Óbudai Egyetem

Doktori (PhD) értekezés

Supporting Enterprise Governance on IT Security Bases

Vállalatok kormányzásának támogatása informatikai biztonsági módszerekkel

Dr. Katalin Szenes

Témavezető:
Dr. Gyula Hermann

Alkalmazott Informatikai Doktori Iskola

Budapest, 2014. február

Table of Contents

1. INTRODUCTION

1.1 Predecessors and sources

The goal of this work is to introduce such a new *governance methodology* for institutions, that supports business or other strategic activity *directly, without any intermediate layer,* by the best practice and experience of information systems security and audit. On the other way around, the methodology helps the justification of security measures by strategic goals. This means, beyond helping to achieve commitment of the top management for security, e.g., facilitating the acceptance of such uncomfortable rules, as requiring the use of entry cards, passwords, and the like, for the sake of preserving the strategically important corporate assets.

I named the methodology as "PCUBE-SEC". "SEC" is for security, and the first part, "PCUBE" - P^3 comes from my expert system, PCUBE, that I developed for the modelling, **P**lanning and simulation of **P**arallel and concurrent **P**rocess systems, which is an organic predecessor of PCUBE-SEC [Szenes, 1987, 1988]. The computerized processing of the PCUBE-SEC knowledge base relies on the (partially) "artificially intelligent" way of PCUBE information processing. This knowledge base can serve as a *framework* to store, and publish information that is worth to be shared, e.g. advice taken from best practice methodologies, different users' problem descriptions, and even already proven preconditions to their solution.

Information systems audit traditionally supports the realization of enterprise strategy, by *checking* the quality of IT support provided to the business systems. Information security deals mostly with *finding ways* to solve the problems, explored by IT audits. Contributing to the security of users' data, both areas serve - *implicitly* - customers' satisfaction. There is no reason here to make difference between these areas in this discussion, so, in the followings we will refer to these two areas together as *"information security - IT audit"*.

In order to serve strategic, business goals *directly* by information security - IT audit ideas, their basic definitions had to be generalized from IT towards corporate operations, after eliminating their inconsequences, contradictions, and other kinds of inaccuracy.

Among the prominent traditional sources, the materials of the Information Systems Audit and Control Association - ISACA, together with some of those standards of the International Standard Organization - ISO were chosen here [CRM, COBIT 1998, COBIT 2000, COBIT 4.0 - 2005, COBIT Map - 2006, COBIT 4.1 - 2007, COBIT 5 - 2010, 11, 12],

[ISO G73, 27001, 27002, 27005, 38500, 27000, 12207]. In the text we will refer to the standards in the form of: "ISO" followed by the number of the standard, for example, ISO 27001.

"CRM" denotes here the CISA Review Technical Information Manual, that we, the Quality Assurance Team yearly update for the Certified Information Systems Auditor - CISA - candidates. This is the handbook for their exam, the same book is used all over the five continents. I have been participating in this work from 1999. I will refer to this study book here as CRM, unless the date of publication is significant.

Methodology COBIT - Control OBjectives for Information Technology - has been developed by ISACA, especially by its research institution, ITGI (IT Governance Institute), for more, than 15 years now. On COBIT here always COBIT 4.1 will be meant, unless otherwise stated, and then the version number will be marked. By 2012 our team, the Subject Matter Expert Team finished COBIT 5, but from the viewpoint of the present discussion mostly version 4.1 is to be relied upon.

The most important definitions have rarely been changed from 1998 to 2007, even if the *methods* presented in the versions of COBIT have been significantly extended. COBIT 5 brought remarkable, and, as it will be seen, not always definitely positive differences.

1.2 The research goals and results. The benefits of the new governance framework

Improvement of the traditional approach

Governance has always been an important ISACA issue, already from COBIT 1998 [COBIT 1998]. The related COBIT and CRM definitions will be analyzed here, and, even if I hope to have improved them here, they certainly are indispensable predecessors of this work. [CRM, COBIT 1998, COBIT 2000, COBIT 4.0 - 2005, COBIT Map - 2006, COBIT 4.1 - 2007, COBIT 5 - 2010, 11, Szenes, 2010, GRC], [ISO G73, 27001, 27002, 27005, 38500, 27000, 12207]

The proposed new definition set is transparently related to the strategy. PCUBE-SEC intends to support the fulfillment of institutional business goals by supporting their decomposition to lower level operational goals by a special *derivation* procedure, which is based on the technics of the already mentioned PCUBE. One of the connections between PCUBE-SEC and information security - IT audit is, that these derivations often use "problem solving receipts", learnt from these disciplines.

