



Egypt-SPIN Newsletter

Issue 11, Jul. – Sep., 2005

Sponsored by SECC

From the Editor (Ahmed S. El-Shikh)

Welcome to our 11th issue of Egypt –SPIN newsletter. In each issue we are trying to put together relevant information in the form of articles and recaps from the previous 6 months events hoping to provide our members of Egypt – SPIN with information to support their current interests.

SECC is pleased to announce that **Cairo Technology Development Center C-TDC - IBM Egypt**, one of the greatest Egyptian software companies, has achieved **CMMI Accreditation Maturity level 5** by means of **SCAMPI** on 5th October, 2005.

Also, **DMS** and **ITSoft** had achieved **CMMI Maturity level 4** on 18th August, 2005 and on 25th August, 2005 respectively. **SECC** wishes other companies the same success.

This issue conducts some hot topics within four series and one independent article such as: discussion of the software industry in Egypt (1st article), explanation of one of CMMI process area (2nd article), sharing real life experience in the field of information security and CMMI implementation (3rd, 4th and 5th article respectively).

Dr. Ramiz Kameel completes his **series to discuss the nature of the Egyptian software industry**. His article introduces a new **hypothetical model to improve the Egyptian software industry**.

Eng. Abdel Meguid Elaraby continues the **series for explaining the CMMI version 1.1 process areas** as presented in the **“Intermediate Concepts of CMMI”** course. His article describes the **Integrated Product and Process Development** process area in a software development organization.

Eng. Amr Shaltoot gives his opinions about **Information Security Dilemma** in Egyptian software industry. He goes through security measures, types and required protection.

Eng. Ahmed Gad Al-Karim starts a **series to discuss the Security in the Virtual Environment**. His article introduces the concept of **information security** vs. the concept of computer security.

Eng. Ahmed Abd El Aziz shares his experience –in form of a series - in **CMMI Implementation** journey according to the **IDEAL** model. His article describes the early phases in the cycle.

We hope we succeed to give you an idea about what is going in our community. Please write to the editor your comments about our progress. We always ask you to submit short articles for publication that deal with your experience in defining, developing and managing software efforts as well as process improvement experience. Remember that our goal is to encourage an interchange between our readers. You can email spin@secc.org.eg or ahmed.elshikh@gizasystems.com

New Age of Software Industry Starts in Egypt.

By: The Editor

By the first week of the fourth quarter, 2005; the **Cairo-Technology Development center (C-TDC)** of **IBM-Egypt** has achieved **CMMI Maturity Level 5** for **Software** model (**Continuous Representation**). Also, during the third quarter of the same year; **DMS** and **ITSoft** have achieved **CMMI Maturity Level 4** for **Software** model (**Staged Representation**); three milestones on the Egyptian roadmap for improving the software industry.

From approximately two years ago; Egyptian companies for software development were outside of the international level of quality. **Software Engineering Competence Center (SECC)** in collaboration with **IT specialists** in Egyptian companies had success to change the image. The dream have become a reality; one company in CMMI level 5, two in CMMI level 4, two in CMMI level 3 and one in SW-CMM Level 2.

The story has not finished yet; a lot of simultaneous activities take place nowadays such as:

- Companies in level 2 and 3 are working hard to achieve higher levels.
- A project, which is funded by the **Industrial Modernization Center, IMC** and executed by **Software Engineering Competence Center (SECC)** with consultation provided by an Indian company "**QAI**", aims to help 20 Egyptian company to achieve CMMI Maturity Level 2 and 3 during the next year, 2006.
- Another project, which will be funded by the **Industrial Modernization Center, IMC** and will be executed by **Software Engineering Competence Center (SECC)**, will start soon to help 20 of the small and medium enterprises "**SMEs**" applying **Software Process Improvement Guide "SPIG"** as a simplified model for software process improvement. SECC had released the first version of the SPIG by the end of December, 2004. SPIG is an adopted quality model, which is based on the SW-CMM, CMMI, and IEEE standards and covers seven process areas that had been selected by SECC, Motorola experts and local consultants.

It is a new age of the Egyptian software industry, having such number of companies with improved production process according to an international standard will open a lot of non-reachable market sectors. In the upcoming issues of the Egypt SPIN Newsletter, we will try to invite experts from IBM-Egypt, DMS and ITSoft to participate with articles that summarize their experience and lesson learned from their success. Also, we will invite experts from SECC to give us more detailed about the previously mentioned projects. Good luck for all Egyptian companies in their efforts to reach the international quality level.

Table of Contents

Toward Egyptian Software Industry Series:

Egyptian Software industry Improvement [Part 2].....5

CMMI Process Areas Explanation Series:

Integrated Product and Process Development.....10

Into the Security Dilemma.....15

Information Security in Virtual World Series.....18

CMMI Implementation Series.....24

Toward Egyptian Software Industry Series: Egyptian Software Industry Improvement [Part 2]

By: Ramiz Kameel

OBJECTIVE

This article "Egyptian Software Industry Improvement" is the second article of a series of articles "Toward Egyptian Software Industry" that concerns with the software industry improvement in Egypt. This article introduces the required procedures that should be followed among ESPC roles [1] to improve the Egyptian software industry from process prospective. This article introduces a new hypothetical model to improve the Egyptian software industry. This model represents the roles' interactions and their duties.

INTRODUCTION

Three main roles originate and formalize the ESPC currently as described previously [1]. Two additional roles will be invited to complete the basic elements of ESPC for industry improvement. These two roles are the governmental role and the consultation role. The main three roles; vendors, customers, and beneficiary; can shared in software industry improvement without any additional role, but this will need a long period of time and will be in local effect. The inviting of two additional roles will effect directly on achieving the improvement in a reasonable period of time, and will encourage the foreign involvement and competition.

Recently, the Egyptian government involved in several activities in the software community to enhance the production environment and to

improve the performance efficiency of the software companies.

On the other hand, the consultation existence and influence in software community is very untouchable compared to the market needs or the actual activities in the software market. The present article represents a design of a new model that can improve the software industry in Egypt. This model can be considered as preliminary model and can be modified in the prospective future after applying it in the Egyptian community.

METHODOLOGY

The model, by definition, is a suggested and developed strategy to be followed by different roles in the system to reach a certain pre-specified aim and to apply an improvement plan in the system. Model can define the outlined interaction relations, among the roles.

The present model consists of a set of nodes and links. Each node represents an actor (role), and each link between two actors (roles) indicates that the former may attain some outputs from the other, or both from each others.

PROPOSED ESPC MODEL

Proposed ESPC model consists of five roles; vendor, customer, beneficiary, consultant, and government. These five roles are linked together with suggested relations; Figure (1). Each role has immediately required and prospective duties, Table (1). In this

model, the consultant is invited to take over the vendor responsibilities to deal with customer. So, in the present model, the consultant will be the connection node between the vendor from one side and the customer and beneficiary from the other side.

