to identify, evaluate, and select new technology for potential use in the program? Describe the new technologies. (See 1.5-1) i. Describe the process used to validate supportability of new technologies and COTS. (See 1.5-7a, 2.1-6b) j. What warranty, data rights, & license requirements are applicable? (See 2.4-6; see also 2.4-3) (See also Areas 1.1, SW Reuse, Architecture, and Domains; 2.1, COTS/GOTS Business Strategy)						
Potential Source of Information: MNS, ORD, Analysis of Alternatives, Army Enterprise Architecture, Acquisition Strategy Reference: Army Software Reuse Strategy						

* The program requirements listed are simplified statements of investment guidance being used by the OMB. Statutory refs in bold type are to Division E of the Clinger-Cohen Act of 1996. Regulatory "Part_" refs are to DoD 5000.2-R.

Figure 8. Sample Matrix+ questions.

SIT Risk Mitigation Process Overview

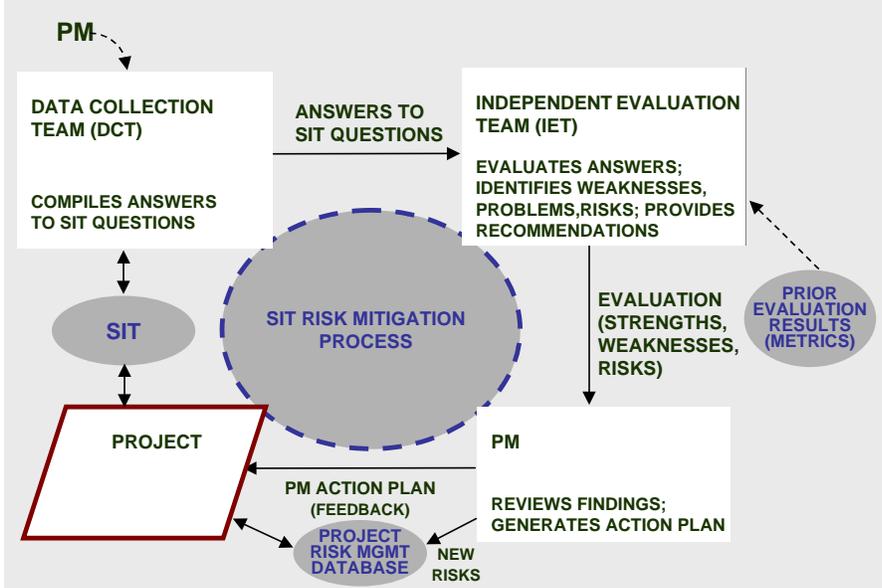
Internal risk mitigation reviews should be initiated by the PM or the software IPT to reduce program risk, particularly for mission-critical programs that are software-intensive. Typically, a data collection team (DCT) will be formed to answer the SIT questions. The DCT should be comprised of program/project software support staff and software IPT members, preferably with the support of life cycle software experts. The answers should be given to an independent evaluation team (IET), typically comprised of trained personnel from a Life Cycle Software Engineering Center (LCSEC) or a software support agency (SSA). Ideally, this IET should be independent of the DCT, but may include a few project experts who were involved in the data collection and response generation, to explain and expand their answers to the questions. The IET would identify any weaknesses and risk areas and provide recommendations to the PM. Additional IET effort may include consultation with the software IPT and the development of an action plan with/for the PM. The action plan should be used as a guide to rectify the program's/project's weaknesses and risks. Risks should be documented in a project risk mitigation database.

SIT Risk Mitigation Process Specifics

The SIT Risk Mitigation process can start with any of the following approaches:

- programmatic view using the Matrix+
- high-level software view using the TQs
- detailed software view, using the questions in the assessment areas, with emphasis on the most critical assessment areas
- mini-review using the first question in each assessment area.

Figure 9. SIT risk mitigation process.



