SCIENTIFIC PAPERS, UNIVERSITY OF LATVIA, 2010. Vol. 757
COMPUTER SCIENCE AND INFORMATION TECHNOLOGIES 53–63 P.

Application of CobiT Maturity Model in Information Security Management and Arising Problematic Issues

Dmitrijs Nogicevs
University of Latvia, Faculty of Computing, 19 Raina Blvd., Riga, LV 1586, Latvia
dmitrijs_n@inbox.lv

Abstract. This paper examines a simplified decision making and achieving process that complies with the management of Information Security. The problems to determine a current position are investigated, as well as their impact, in order to diminish the risk of making a faulty decision, which can originate when the current position is incorrectly or inaccurately defined. The work focuses on the following problem: due to imperfect and defective methods used for determination of a current position, in addition to the great impact this process has on the determination of objectives and activity planning, besides the management of the both and IT overall management, there persist great risks of improper decision making, position defining and consequently the use of resources. Not only the decision making process, but also the current methods, as well as alternatives, of determination of Maturity Model (MM) and Maturity Level (ML) are analysed. By forecasting the development of a process, the guidelines for the abatement of the existent imperfections are offered. Decision making stages, particularly the determination of the current position, the use of equitable indicators, automatic collection of data and interconnected processes are being emphasized throughout the paper.

Keywords: CobiT, Maturity Model, Maturity Level, Information Security.

1 Introduction

In recent years, Security Maturity Model (ISMM) and Information Security management issues have been addressed in various studies, hence a sensible progress has been made – from Mikko Sipone to ISM3 [1], which is associated with the application of qualitative indicators. Likewise, the indirect relationship between security activity and security goals [2] has been inspected. ROSI as one of the main MM components is often mentioned in various studies, and in some of them ROSI related problematic issues [3] are covered, which, in my judgment, are more related to the selection of routes and activities as one of many, furthermore ambiguous criterions. By proffering new MM visions, relations, as well as congruencies between ISO and other standards, guidelines and ISMM have been explored [4], [5], and different MM have been compared [6]. This interest is coherent to the fact that MM can readily be put to use in the management of various processes, *inter alia*, Information Security processes.

Determination of the current state is one of the main stages combined into IT governance, decision-making and accomplishment of purposes. However, determination of a current state is required not only *per se*, but also in the context of future actions. Think about the purpose first, and then choose the method [7]. At present there are many MM visions. Avenues of approach vary for so do the purposes of MM application.

In this research process are observed from two points of view, first, the decision-making and the accomplishment of purposes, on the second hand. The role of MM in the process is defined and aims and recommendations are offered accordingly.

Different approaches are used for analysis, mostly CobiT and ISM3. The reasons are: **CobiT** – very popular (classic), relatively well developed, can be analysed together with CobiT Security Baseline (IT Security orientated); **ISM3** – new, IT Security orientated, use quantitative method.

Other reasons are given in the part 3.

2 CobiT and Decision Theory

In order to illustrate position and importance of the Maturity Model (MM) [8] in Information management processes, let us first consider its Decision making main stages (levels) and than the coincident CobiT/ISM3 tools.

Main stages of decision making and goal achievement process:

1. Determination of the initial (current) state;
2. Definition of the desirable position (target state);
3. Determination of the possible routes (from current to desirable position);
4. Selection of the best routes;
5. Checkpoint (sub target) setting (in order to maintain the control of the process and allow the rectification of the path in case of necessity)
6. Inspection, whether the desirable position has been reached.

The visualization of this process is given in the following figure (see Fig.1.).

Let us only briefly describe the process. Primarily, the current state is determined (C.S.). Then, taking the latter into consideration, the target state (T.S.) is defined, moreover – the desirable position is accessible and meets the organization's objectives. In order to shift from the current to the desirable position, the possible routes have to be determined. The routes are formed by successive activities (Act. x.y., where „x" denotes the route number and „y" – the activity number in respective route). Examples of possible activities are alteration of policies or procedures and notable projects, such as DLP (Data Loss Prevention) or IPS (Intrusion Prevention System).

Each activity leads either to the intermediate state or to a sub-target (I.S.x.y., shall „x" be the route number and „y" – the checkpoint number in a respective route). Sub-targets help maintain the control of the process (verification of the direction and position should occur). In case of necessity, revision of the list of activities (or checkpoints) can be implemented.