The vendor will receive the requirement from consultant in a standard format based on standard models (such as; ISO, TQM, CMMI ...). The vendor will deliver the required software to the consultant depending on the same standard models.

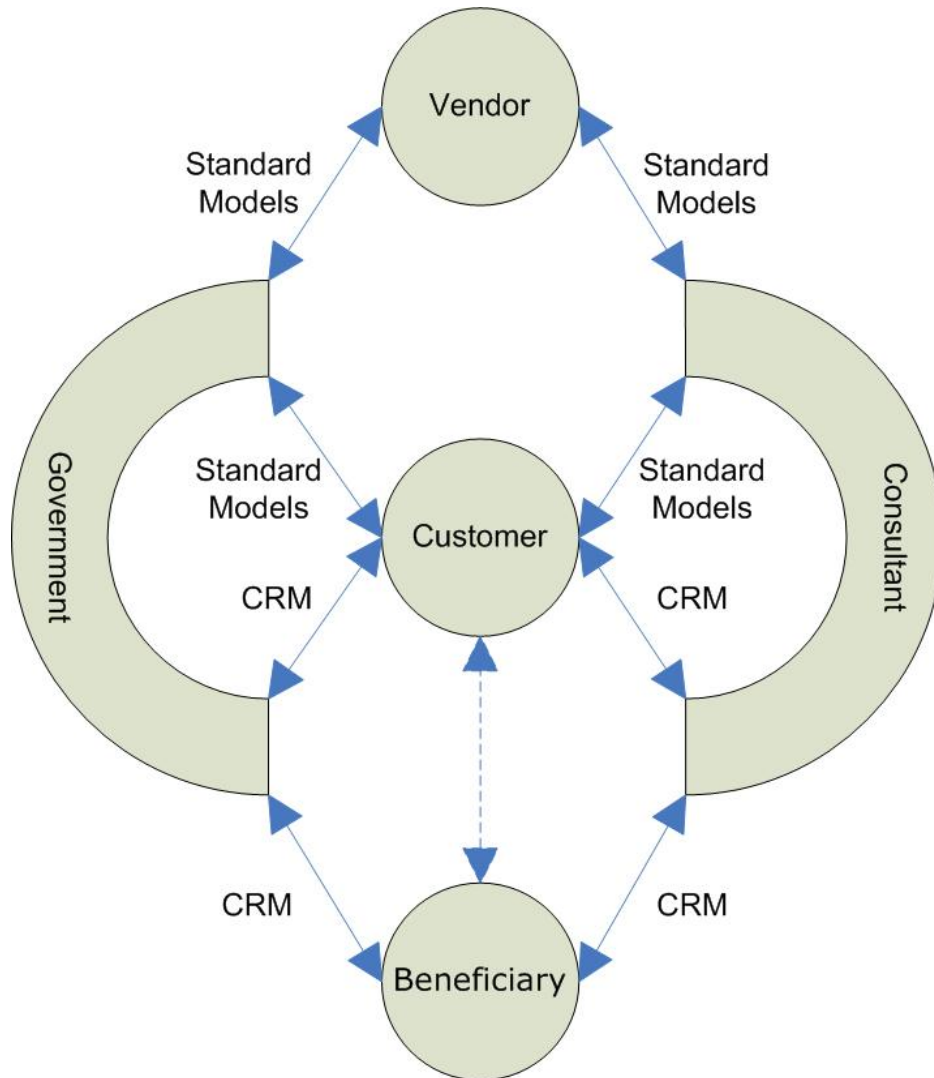


Figure (1): Proposed ESPC Model

The software requirement that are delivered to vendor by consultant, will be received from the customer based on the standard methodologies and using the Customer Relation Management (CRM) technology that is introduced to manage the customer's wants and needs [2].

The consultant has another relation with customer, which can be classified under the CRM technology, but has an important impact on Egyptian production community to push it forward toward stable industry, review Annex.

Table (1) Immediately required and prospective duties of each role

Role	Immediately Required Role	Prospective Role
Vendor	Follows the creating process	Follows the manufacturing process
Customer Beneficiary	Should be trained on CRM *	Should be trained on standard models
Consultant	Follows the CRM	Follows the standard models
Government	Provides training programs for standards and supporting procedures	

* Review the Annex for success CRM applying

This relation can be defined as the consultant support to the customer for standardizing the customer's requirements based on the recent methodologies (such as; ISO, TQM, CMMI ...) and strategies of the Egyptian software industry improvement. The consultant should be in continues contact with beneficiaries to receive their requirement and integrate with customer's requirements.

The consultant should update the beneficiary by the progress in the project with customer.

The customer has an important role in the software industry improvement process by applying new methodologies, review Annex. Customer is responsible with manufactures of software to improve and standardize the software production line.

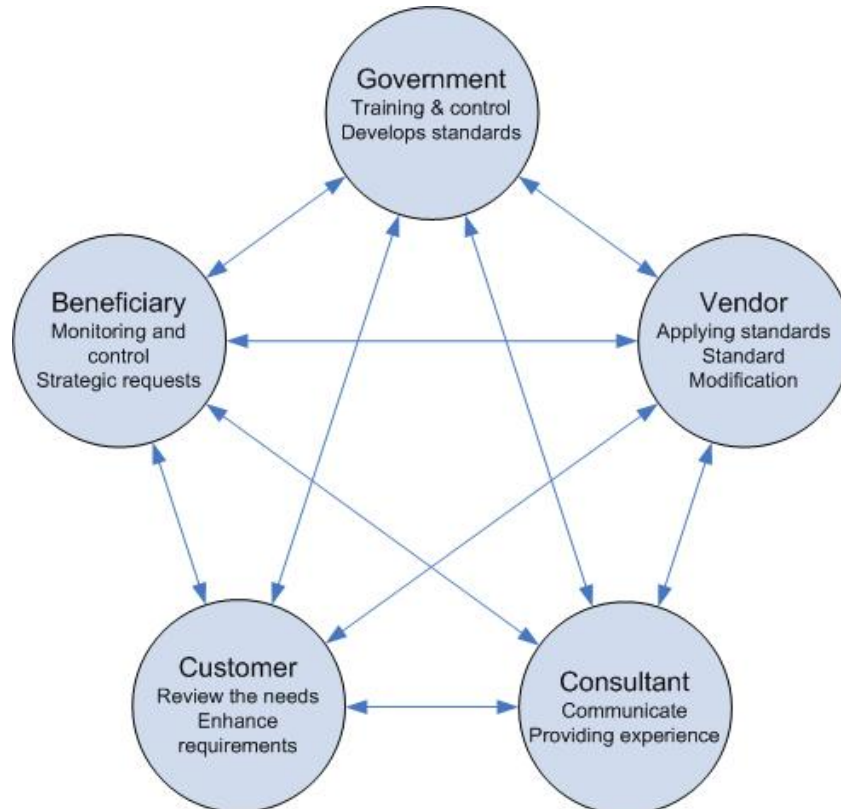


Figure (2): Roles' contribution in the ESPC's network associations

The government is invited in this model to play an important role to support the vendors by training on the standard models in Software Development Life Cycle (SDLC). In this model, the government and consultant roles are represented as two separated half of a rounded circle to represent the required integration between two roles in the Egyptian market. Several network societies and associations should be formalized to create the proper environment for all roles to contribute in the industry improvement [3].