The Data Collection Team PMs should form a DCT, which includes their software experts and/or software IPT, to adequately respond to the questions. Additional team members should be obtained from the appropriate SSA or LCSEC. To make the reviews meaningful, it is essential that the DCT consists of very knowledgeable, technically qualified software engineering and software acquisition personnel, who thoroughly understand software life cycle issues and are familiar with the project.

Collecting the Data

Reviewing the questions in advance of the data collection should enhance the team's comprehension, as well as improve the quality and completeness of the answers. The DCT collects the responses to the questions, and copies of certain project material (e.g. software development plans or any other referenced documents or materials). When information already exists in a documented form, the response should reference this information (e.g. citing specific document and paragraph numbers) and copies of the referenced materials should be provided. The answers can be brief where examples and other information are referenced and provided.

Obviously, judgment should be used for selecting and addressing the questions for each project. If a phased approach is to be used, the most critical assessment

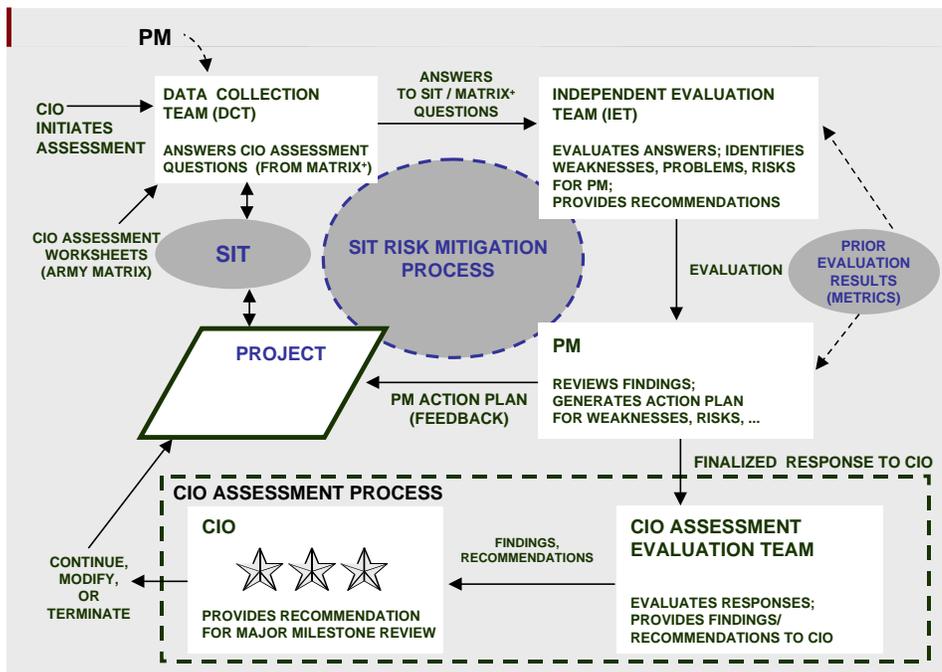


Figure 10. Use of SIT for CIO assessments.

areas should be addressed in the initial phase. For some projects, a question with a bullet in a milestones column may not be relevant, and may be tailored out for a valid reason. If a question or subquestion is not relevant or important to the project, the DCT may tailor it out with a brief, specific justification. Questions should be interpreted in a phase-appropriate manner; e.g. if it is too early for an action, the response should describe the plans and approach to be taken (i.e. identify what will be done to ensure that the objective is accomplished).

The Independent Evaluation Team

The IET should be independent of the DCT. IET members should be experienced software, system, and program personnel who understand the technical and programmatic depth and breadth of acquisition and development programs. They also should be trained in the evaluation methodology and understand the goals and activities associated with each assessment area. In addition to identifying program/project strengths, weaknesses, and risk areas, the IET (in coordination with the PM) also can help generate an action plan to rectify the weaknesses and risks.