The best route is the one that satisfies the defined conditions. In our example it could be the route number 2.

As the last the check-out procedure is put in use in order to verify whether the target position is reached. It means that achieved position is compared with the desired by an application of appropriate measurements.

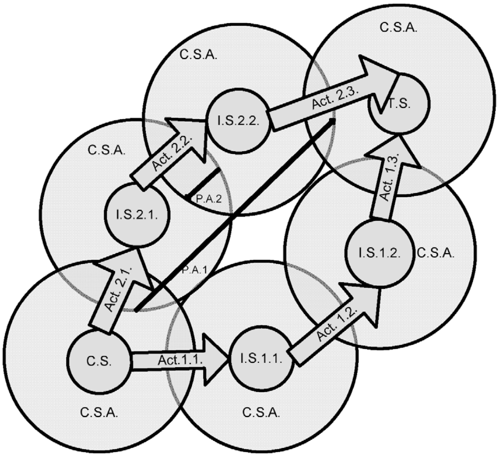

Fig. 1. Illustration of goal setting and achieving process.

Significantly, each time when a current position is determined it is done with a certain precision that has to be taken into account. Thus, there is actually a „current state area" (C.S.A.) rather than a definite position known, moreover the greater the C.S.A. the higher the risk of faulty activity planning. The Fig. 1. depicts a possible mismatch of a planned activity (for example, Act. 2.2.) and an activity that could be practically performed (P.A.2). Consequently, such initial irregularities can substantially affect the achievement of the marked goal. There exist the following risks:

1. The activities require greater resources than expected.
2. Activities cannot be successfully accomplished at the current state.
3. The accomplished activities have unexpected, or even negative, outcomes.

Table 1.

CobiT and ISM3 tools that can be used to support the decision-making process

The Main stages of decision making and consummation	CobiT[8], [2], [7], [10]	ISM3 [11]
Determination of the current state[1]	MM, (Detailed) Control Objectives (DCO)	system configuration, metrics, ISM3 levels
Definition of the target state	MM (Rising Star), KGI (Key Goal Indicators). BSC (Balanced Scorecard) can be used	Service quality (see 4.1.)
Determination of the possible routes	Practically does not support, CSF (Critical Success Factors), DCO [15]	Practically does not support, Process (description), Related Methodologies
Selection of the best routes[2]	Practically does not support, PO domen	Practically does not support, ROSI, Related Methodologies
Subtarget setting	KPI (Key Performance Indicators), see also Determination of the current state[3], MM, DCO	see Determination of the current state
Assessment of the target accomplishment	MM, KGI	see Determination of the current state

[1] Results of the Risk and Vulnerability Analysis have also been frequently used (applying the principles of priority) [12]

[2] ValIT [13], CRAMM [14] have been mentioned

[3] Correlation with Determination of the current state is low

We can now turn to the decision-making supportive tools provided by CobiT and ISM3

Some of the mentioned stages are also considered by such solutions as CRAMM Risk Matrix [14], PRINCE2 *et cetera*.

Functionally these stages form three groups of operations:

1. Determination of the initial position.
2. Detection of the possible ways how the target could be met.
3. Identification of the best route.

In the following sections we will focus on the current state detection process.

3 Determination of the State: Problems and Potential

In order to assess the stage of IT system development, many organizations use CobiT Maturity Model, which enables the determination of so-called Maturity Level or ML. This method allows the governing body to identify the current situation and to decide on needful and desirable steps that should be taken to improve the situation, as well as to realize the extent of required changes.

We will further investigate MM application related problems using CobiT MM as an example.

3.1 Problematic Issues Incidental to the Application of a Maturity Model Method

Since CobiT defines only general principles for the determination of ML, there is a high probability that the value subjectively influences the conclusions. The general principles allow to be treated variously [7], thus the positions can be determined (measured) inaccurately, consequently the targets, which are the purpose of the ML measurements, are met in an inefficient way.

The main disadvantages of the current (CobiT) method are its insufficient formalization, excessive usage of qualitative evaluation and a lack of quantitative measurements.