All roles are invited to formalize these network associations and control them, Figure (2).

Each role has to contribute in these formalized network associations and these contributions are divided to current contributions and prospective contributions. The present contributions should be matched with the creating process in the production community. The prospective contributions should be matched with the manufacturing process in the production community, Table (2).

Table (2) Present and prospective contributions of each role in community's associations

Role	Present Contribution	Prospective Contribution
Government	Provides training programs for elected standard and controls the community using it.	Develops local standard that can match with all requirements of different roles
Vendor	Applies suggested standards and gives the feed back.	Sharing in the creation of the local standard.
Consultant	Communicates with customers and shares in the training programs.	Provides the experience to the market and the stakeholders.
Customer	Reviews the needs and requirements to provide complete data. *	Enhances the requirements based on the standards.
Beneficiary	Monitors and controls all customer activities.	Suggests new strategic requests based on enhanced requirements.

* Review the Annex for success CRM applying

CONCLUSION

From mentioned above, The Egyptian software industry improvement is the responsibility of all different roles in the Egyptian Software Production Community. The suggested ESPC model should be characterized and distinguished by several features such as; providing the training programs for standards and supporting procedures for different roles. The governmental role is invited in this model to provide the main features of the model. In addition to the self duties of the governmental role, other roles should

formalize and control industrial societies, which consist of these different roles themselves. The government is responsible to improve the software customers as its responsibility toward the software vendors.

The consultation role will play the complete management role with customers and beneficiaries. The consultation role is responsible for achieving the success in the different stages of the projects and in the whole project. The consultation role is invited

to provide the experience to the market and stakeholders.

Customer has an important role in the software industry improvement process. Customer is responsible with manufactures of software to improve and standardize the software production line.

FUTURE WORK

Prospective articles will concern with identifying the standards that should control the relation between different roles, especially the standards among vendors, consultants, and customers. The prospective articles will study the role of government toward the vendors. These articles will analyze the presented standard methodologies and their feasibility for the Egyptian community.

ANNEX

Customer Relation Management (CRM) Technology [4]

CRM is so complex that it's easy to blame problems on vendors or consultants or resellers. However, CRM users must take responsibility for their own success during all phases of an initiative--planning, product selection, implementation, and ongoing maintenance and improvements. Here's what every CRM project leader must do when dealing with internal staff, vendors, integrators, and consultants to ensure the CRM initiative is truly fruitful.

1. **Get an Attitude:** Break out the positive attitude. Planning and implementing an ideal CRM initiative takes a lot of communication with customers, internal staff, and vendors to uncover their ideas, needs, and concerns. Communication of this depth requires a healthy attitude and lots of listening.

2. **Be Educated:** Organizations that use CRM strategies and technologies need to know their customers and their own business. Only then will they know what CRM solution will work best for them.
3. **Get Buy-In:** "You cannot be a good CRM customer if no one is using the tool," Fields says. "The users are driving the solution." Although executive and user buy-in is critical, they are only two of the multiple-stakeholder acceptances required for CRM success. Other stakeholders, like customers, business partners, and of course the internal IT department, are equally critical to the CRM initiative's success.
4. **Remember That Vendors are Partners:** True CRM is an evolution, not a one-time implementation. This is why it is important to select a vendor that you can consider a partner.
5. **Make a Commitment to Success:** CRM project leaders and users, and the executives who support the initiative, not only have to want to be successful; they need to make a major commitment to it. And if something doesn't work out, and then it should be like the adage--try, try again.

References

- [1] Kameel, R., 2005, Toward Egyptian Software Industry: Egyptian Software Production Community, Egypt-Spin Newsletter, SECC, Issue 10, Apr. – Jun. 2005, Pages 10-13.
- [2] Swanson, E.B. and Ramiller, N.C., 1997, The Organizing Vision in Information Systems Innovation", Organization Science, (8:5)

September – October 1997, pp. 158-474.

[3] Abd El-Hady, A., 2005, Private Communication.

[4] Picarille, L., 2003, Five Ways to Be a Good Customer, CRM Magazine, December 2003.

ACKNOWLEDGEMENT

This work is supported by Research Activities in Quality Dept. of Prima Soft. The author is grateful to, Eng. Ahmed A. Hady, for his valuable recommendations.

Biography

Ramiz Kameel is SPI Consultant of Egyptian Software and Systems; Prima Soft. Author holds a Ph.D. in Engineering. Author is SPI Consultant of Information Technology Institute - ITI.

Feedback Contacts

Feedback, comments and questions are appreciated by the author.

Email:

rekameel@primasoft.com.eg

CMMI Process Areas Explanation Series: Integrated Product and Process Development An Overview

By: Abdel Meguid Elaraby

The Editor requested each participant in the "Intermediate Concepts of CMMI" training course to write an article about the Process Area he presented during the course. I presented "Organizational Environment for Integration Process Area". This Process Area supports Integrated Project Management Process Area for Integrated Product and Process Development. Since Integrated Product and Process Development is a new philosophy and concept to most of the readers, I found that it is better to give an overview about it, before discussing Organizational Environment for Integration.

1. Introduction

1.1 Evolution

Integrated Product and Process Development traces back in time to 1986, when the United States of America President's Blue Ribbon Commission (also known as the Packard Commission) on Defense Management concluded that many of our weapon systems cost too much, take too long to develop, and by the time they are fielded, incorporate obsolete technology. This means that the *customer* and *users* are not satisfied by the products (weapon systems) delivered to them. Customer is not satisfied because it takes too long to develop and cost too much, while users are not satisfied because it delivered late and incorporate technology that is considered obsolete at delivery time.

As a result of the Packard Commission Report the Under Secretary of Defense

for Acquisition requested the Institute for Defense Analyses (IDA) to examine concurrent engineering practices. In December 1988 The IDA's recommended and defined ("The Role of Concurrent Engineering in Weapon System Acquisition"). The concept continued to evolve under the Air Force Systems Command and in 1991; the Advanced Tactical Fighter program management and industrial partners (circa 1991) couched the philosophy of concurrent engineering in an innovative management structure, called the Integrated Management System.