Transcending Questions

At the end of the SIT data collection and

internal evaluations, the SIT user should return to the TQs and summarize the findings (see, particularly, TQ8 in Figure 4). Risks that have been identified should be included in the project risk management tracking system.

Estimated Time Frames

Depending on the size and complexity of the program's software, a complete internal risk mitigation review (all relevant assessment areas) may require about one month to prepare the answers/responses by the DCT, and approximately two months to evaluate the responses by the IET. Action plan generation will require additional time. Given the review results and the perceived risk, an internal SIT risk mitigation review may be conducted at 10- to 18-month intervals.

Instead of a complete review, a partial review or a series of shorter incremental reviews (e.g. three to six assessment areas per month) may be conducted, each focusing on different assessment areas identified as key for the particular program at its current point in the life cycle. Program risk profiling to identify critical areas for review, or to plan the sequence of incremental reviews, may take one or two days. Another alternative is a mini-review, prescreening using the first question in each relevant assessment area to identify areas of significant risk for further study;

the prescreening would take about two weeks.

Protecting PM Information

Protection must be provided to the responses, and the findings should be given only to the PM. The PM can ask the IET for specific recommendations to address any weaknesses or risks found, and may also ask the IET for support in the preparation of an action plan to address the weaknesses and risks.

CIO Assessments

Purpose of the CIO Assessment

The CIO assessment will be conducted prior to MS reviews, consistent with the Clinger-Cohen Act (ITMRA) [1] and the related DoD policy [2]. In the Army, these assessments are based on the program requirements in the Army matrix [11, 12]. Other services and DoD agencies may utilize similar CIO assessment processes to ensure that programs meet the DoD and service information technology) program requirements [1, 2]. Throughout the CIO assessment, it should be foremost in the minds of the various teams and the PM staff that the CIO assessment is intended to support the PM in ensuring successful acquisition of high-quality, supportable systems and software to meet the critical needs of DoD war-fighting personnel.

CIO Assessment Overview

A program preparing for a CIO assessment should utilize the SIT risk mitigation process as the front-end of the CIO assessment to help ensure the success of the CIO assessment and the related major MS review. Figure 10 illustrates the use of the SIT for CIO assessments.

The upper portion of Figure 10 identifies the PM data collection process for the CIO assessment, which utilizes the SIT risk mitigation process. The lower portion of Figure 10 identifies the additional activities in the Army CIO's assessment process. A CIO assessment evaluation team (AET) evaluates the data the PM submitted and makes program recommendations to the CIO. Then the CIO makes the recommendation to the Defense Acquisition Board or appropriate MDA to modify, continue, or terminate

the program.

Preparing for a CIO Assessment
Preparing for a CIO assessment should start several months prior to the MS reviews specified in DoD 5000.2-R. A significant time saving will be realized where internal risk mitigation reviews have been performed previously and regularly. A sufficient amount of time should be allowed (e.g. about one month each) for the DCT to prepare the answers and for the IET to analyze the answers and generate findings. The IET will analyze the responses to the Army matrix (or Matrix+) questions, as well as to appropriate SIT questions. (To be better prepared, the PM should address the additional questions in the Matrix+ and selected questions from the assessment areas.) The IET will identify any weaknesses, potential problems, or risks, and discuss them with the PM. The PM thus will be informed of potential risks in advance of the CIO assessment. The PM should formulate an action plan, with help from the IET, to address any weaknesses, problems, and risks. Work should begin prior to the CIO assessment and major MS review, on the actions to proactively address these issues and reduce project risk.

About two to three weeks should be allowed for the PM and the IET to revisit the questions in the CIO assessment (for the Army, the basic Army matrix¹) and prepare the final answers to be sent to the CIO. The PM should have actions already under way to address any issues before sending the response to the CIO. The PM can proactively develop an action plan (with help from the IET) prior to, or concurrent with, submission of the responses to the CIO.