The goal of PCUBE-SEC is to *support* the achievement of the PCUBE-SEC users' goals by *advice on choosing* such subgoals and activities leading to these goals, that express, where possible, measurable, concretely identified efforts. These users' goals can be strategic goals, too. Besides, as a further support of strategic-based governance, PCUBE-SEC offers systems analysts' methods for *identifying* strategic goals.

This PCUBE-SEC support helps exploring the mutual relations between: the users' goals, the activities, that improve corporate operations, their domain, range, and resources, and the area where the expected result will be seen. In the practice usually this latter area will even be modified by the improving activities. These six dimensions are based partly on those clarified, already contradiction-free definitions taken from ISACA and ISO materials, that PCUBE-SEC extends towards operations, in order facilitate the identification of such procedures, that affect business positively, through improving operations. [Szenes, 2010, GRC], [Szenes, 2011, Appls.], [Szenes, 2011, Gov.]

A more important PCUBE-SEC contribution to the ISACA / ISO knowledge, besides *extending* their solutions from IT to *operational level* is adding such *other, measurable dimensions* to the basic notions, that help solving practical problems by *clarifying the requirements of the improving activities.*

All this required the introduction of such new, concrete parameters, both for the operational activities and -objectives, like, for example: who does what, using what, and what is gained by all these. The parameters of the users' goals can also be scalable values, where scaling, values and measures are all interpreted by their *relations to each other*. Thus, what PCUBE-SEC is able to help, is the evaluation of alternative courses, by supporting the *comparison* of the *effect*, or that of the *roles* of different subgoals or activities, in fulfilling the original users' goals. [Szenes, 2011, Hack.], [Szenes, 2011, Appls.], [Szenes, 2012, MM], [Szenes, 2013, ICCC]

Generalizing and extending information security and IT audit *requirements*, the *evaluation and improvement of enterprise processes* will be possible, showing, how to gain *business profit from operational efforts*. The novelty of the resulting method is, that it is again *directly* based on already proven information security and IT audit methodologies. The expansion of special IT-related disciplines results in such a *new type of enterprise governance framework*, that might support the market success of companies in a new way, exploiting methods formerly used for different purposes.

Excellence criteria
In order to provide for this kind of users' support, and to suggest concrete goals, that are able to serve the fulfillment of strategic goals,
PCUBE-SEC defines a complex system of excellence criteria.

These criteria consists of two groups. The first group, a kind of generalization of ISACA and ISO criteria, deals explicitly with asset management, while the other focuses at operational quality [Szenes, 2007, SOA], [Szenes, 2010, GRC], [Szenes, 2011, Appls.], [Szenes, 2011, Hack.,], [Szenes, 2012, MM], [Szenes, 2013, ICCC].

The criteria have already been proven to be useful in such research areas, too, that have nothing to do with our subject. Gabriella Nagy evaluated so-called Ambient Assisted Living systems, using them. These voice-controlled systems improve the way of living of elderly or disabled persons [G. Nagy]. Tibor Istvan Nagy and Jozsef Tick used these criteria investigating military sensors [T. I. Nagy, J.Tick].

Operational security
PCUBE-SEC offers such an operational security definition, that establishes a direct, mutual connection between security and institutional operations, in order to exploit security tools in improving operations, and, on the other way around, to justify security goals by operational ones.

Similarly to the operational activity above, this operational security can be characterized by such concrete, measurable, predictable requirements, that depend on scalable preconditions. The security of the corporate IT system is defined as a special case of this operational security. Thus both the development and the evaluation of this kind of IT security can be directed by similarly *concrete* requirements [Szenes, 2006, SOA], [Szenes, 2007, SOA], [Szenes, 2010, GRC].

I do not want to pretend to have reinvented the wheel by finding close connection between business and information security. It must be noted, that professionals have already been arising the question many times, how business and information security could be drawn closer to each other? By inserting operational-level goals and procedures between the strategic level and the everyday practice, the PCUBE-SEC answer is different, regarding both the established connections, together with their exploitation, and the way of practical support it offers to its users.

Facilitating a direct understanding, and, this way, a closer cooperation between top management and experts of information security - IT audit, this framework of cooperation makes possible the *transfer of benefits* between the two areas: business, and a supporting operational area, the security. Security goals can be justified by strategic, business goals, while to the achievement of strategic goals such ideas might be used, perhaps in a generalized form, that are learnt from security methodologies.

Thus management's expectations concerning security can go beyond simply obtaining the *trust* of the customers and partners, and beyond the fulfillment of the different compliance criteria required by mother companies, by shareholders, by governmental and other external authorities, etc., towards even more sophisticated strategic goals [Szenes, 2006, SOX].