1.2 The Term

The term Integrated Management System was primary changed to Integrated Product Development by the U.S. Department of Defense as a name, which better reflects the participation of manufacturing and other downstream functions in product development, and lastly to Integrated Product and Process Development to reflect the collaboration of *relevant stakeholders* to integrate and concurrently apply all necessary processes and resources to provide rapid, cost effective, customer focused product development that satisfies customer's needs.

1.3 Usage

Integrated Product and Process Development (IPPD) is a relatively new philosophy and concepts that is used for manufacturing complex products and systems such as: Airplanes, Missiles, and Ships, Aerospace industry, automotive industry and Military Weapons.

interdependent/ interactions among tasks). Since tasks are based on WBS, which reflects the product decomposition architecture, then Component/ Subcomponent is developed in parallel.

2.3 Integrated Teaming

The underlying concept is that new products should be designed by collaboration between those associated with the lifecycle of the product, to develop products that better satisfy customer needs. This would include those from functions (e.g. design, manufacturing, assembly, test, quality and purchasing) as well as suppliers and customers to ensure that product requirements are understood and properly flowed to lower level team assigned to developing subcomponent, taking into consideration that these functions could be geographically dispersed.

The philosophy of Integrated Teaming is to establish a product oriented organization based on the decomposition of the product. The structure of the organization is broken down into two levels: the Product level and the Component/ Subcomponent level, and each level should have a leader. The customer of the Subcomponent is its ancestor in the product decomposition architecture (previous level Component/ Subcomponent), which is going to integrate these Subcomponents into Component/ Subcomponent (depending on the decomposition architecture).

The size of the team at each Component/ Subcomponent level should be based on a risk assessment (i.e. a greater proportion of the Integrated Team might be included in the risky Component/ Subcomponent). The majority of the team at any time depends on the phase (i.e. during the design the majority of the team are designers in addition to at least a

single person full/ or part time from each of the other functions as well as a representative of supplier and customer).

The Integrated Team (IT) is empowered by providing them with adequate resources and enables them to make intelligent decisions at the lowest appropriate level (Component/ Subcomponent), so that they conduct business in an integrated and empowered manner.

3. Benefits

The benefits of using Integrated Product and Process Development should be more than just resolving all the issues and problems aroused in traditional products development methods. A sample of the benefits can be summarized in:

1. Reduced development time by:

- Simultaneous development of components and sub components,
- Integrated Team, where decisions are made at the component and sub component level,
- And the reduction of the need for redesign, rework, or contract modifications since all appropriate disciplines are involved concurrently in the decision processes.

2. Reduced development cost by:

- Reducing the time to deliver the product to the customer,
- And the reduction of the need for redesign, rework, or contract modifications

3. Improved Product quality by:

- The use of Integrated Team, where decisions are made at the appropriate level,
 - The use of Component Based Development which reduces the risk of the critical component/subcomponent by the creation of a lower level sub components,
 - And the application of all the necessary processes and resources to provide focused product development that satisfies customer's needs.
4. Improved Information Sharing by:
- The use of Integrated Team that enable well structured collaboration of information through continuous capturing of relevant information thus eliminating or considerably reducing duplication,
 - Dissemination only of the required information between entities that enables it to do the task at hand,
 - But share no other information or the classified one, to protect an organization's information ownership in a joint project.
5. Reduced Risk by the creation of sub components to the risky component/ subcomponent.
6. Improved customer satisfaction by customer involvement throughout the product development (i.e. Customer requirements and expectations will more likely be met).

Glossary

Customer: In the CMMI terminology, Customer is defined as: "the party (individual, project or organization) responsible for accepting the product or for authorizing payment. The customer is external to the project (except possibly when Integrated Product Teams are used, as in IPPD), but not necessarily external to the organization. Customers are subset of stakeholders.

Concurrent Engineering is defined by Department of Defense as: "a systematic approach to the integrated, concurrent design of products and their related processes including manufacture and support".

Integrated Product and Process Development (IPPD): Integrated Product and Process Development is commonly defined as: "a philosophy that systematically employs a teaming of functional disciplines to integrate and concurrently apply all necessary processes to produce an effective and efficient product that satisfies customers' needs". In the CMMI terminology, Integrated Product and Process Development is defined as: "a systematic approach to product development that achieves a timely collaboration of relevant stakeholders throughout the product lifecycle to better satisfy customer needs".

Integrated Team In the CMMI terminology, Integrated Team is defined as: "a group of people with complementary skills and expertise who are committed to delivering specific work products in timely collaboration. Integrated team members provide skills and advocacy appropriate to all phases of the work products' life and are collectively responsible for delivering work products as specified. An integrated team should include empowered representatives from organizations disciplines, and functions that have a

stake in the success of the work products”.

Relevant Stakeholder: In the CMMI terminology, Relevant Stakeholder is defined as: “a stakeholder that is identified for involvement in specified activities and is included in a plan”.

Stakeholders: In the CMMI terminology, Stakeholders is defined as: “a group or individual that is affected by or is in some way accountable for the outcome of an undertaking. Stakeholders may include project members, suppliers, customers, end users and others”.

User: In CMM-SW terminology, User is defined as: “the individual or group who will use the system for its intended operational purpose, when it is deployed in its environment”.

References:

- [1] CMMI, Guidelines for Process Integration and Product Improvement. Mary Beth Chrissis, Mike Konrad and Sandy Shrum, Addison-Wesley.
- [2] Integrated Product Development Implementation Guide, Headquarters Space and Missile Systems Center, Los Angeles AFB, CA, USA.
- [3] RULES OF THE ROAD “A GUIDE FOR LEADING SUCCESSFUL INTEGRATED PRODUCT TEAMS Revision 1”, Under Secretary of Defense for Acquisition, Technology and Logistics, Department of Defense, USA.
- [4] System of Systems Acquisition and Collaborative Engineering Environments, Dr. Ave K. Kludze, Jr., NASA Langley Research Center Hampton, VA 23681, USA.

Biography:

Abdel Meguid Elaraby Is a Freelance Consultant Engineer in the Areas of Information Technology and Process Engineering. He is a Certified Consultant Engineer in the field of Systems Engineering from Egyptian Engineering Syndicate since 1992 and has 30+ Years experience in Information Technology of which over fourteen years of experience as a manager and eight years as a consultant. He has extensive experience as a Business & Information Strategist, and has been actively engaged in Developing and Leading Information Systems Projects that have delivered significant performance and improvement. He has concentrated on Process Improvement, Business Process Reengineering, Software Development Methodologies, Project Management and Acquisition from the perspective of both Purchaser and Supplier.