The CIO Assessment Evaluation

The CIO AET will then analyze the responses to the Army matrix questions to determine strengths, weaknesses, and any significant risks, and report its findings/recommendations to the CIO. The AET will need about one month to complete the evaluation and report the findings to the CIO. The findings and recommendations should be completed and made available well before the formal MS

review to allow time for the CIO to review and, if necessary, discuss any concerns or issues with the PM. The final assessment result will be the CIO's decision to recommend continuation, termination, or modification of the program to the MS decision authority (MDA). The decision of the MDA MS Review is then fed back to the PM. The PM can request recommendations from the AET.

Protecting CIO Information

The DCT, the IET, and the CIO AET must protect the information and treat the findings as sensitive information to be given only to the individual who chartered the team's effort, i.e. the PM and/or the CIO, or their designated representatives.

Summary

The purpose of the SIT is to support program management (i.e. the acquirer) in identifying and addressing software-intensive program strengths, weaknesses, and performance risks to meet the critical needs of the soldier, the airman, or the sailor, and to reduce overall program risk and TOC. The focus of either an internal risk mitigation review or a CIO assessment is on identifying potential or actual performance problems and risks, on identifying potential areas for cost or schedule overruns, and on giving the PM advance opportunity for resolution or mitigation of problems and/or risks. The SIT will help the PM keep the project on the road to success and to be prepared for CIO assessments.

SIT Access

The SIT is a Web-based tool and may be accessed from the CECOM SEC Web page, www.sed.monmouth.army.mil/sit.

It may also be accessed from (1) the Army DISC4 Web page, www.army.mil/disc4/acq. (Scroll down to "Software Development and Engineering Insight" and select "Software Insight Tool to Prepare for Milestone Reviews"); and (2) the DoD Under Secretary of Defense Acquisition and Technology (USD [A&T]) Director, Test, Systems Engineering, and Evaluation (DTSE&E) risk management Web page, www.acq.osd.mil/te/programs/se/risk_man

agement. (Select "Related Web sites"; then select "Army CECOM SEC Software Insight Tool").

For general questions, comments, and requests to be informed of new versions, contact Army CECOM SEC, AMSEL-SE-OPS-SPPD, Fort Monmouth, N.J. 07703, DSN 992-2502 (732-532-2502), Attn: Jerry Kastning (kastning@mail1.monmouth.army.mil).

For SIT technical questions or comments, contact James Heil (james.heil@telos.com) or Marilyn Ginsberg-Finner (marilyn.ginsberg@telos.com) at 732-842-1717.

For questions or comments on the Web-based tool, contact Marilyn Ginsberg-Finner. ♦

About the Authors



Jerry Kastning is the Division Chief for the Strategic Planning and Policy Division of the Operations Directorate for the Software Engineering Center (SEC) at Fort

Monmouth, N.J.

Kastning has been with SEC for the past 14 years. In addition, he has held several first line supervisory positions in SEC, including the Acquisition Streamlining and Risk Management, Information and Engineering Support Branch, the Automatic Test and Software Support Branch, the Software Configuration Management Branch and the Office of Process Improvement. Prior to his employment with SEC, he was the software project leader with PM TMDE (Test Measurement and Diagnostic Equipment) for eight years. In this capacity he was responsible for the development and testing of all system and application software. He also has many years of hands-on experience with designing, coding, and testing various software application programs for military systems, as well as computer hardware design.

Kastning earned his bachelor of science and master's of science degrees in electrical engineering from the University of Illinois and a master's degree in business administration from Monmouth University.

Division Chief
Software Engineering Center
AMSEL-SE-OPS-SPPD

Fort Monmouth, N.J. 07703-5207
 Voice: 732-532-2502
 Fax: 732-532-0752
 e-mail: kastning@mail1.monmouth.army.mil



James Heil is a technical manager at Telos Corp., Fort Monmouth, supporting the CECOM Software Engineering Center. Previously, he worked at MITRE — Fort

Monmouth Software Engineering Center, on Fire Control Systems software, Acquisition Support, and software Standards (IEEE/EIA-1498/J-STD-016, and ISO 12207.

