Process Capability and Maturity in Information Security

Alpana Kakkar, Ritu Punhani, D. Jain

Process Capability and Maturity in Information Security

Alpana Kakkar

Deputy Director, Institute of Information Technology,
Amity University, Noida, U.P – India

Ritu Punhani

Asstt. Professor, Institute of Information Technology,
Amity University, Noida, U.P – India

D. Jain

HCL Technologies Ltd., India

Process Capability and Maturity in Information Security

Abstract

Information security has been more prominently considered under product approach in which this is considered as a framework of products providing different functionalities or features of information security like information availability, authenticity, non-repudiation, etc. But there is another important view point of information security. This is the Process View of information security in which the information security is considered as a process rather than a product. The process approach provides the benefits of repetitiveness, simplicity, and also statistically measureable and controllable. One can statistically manage the process for its maturity and capability.

This white paper talks about understanding the information security as a process and then understanding the concepts of process maturity and capability for Information Security in organizations.

Understanding Process of Information Security

Process is a set of ordered repeatable steps that are executed to accomplish specific tasks. Any process has very specific entry and exit criteria. A process addresses problems and solutions in a structured way including interrelationships and dependencies.

Information security has been more prominently considered under product approach in which this is considered as a framework of products providing different functionalities or features of information security like information availability, authenticity, non-repudiation, etc. But there is another important view point of information security. This is the Process View of information security in which the information security is considered as a process rather than a product.

This is well proven that the people who understand the value and purpose of focused and effective processes (i.e. have a process mindset) can create a well-run business complete with the required checks and balances. Inherent in these organizations will be a foundation and culture that will be poised to exponentially grow with the improved productivity, quality, and reduced chaos.

This makes the process mindset of information security more important. In this process mindset of information security, the information security framework can be considered as a process providing repeatability, continuity, and simplicity.

Understanding Process Capability

One must understand that process control is not same as process capability. The AT&T Statistical Quality Control Handbook states, “The natural behavior of the process after unnatural disturbances are eliminated is called the process capability.” The handbook emphasizes that a process capability study is a systematic investigation of a process by using control charts to determine its state of control, checking any lack of control for its cause and taking action to eliminate any nonrandom behavior when justified in terms of economics or quality.

Process control talks about the stable nature of the process using agreed performance measures of the process over a given distribution of time and hereby address the inner voice of the process. This signifies that the process performs in an expectable distribution and hereby shows a stable behavior.

The process capability on the other hand talks about how good the process is. This in fact takes in it the “voice of customer” in terms of specification limits and “voice of process” in terms of control limits of the process.

The objective of process capability is to get as close to the theoretical best variation that the process can achieve by eliminating special causes of variation, so that only common causes are acting on the process, and then to reduce these to a minimum whenever possible.

Understanding Process Maturity

Process maturity is an indication of how close a process is to being complete, and capable of continuous improvement through quantitative measure and feedback. In today's business environment many organizations face the challenge of complying with regulatory, industry or contractual standards. The challenge is not just about complying but the organizations must also prove their compliance. Most competitive businesses around the globe are focusing on their processes for quality improvement, cost reduction and delivery-time reduction. They also are looking at other ways of achieving an edge over competitors, and for this they believe on making their processes more and more mature.

Organizations never hesitate to go for third party international standards and process audits for timely assessment of their process maturity and this in fact has made the international standard process maturity certification like CMM, CMMi, ISO, PCMM, ITIL, COPC etc. very popular.

Understanding in minimum words, the maturity of a process indicates the directive efforts of the entire team to meet the common goal. For the overall effort to be successful, decisions and actions must be coordinated among individuals and between groups. They also must be consistent and yield satisfactory results at reasonable cost. Generally businesses follow an approach or framework which is a top down structure from planning to action, as illustrated in Figure 1.

For the overall effort to be successful, decisions and actions must be coordinated among individuals and between groups. They also must be consistent and yield satisfactory results at reasonable cost. Generally businesses follow an approach or framework which is a top down structure from planning to action, as illustrated in Figure 1.