Feedback contacts

Feedback, comments and questions are appreciated by the author.

Email:

amelaraby@yahoo.com

Into the Security Dilemma:

By: Amr Shaloot

Who are responsible for the security measures in the sold and manufactured Information Technology Systems in Egypt?

This question particularly makes me nervous when I get involved in checking; wither, an IT system, a subsystem, a product or a Security Policy -in general.

What is the code for the governmental interconnectivity? What if a Ministry applies strong Security Policy and another uses a medium one or no one at all? What if one of its subsystems don't force a certain policy or minimum precautions?

What are the minimum security measures an application or device/apparatus must have before it is allowed to run in Egypt?!

Several governmental agencies import applications that may conflict with Egypt's National Security... Who are the responsible organizations for such compliance and what are the procedures they followed to import such? And who verified these procedures?

What about both Public and Private Sector companies? Privacy? Is it only about privacy? What if an application sends information using outbound ports and it is allowed to pass? Who tests these applications and all the security products -them selves, and ensures us that they does not conflict with our interest nor National Security issues?

All the above endless stream of questions upsets me and makes me nervous too.

When you get involved with an IT system you need to verify each and every component of such a system vastly. The hardware now has wireless capabilities and such capabilities must be monitored in both ways, telecommunications and networking. These devices are capable now to transcend to several kilometres and could transmit secret or private data without even accessing any port in the firewall?! Also, even these devices came under strong telecommunications security measures still suffer the noise which can easily be captured wirelessly! Who designed the working environment of these devices? Is it isolated enough?

Who is the one responsible for telling us if such hardware devices are secure or not?

Also, applications now need a continuous connection to manufacturer's website and once it is allowed to pass through the firewall i.e. to get updates, it is very easy to direct the traffic to another pool or in minor cases -especially when using weak firewalls, it really, could transfer all the current processed data to the connected remote machine.

What are other measures enforced in an accounting application that complies with international transparency regulations and international accounting code and standards?

Who certifies all this number of available in the market ready made COTS (Commercial On The Shelf) products either imported or home made rather than those tailor-made currently overspread into the market?

Where are the certifying bodies and do we have the capable staff to run it?

In the last five years, I saw many RFPs asking bidders to provide the source code! While I never could figure why is the reason for such a request, because of other dramatic technical mistakes you can easily find everywhere in the RFP, which tell you -just right away, that no one in this IT unit who wrote such a RFP can even understand one single line of the source code they ask bidders to supply! Or may be it was just because of the open source fever invaded the world after the lovely Linux ®! While I can understand the factors which made such personnel occupying these very-specialized positions even their capabilities are - completely, not suitable for doing it, (some where data entries and promoted to be head of the IT or IS division of a governmental unit or ministry) I still can not un-reveal the secret behind placing such a condition in the RFP. In most optimistic way of thinking asking for the source code was for making the buyer able to modify any part of the application to fulfill any futuristic modifications. But I'm quiet sure that no one will test the code for security issues because no one do understand this strange word Security! Also this raise the question, are this buying entities paying for the source code? And what regulations protect the intellectual rights of developing companies and wither the law enforce NDAs (Non for Disclosure Agreement) or not. What are the compensation packages could match years of developing and Competitors' Intelligence spending to reach this source code if the buying entity disclosed the source code?

This point must be discussed widely with the presence of all parties. An establishment for a unit which is responsible for security measures in the government and also can provide guidance to the private sector, which

has among its members professionals in security, business, military, governmental, and higher education staff, will help Egypt pass this dark tunnel of completely unsafe IT environment.

No one can neglect the dramatic change in the RFPs look when MCIT (Ministry of Communications and Information Technology) started to help other sisters in both governmental and public sectors, but still missing the security part of course.

In the intelligence, military, and police sectors, the security problem is a serious one, and they must establish a sophisticated organization for such purpose. It is no more accepted that these security-based establishments can go with hardware and software anymore the way they are performing nowadays.

I rather would say it loud and clear some security measures in such sensitive state departments does not meet the standards. Some are behind firewalls, IDS, IPS (Intrusion Detection System, Intrusion Prevention System, respectively) and other hardware/software security applications which some of its parts are developed in hostile countries i.e. Israel even a signed treaty still exist! Israel committed several intelligence operations against both state and industrial USA targets. What about Egypt!!! Who tested these wireless devices and its OS (Operating System) and the application it runs? Who either tested the software applications and other hardware that run and all are responsible for the security measures in such departments?! And who are the capable personnel who can do the job?!! What about other applications runs over these layers? Are they secure? Enough?!

Someone help me please here! When a sophisticated peace of information have been decided upon to be physically transmitted by other means ICT not among them, i.e. an aeroplane or a ship, what are the security measures -from encryption to physical security?

Security is no more -in this era of uncertainty, is a pleasure. If such serious thinking and proof of steps to be found on the ground of national ICT infrastructure, no one can tell the consequences. But smart ones can figure them out. Are we going to figure them? Are we going to counter-attack them?

I do not know, but I ask God sincerely not to read the Headline in Al Ahram that a supreme state department have been hacked and serious information are stolen!

Biography

Amr Shaloot, Software Engineer, holds MBA in Strategic Marketing and Business Intelligence. Also he is a Doctoral student in Marketing Intelligence. He is interested in: Investment management, Strategic Marketing and Start Up-s.

Feedback contacts

Feedback, comments and questions are appreciated by the author.

Email:

amr@shaloot.net

Information Security in the Virtual World Series:

By: Ahmed Gad Al-Karim

Introduction

Many organizations today are susceptible to internal and external threats which may abuse its image against its customers. The problem may be extended to harming the business at all specially that most web sites today are commercially based upon payment transactions. Common risks in today's world may be, but not limited to, financial loss, loss of competitive advantage, or legal penalties. The concept of information security nowadays becomes obscured. Many IT employees merge between the computer security and information security. Computer security refers to protecting data on PC's or servers; nonetheless, information security refers to the most generalized form of protecting data in all formats (paper or paperless) on all media types. Some organizations are interested in protecting computer data without any attentions to other data formats' protection. This paper highlights some introductory points about information security with promise to extend and detail these points in upcoming articles.

Security; Problem and Solution

Statistics shows terrible results about security breach consequences on business.

Highlights of the "2002 Computer Crime and Security Survey" include:

- o 90% of respondents (primarily large corporations and government agencies) detected computer security breaches within the last twelve months.

