

INFORMATION SYSTEMS AUDITING STANDARDS, GUIDELINES, BEST PRACTICES

Question 1

What do you understand by Software Process Maturity? Discuss five levels of Software Process Maturity of Capability Maturity Model (CMM). (10 Marks) (Nov 2008)

Answer

A software process is a set of activities, methods, practices, and transformations that are used to develop and maintain software and the associated products such as project plans, design documents, code, test cases, and user manuals.

Software process maturity is the extent to which a specific process is explicitly defined, managed, measured, controlled, and effective. Maturity implies a potential for growth in capability and indicates both the richness of an organization's software process and the consistency with which it is applied in projects throughout the organization. As a software organization gains in software process maturity, its institutionalization in software process building takes place.

The Five Levels of Software Process Maturity

Continuous process improvement is based on many small, evolutionary steps rather than revolutionary innovations. The CMM provides a framework for organizing these evolutionary steps into five maturity levels that lay successive foundations for continuous process improvement. These five maturity levels are discussed below and shown in the figure:

- (i) *Level 1 - The Initial Level:* At the Initial Level, the organization typically does not provide a stable environment for developing and maintaining software. At this Level, capability is a characteristic of the individuals, not of the organization. During a crisis of software success depends entirely on having an exceptional manager and a seasoned and effective software team. But if someone leaves the project, it is difficult to handle the crises and a challenging task.

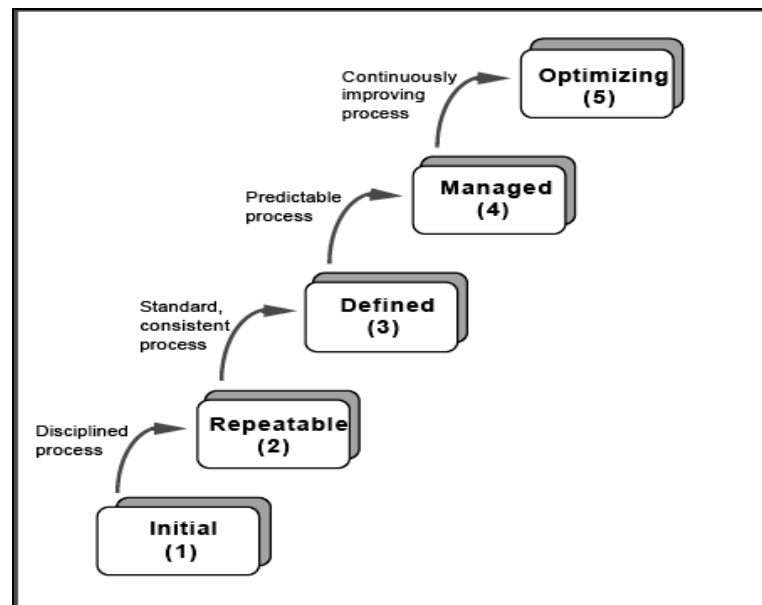


Fig.: Levels of CMM

- (ii) *Level 2 - The Repeatable Level:* At this Level, policies for managing a software project and procedures to implement those policies are established. Planning and managing new projects is based on experience with similar projects. An effective process can be characterized as one which is practiced, documented, enforced, trained, measured, and able to improve. This Level makes the organizations to install basic software management controls. Software project standards are defined. The project's process is under the effective control of a project management system, following realistic plans based on the performance of previous projects.
- (iii) *Level 3 - The Defined Level:* At this Level, documentation for development and maintenance is prepared. This standard process is referred to throughout the CMM as the organization's standard software process, to help the software managers and technical staff perform more effectively. A group of experts standardize the process. An organization-wide training program is implemented to ensure that the staff and managers have the knowledge and skills required to fulfill their assigned roles. This process capability is based on a common, organization-wide understanding of the activities, roles, and responsibilities in a defined software process.
- (iv) *Level 4 - The Managed Level:* At the Managed Level, the organization sets quantitative quality goals for both software products and processes. Productivity and quality are measured for important software process activities across all projects as part of an organizational measurement program. An organization-wide software process database is used to collect and analyze the data available from the projects' defined software processes.