Earlier, Heil was a software development manager and SQA manager at ITT Avionics, and a software development manager at IBM.

He was CODSIA Industry Task Force chairman for MIL-STD-2167 and 2167A, and served on MIL-STD-498, IEEE 1498/EIA 640 (J-016) and 12207 working groups.

Heil chaired the NSIA SQA group, and has led conferences and seminars on software quality, process improvement, software acquisition, standards, and testing. He chairs the North Jersey SPIN. Heil was an invited participant at Orlando II and San Antonio DoD Workshops.

He authored "Practical Applications of Software Quality Assurance to Mission-Critical ... Software" in *Handbook of Software Quality Assurance*, 2nd Ed., and 3rd Ed.

Heil has a bachelor of science degree in mechanical engineering and a master's degree in electrical engineering, and a master's degree in industrial engineering (operations research), and a master's degree in business administration.

Technical Manager
 Telos Corporation
 55 North Gilbert Street
 Shrewsbury, N.J. 07702-4929
 Voice: 732-842-1717
 Fax: 732-530-5440
 e-mail: james.heil@telos.com

Jeffrey Herman is a computer systems analyst with the U.S. Army CECOM Software Engineering Center. Herman has more than 16 years experience in software acquisition. He is a member of the Army Acquisition Corps (AAC) and completed the master's



program in software engineering Monmouth University. From January 1991 to January 1992, Herman was a resident affiliate at SEI and was a board member on the

Common Based Appraisal Advisory Board at SEI. A founding member of the Tri-Service Process Working Group and a member of the CMMSM review group, the SA-CMM review group, and the Command, Control, Communications, Computers, Intelligence, Electronic Warfare, and Sensors (C4IEWS) Standardization Process Team (SPT) C4IEWS SPT, he has focused on areas including capability evaluation, process improvement, DoD and Army policy, government and commercial standards, acquisition reform, and acquisition risk management. He has lectured at many conferences and has published articles in *IEEE Software*. He has led software capability evaluation teams and has participated in numerous source selections for software-intensive acquisitions.

Computer System Analyst
 Software Engineering Center
 AMSEL-SE-OPS-SPPD
 Fort Monmouth, N.J. 07703-5207
 Voice: 732-532-8071
 Fax: 732-532-0752
 e-mail:hermanj@mail1.monmouth.army.mil



Marilyn Ginsberg-Finner is Task Leader Acquisition Business Practices with Telos, supporting the U.S. Army CECOM SEC in areas including software engineering (SE), software program assessment, risk management, Army software strategy, and standards. She is a representative to the U.S. Technical Advisory Group on International Software Life Cycle Standards, program chairwoman for Jersey Shore SIGAda, and on the executive committee of the IEEE SE Standards Committee, IEEE/CS, ACM, AFCEA, and North Jersey SPIN. She has served on working groups, including MIL-STD-498, EIA/IEEE J-STD-016, IEEE/EIA 12207, DISA Center for Standards SE Standards, and the C4IEWS Standardization Process Team. Her previous work at Teledyne Brown Engineering and

Concurrent Computer included IV&V, SQA, and software methodology, development and support. She received her bachelor of arts degree in math from Rutgers and a master of science degree in computer science from Monmouth University.