- o 80% acknowledged financial losses due to computer breaches.
- o 44% (223 respondents) were willing and/or able to quantify their financial losses. These 223 respondents reported \$455,848,000 in financial losses.
- o As in previous years, the most serious financial losses occurred through theft of proprietary information (26 respondents reported \$170,827,000) and financial fraud (25 respondents reported \$115,753,000).
- o For the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).
- o 34% reported the intrusions to law enforcement. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)

Respondents detected a wide range of attacks and abuses. Here are some examples of attacks and abuses [1]:

- o 40% detected system penetration from the outside.
- o 40% detected denial of service attacks.
- o 78% detected employee abuse of Internet access privileges (for example, downloading pornography or pirated software, or inappropriate use of e-mail systems).

- o 85% detected computer viruses.

For the fourth year, we asked some questions about electronic commerce over the Internet. Here are some of the results:

- o 98% of respondents have WWW sites.
- o 52% conduct electronic commerce on their sites.
- o 38% suffered unauthorized access or misuse on their Web sites within the last twelve months. 21% said that they didn't know if there had been unauthorized access or misuse.
- o 25% of those acknowledging attacks reported from two to five incidents. 39% reported ten or more incidents.
- o 70% of those attacked reported vandalism (only 64% in 2000).
- o 55% reported denial of service (only 60% in 2000).
- o 12% reported theft of transaction information.
- o 6% reported financial fraud (only 3% in 2000).

(Source:
<http://www.gocsi.com/press/20020407.html>)

Some conclusions are derived from above distinct figures:

- o The computing environment breach is accelerating. It targets primarily DOT COM institutions (corporations with e-Business existence).
- o Data loss is the main incident to most corporations. Most corporations become able to quantify and qualify their information and consider them

as the main asset which make corporation susceptible to major losses if they are lost or treated in unprotected manner.

- o From the point above, most corporations understand the importance of asset classification and data protection levels. Even some countries have Data Protection Acts.
- o The report identifies that breach percent from insiders is more than from outsiders. Employees, if they are not put under restricted security policy, may misuse company assets in a way that inhibit business progress.
- o Most companies penetrate the e-Business world to cope with market complexities.
- o Computing attacks become more sophisticated. The hallow effect that viruses is the main source of breaching become obsolete. Denial of service, viruses, worms, Trojan horses, or even blended threats (which contain more than on technique from the previous) are exaggerated these days.
- o Computer security (logical security) may be insufficient to protect data. Other security methods (physical, personal, procedural ...etc) may be the correct solution.

Nowadays, many external internal and external attacks exist like, but not limited to the following:

- o Telecom eavesdropping
- o System penetration
- o Denial of service
- o Theft of proprietary information
- o Telecom fraud
- o Financial fraud
- o Social engineering

- o Sabotage
- o Insider net abuse
- o Assets theft
- o Unauthorized insider/ outsider access

From the above mentioned threats, it's obvious that Security is not just placing network security appliances like IDS/ IPS, firewalls, Anti-virus servers ...etc. Nowadays computing attacks became more sophisticated. The attack itself becomes unidentifiable whether it's a worm, a virus, or Trojan horse. It may contain all or some types collectively. For example, ZOTOB attack hits Microsoft vulnerabilities that enable remote code execution, in the following sequence:

1. Creates the mutex "wintbp.exe", so that only one copy of the worm runs at one time.
2. Copies itself as %System%\wintbp.exe.

Note: %System% is a variable that refers to the System folder. By default this is C:\Windows\System (Windows 95/98/Me), C:\Winnt\System32 (Windows NT/2000), or C:\Windows\System32 (Windows XP).

3. Adds the value: "Wintbp.exe" = "wintbp.exe" to the registry sub-key: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run so that it runs every time Windows starts.
4. Attempts to detect network connections and a routable IP address. The worm may fail to operate correctly if it determines it is not connected to a network or if the computer's IP address is non-routable.

5. Attempts to connect to the IRC server 72.20.27.115 on TCP port 8080 to listen for the following commands:

- o Download and execute remote files
- o Terminate the worm and delete the file from the compromised computer

6. Opens UDP port 69 to initiate TFTP.

7. Sends packets to IP addresses generated at random based on the IP address of the compromised computer. The IP addresses generated use the first 2 octets of the compromised computer, and randomly generated values for the third and fourth octets. The worm will begin to generate entirely random IP addresses after 32 failures on local IPs or after 512 failures, if it was successful at least once.

8. Attempts to spread by exploiting the Microsoft Windows Plug and Play Buffer Overflow Vulnerability (described in Microsoft Security Bulletin MS05-039), using TCP port 445.

9. If successful, the exploit code will open a back door using TCP port 8594 on the remote computer.

10. Sends the file %Temp%\[NUMBER].bat to the target computer via the back door. This file contains a TFTP script that will download a copy of the worm from the compromised computer.

Note:

- o [NUMBER] represents several random numbers from 0 – 9

- o %Temp% is a variable that refers to the Windows temporary folder. By default, this is C:\Windows\TEMP (Windows 95/98/Me/XP) or C:\WINNT\Temp (Windows NT/2000).

11. Saves this file as %Windir%\a[NUMBER].exe on the target computer and executes it.

Note: %Windir% is a variable that refers to the Windows installation folder. By default, this is C:\Windows or C:\Winnt.

12. Logs the successfully exploited IP addresses to the IRC server 72.20.27.115.

This example clarifies how complexity become today's attacks. They become more sophisticated, or what are named as blended threats.

Information Security has a more broaden view. Security has CIA 3 corner stones: Confidentiality, Integrity, and Availability.

Confidentiality:

Information is accessible only to the authorized.

Integrity:

Accuracy and completeness of information and processing methods.

Availability:

Authorized users have access to information and associated assets when required.

To identify these concepts, let's take a strange example:

A network that is hardened (secured) by placing security countermeasures on all levels (Perimeter/ internal network, servers, and applications)

may be susceptible to interrupted operation because there are no levels of redundancy (e.g. clustering, load balance, shortage in computing spare parts ...etc), This means that availability cornerstone of security is not achieved properly, so a major cornerstone of the security is breached. So that security is a major concern in operations management.

Some other examples that may harm network without properly planning and designing, on all levels, for security:

- o Opening unsolicited mail without verifying its source.
- o Failing to batch your system.
- o Installing screen savers and games without verifying that they are safe.
- o Not making and testing backups.
- o Connecting modem to your PC while connecting it at the same time to the LAN.
- o Assigning untrained people to do jobs.
- o Failing to understand the relationship between security and business value.
- o Making few fixes to your system without ensuring that the root cause to the problem is resolved.
- o Relying primarily on firewalls, or running firewalls that allow incoming/ outgoing malicious traffic.
- o Failing to understand the money value of your business information so that you can place security countermeasures that reserve this value.
- o Pretending problem will go away if it's ignored.

- Connecting your LAN to the internet without hardening it.
- Setting your systems with default accounts.
- Using unencrypted connections over untrusted media (e.g. Internet)
- Giving sensitive information to users over phone, e-mail, or chat.
- Running unnecessary services on the server.
- Failing to update your systems.
- Failing to design and implement a proper security policy.