This level of capability allows an organization to product trend in process and product quality within qualitative limits. Because of the stability and measured data when some exceptional circumstance occurs, the special cause of variation can be identified and addressed. The software products are of predictably high quality.

- (v) *Level 5 - The Optimizing Level:* The entire organization is focused on continuous process improvement. The organization has the means to identify weaknesses and strengthen the process proactively, with the goal of preventing the occurrence of defects. Data on the effectiveness of the software process is used to perform cost benefit analyses of new technologies and proposed changes to the organization's software process. In short, the cost of development is cut, best engineering practices are developed and used. Continuous improvement is done. Technology and process improvements are planned and managed as ordinary business activities.

Question 2

State and briefly explain the contents of a Standard Information System Audit Report.

(5 Marks) (Nov 2008)

Answer

According to the recommendations, IS Audit reports broadly include the following sections: title page, table of contents, summary including the recommendations, introduction, findings and appendices. These components of an audit report are discussed below:

- (i) *Cover and Title Page:* Audit reports should use a standard cover, with a window showing the title: "Information System Audit" or "Data Audit", the department's name and the report's date of issue (month and year). These items are repeated at the bottom of each page. The title page may also indicate the names of the audit team members.
- (ii) *Table of Contents:* The table lists the sections and sub-sections with page numbers including summary and recommendations, introduction, findings (by audit field) and appendices (as required).
- (iii) *Summary / Executive Summary :* The summary gives a quick overview of the salient features at the time of the audit in light of the main issues covered by the report. It should not normally exceed three pages, including the recommendations.
- (iv) *Introduction:* Since readers will read the summary, the introduction should not repeat details. It should include the following elements:
 - “ *Context:* This sub-section briefly describes conditions in the audit entity during the period under review, for instance, the entity's role, size and organization especially with regard to information system management, significant pressures on information system management during the period under review, events that need to be noted, organizational changes, IT disruptions, changes in roles and programs, results of internal audits or follow-up to our previous

audits, if applicable.

- “ *Purpose:* This sub-section is a short description of what functions and special programs were audited and the clients' authorities.
 - “ *Scope:* *The scope lists the period under review, the issues covered in each function and program, the locations visited and the on-site dates.*
 - “ *Methodology:* *This section briefly describes sampling, data collection techniques and the basis for auditors' opinions. It also identifies any weaknesses in the methodology to allow the client and auditee to make informed decisions as a result of the report.*
- (v) *Findings:* Findings constitute the main part of an audit report. They result from the examination of each audit issue in the context of established objectives.
- (vi) *Opinion:* If the audit assignment requires the auditor to express an audit opinion, the auditor shall do so in consonance to the requirement.
- (vii) *Appendices:* Appendices can be used when they are essential for understanding the report. They usually include comprehensive statistics, quotes from publications, documents, and references.

Question 3

When an organization is audited for the effective implementation of ISO 27001 Information Security Management System, what are to be verified under:

- (i) *Establishing Management Framework*
- (ii) *Implementation*
- (iii) *Documentation.* (10 Marks) (Jun 2009)

or

An organization is audited for effective implementation of ISO 27001 – Information Security Management Standard. What are the factors verified under:

- (i) *Establishing management framework?*
- (ii) *Implementation?*
- (iii) *Documentation?* (8 Marks) (May 2011)

Answer

ISO 27001 – Specification for Information Security Management Systems

It deals with the Information Security Management Standard (ISMS). In general, organizations shall establish and maintain documented ISMS addressing assets to be protected,

organization approach to risk management, control objectives and control, and degree of assurance required.

