The Quality of IS/IT: How It Can Be Assessed?

Vlasta Svata
Faculty of Informatics and Statistics,
University of Economics, Prague
svata@vse.cz

Abstract: Higher quality for less money is the constant dream of all managers across all the industries IT industry included. But the term quality is very complex and this complexity was accelerated by the massive introduction and evolution of information systems and information technologies. The article deals with the quality in general and then focuses on the specifics of the quality assessment within the IS/IT. The mutual relationships between the quality of IT processes, IT products and services and business products and services are discussed. The two core assumptions for quality management are formulated: understanding the characteristics/features of IS/IT quality and ability to measure the degree of correspondence between the regulations (models) and practice. Examples of models covering the quality attributes of information, software products and services and processes are introduced and their positive and negative aspects are discussed.

Key words: Information model, Cobit 4.1, Cobit 5, SCAMPI, CMM, PAM, SQuaRE

1. Introduction

The concept of quality is an integral part of our lives. We are all trying in our various activities to get "high quality at an affordable price," which implicitly assumes that the quality and price should be directly proportional. But all these facts are based on the assumption that we are able to define quality and at the same time to determine what should be the price. For this reason, it is not usual to deal with the concept of quality in general, we can leave it to the philosophers, but we apply quality to some useful, important product or service. When we attempt to clarify the qualitative characteristics of products and services we very quickly will come to the conclusion that their quality is influenced by the quality of production and technological processes that need to be done to make the product / service available. Therefore, besides the quality of the resulting products and services we have to think about the quality of business and IT processes.

At the same time it is apparent that there is a need to develop and apply quality standards that based on the best practices can help organizations both the integration, deployment and operation of various aspects of quality management into one management system and to provide the complex and objective quality assessment that can be crowned by some kind of certification.

The article is an attempt to familiarize the reader with the difficult but in the same time required quality assessment of objects in the IS/IT. Section 2 provides short description of the relative concept of quality based on ISO 9000 family.

Next section 3 introduces the core objects of quality management and their mutual relationships.

Section 4 describes different types of quality attributes for three core objects of quality management: information, IT products and services and IT processes. The examples of attributes are taken from relevant ISO norms and best practices (Cobit 4.1, Cobit 5).

Section 5 focuses on activities helping us measure the degree of correspondence between quality features and requirements. The mutual relationship between assurance and assessment activities is presented together with the different types of assurance.

The last section 6 summarizes five conclusions dealing with the IS/IT quality assessment.

2. Relative concept of quality

But what is quality in general? The first attempts to define quality go back to Aristotle. Aristotle analyzed qualities in his logical work, the Categories. He viewed quality as one of the ten categories of highest kind: (1) substance; (2) quantity; (3) quality; (4) relatives; (5) somewhere; (6) sometime;
(7) being in a position; (8) having; (9) acting; and (10) being acted upon. Aristotle divided quality as follows:

- Habits and Dispositions
- Natural Capabilities and Incapabilities
- Affective Qualities and Affections
- Shape.

Current more pragmatic approaches are based on definition that was published in ISO 9000: 2005 and stays: "quality is the degree to which a set of inherent characteristics fulfils requirements". In other words (Glossary, 2014) „quality is the totality of features and characteristics of a product or service that bear on its ability to satisfy stated or implied needs (requirements)”. The quality of assessed objects can be determined by comparing a set of inherent characteristics with a set of requirements. In case, that inherent characteristics meet all requirements, than high or excellent quality is achieved. When characteristics do not meet all requirements - a low or poor level of quality is achieved. These assumptions lead us to conclusions, that

- Quality is a question of degree
- Quality depends on a set of inherent characteristics and a set of requirements and how well the former complies with the latter

According to these definitions, quality is a relative concept. This is the reason, why for instance the ISO 9000 family distinguishes between requirements for quality management systems and requirements for products. Requirements for quality management systems are specified in ISO 9001 and they are generic and applicable to organizations in any industry or economic sector regardless of the offered product category. ISO 9001 itself does not establish requirements for products.