The technical toolset of PCUBE-SEC
supports finding *necessary* operational-level conditions of strategic, business goals by the means of a special derivation process. The toolset relies on the PCUBE-SEC knowledge base and its processing, providing for a simple way of storing and retrieving already proven "experts' and users' receipts" in such a way, that these receipts can be "re-used to the fulfillment" of the current users' goal [Szenes, 1976-77], [Szenes, 1982, 1987, 1988] [Szenes, 2006, SOA].

In order to identify

- the domain and range of the improvement activities, that is the area to be improved, and the type of the activity to be done, and
- the scope of the excellence criteria, or
- the scope of other, user-defined operational objectives

I defined *the pillars of operations.*
Their ancestor had been the pillars of IT security, that have already been proven to be useful classification aspects for IT improvement [Szenes, 2002, risk], [Szenes, 2010, GRC]. With the extension of the PCUBE-SEC terminology and scope, from IT towards corporate operations, the pillars had to be generalized, too.

The strategy-driven goal & operational risk management of PCUBE-SEC
While the traditional risk management focuses on the availability and confidentiality of information, and reflects a *defensive* standpoint, the PCUBE-SEC practice, instead of mitigating *problems*, has focused on *achieving* the strategic *goals* already from the starting point of its development [Szenes, 2002, risk]. By choosing, for objectives, the polished, extended, and the new definitions of the excellence criteria, and by identifying the areas to be improved using the pillars of operations, PCUBE-SEC *proactively* helps its user in

finding necessary conditions of reaching his / her strategic goals, contributing, this way, to the market success of the institution. The novelty, that the efforts are scalable and comparable, is due to a special risk definition. This is the so-called "asset risk", that extends the traditional definitions by reflecting *explicitly* the strategic importance of the resource or property in question [Szenes, 2012, MM].

It should be noted, that some of the PCUBE-SEC facilities are published here at the first time. The knowledge base, and its processing will be illustrated on practical, everyday problems.

2. THE BASIC FACTORS OF THE SECURITY-SUPPORTED GOVERNANCE METHODOLOGY

The basic factors of PCUBE-SEC governance are

- the goals to be achieved,
- the tools that contribute to the fulfillment of the goals, and
- the notion of governance itself, that determines the definition and handling of these goals and tools.

The predecessors of the elements of this triad are already available in the traditional methodologies. To the *goal*, to the PCUBE-SEC operational objective, the traditional control objective, to the PCUBE-SEC operational activity, which is a vital *tool*, the so-called control measure correspond. Governance and IT governance have also been frequently discussed terms. [COBIT, CRM, ISO 27000 family, ISO 38500]

In this chapter the problems of these traditional definitions, and their PCUBE-SEC solution will be analyzed, with the exception of the *control objective - operational objective pair,* as the PCUBE-SEC operational objective can not be introduced without such other PCUBE-SEC-specific notions, as the pillars of operations.

It will be seen here, that relying on the *direct* connection between governance goals and information security - IT audit methods, that PCUBE-SEC is to establish, the mutual direct support yields

- an effective and efficient support of enterprise strategy by derivating concrete everyday improving goals and actions from strategic goals
- a possibility of tailoring and tuning the strategy based on a *direct,* and *operations-related* feedback provided by collecting those basic problems of institutional operations, that are to be solved using information security methods.

This mutual dependence presents such an easy to use common language and methodology, that can be shared between top management, business, security, audit, and other business-supporting areas. This way top management will be able to promote strategy by using *directly* the human and material resources, disciplines, and tools of information security - IT audit.

A trivial example is the well-known information security requirement of customers' satisfaction, data confidentiality. Without customers there is no success in the market, which is, in its turn, an important goal of corporate strategy. Thus we found a strategic base

for confidentiality. Starting from security we got to corporate strategic level. The other way around, market success will be a good reason why confidentiality has to be satisfied. Here information security methods contributed to the achievement of strategic goals, while, from strategic goals, information security tasks could be derived.

As besides IT-level measures, to achieve confidentiality, organizational, and other operational-level activities are also needed, this is an example for an important novelty of the new PCUBE-SEC framework: it supports the *insertion of operational* procedures between low-level, practical goals, and corporate strategy.

In 2009 ISACA published its Business Modell for Information Security, BMIS, which is, in a way, also a step towards the alignment of business and security goals. In its Appendix a case study is given on aligning the security goals to the business goals [BMIS, 2009].

BMIS also wants to find a common language for business managers and information security people, to support the integration of information security *into* business. However, there are important differences between BMIS and PCUBE-SEC, as far, as goals, direction, and approach are concerned. For BMIS security comes first, and this is aligned to business, while the PCUBE-SEC view is bidirectional. Starting from corporate success PCUBE-SEC proceeds to strategy, then to business goals. Its other direction justifies, by business benefits, security / audit goals.