Understanding CMM

The Capability Maturity Model (CMM) was originally intended to characterize processes involved in software development that affect the quality of the code that is produced. In a nutshell, the lowest CMM level (level 0) is called "nonexistent;" there is no awareness of the need for systematic development processes. At the highest level (level 5), development processes are optimized by being implemented, monitored and managed throughout an entire organization. The Software Engineering Institute (SEI) validated this model by empirically showing the relationship between processes in real-world software development settings and quality metrics such as number of bugs per 1000 lines of code.

In 1987, Software Engineering Institute of Carnegie Mellon University – USA started the project for introducing CMM or Capability Maturity Model as a reference for an objective evaluation of different software devices' ability to perform for the government. Capability Maturity Model (CMM v1.0), the very first CMM, was developed and released in August of 1990.

This reference model is a five level assessment model developed with a focus to illustrate the best practices regarding engineering and management, specifically in software development. It is proved to be an evolutionary model of the movement of any software developing group or organization.

Capability Maturity Model

The capability maturity model (CMM) is not a process model for software development but is a model that describes the maturity of the organization or the team developing the software and the process of development. The CMM was defined by the Software Engineering Institute (SEI) of Carnegie Mellon University along with many other organizations with an intention of measuring the efficiency and sense of maturity of the process of development.

In its structure, CMM categorizes hierarchically software-developing organizations on the basis of the maturity of their process, in five distinct levels (Figure 2). Each of these levels is defined with set of associated process goals. These levels are defined here.

1. **Initial:** The first and lower most CMM level is known as 'initial'. At this level, most of the processes run on ad-hoc practices and the success of the process depends on the expertise of developers. But the success history does not repeat so often in any defined manner. This is due to the unavailability or non-adoption of any formal method with retainable documentations. The process at the initial level is disorganized and crisis probable.

2. **Repeatable:** The second-lowest level of the CMM is named as ‘repeatable’. At this level, strategies for carrying out the development process are formally planned and the development is tracked. As the name of the level suggests, the process is repeatable for its success because of formal planning.

3. **Defined:** At the third level from the bottom of the hierarchy in CMM, the ‘defined’ level, the process of development is formally defined at all levels of organization. A formal organizational constitution is defined, which is followed at all levels of development to develop a formal management control over the process.

4. **Managed:** At the next level of CMM, organizations establish metrics and measured controls over the process. This leads to a fair management of the process with quantitative definitions of goals and process to achieve these goals.

5. **Optimization:**The top most level of CMM is ‘optimization’, where the goal of the organization is not only the user satisfaction and development of highly efficient software but also contribution to their social and ethical responsibilities towards software practices in a formal manner. At this level, organizations work for the betterment of not only the products but also of the process. This level in CMM has a set goal of making improvements in traditional processes of software development.

The CMM is important to compare the software-engineering processes for maturity of their approach and efforts to improve the software products and development processes for better quality and better process control. It is used as a guideline for software process improvement efforts. The CMM categorizes software-development organizations on the basis of their contribution to the software market in terms of improvement in the software product quality by enhancing the development life cycle process. It specifies the ethical and social responsibilities associated with the development procedures for software. It describes the parallel importance of process improvements along with product improvement as user satisfaction. It also introduces hierarchy in software industry, based on maturity of the work of organization. Some major responsibilities defined at each level of CMM are mentioned in Figure 3.

Focus of CMM

Not surprisingly, the CMM model is also widely applied to information security practices to the point that it has become a major basis for measuring the performance of an information security practice. There is a certain intuitive goodness to the CMM model; as one goes to higher CMM levels, more processes that appear to systematically address risk are present. At level 2, for example, processes are repeatable but intuitive; comprehension the nature of risk and the need for security is just starting to happen. At level 3, there are defined processes, as evidenced by an organization-wide security risk management policy and the emergence of security training and awareness.