3. The specifics of the quality assessment within the IS/IT

Without any doubt information is a key resource for all enterprises. With the advent of information technology and the introduction of information systems, quality management became considerably difficult. The reasons are, that information technology and information systems have against the quality twofold position:

- They represent important products and services that require standardization of good quality and at the same time for delivery of these IT products and services there is a need to implement special IT processes whose quality affects the quality of IT products and services
- The final output of IT processes, products and services is information that supports the implementation of business processes. They represent criterion affecting the quality of business processes and business products. The mutual relationships are represented in Fig. 1.

![Fig. 1: The core objects of quality management](source: author)

Next important issue deals with the fact, that quality - as was already mentioned - is relative concept. In other words it means, that quality of IS/IT depends on a set of inherent characteristics and a set of users requirements. There exist a lot of different categories of users or stakeholders of IS/IT from both the outside and inside the organization. Each category prefers other priorities in their requirements. Consequently inherent characteristics of IS/IT depends on the quality of IS/IT development, not only on the quality of acquisition, implementation and maintenance.
In case, that we admit that the quality is a question of degree between the stated or implied features and characteristics of IS/IT and different stakeholder's requirements, we have to be able to

- Understand the characteristics/features of IS/IT quality.
- Measure this degree of correspondence.

4. Quality attributes of IS/IT

According to Fig. 1, in the next text we will distinguish among the models of information quality, quality of software products and services and quality of IT processes.

4.1 Examples of models covering information quality attributes

Looking at the available IS/IT process frameworks Cobit 4.1 and Cobit 5 we came to conclusion, that mainly Cobit 5 deals with the information quality attributes more seriously comparing e.g. ITIL.

Cobit 4.1 presents the idea, that in order to satisfy business objectives, information needs to conform to certain control criteria, which Cobit 4.1 refers to as business requirements for information. Based on the broader quality, fiduciary and security requirements, seven distinct, certainly overlapping, information criteria are defined as follows (Cobit 4.1, 2007):

- Effectiveness deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
- Efficiency concerns the provision of information through the optimal (most productive and economical) use of resources.
- Confidentiality concerns the protection of sensitive information from unauthorized disclosure.
- Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
- Availability relates to information being available when required by the business process now and in the future. It also concerns the safeguarding of necessary resources and associated capabilities.
- Compliance deals with complying with the laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies.
- Reliability relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

Cobit 5 (ISACA, Cobit PAM, 2011) introduces much more comprehensive information model that comprises all aspects of information including:

- Stakeholders: Stakeholders can be internal or external to the enterprise. The generic model also suggests that, in addition to identifying the stakeholders, their stakes—i.e., why they care or are interested in the information—need to be identified.
- Goals (quality): The goals of information are divided into three sub-dimensions of quality. Each of them is described by the more detailed attributes:
  - Intrinsic quality—the extent to which data values is in conformance with the actual or true values.
  - Contextual and representational quality—the extent to which information is applicable to the task of the information user and is presented in an intelligible and clear manner, recognizing that information quality depends on the context of use.
  - Security/accessibility quality—The extent to which information is available or obtainable and secured.
- Life cycle stages: The full life cycle of information needs to be considered, and different approaches may be required for information in different phases of the life cycle. The COBIT 5 Information model distinguishes amongst the following phases: plan, design, build/acquire, use/operate.
- Good practices (information attributes): The concept of information is understood differently in different disciplines such as economics, communication theory, information science, knowledge management and information systems; therefore, there is no universally agreed-on definition for information. (Cobit5 Enabling Information, 2013) provides structure of six levels, or layers, to define and describe properties of information (see Fig. 2). These six levels present a continuum of attributes, ranging from the physical world of information, where
attributes are linked to information technologies and media for information capturing, storing, processing, distribution and presentation, to the social world of information use, sense-making and action.

**Fig. 2: Information attributes (COBIT 5 Enabling Information, 2013)**

### 4.2 Examples of models covering software products and services quality attributes

The core model for software product quality measurement is a set of standards ISO/IEC 25000 called SQuaRE. Software product in SQuaRE refers to the same definition as in ISO/IEC 12207:1998 (ISO/IEC 12207, 2008): a set of computer programs, procedures, and possibly associated documentation and data. Another important term in SQuaRE is system: combination of interacting
elements organized to achieve one or more stated purposes. A system may be considered as a product or as the services it provides. Software quality is defined as a degree to which the software product satisfies stated and implied needs when used under specified conditions.