In the case of ISM3, the following obstacles can be mentioned:

1. It may be complicated to compare two states representing different fields (directions) in order to prioritize and boost the decision-making process.
2. Qualitative measurements are emphasized, thus leaving the vision to MM Control Objectives and activities poorly established (see 4.1). As a consequence, the process that has been carried out does not actually clarify, neither what one should do, nor in which direction.
3. The acquired results are equivocal (also due to the selection of indicators).
4. Process metrics, except for ML 5, are not compulsory. [11]

3.2 Alternative

We have concluded that the extant MM and ML methods are impotent to provide adequate results when applied for the determination of a current state. Despite the approaches' great potential, its current development does not comply with the requirements set by the process of decision-making and consummation. Therefore, there are the following possibilities:

1. To abandon the MM and use other approaches.
2. To explicate MM's avenue of approach by implementing existent tools or by modelling new ones in order to abate the imperfections mentioned above.

Continuing on the first possibility, an example of another approach is the keystone method which is commonly used in guidelines and standards, also in ISO (for example, 27001[16], 27002 that concern information security management [10] or ISO 9001). The application of this method provides the picture of an ideal (target) situation, but does not give any information about the possible inter-states, their interactions or developments. The keystone method can help compose a check list but the method is not useful when the stage of development or analysis of the current position is relevant. Besides it does not make provisions for the priority establishment and goal achievement which is possible if MM is applied. Only with maturity levels it is possible to show progress towards better security management [5].

Available metrics possess presumable complications such as, primarily, detection of those who are purpose-suitable and, secondly, metrics can be of little value when security management has to be ensured [2]. After consideration of the restrictions, we deduce that it would be suitable to develop the method on the basis of MM, applying the approach of keystone method as an adjuvant for composing ML questionnaires.

The current state determination methods should comply not only with metrics criteria, like S.M.A.R.T. [2], but also with the following:

1. They are uniform, ensuring that equate positions after processing give the same result.
2. It is possible to determine the position with a high precision, the C.S.A („current state area"; see Fig. 1.) is modest.
3. The level is defined in terms of controls and activities, thus facilitating the retracing the process of development.
4. The determined state can be compared with others (e.g., historic) correctly.
5. The components of the defined state can be evaluated and analysed asunder enabling the identification of weak (and strong) links.
6. It is possible to define and prioritize controls and activities.
7. These methods are perceivable by the concerned.

Conclusion:

Organizations are still after tools that could help determine the routes to which more attention should be paid in order to improve the consummation of the goal.

The analysis of alternatives has led to a conclusion that the most appropriate action to approach the solution of the problems associated with the determination of the current state is a further development of MM (using CobiT MM as the basis). The odds of other standards and guidelines should be used to improve checklists.

4 Suggestions for Improvement of ML Assessment Method

In order to improve CobiT ML model and to support the congruence with the criteria put forward, it would be rational to work out a checklist that could be implemented to assess the current position. Please note that this checklist may touch fields irrelevant to some organizations (e.g., the controls for a shop differ from those of a bank). Moreover, it does not necessarily mean that the organization has a higher ML if some of the criteria are not topical.

It is possible to create a ML profile, which is categorized by fields. If an organization has no need for particular controls, they are not evaluated. Filters for requisite criteria can be made by comparing organizations and analyzing the progress.

4.1 Determination of ML: The Basal Principles

There are two main ways how ML of IT processes can be defined:

1. By inspecting the quality of IT management.
2. Considering the quality of IT services.

Let us now pay regard to each of them in a bit more detail.

Evaluation of IT management quality means that primarily, sufficiency of control measures are evaluated, secondly, control and process levels of development are defined. In the case of CobiT, the controls, which are essential to meet the targets, are chosen and it is said that the situation is good and the goals are achieved if only it can be agreed that all controls are sufficiently well-developed.

We can see that here the focus is on the query, whether the IT management is in correspondence with a good practice, rather than on – in truth – the main question, i.e., how safe the IT environment is. The latter remains unanswered.

Another drawback of this approach is the high probability of a mismatch of supposed IT security conditions with the actual situation in the organization. Such risk can be regarded as a multiplication of the following factors:

1. The risk of inaccurate determination of the current situation;
2. The risk to choose inappropriate directions;
3. The possibility to choose unsuitable controls;
4. Wrongly chosen activities for implementation of controls;
5. Faulty assessment of the factual impact the implemented controls have on the information security.

Therefore it is advisable not only to use the assessment of IT management quality, but also to consider the quality of respective services, which could help clarify the *de facto* situation (e.g., DS5).