At the time of development and release, the main focus of CMM was to aid the US government in evaluating software providers' abilities to handle large projects. They were interested to ensure the measurability of capability of the software development groups to produce high quality and reliable software products by following well defined, properly controlled, and highly mature development processes.

The focus was to ensure more established and advanced processes for software development with lesser flaws in scheduling and budgeting of the projects. Also, there were needs to improve the quality of the product with lesser defects by improving in the development process. CMM reference model improved the things and helped in providing effective solutions to most of these challenges.

Applying CMM on Information Security Process

The CMM model has been applied to information security practices for at least a decade. But assessments of information security practices often find that the information security processes seldom reach the highest level of 04 or 05. These processes face high challenges and usually are found to reach only to the CMM levels of 02 or maximum 03

Dr. Eugene Schultz finds several reasons for this [2]:

1. Failure on the part of information security managers (ISMs) to truly understand the nature of the business(es) that they are supposed to defend, support and enable. Without a genuine understanding of the business itself as well as the business processes involved, a large gap between senior management's and the ISM's expectations is likely to develop, something that almost always costs information security practices in terms of credibility, leverage, and resources needed to effectively manage risk.

2. A general lack of knowledge regarding information security management. Too often technically competent people are pushed into information security management with any kind of appropriate information security management knowledge and skills. Many lack even the most basic knowledge of security, let alone security management. The result is inevitable—"barking up the wrong tree" (or sometimes simply wallowing in indecision) when it comes to managing security risk correctly and efficiently.

3. Obstacles imposed by senior management. Senior management's lack of knowledge concerning information security is one of the most formidable obstacles to the maturity of information security practices. Without suitable knowledge, senior management is unlikely to adequately support information security efforts in terms of elevating the ISM position to a suitable level within the organization, signing off on policies, standards and procedures, providing adequate resources, and more.

4. Lack of oral communication and interpersonal skills on the part of ISMs. Although many ISMs excel in oral communication and interpersonal skills, some do not. The people factor is essential in on-the-job success (not just in information security, but also in just about every job and task); communication and interpersonal skills are thus essential if ISMs are going to bring their practices to levels of greater maturity.

5. Failure to set proper security goals for information security practices and to monitor and report progress. Too often ISMs do not set appropriate goals for their information security programs, or it they do, they do not design and put in place processes for monitoring and communicating (e.g., to senior management) the degree to which goals are or are not being met.

6. Failure to cooperate with and leverage other, similar functions within organizations. Other functions within organizations such as physical security and audit have many common interests and goals with information security. Given that resources available to information security are almost invariably limited, cooperating closely with and leveraging these other functions in mitigating risk is the most logical course of action. Some ISMs neglect doing this, however.

There are additional reasons that information security practices do not achieve greater levels of CMM maturity. The ones I have presented are in my mind the most critical ones, however.

Conclusion

Information security can be understood as a process mind set also. The concepts of process capability and maturity can be applied to processes of information security also. The implementation of CMM in information security processes can make this more mature and capable, but this faces many challenges and need more researches and practices to be implemented.

Figures and Tables

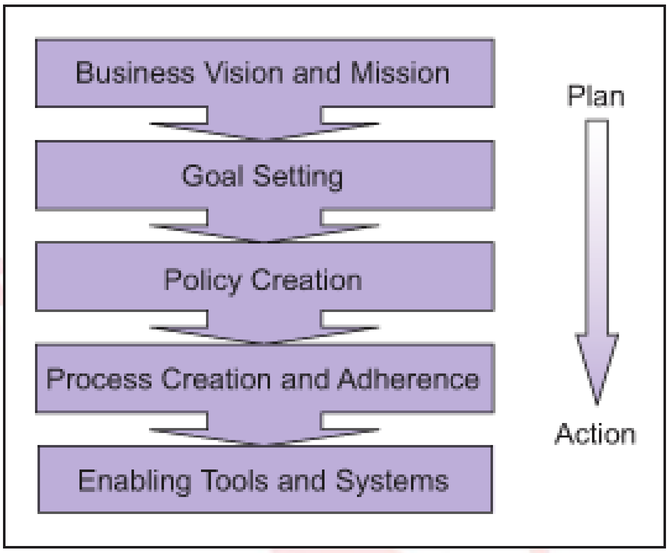
Business Vision and Mission
Goal Setting
Policy Creation
Process Creation and Adherence
Enabling Tools and Systems
Plan
Action