Initial part of the SQuaRe series provides general introduction to different types of software product properties. Some software properties are inherent in the software product; some software properties are system dependent; some are assigned to the software product. The quality of a software product in a particular context of use is determined by its inherent properties. Inherent properties can be classified as either functional properties or quality properties. Functional properties determine what the software is able to do. Quality properties determine how well the software performs. In other words, the quality properties show the degree to which the software is able to provide and maintain its specified services. Quality properties are inherent to a software product and associated system. An assigned property is not considered to be a quality characteristic of the software, since it covers managerial aspects of software product. Thus it can be changed without changing the software. Therefore SQuaRE focuses only on quality properties. Table 1 illustrates this classification of software properties.

### Table 1: Software properties (ISO/IEC 25010, 2011)

<table>
<thead>
<tr>
<th>SW properties</th>
<th>Inherent properties</th>
<th>Domain specific functional properties</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Quality properties (functional suitability, reliability, performance efficiency, operability, security, compatibility, maintainability, transferability)</td>
<td></td>
</tr>
<tr>
<td>Assigned properties</td>
<td>Managerial properties (price, delivery date, product future, product supplier)</td>
<td></td>
</tr>
</tbody>
</table>

In SQuaRE series ISO/IEC 25010 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models is based on ISO/IEC 9126 Software engineering — Product quality which was an international standard for the evaluation of software quality. It has been replaced by ISO/IEC 25010 in 2011.

ISO/IEC 9126 quality model was based on three sub-models of software products quality (internal quality, external quality and quality in use), 10 quality characteristics, 24 sub-characteristics and more than 250 measures proposed to quantify these quality characteristics and sub-characteristics. Internal and external models had the same characteristics and sub-characteristics, the difference was in quality measures. Quality in use model had no sub-characteristics. The whole concept is shown in Fig. 3.

**Fig. 3: The mutual relationships between the different attributes of software products**

(ISO/IEC 9126, 2001)

Current software quality model is based on two models (ISO/IEC 25010, 2011):

a) A quality in use model composed of five characteristics (effectiveness, efficiency, satisfaction, freedom from risk and context coverage). Some of which are further subdivided into sub-characteristics that relate to the outcome of interaction when a product is used in a particular context of use. Characteristics can be measured when a product is used in a realistic context of use. This system model is applicable to the
complete human-computer system, including both computer systems in use and software products in use.

b) A product quality model composed of eight characteristics (functional suitability, reliability, performance efficiency, usability, security, compatibility, maintainability and portability) which are further subdivided into sub-characteristics that relate to static properties of software and dynamic properties of the computer system. The characteristics can be measured internally or externally. The model is applicable to both computer systems and software products.

Although the scope of the product quality model is intended to be software and computer systems, many of the characteristics are also relevant to wider systems and services. ISO/IEC 25012 contains a model for data quality that is complementary to this model.

IT services comparing previous software products and systems represent more complex output from IT processes. Their quality attributes are much more influenced by the user requirements and therefore we cannot assign to all IT services one set of attributes and measures. Nevertheless, there is a new standard under development called ISO/IEC CD 25011 Information technology -- Service Quality Requirement and Evaluation (SQuaRE) -- IT Service Quality Model. ISO/IEC 25011 will define a general service quality model that is applicable to the design, deployment, delivery and improvement of services that use or support IT, and provides the guideline to use the quality in use model of ISO/IEC 25010 to describe the quality in use of service, which relates to the performance of service that customers perceived in a particular context of use. Another way how to measure and improve IT service quality is to establish SMS (Service Management System) which increases probability, that final IT services will attain the quality attributes that are defined in special documents - SLA (Service Level Agreements). The most important standards for ITSM is ISO 20000 which is closely related to ITIL and represents the world's first standard for IT service management.

4.3 Examples of models covering IT process quality attributes

SCAMPI (The Standard CMMI Appraisal Method for Process Improvement) is the official Software Engineering Institute (SEI) method to provide benchmark-quality ratings relative to Capability Maturity Model Integration (CMMI) models. SCAMPI appraisals are used to identify strengths and weaknesses of current processes, reveal development/acquisition risks, and determine capability and maturity level ratings. They are mostly used either as part of a process improvement program or for rating prospective suppliers.