If the evaluation of IT management shows good results (a fine development) but the evaluation of IT services – modest, unsatisfactory or even negative effect, the following questions should be considered:

1. Does the organization focus on the right IT security areas;
2. Are the controls correct;
3. Do the chosen activities ensure (effective) achievement of controls?

The conclusions could be helpful in planning and implementing activities in the future. On the other hand, if both approaches give a common result, there is a high probability of being on the right track.

Evaluation of IT service quality denotes the inspection of the actual situation. In order to screen the real situation by means of a checklist, ISO (27002 – in the case of information security) or ISM3 can be successfully applied. Yet another option for the question compilation is Universal Vulnerability Matrix which supports a risk-based approach.

The questions should be composed so that the possibility to make a subjective assessment would be diminished or excluded. Besides, they should ensure the comparability of data, i.e., with each other, as well as within time and with those of other organizations. Questions should be as uniform as possible (applicable to a wide range of organizations) and may be meeting numerous requirements usually characteristic of business continuity, availability, protection of classified data, compliance of the necessary regulatory requirements. It is advisable not to overload the questionnaire; otherwise its usage may become inconvenient.

4.2 Suggestions and Recommendations on Compilation, Completion and Analysis of a Questionnaire

The great bulk of suggestions and recommendations are represented in Table 2.

The General Guidance on Selection of Indicators:

1. In order to diminish the impact of subjectivity on the ML assessment process, quantitative, rather than qualitative, approach should be adapted.
2. To a feasible extent the quantitative indicators should be attained from statistical data, e.g., from databases (see Table 2., „Information Source"; paying particular attention to uniformity of configuration, i.e., principles of evaluation), but the remainder – from IS administrators (or technical process owners) provided with concise and unambiguous questionnaires (consequently, not time-consuming). Furthermore, the latter could also be useful for executive officers (to raise the level of understanding) or as a part of *Self assessment*.
3. Sufficient amount of time should be devoted to prepare the statistical data, including their verification, before the ML assessment (meeting) takes place. What is more, the data should tend be indisputable, so that subjective assessments, conflicts of interest and misunderstandings could be avoided.
4. The questions incorporated in the questionnaire should be grouped by common sub-process (controls) rather than by MLs, and formed on the basis of parameters characterizing the quality of a current state (Table 2, column nr. 1).
5. The questions should form short unambiguous sentences, each including only one statement. For instance, an affirmative sentence like this – *„security-relevant information is produced by systems, but not analysed*" – should be split into two separate sentences before being incorporated into the questionnaire.
6. The number of questions that may have more than one answer should be minimized. On the other hand, each question should be unique (should not be repeated), furthermore, independent (thus, two questions that are in conflict with each other, e.g., *„a small part is involved"* and *„the majority is involved"* – cannot be used within the same questionnaire).
7. To determine the current state more precisely, not only the indicators that cover a certain IT process, but also interactions between these processes (and identifiers)

should be incorporated in the ML determination procedure (see Interpretation of Results: Application of Interconnected Processes). Such approach enables the detection of so called „sensitive links”[4].

8. Relevant parameters and metrics have to be defined (Table 2.).

It should be taken into the consideration that the satisfaction with the system-functioning is by definition subjective, therefore it is impossible, as well as unnecessary to make an effort to replace all qualitative indicators with quantitative.

Guidance on Compilation of Assessment Questionnaires

Source material: Depending on the desirable accuracy of the assessment, it is advisable to choose within the ensuing openings:

1. CobiT Maturity Model Questionnaire, ISM3;
2. CobiT Controls [8];
3. CobiT CSF/KGI/KPI (Critical Success Factors, Key Goal Indicators, Key Performance Indicators) [15], CobiT Security Baseline [17];
4. Other organization-relevant standards (e.g., ISO 27002).
5. On the contrary, cumulative parameter compliance to requirements of regulators should be avoided due to following reasons:
   a. Such approach is resource-demanding, therefore would likely impede the ML evaluation process;
   b. Compliance with certain parameters is more essential than the total conformance.
6. A relative importance (weight) can be granted to each question. As means of assistance, ratings (and other methods embodied in Decision-making theory) can be used.
7. When compiling response options the criticality of the object should be considered (crucial IS or processes).