Figure 1: A general business framework

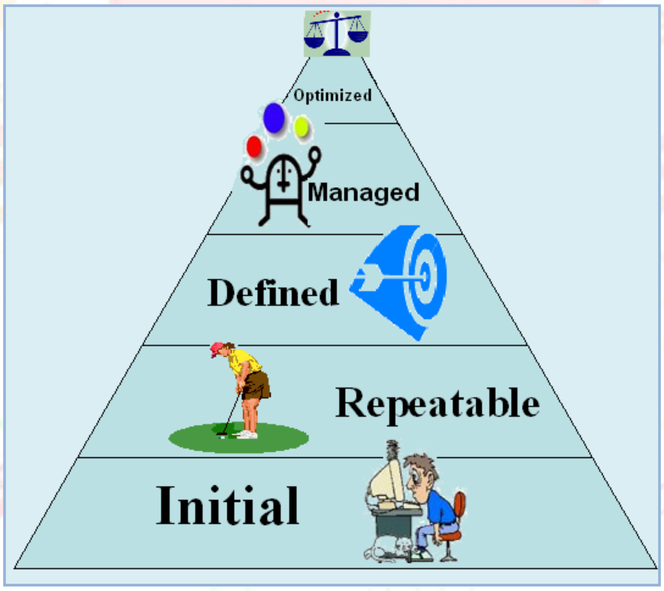

Figure 2: 5-Level Process Maturity Reference Model (CMM)

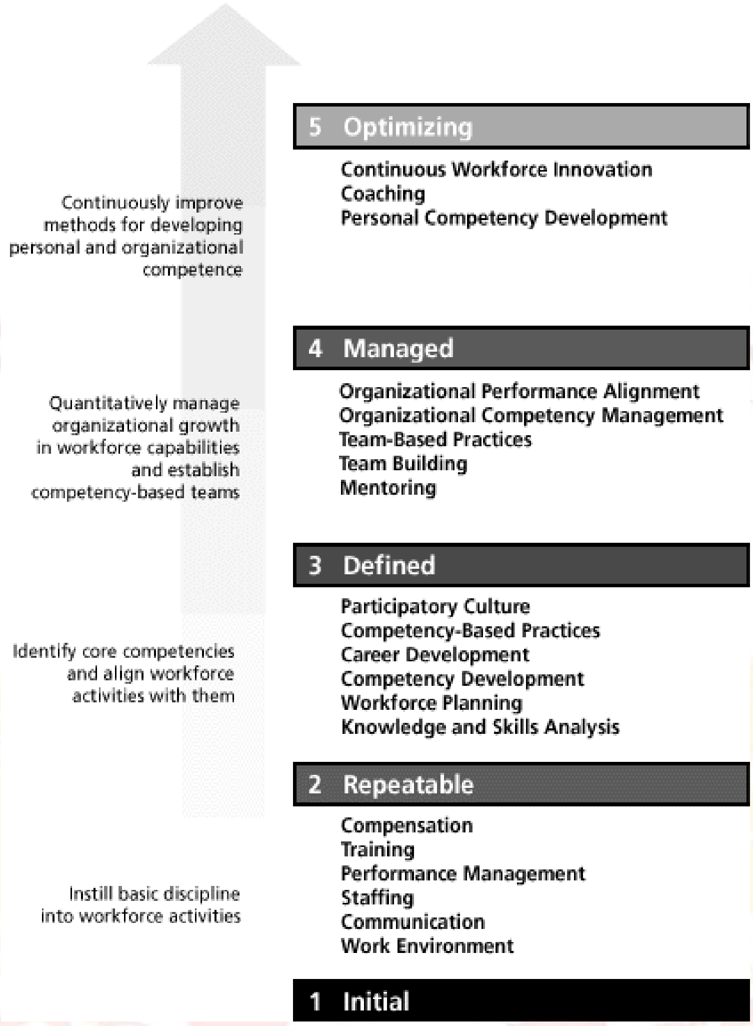
5 Optimizing
Continuous Workforce Innovation
Coaching
Personal Competency Development
Continuously improve methods for developing personal and organizational competence
4 Managed
Organizational Performance Alignment
Organizational Competency Management
Team-Based Practices
Team Building
Mentoring
Quantitatively manage organizational growth in workforce capabilities and establish competency-based teams
3 Defined
Participatory Culture
Competency-Based Practices
Career Development
Competency Development
Workforce Planning
Knowledge and Skills Analysis
Identify core competencies and align workforce activities with them
2 Repeatable
Compensation
Training
Performance Management
Staffing
Communication
Work Environment
Instill basic discipline into workforce activities
1 Initial