The ARC (Appraisal Requirements for CMMI) defines appraisal classes that represent three levels of formality for appraisals: Class A, B, and C. Formal (Class A) SCAMPIs are conducted by SEI-authorized Lead Appraisers who use the SCAMPI A Method Definition Document (MDD) to conduct the appraisals.

Key differentiating attributes for appraisal classes include
- the degree of confidence in the appraisal outcomes
- the generation of ratings
- appraisal cost and duration

SCAMPI uses four level capability level rating (see Table 2).

Table 2: SCAMPI capability levels

<table>
<thead>
<tr>
<th>Capability Level</th>
<th>Process Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Default Rating</td>
</tr>
<tr>
<td>1</td>
<td>Generic goal for capability level 1 is rated Satisfied. (All specific goals are rated Satisfied.)</td>
</tr>
<tr>
<td>2</td>
<td>Generic goals for capability levels 1 and 2 are rated Satisfied. (All specific goals are rated Satisfied.)</td>
</tr>
<tr>
<td>3</td>
<td>Generic goals for capability levels 1, 2, and 3 are rated Satisfied. (All specific goals are rated Satisfied.)</td>
</tr>
</tbody>
</table>
The attributes of evaluation are called Practice Implementation Indicators (PII). They are pieces of evidence that a given CMMI Practice (that supports a goal) has indeed been implemented. The idea is that performing a Practice will leave a footprint or evidence that the practice has been performed. A PII could be a document (for example a Requirements Traceability Matrix, RTM) that is directly produced from a Practice, i.e. within the Requirements Management process area for the RTM.

Each practice is characterized as one of the following values:
- Fully Implemented (FI)
- Largely Implemented (LI)
- Partially Implemented (PI)
- Not Implemented (NI)
- Not Yet (NY)

The SCAMPI method provides for the collection and analysis of data from the following types of objective evidence (SCAMPI, 2011):

- **Artifacts** - a tangible form of objective evidence indicative of work being performed that represents either the primary output of a model practice or a consequence of implementing a model practice. These artifacts may include organizational policies, meeting minutes, review results, or other implementation-level work products. Sufficient artifacts demonstrating and corroborating that the work is being done are necessary to verify the implementation of associated model practices.

- **Affirmations** - an oral or written statement confirming or supporting implementation (or lack of implementation) of a model practice provided by the implementers of the practice, provided via an interactive forum in which the appraisal team has control over the interaction. These statements are typically collected using interviews, demonstrations, questionnaires, or other means. Note that negative affirmations confirming the lack of implementation of a practice are possible.

Cobit 4.1 process assessment is based on CMM (Capability Maturity Model). This approach is derived from the maturity model that the Software Engineering Institute (SEI) defined for the maturity of software development capability. Although concepts of the SEI approach were followed, the COBIT implementation differs considerably from the original SEI, which was oriented toward software product engineering principles and on the base of this formal appraisal model there is possibility for developers to be “certified”. In COBIT 4.1, a generic definition is provided for the COBIT maturity scale, which is similar to CMM but interpreted for the nature of COBIT’s IT management processes. A specific model is provided from this generic scale for each of COBIT’s 34 processes. The purpose is not to assess the level of adherence to the control objectives, but to identify where issues are and how to set priorities for improvements (Cobit 4.1, 2007).

**Table 3: Generic maturity model (Cobit 4.1, 2007)**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Non-existent - Complete lack of any recognisable processes. The enterprise has not even recognized that there is an issue to be addressed.</td>
</tr>
<tr>
<td>1</td>
<td>Initial/Ad Hoc - There is evidence that the enterprise has recognised that the issues exist and need to be addressed. There are, however, no standardised processes; instead, there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.</td>
</tr>
<tr>
<td>2</td>
<td>Repeatable but Intuitive - Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.</td>
</tr>
<tr>
<td>3</td>
<td>Defined Process - Procedures have been standardized and documented, and communicated through training. It is mandated that these processes should be followed; however, it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.</td>
</tr>
<tr>
<td>4</td>
<td>Managed and Measurable - Management monitors and measures compliance with procedures and takes action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.</td>
</tr>
<tr>
<td>5</td>
<td>Optimized - Processes have been refined to a level of good practice, based on the results of continuous improvement and maturity modelling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.</td>
</tr>
</tbody>
</table>
The maturity models are built up starting from the generic qualitative model (see Table 3) to which principles from the following attributes are added in an increasing manner through the levels:

- Awareness and communication
- Policies, plans and procedures
- Tools and automation
- Skills and expertise
- Responsibility and accountability
- Goal setting and measurement.