Task Leader Acquisition Business Practices
 Telos Corporation, Fort Monmouth Operations
 55 North Gilbert Street
 Shrewsbury, N.J. 07701-4929
 Voice: 732-842-1717
 Fax: 732-530-5440
 E-mail: marilyn.ginsberg@telos.com

References

1. "Clinger-Cohen Act of 1996 (Division E)," also referred to as the Information Technology Management Reform Act (ITMRA) of 1996.
2. Office of the Secretary of Defense (OSD), OSD Memorandum, "Requirements for Compliance with Reform Legislation for Information Technology (IT) Acquisition (Including National Security Systems)," May 1, 1997 (signed by Paul G. Kaminski/Under Secretary of Defense for Acquisition and Technology, John J. Hamre/Under Secretary of Defense-Comptroller and Chief Financial Officer, and Emmett Paige, Jr./Assistant Secretary of Defense for Command, Control, Communications, and Intelligence/CIO).
3. Headquarters Army, SAIS-IAA-S, DA Memorandum, "Chief Information Officer (CIO) and DoD Program Assessment Requirements," Nov. 14, 1997 (signed by Lt. Gen. William H. Campbell/Army CIO, Helen T. McCoy/Assistant Secretary of the Army/Financial Management and Comptroller, and Robert M. Walker/Army Acquisition Executive).
4. Department of Defense, DoD 5000.2-R, "Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information Systems (MAIS) Acquisition Programs," Sept. 4, 1998.
5. Paulk, M. et al, Software Engineering Institute (SEI), "SEI Capability Maturity ModelSM for Software (CMMSM), Version 1.1," SEI-93-

- TR-24, Feb. 1993.
6. Electronic Industries Association (EIA)/Institute of Electronics and Electrical Engineers (IEEE) J-STD-016, "Software Life Cycle Processes, Acquirer-Supplier Agreement," July 1995.
 7. Byrnes, P. and D. Phillips, Software Engineering Institute (SEI), "Software Capability Evaluation - Version 3.0, Method Description (SCEMD)," Carnegie-Mellon University (CMU)/SEI-96-TR-002, April 1996.
 8. Brown, N., DoD Software Program Manager's Network (SPMN), "The Program Manager's Guide to Software Acquisition Best Practices, Version 2.2," June 1998.
 9. Carr, M. et al, Software Engineering Institute (SEI), "Taxonomy-Based Questionnaire, Taxonomy-Based Risk Identification," CMU/SEI-93-TR-6, June 1993.
 10. Ferguson, J. et al, Software Engineering Institute (SEI), "Software Acquisition Capability Maturity Model (SA-CMM) Draft Version 1.01," CMU/SEI-96-TR-020, Dec. 1996.
 11. CECOM SEC Web page, www.sed.monmouth.army.mil/sit, "Software Insight Tool for Internal Risk Mitigation Reviews and CIO Assessments," Version 3.1, February 1999.
 12. Headquarters, Department of the Army (DA), DA Pamphlet 70-3, "Army Acquisition Procedures," Appendix XIII, Final Draft, Dec. 1998.
- Note**
1. For the Army CIO assessment, only the responses to the basic Army matrix

questions are required; however, responses to the "plus" questions provide assurance that critical software issues are covered and are a basis for action by the PM, where needed. Further, using the assessment areas can identify relevant issues at MSs that are not specifically noted as applicable in the Army matrix. The responses to the basic Army matrix will be reported to the CIO in advance of the MS review and analyzed by the CIO assessment evaluation team. If the responses do not provide adequate information, follow-up information may be needed. Using the more detailed questions in the SIT will facilitate more thorough analysis in advance and can expedite the response.

An Open Invitation to Subscribe to AcqNOW!

AcqNOW! is a subscription service that provides immediate e-mail notification of changing acquisition information. Simply fill in the electronic subscription form at <http://www.deskbook.osd.mil/acqNOW> and mark the information types that affect you when they change: FAR, DFARS, DoD D5000.1 and 5000.2-R, SAMM, DCAAM, and others.

As changes become available, AcqNOW! will send a brief e-mail and a link to the "raw" source document on the Deskbook Web site.

If you are already a subscriber but have changed your job or address, click AcqNOW! and update your contact information, along with any changes in your information preferences.

Acquisition reform is accelerating; AcqNOW! to keep up.