- (i) *Establishing Management Framework*: This would include the following activities:
 - .. Define information security policy;
 - .. Define scope of ISMS including functional, asset, technical, and locational boundaries;
 - .. Make appropriate risk assessment ;
 - .. Identify areas of risk to be managed and degree of assurance required;
 - .. Select appropriate controls;
 - .. Prepare Statement of Applicability.
- (ii) *Implementation*: Effectiveness of procedures to implement controls to be verified while reviewing security policy and technical compliance.
- (iii) *Documentation*: The documentation shall consist of evidence of action undertaken under establishment of the following:
 - .. Management control
 - .. Management framework summary, security policy, control objective, and implemented control given in prepare Statement of Applicability
 - .. Procedure adopted to implement control under Implementation clause
 - .. ISMS management procedure
 - .. Document Control: The issues focused under this clause would be
 - o Ready availability
 - o Periodic review
 - o Maintain version control;
 - o Withdrawal when obsolete
 - o Preservation for legal purpose
 - .. Records: The issues involved in record maintenance are as follows:
 - o Maintain to evidence compliance to Part 2 of BS7799.;
 - o Procedure for identifying, maintaining, retaining, and disposing of such evidence;
 - o Records to be legible, identifiable and traceable to activity involved.
 - o Storage to augment retrieval, and protection against damage.

Question 4

Briefly explain Asset Classification and Control under Information Security Management Systems.
(5 Marks) (Jun 2009)

Answer**Asset Classification and Control**

One of the most laborious but essential task is to manage inventory of all the IT assets, which could be information assets, software assets, physical assets or other similar services. These information assets need to be classified to indicate the degree of protection. The classification should result into appropriate information labeling to indicate whether it is sensitive or critical and what procedure, is appropriate to copy, store, transmit or destruction of the information asset.

An Information Asset Register (IAR) should be created detailing each of the following information asset within the organization:

- Databases,
- Personnel records,
- Scale models,
- Prototypes,
- Test samples,
- Contracts,
- Software licenses, and
- Publicity material.

The Information Asset Register (IAR) should also describe who is responsible for each information asset and whether there is any special requirement for confidentiality, integrity or availability. For administrative convenience, separate register may be maintained under the subject head of IAR e.g. 'Media Register' will detail the stock of software and its licenses. One major advantage of following this practice is that, it provides a good back-up for example, in case the carton/label containing password is accidentally misplaced, media register will provide the necessary information. Similarly, 'Contracts Register' will contain the contracts signed and thus other details. The impact that is an addendum to mere maintenance of a register is control and thus protection of valuable assets of the corporation. The value of each asset can then be determined to ensure that appropriate security is in place.

The detailed *control and objectives* thereof are as follows:

- *Accountability for assets:* to maintain appropriate protection of organizational assets,

- *Information Classification*: to ensure that information assets receive an appropriate level of protection.

Question 5

Discuss 'Physical and Environmental Security with Control and Objectives' with respect to information Security Policy?
(5 Marks) (Nov 2009)

Answer

Physical and Environmental Security: This is the beginning point of any security plan. It is designed to prevent unauthorized access, damage and interference to business premises and information. This involves physical security perimeter, physical entry control, creating secure offices, rooms, facilities, providing physical access controls, providing protection devices to minimize risk ranging from fire to electromagnetic radiation, providing adequate protection to power supplies and data cables are some of the activities. Cost effective design and constant monitoring are two key aspects to maintain adequate physical security control.

Maintenance of the physical operating environment in a computer server room is as important as ensuring that paper records are not subject to damage by mould, fire or fading. Supporting equipment such as air conditioning plant or mains services should be properly maintained. Physical controls can be difficult to manage as they rely to some extent on building structure, but good physical security can be very effective.

The detailed *control and objectives* for this type of security are:

- *Secure areas*: To prevent unauthorized access, damage and interference to business premises and information,
- *Equipment Security*: To prevent loss, damage or compromise of assets and interruption to business activities, and
- *General Controls*: To prevent compromise or theft of information and information processing facilities.

Question 6

What do you understand from Type I and Type II reports from a Service auditor?

(4 Marks) (Nov 2010)

Answer

Service Auditor's Reports

One of the most effective ways, a service organization can communicate information about its controls is through a Service Auditor's Report. There are two types of Service Auditor's Reports, namely, Type I and Type II.

A Type I report describes the service organization's description of Controls at a specific point in time.

In a Type I report, the service auditor will express an opinion on (1) whether the service organization's description of its controls presents fairly, in all material respects, the relevant aspects of the service organization's controls that had been placed in operation as of a specific date and (2) whether the controls were suitably designed to achieve specified control objectives.

A Type II report not only includes the service organization's description of Controls, but also includes detailed testing of the service organization's controls over a minimum six month period.