COBIT 5 discontinues the COBIT 4.1 CMM-based capability maturity modelling approach and is supported by a new process capability assessment approach based on ISO/IEC 15504 called PAM (Process Assessment Model).

The assessment process involves establishing an ISO-defined capability rating for each process. It involves using the standard rating scale to assess the process attributes (based on the attribute indicators) that apply to each of the six capability levels (all of which are defined in ISO/IEC 15504–2):

- Level 0: Incomplete process. The process is not implemented, or fails to achieve its process purpose. At this level, there is little or no evidence of any systematic achievement of the process purpose.
- Level 1: Performed process. The implemented process achieves its process purpose.
- Level 2: Managed process. Performed process is now implemented in a managed fashion (planned, monitored and adjusted) and its work products are appropriately established, controlled and maintained.
- Level 3: Established process. Managed process is now implemented as a defined process that is capable of achieving its process outcomes.
- Level 4: Predictable process. Established process now operates within defined limits to achieve its process outcomes, as a measured and controlled process.
- Level 5: Optimizing process. Predictable process is continuously improved to meet relevant, current and projected business goals, incorporating process innovation and optimization.

Within the COBIT PAM, the measure of capability is based on the nine process attributes (prefixed by PA) defined in ISO/IEC 15504-2, as shown in Table 4. Each attribute applies to a specific process capability. Process attributes are used to determine whether a process has reached a given capability.

**Table 4: Process capability levels and their attributes**

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
<th>Attributes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Level 0 - Incomplete</td>
<td>The process is not implemented or fails to achieve its purpose.</td>
<td></td>
</tr>
<tr>
<td>process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 1 - Performed</td>
<td>The process is implemented and achieves its process purpose</td>
<td>PA1.1 – Process performance</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Level 2 - Managed</td>
<td>The process is managed and work products are established, controlled and</td>
<td>PA2.1 – Work product</td>
</tr>
<tr>
<td>process</td>
<td>maintained.</td>
<td>management</td>
</tr>
<tr>
<td>Level 3 – Established</td>
<td>A defined process is used based on a standard process.</td>
<td>PA3.1 – Process definition</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td>PA3.2 – Process deployment</td>
</tr>
<tr>
<td>Level 4 – Predictable</td>
<td>The process is enacted consistently within defined limits</td>
<td>PA4.1 – Process measurement</td>
</tr>
<tr>
<td>process</td>
<td></td>
<td>PA4.2 – Process control</td>
</tr>
<tr>
<td>Level 5 – Optimizing</td>
<td>The process is continuously improved to meet relevant current and projected</td>
<td>PA5.1 – Process innovation</td>
</tr>
<tr>
<td>process</td>
<td>business goals</td>
<td>PA5.2 – Process Optimization attribute</td>
</tr>
</tbody>
</table>

Assessment indicators in the COBIT PAM provide the basis for determining whether process attributes have been achieved.

As part of the assessment to determine whether capability level 1 is being achieved, assessors must determine whether the purpose of the process is being achieved. Each process has its specific indicators for this level achievement. A process achieves its purpose if the practices defined are being performed and the outputs/outcomes (or established alternatives) are being delivered.
In contrast to capability Level 1, the assessments of capability Levels 2 through 5 are based on generic process indicators of performance. These are called generic because they apply across all processes at each level of capability globally, irrespective of process purpose, enterprise type, size or line of business.

It is generally understood that the higher the process capability level reached, the lower the risk of the process failing to meet its intended purpose. It is also generally understood that the higher the capability, the more costly the process is to operate.