Figure 3: Responsibilities defined at each step of CMM

References

1. D. Jain (2008), Software Engineering: Principles & Practices, Oxford University Press

2. Eugene Schultz (Jan 2008) The Capability Maturity Model in Information Security; DOI: http://blog.emagined.com/2008/01/17/the-capability-maturity-model-in-information-security

3. James LaPiedra (2011), The Information Security Process Prevention, Detection and Response, Global Information Assurance Certification Paper, GIAC directory of certified professionals.

4. Juhi Vasisht (2006), A Process Mindset: A Foundation for Information Security, Technical Enterprises, Inc., The ISSA Journal, January 2006

5. Kakkar, Alpana, Ritu Punhani, and D. Jain, (2011) "HARVESTING THE WEB TO PROCURE SECURE INFORMATION FOR ENTERPRISE" IARS' International Research Journal, DOI: http://irj.iars.info/index.php/82800101201105

6. Karen Ferraiolo (2000), The Systems Security Engineering Capability Maturity Model, ISSEA

7. Kelley Dempsey, Arnold Johnson, Ronald Johnston, Alicia Clay Jones, Angela Orebaugh, Matthew Scholl, and Kevin Stine (2011), Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, Gaithersburg, MD, USA.

8. Mark C. Paulk and Michael D. Konrad (1994), MEASURING PROCESS CAPABILITY VERSUS ORGANIZATIONAL PROCESS MATURITY, Software Engineering Institute, Carnegie Mellon University, Pittsburgh

9. Mitchell Rowton (2011), Information Security as a Process, PacketSource — Security White Papers, DOI: http://www.packetsource.com/article/policy-guides/38249/information-security-as-a-process

10. S.W. Smith, Eugene H. Spafford (2004), Grand Challenges in Information Security: Process and Output, IEEE SECURITY & PRIVACY, IEEE COMPUTER SOCIETY.

International Association of Research Scholars
IARS
Transforming Research
Since 2011
www.iars.info

Certificate of Recognition

This certificate is awarded to

Alpana Kakkar

in recognition of his / her contribution

"Process Capability and Maturity in Information Security"

to Vol. 01, No. 02, 2011 *of*

IARS International Research Journal
An International Refereed Research Journal
ISSN 1839-6518 (Australian ISSN Agency)

Editor in Chief

International Association of Research Scholars
IARS
Transforming Research
Since 2011
www.iars.info

Certificate of Recognition

This certificate is awarded to

Ritu Punhani

in recognition of his/her contribution

"Process Capability and Maturity in Information Security"

to Vol. 01, No. 02, 2011 *of*

IARS International Research Journal
An International Refereed Research Journal
ISSN 1839-6518 (Australian ISSN Agency)

Editor in Chief