Dependence on information systems and services means organizations are more vulnerable to security threats. The interconnecting of public and private networks and sharing of information resources increases the difficulty of achieving access control. The trend to distributed computing has weakened the effectiveness of central, specialist control. Many information systems have not been designed to be secure. The security that can be achieved through technical means is limited, and should be supported by appropriate management and procedures. Identifying which controls should be in place requires careful planning and attention to detail. Information security management needs, as a minimum, participation by all employees in the organization. It may also require participation from suppliers, customers or shareholders. Specialist advice from outside organizations may also be needed.

I think that we all agree on considering security as the main solution to the business sustainability.

When you are dealing with information security as security specialist, you must consider eight general principles:

1. Information security should support company goals. Security is business enabler not inhibitor. It protects organization's assets, enables new business opportunities, helping to promote customer loyalty, and perceives business added values. Some people wrongly think that security means closing freedom valve. The reply to this mistaken idea is that freedom doesn't mean giving attackers the chance to elevate wrong privileges. If the business sustainability needs the freedom valve closing, let's agree upon doing that.
2. Information Security is an integral part of good management. Management should be well educated about the security importance. Different security training levels must be given to all employment levels in the company.
3. Information security should be cost-effective. The costs of implementing information security, and the benefits that it will bring, should be carefully examined to ensure that the cost of security controls doesn't exceed the expected benefits.
4. Information security responsibilities and accountability should be stated explicitly to everybody inside and outside the corporation even across cross organizational boundaries.
5. System owners have information security responsibilities outside their own organizations. If an organization's system has external users, the owners of that organization have a responsibility to these users to share sufficient knowledge with

them about existence and general extent of any security systems, thus reassuring them that the systems are adequately secure. The owners have the responsibility to act in a timely and coordinated manner, to prevent and respond to any breaches to security.

6. Information security requires comprehensive and integrated approach to a number of areas inside and outside the field of information security to assure that an effective information security is provided.
7. Information security should be reassessed periodically. Security requirements are changing continually with the sophistications of computer systems, information attacks, and many other considerations.
8. Information security is constrained by social factors. Security measures should be selected and implemented with due regard to the rights and legitimate interests of others. This may involve weighting the security requirements of the users with the social issues in that area. Such issues as privacy need to be considered.

Steps needed to establish a good security system, concept of layered security, concept of Defense-in-Depth and definition and importance of Security standards are to be raised in the coming article.

References

- [1] Egyptian e-Gov Security code of practice – By e-Gov workgroups, publication 2002 – <http://www.egypt.gov.eg/arabic/documents/default.asp>.
- [2] Symantec Security response – ZOTOB attack on Microsoft windows Plug and Play Buffer overflow vulnerability that enables remote code execution.
- [3] Internet Security Systems (www.iss.net)
- [4] Computer Security Institute (CSI) Survey – Cyber crime bleeds U.S. corporations (<http://www.gocsi.com/press/20020407.html>)

Biography

Ahmed Gad Al-Karim, is a security and infrastructure consultant in the Egyptian e-Gov Program. He has 7 years of experience in the field of information technology. Currently, he is a Techno-MBA student. Information security is his major interest. His interests include ISO 17799, BS 7799 security systems.

Feedback contacts

Feedback, comments and questions are appreciated by the author.

Email:

ahgad@mcit.gov.eg

CMMI Implementation Series

By: Ahmed Abd El Aziz

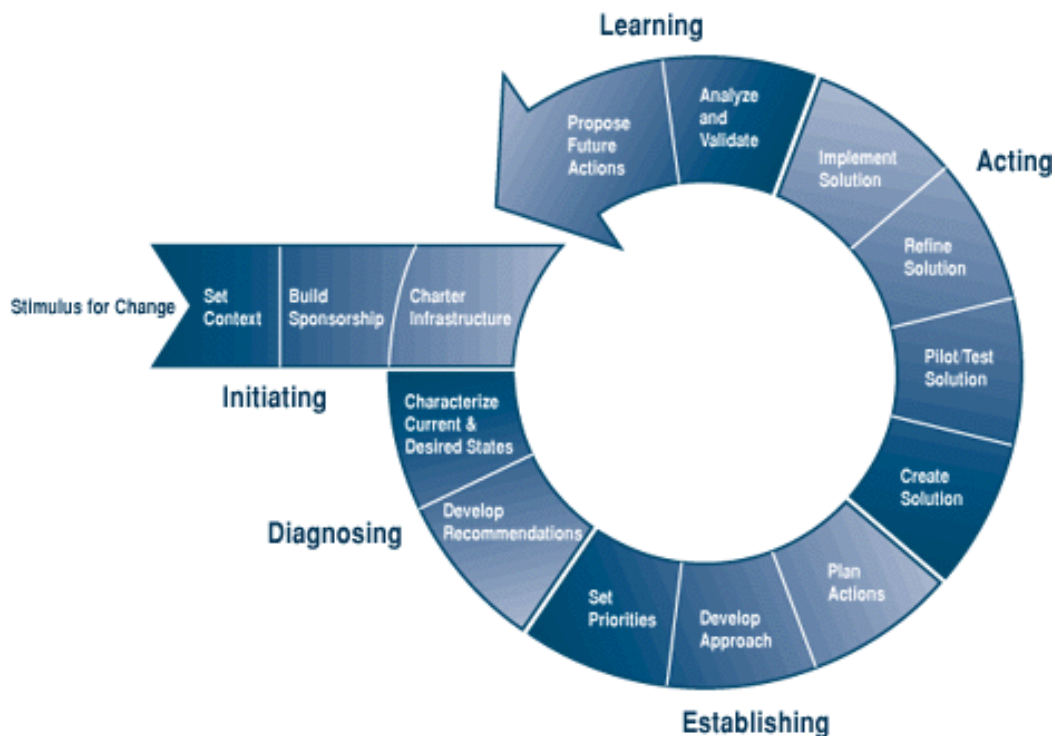
As we all know, SECC has started one of its greatest projects since the start of July 2005 to the end of June 2006 which aims to supporting 20 companies in implementing CMMI and will end up with certifying 5 of these companies to maturity level 3 or at least maturity level 2. This is one step on the road. It is not the first one, and of course it will not be the last. I had an excellent opportunity to attend the "Intermediate Concepts of CMMI" in June 2005 and to participate in implementing CMMI in one of the 20 companies. I admit that I am beginning my trip with Process Improvement. As a matter of fact I faced many difficulties. I would like to share with you my little experience from my little work in process improvement and from my discussions with colleagues in other companies.

This article is the first in a series of articles that will document the lessons I learned while implementing CMMI. I will use the IDEAL approach as a lifecycle for Process Improvement and I will write my on points on each phase.