Each attribute is rated using a standard rating scale defined in the ISO/IEC 15504 standard (ISO/IEC 15504, 2010). Ratings are translated into a percentage scale showing the extent of achievement (see Table 5).

### Table 5: PAM ratings and their percentage scale

<table>
<thead>
<tr>
<th></th>
<th>Not achieved</th>
<th>0 to 15% achievement</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>Partially achieved</td>
<td>&gt;15% to 50% achievement</td>
</tr>
<tr>
<td>P</td>
<td>Largely achieved</td>
<td>&gt;50% to 85% achievement</td>
</tr>
<tr>
<td>L</td>
<td>Fully achieved</td>
<td>&gt;85% to 100% achievement</td>
</tr>
</tbody>
</table>

Documents (Cobit PAM, 2013), (Cobit Assessor Guide, 2013), and (Cobit Self Assessment Guide, 2013) enable practitioners to efficiently provide both the scoping (identification of the Cobit5 processes that may have higher priority for assessment based on relation between the business goals, IT goals and process goals) and assessment itself.

5. **Examples of activities measuring the degree of correspondence between quality features and requirements**

The activities that help us to measure the degree of correspondence between the quality features and user’s requirement within the IS/IT are part of more complex procedures called IS/IT assurance or audit. Assurance means that: „pursuant to an accountability relationship between two or more parties, an IT audit and assurance professional may be engaged to issue a written communication expressing a conclusion about the subject matters to the accountable party” (Cobit 5, 2013). Assurance refers to a number of related activities designed to provide the reader or user of the report with a level of assurance or comfort over the subject matter. For example, assurance engagements could include support for audited financial statements; assessment of value provided by IT to the enterprise; reviews of controls; compliance with required standards and practices; and compliance with agreements, licenses, legislation and regulations. Assurance is based on the relationships and cooperation between next three parties:

- An accountable party (the individual, group or entity (auditee), usually involving management, that is ultimately responsible for subject matter, process or scope.
- The user could include a variety of stakeholders, such as shareholders, creditors, customers, the board of directors, the audit committee, legislators or regulators. For some types of assurance activities, the auditee and the user can be identical, e.g., IT management.
- The assurance professional (auditor) is the person who has overall responsibility for the performance of the assurance.

An inherent part of assurance is an assessment. (Cobit Assessor Guide, 2013) provides definition of assessment:” a broad review of the different aspects of a company or function that includes elements not covered by a structured assurance initiative. May include opportunities for reducing the costs of poor quality, employee perceptions on quality aspects, proposals to senior management on policy, goals, etc.”

The basic elements of each assurance/assessment are subject matter, suitable criteria, formalized realization and communication of the assessment conclusion. The last element – communication of the assessment conclusion is provided by the help of the written audit report. (ISACA, 2015) states that the IS audit report is driven mainly by the type of audit engagement-whether it is a review, an audit (examination) or an agreed-upon procedures engagement.

A review is designed to provide limited assurance about an assertion. As the name implies, a review consists primarily of review work with less emphasis on testing or verification. A review can be more process oriented, focusing on the appropriateness of the tasks and activities that the audit entity performs and the associated controls. The level of evidence that is gathered is less than in an audit,
and testing is generally limited or none is performed. As a result, reviews do not include audit opinions. Instead, conclusions may often be stated negatively. For example: “Nothing came to our attention to indicate that the assertion is not true”.

An information system audit can be performed as an examination, which is a systematic process by which a competent, independent person objectively obtains and evaluates evidence regarding assertions about an entity or event, processes, operations or internal controls, for the purpose of forming an opinion and providing a report on the degree to which the assertions conform to an identified set of standards. An examination is an attestation process that provides the highest level of assurance about an assertion that an auditor can provide. An examination encompasses gathering and evaluating sufficient, competent evidence and performing appropriate tests and other procedures to form the opinion about an assertion for presentation in an audit report.

In agreed-upon procedures engagements, a third party and the auditor agree on specific procedures that will be performed to obtain the evidence on which the third party is willing to rely as a basis for a conclusion. Depending on the requirements of the third party, the agreed-upon level of evidence may be significantly limited or extensive. The auditor may need to obtain a substantial amount of evidence; in some cases, more than that is required for an audit.