In a Type II report, the service auditor will express an opinion on the same items in a Type I report, and also on (3) whether the controls that were tested, also operate with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives were achieved during the period specified.

Question 7

How will you define a software process? What do you mean by its capability, performance and maturity?
(4 Marks) (Nov 2010)

Answer

Software Process: A software process can be defined as a set of activities, methods, practices and transformations that people use to develop and maintain software and the associated products. Examples include project plans, design documents, code, test cases and user manuals etc.

Software process capability: It describes the range of expected results that can be achieved by following a software process. It focuses on results expected from the next software project.

Software process performance: It represents the actual results achieved by following a software process. It focuses on the results achieved.

Software process maturity: It is the extent to which a specific process is explicitly defined, managed, measured, controlled and effective. It helps the organization in institutionalization of its software process via policies, standards and organizational structure.

Question 8

Write short notes on the following:

(a) *SysTrust and WebTrust Services* (4 Marks) (Nov 2010)

(b) *Capability Maturity Model* (4 Marks) (May 2011)

Answer**(a) SysTrust and WebTrust**

SysTrust and WebTrust are two specific services developed by the AICPA that are based on the Trust Services Principles and criteria. SysTrust engagements are designed for the provision of advisory services or assurance on the reliability of a system. WebTrust engagements relate to assurance or advisory services on an organization's system related to e-commerce. Only Certified Public Accountants (CPAs) may provide the assurance services of trust services that result in the expression of Trust Services, WebTrust or SysTrust opinion and in order to issue SysTrust or WebTrust reports, CPA firms must be licensed by the AICPA.

The following principles and related criteria have been developed by the AICPA for use by practitioners in the performance of trust services engagements such as SysTrust and WebTrust.

- (i) *Security*: The system is protected against unauthorized access (both physical and logical)
- (ii) *Availability*: The system is available for operation and use as committed or agreed.
- (iii) *Processing Integrity*: System processing is complete, accurate, timely and authorized.
- (iv) *Online Privacy*: Personal information obtained as a result of e-commerce is collected, used, disclosed and retained as committed or agreed.
- (v) *Confidentiality*: Information designated as confidential is protected as committed or agreed.

(b) Capability Maturity Model (CMM)

The CMM presents sets of recommended practices in a number of key process areas that have been shown to enhance software process capability. The CMM is based on knowledge acquired from software process assessments and extensive feedback from both industry and government.

The capability maturity model for software provides software organizations with guidance on how to gain control of their processes for developing and maintaining software and how to evolve toward a culture of software engineering and management excellence. The CMM was designed to guide software organizations in selecting process improvement strategies by determining current process maturity and identifying the few issues most critical to software quality and process improvement. By focusing on a limited set of activities and working aggressively to achieve them, an organization can steadily improve its organization-wide software process to enable continuous and lasting gains in software process capability.

Question 9

Why do you think a separate standard (SAS 70) is useful for auditing a service organization especially with respect to examination of general controls over Information Technology and related processes?
(4 Marks) (Nov 2010)

Answer

Yes, to our opinion, a separate statement on Auditing Standard (SAS) No. 70 is useful for auditing a service organization especially with respect to examination of general controls. A SAS 70 audit or service auditor's examination is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over Information Technology and related processes.

SAS 70 is the authoritative guidance that allows service organizations to disclose their control activities and processes to their customers and their customers' auditors in a uniform reporting format. A SAS 70 examination signifies that a service organization has had its control objectives and control activities examined by an independent accounting and auditing firm. A formal report including the auditor's opinion (Service Auditor's Report) is issued to the service organization at the conclusion of SAS 70 examination.

SAS 70 provides guidance to enable an independent auditor (Service Auditor) to issue an opinion on a service organization's description of controls through a Service Auditor's Report. SAS 70 is not a predetermined set of control objectives or control activities that service organization must achieve.

SAS 70 is generally applicable when an auditor (user auditor) is auditing the financial statements of an entity (user organization) that obtains services from another organization (service organization). Service organizations that provide such services could be application service providers, bank trust departments, claims processing centres, Internet data centres or other data processing service bureaus.