Algorithm for question compilation:

1. Set up the basic structure;
2. Use checkpoints or activities for questions and controls or parameters of quality (Table 2.) for response options;
3. Choose units (e.g., a percentage, a number or a certain state-indicator) and establish an evenly (<25-50-75-100) or unevenly (<80-90-95-100) divided scale;
4. Create a clear structure: group questions thematically. If applicable, extend the existing CobiT „*Maturity Model Attributes*” or ISM3 (this will help determine positions that call for further measures) and apply crucially characterizing parameters („Crucial Systems” (CS), „CS and up to 30 % of other systems” etc.).

[4] Sensitive link – a parameter that is tightly bound to several other indicators, thus even slight its improvement can well affect many other factors. Examples of such „sensitive links” are formalization of a training process and implementaton of examinations.

Collection and assessment of results. Results can be collected by heeding:

1. Directions (fields), e.g., *„Understanding and Awareness”, „Goals and Metrics”, „Security policies and procedures”* etc. according to CobiT [8] (please pay attention to Table 2.).
2. By processes.
3. Interrelationships (e.g., questions concerning existence of audit trails, their quality and application are all related).

The potency to gain information on different stages enables profound use of available data, thus, empowering the process analysis, consequently, better decisions can be made. Let us now learn how the assessment of results occurs. Let us start with an example.

Shall all answers correspond to ML 1, it is then not difficult to understand that the result (ML of the topic) is as well 1. This also applies to other ML, i.e., ML 2, 3 *et cetera*. Put in mind that the ML of each topic follows the answers to *all* corresponding questions unless the response option that would cover the ML under consideration is not provided. In such a case the question is left out in the particular phase of calculation. The latter grants avoidance of situations when affirmative responses (to all provided questions) within the second level result in ML 3.

When interrelationships are taken into account risk determination analogous treatment is applicable - probability should be multiplied by possible detriment.

Interpretation of Results: Application of Interconnected Processes. The next step within advancement involves the application of consequences emerging from interconnected processes, since indeed many IT processes are closely related, e.g., DS5 [8] (Information provision process) to M1 [8] (monitoring process).

Table 2.

Fragment of a sample questionnaire

	Maturity Level for "Ensure Systems Security" (DS5)						
Maturity Level	0	1	2	3	4	5	Information Source
Understanding and Awareness							
	Not used	Depends on the individual	Formalized and executed for critical	Formalized and executed for all systems, meets the regulator's requirements	3 + periodically reviewed	4 lvl + best practice	technical resourse holder/CMDB
Information classification (quality)							
System classification (quality)							
Authentication and authorisation							
Identity Management system used (for system, in %):	Not at all	Critical <50%	Critical - 100%	Critical, Total <40%	Critical, Total 41 - 90%	Critical, Total >90%	
							IDM/CMDB
The rights depository are used for (system, in %):							IDM
Data in the rights depository are verified with the data in systems (for system, in %)							IDM settings
User identification is standardised for systems							IDM, systems settings
User authentication is standardised for systems							IDM, systems settings
Data in the rights depository are verified with the data in systems (period)	Not verified	After request (not periodically)	Not all data, periodically, manually	Automatically, not one-line	On-line after changes	On-line after changes + 1 per day	
							IDM settings

The evaluation can be carried out in two distinct ways:

1) In the frame of DS5 evaluation process 2 questions showing relation with M1 development should be composed. One of them could focus on the range of monitoring (only CS, all systems etc.), the other – on the quality of monitoring, which could be expressed quantitatively;
2) The other approach is applicable when all the processes have already been evaluated (including allocation of relative importance's (weights)) and explicable by means of the following example.

If the weight of DS5 is 3.5, but that of monitoring is 2 and the impact weight is assumed as one twentieth or 0.05, then it can be deduced that monitoring affects DS5 negatively, hampering it by a value of (3.5-2)*0.05=0.075.

The main benefit of application of interconnected processes is the acquired opportunity to reveal the operations substantially impeding or accelerating others.

For instance, as mentioned before, monitoring impedes other processes with a weight of 0.5, while the Change Management - with only 0.25. Consequently, provided equal amount of resources is utilized, monitoring affects the situation more than Change Management. At the same time, these calculations are theoretical, furthermore, the costs to ensure these changes are not taken into account.

Application of results in situation modelling: An additional gain from formalized ML determination is the establishment and introduction after certain rules providing an insight into a generalized course of action. This helps to plan the sequence of necessary actions to approach to and achieve the desired goal.

5 Conclusion

On balance, determination of ML is a prerequisite to making decisions and meeting targets; at present methodologically the best tool to carry out this process is MM. The area for future inquiries is broad.