The communication of the different objects assessment conclusions within IS/IT environment can follow all above types of audit engagement. It depends on the requirements and expectations set forth between the audit organization and the auditee.

6. Conclusion

There exist a lot of different models helping the involved people to assess the quality of different IS/IT assets. Short description of some of them can help readers to understand their different and common features. We can summarize them into the next five conclusions.

For the first, quality of IT processes and quality of IT products and services are in responsibility of IT people, while the quality of information is in the shared responsibility of IT and business people. Therefore the information model must be sufficiently comprehensive in order to cover all the different information aspects and attributes of different stakeholders, but in the same time there should be available some tools helping IT and business people to provide scoping and prioritization of numerous attributes and thus focus on the chosen subset that will be managed and assessed within a specific organization. Such a identified and agreed information quality attributes should be an inherent part of organizational Data architecture.

For the second, all the presented quality models are based on the whole hierarchy of different attributes, requirements, properties, indicators, measures etc. But we can notice, that in each case there exist at least three basic types of attributes: specific functional attributes that vary according to particular product, service, process; common inherent attributes (another set of attributes is common for software product, another for IT process or IT services); specific attributes that take in account the specific context (environment) in which the object operates.

For the third, focusing on process quality assessment, there exist close relationship between the assessment models and process frameworks. The reason is that each assessment is based on the formal evidence of process practices and process outputs which are an inherent part of process frameworks. In the Table 6 the possible combinations between the IT process frameworks and assessment models are presented.

Table 6: Relationships between the examples of assessment models and process frameworks

<table>
<thead>
<tr>
<th>Assessment model</th>
<th>Process model</th>
<th>SCAMPI</th>
<th>CMM</th>
<th>PAM (ISO/IEC 15504)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cobi 4.1</td>
<td>NO</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Cobi 5</td>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>ITIL</td>
<td>Integration CMMI-ITIL enables SCAMPI appraisals</td>
<td>YES (individual approach of each consulting provider)</td>
<td>YES (individual approach of each consulting provider)</td>
<td></td>
</tr>
</tbody>
</table>
For the fourth, models differ in complexity and the detail of assessment. SCAMPI and PAM are more complex comparing CMM of Cobit 4.1. It is evident, that the more the model is complex and accurate the more time it takes to provide assurance and assessment activities and the higher are the costs of such an assessment. Therefore within each assessment model there exist different levels of formal assessment (see A,B,C levels of formality in SCAMPI or three types of Cobit 5 Assessment Programme).

For the fifth, the context of evaluation is not the same for all the maturity and capability levels focusing on CMM and PAM models. The lower levels need individual knowledge of people involved in specific IT process and they are based on the formal benchmarking whether the process purpose was achieved (work products and practices). The higher levels of maturity needs corporate knowledge and they are based on less formal communication across the whole enterprise (generic work products and generic practices) (see Table 7). The negative result of these differences is the fact, that the same process being evaluated by the CMM model can attain the maturity level 2 while being evaluated by the model PAM the same process will attain the level 0. The positive consequence is that incorporating the PAM assessment model will potentially enable an enterprise to obtain independent and certified assessments aligned to the ISO/IEC standard.

Table 7: Terms used for process maturity/capability

<table>
<thead>
<tr>
<th>CMM maturity levels</th>
<th>PAM capability levels</th>
<th>Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>5. Optimized</td>
<td>5 Optimizing</td>
<td>Enterprise view/corporate knowledge</td>
</tr>
<tr>
<td>4. Managed and measurable</td>
<td>4 Predictable</td>
<td>Instance view/individual knowledge</td>
</tr>
<tr>
<td>3. Defined</td>
<td>3 Established</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>2 Managed</td>
<td></td>
</tr>
<tr>
<td>N/A</td>
<td>1- Performed</td>
<td></td>
</tr>
<tr>
<td>2. Repeatable but intuitive</td>
<td>0 Incomplete</td>
<td></td>
</tr>
<tr>
<td>1. Initial/Ad hoc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>0. Non-existent</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

References

ISACA, 2015, Information Systems Auditing: Tools and Techniques, IS Audit Reporting,
ISO 9000,2005, Quality Management Systems - Fundamentals and Vocabulary


JEL Classification: L15, M15