The CMMI Implementation

IDEAL is not one word. These are the first letters of five words that constitute the main process improvement phases. These words are **I**nitiating, **D**iagnosing, **E**stablishing, **A**cting, and **L**earning.

For more information about the ideal model, please refer to the SEI site.



Now we will talk about the main and sub phases of the model. In this article I will discuss the Initiating and Diagnosing phases only. In the next SPIN issue I will continue with the other phases.

The Initiating Phase

Stimulus for Change

Why do we want to improve our processes? What problems we have? What are our weaknesses and our strengths? These are basic questions at the start of the process improvement trip. But guess what. Many of us did not think about these questions. We start in implementing CMMI may be because we think it is good, because we want to be one of the 5 companies selected for final appraiser, because management wants that, or whatever. There is no doubt that these are good objectives, but are they enough to start such big effort and annoy all our staff with new processes and forms and so on?

Absolutely not; people usually resist change. They must feel that the change really helps them do things better. Before we start any process improvement activities, we must first analyze our strengths and weaknesses. Then we do the effort required to overcome our weaknesses and keep our strengths. This helps us to get buy-in from people developing and implementing the new processes because they know that these processes are there to fix their problems, not only to get certificate or satisfy management or owners.

Set Context

I heard this statement from many people in companies that implemented ISO, CMM, or CMMI: "We are certified but we do not get real benefit from the system. It is just a documentation system." I think the main reason of

that is that the context was not clear. "Setting context" means being very clear about where this effort fits within the organization's business strategy. What specific business goals and objectives will be realized or supported by this change? How will it affect other initiatives and ongoing work? What benefits (such as return on investment or improved capabilities and morale) will result?

Here come other problems. One would say "Ha, we do not have business goals and objectives". The other would say "We do not have measures at the moment, so how can we know if we really got some benefit or not?" This is really the case in most of our companies. So I think that the most important process improvement objectives that we have to start with are overcoming our weaknesses and the ability to predicting our state. I think prediction itself is the main goal of the first process improvement. Later we will have measures, as a consequence of the first process improvement effort, and hence we can monitor them. Saying that "By implementing CMMI we will increase productivity and decrease rework" is meaningless if we do not have measures to our current productivity or rework. Predict first then improve. Otherwise, saying we improved or not is just an opinion.

Build Sponsorship

I will not explain what sponsorship means, as we all know that. I will explore some of real life situation I faced or heard about that show "Oral Sponsorship" not real and effective sponsorship.

Some of the companies deal with the process improvement leader as an expert in many topics – e.g. project management – beside process improvement. In most of cases he is really expert in these issues. Then the

management asks him for other tasks or consultancy in these topics. The management says that these topics are much more important at the moment. As a consequence, he loses concentration in process improvement. This way we lose him as a process improvement leader. Finally we end up with nothing because can not wear two big hats at the same time.

In some companies the management promises the process improvement leader to assign him some resources for 20 % of their time. In the same time they assign these resources many development tasks that need more than 120 % of his time. When the process improvement leader asks these resources to do some process improvement effort, they excuse and say that they are doing "real work" now and when they have some free time – which most probably will not happen – they will do the process improvement work.

Charter Infrastructure

Infrastructure means mainly the human resources allocated to the process improvement effort. There are two many variations in defining the infrastructure. It could be permanent or temporary. Its name could be Process Improvement Group (PIG), Engineering Process Group (EPG), Software Engineering Process Group (SEPG), or whatever.

I will not discuss these issues here. Actually I do not have enough experience to do so. What I want to explore is the two approaches I see that companies follow and my own judgment on both.

The first approach is assigning and fully dedicating some one as the process improvement leader and assigning many other people as EPG members in 20 % of their time. The second approach is to fully assign and

dedicate three or four people for the process improvement effort with little support from other staff.

What I see so far is that the second approach is more successful than the first one. When it comes to reality, it is very hard to get this 20 % from people's time in process improvement whatever their commitment and their management's commitment is.

The Diagnosing Phase

Characterize Current and Desired States

This step is greatly supported by SECC. One of the early steps in the current program is "Gap Analysis". The QAI consultant, SECC consultant, and the company staff together see the gaps between the current company processes and practices and the CMMI requirements. They end up by defining the target maturity level, the disciplines, and high level action plan.

At the time of writing this article, the gap analysis is already done in most of the 20 companies. My advice to those who did not start gap analysis yet is not to wait for gap analysis and to start planning and process improvement activities. You can define most of the gaps yourselves and wait for the formal gap analysis to make sure you are on the right way.

Take care that in gap analysis, QAI consultant is mainly concerned with understanding how work is done in your organization to detect gaps, not in providing consultancy or solutions. So it is not recommended to invite many people to the interviews or to be part of the appraisal team as this may waste their time.

The desired state could be maturity level 2 or 3. I see most of the companies are running forward towards maturity level 3. Some of

these companies do not have any documented processes or certified in ISO, CMM or CMMI. They take it as a challenge, to reach maturity level 3 in 7 months – from September 2005 to Mars 2005. It is really a big challenge, but I do not think it is beneficial to move from maturity level 1 to maturity level 3 in 7 months. Many activities in maturity level 3 organizations require historical data. These historical data can not be built and used within 7 months only! Another point, 7 months are not enough period to “institutionalize” all maturity level 3 processes. Look also to the number of new processes and templates the people have suddenly to follow in this short period. You can not suddenly ask people to follow about 50 or more different process, templates, checklists, and so on while they were not used to follow any documented process before. You may achieve the desired maturity level and lose your main assets, your staff!

Develop Recommendations

You must define how many types of projects are there in your company and how you will write the processes for them. You may decide to write high level processes and for each process there could be different procedures for every type of projects or you may decide to write different sets for processes for every type of projects. Which one is the best? The famous SEI answer, it depends. But let’s say that the best is what fits with the company needs and what is read by the staff.

Another point you have to care about, should the process be long and document and detail everything or it should be small and compact? Again, it depends. But as a matter of fact, people hate to read. They want simple instructions and diagrams to follow. If you ask them to follow 50 pages process, I am sure they will not even

read it. If it is not read, then it is not followed!

Biography

Ahmed Abd El Aziz, has more than eight years of experience in the Software Development field. He worked as a programmer, a project manager, and Internet Department Manager. He is now member in the process improvement team in HARF Information Technology. He is certified as Project Management Professional (PMP). He passed the “Intermediate Concepts of CMMI” course. He has a B.Sc. Of Engineering from Cairo University and a Diploma in Computer Science and Information from Cairo University, Institute of Statistical Studies and Research (ISSR).

Feedback Contacts

Feedback, comments and questions are appreciated by the author.

Email:

aaz@harf.com