Primarily, the other stages of the complex decision making and consummation process (see section 2) should be investigated. Furthermore, the adaptation of the commenced approach in the continuing research is advisable, since it could ensure natural integration of the groups in the whole process while assuring effective problem solving and task accomplishment separately - in each of them.

Taking into account that ML should be determined in line with future activities (like implementation of new controls or alteration of the existent), MM helps select the most appropriate directions, or fields, (Table 2. provides an example) for the performance of activities, not the activities themselves. What is more, MM supports the determination of ML, rather than of possible or best routes.

MM requirements, as well as recommendations employable to assure meeting them have been given throughout the inquiry. Though it is proper to emphasize afresh that a greater attention should be paid to connections between processes, controls, states and activities. Information Security process is very complex, therefore deficiencies emerging from stage most likely could prohibit success in another.

Determination of ML and the development of other stages should support the decision-making process, as well as control mechanisms, for they help determine, whether the goal has been achieved. Simultaneously the ML determination should advance toward boosting the situation modelling, which – as brought to front at the end of section 4.2 – could be possible providing the acquired results were accurately applied.

Situation modelling allows, first, operative audit (whether the (intermediate) target state is reached (see Fig. 1.) and credible forecasts, in the second place, regarding effects of alteration, advancement possibilities and risks. Moreover, it possesses a potential of being helpful in decision-making.

The issues faced in the research, as well as current MM and ISM management tendencies, have lead us to the following conclusions:

1. Other stages of decision making and aim achievement processes should be investigated on the given basis;
2. A clear and formal definition of aims and scope of MM application is needful;
3. Situation modelling should be encouraged;
4. Connections, including multidimensional, between various activities, controls and aims are supportable;
5. The use of Risk and Vulnerability approach should be encouraged.

References

1. Abhishek Vaish and Shirshu Varma: Proposed Next Generation Information Security Management Effectiveness Measurement Model, *http://amrita.edu/cyber-workshop/proceedings/icscf09_submission_101.pdf*
2. ISM3, *http://ism3.wordpress.com/*
3. Wes Sonnenreich, Return On Security Investment (ROSI): A Practical Quantitative Model, *http://www.infosecwriters.com/text_resources/pdf/ROSI-Practical_Model.pdf*
4. Saad Saleh AlAboodi, *http://www.itgi.org/Template.cfm?Section=Home&CONTENTID=34805&TEMPLATE=/ContentManagement/ContentDisplay.cfm*
5. ISM3 Comparet to ISO27001, *www.ism3.com/page2.php*
6. Lessing MM: Best practices show the way to Information Security Maturity, *http://researchspace.csir.co.za/dspace/bitstream/10204/3156/1/Lessing6_2008.pdf*
7. Erik Guldentops: Maturity Measurement—First the Purpose, Then the Method. J. Information Systems Control Journal, Vol 4 (2003), *http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=16267&TEMPLATE=/ContentManagement/ContentDisplay.cfm*
8. The IT Governance Institute®, CobiT 4.1. *http://www.isaca.org/*
9. Andrea Pederiva: The COBIT Maturity Model in a Vendor Evaluation Case . J. Information Systems Control Journal, Vol 3 (2003), *http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=16253&TEMPLATE=/ContentManagement/ContentDisplay.cfm*
10. ISO 27002, *http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297*
11. ISM3 v2.10, *http://www.ism3.com*
12. Microsoft Corporation. The Security Risk Management Guide 2006, *http://www.microsoft.com/downloads/details.aspx?FamilyID=c782b6d3-28c5-4dda-a168-3e4422645459&displaylang=en*
13. Erik Guldentops: Enterprise Governance of IT Implementation and Assurance Advice when using CobiT and ValIT, *http://www.isaca.lv/gl/easyfile/index.php?folder=14*
14. CRAMM (v 5.1, v5.2), *http://www.cramm.com/*
15. CobiT Management Guidelines, *http://www.isaca.org/*
16. ISO 27001, *http://www.iso.org/iso/catalogue_detail.htm?csnumber=42103*
17. CobiT Security Baseline: An Information Security Survival Kit, 2nd Edition, *http://www.isaca.org/Template.cfm?Section=Research2&CONTENTID=36883&TEMPLATE=/ContentManagement/ContentDisplay.cfm*