While BMIS wants to *raise* information security issues to business level, PCUBE-SEC wants to support the *derivation* of concrete *operational* goals and tasks from business goals. For PCUBE-SEC either IT, or information security are *just special case for operational areas*.

This does not mean, of course, omitting the fact, that most of the information security measures try, *at first*, to affect positively enterprise operations actually through the improvement of *just those* IT services *upon which just those activities rely* that serve the strategic goals of the company the best way.

PCUBE-SEC exploits the relations between the so-called information security control measures (these are activities, that serve security goals), and IT, and those between IT and other enterprise operations, in order to improve three important, complex process types: IT, operations and business.

In order to develop such an interpretation of the information security and IT audit disciplines that satisfy the goals above, the basic traditional terms had to be thorougly cleaned and reformulated.
Thus the new definitions follow, together with an analysis of the present traditional ones.

2.1 The history of corporate governance - enterprise governance - IT governance, and the problems of the traditional definitions

2.1.1 Governance, IT governance, IT security governance - ISACA

The scope of enterprise governance is becoming more and more extensive. However, there is an other, important stream, flowing just in the opposite direction, that tries to specify a more closely determined road towards enterprise governance. The ISACA governance definition is an example, too. In the "Corporate Governance" section of CRM the definition is the same, almost word-by-word, as the definition in the COBIT 4.1 Glossary:

"Enterprise governance—A set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly" [COBIT].

Including strategy into the definiton of enterprise governance is close to my approach, but the *goal* of this strategy, the success on the market, which is, I think, the most important, is not specified. The responsible use of resources belong to the armoury of the strategy-driven goal and risk management of PCUBE-SEC, too, but from this definitional level such considerations should have been omitted. Besides, emphasizing just these, among the many other weapons available, seems to be a little bit random choice. I will, of course, introduce these kind of toolkits, too, but in their context, equipped with separate, operational level definitions.

Rising market success to this definitional level is justified by the requirement, that to achieve this success, is just the first common responsibility of both the top management, and that of the staff [Szenes, 2011, Gov.] [Szenes, 2011, Hack.] .

In this first decade of the 21th century, when governance, especially IT governance came into focus, with quite various interpretations, everybody tried to relate the two notions somehow. "IT governance is just a part of enterprise governance" - said John Thorpe, a

Canadian enterpreneur, simplifying it a bit, at at an IT roundtable discussion, in Brisbane, Australia, 2008 [ITGI, Roundtable].

According to such acknowledged expert of this field, as ISACA, successful IT governance is rather a necessary condition of a successful enterprise governance, than being simply just its subset.

Now it is the time to ask, if enterprise, or corporate, or institutional governance is the thing to be discussed? I have chosen "enterprise". "Corporate" often refers to big companies. The best would be "institutional", as the followings apply to both sectors, private, or government, too, but "enterprise governance" is more conventional, it seems to be an already accepted terminology. Thus "our" governance here an enterprise governance according to the style of PCUBE-SEC.

ISACA places IT governance into the centre of enterprise governance, stating, in the Overview of Governance and Management of IT in the CISA Manual, that IT governance is an "integral part" of enterprise governance. ISACA defines it, as: "IT governance, one of the domains of enterprise governance, comprises the body of issues addressed in considering how IT is applied within the enterprise." [CRM]

The COBIT IT governance formulation in the Executive Overview is somewhat different: "the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives." [COBIT]

The COBIT definition of the process "Provide IT Governance" adds to this, that the "enterprise IT investments" have to be "aligned and delivered in accordance with enterprise strategies and objectives", and requires the integration of "IT governance with corporate governance objectives and complying with laws, regulations and contracts".

Besides requiring the close cooperation between IT governance and corporate governance objectives, too, my concept will explicitly *allocate* the responsibility for the fulfillment of strategic objectives *to the whole staff*, not only to IT.

We have in CRM information security governance, too: "the responsibility of the board of directors and executive management, and must be an integral and transparent part of enterprise governance. Information security governance consists of the leadership, organizational structures and processes that safeguard information." [CRM]

Raising the discussion of IT governance to corporate strategic level, the repeated list of "leadership, organizational structures and processes" of COBIT IT governance and CRM information security governance had to be replaced by the wider scope, defined by my pillars: the organization, the regulational system, and the technical infrastructure.

This pillar notion, that has been extended to classify the operational areas I have presented first as pillars of IT and IT security, then I redefined them, to have them to cover a broader scope, the whole operational arena [Szenes, 2010, GRC], [Szenes, 2011, Gov.]. A more detailed elaboration of the pillars come soon, here the colloquial meaning is enough.

Even if PCUBE-SEC extends the domain of the activities, IT will preserve its basic role in enterprise governance. Besides supporting the computerized part of the corporate information system - or even contributing to the *identification* of the still not automatized processes - using *systems analysis tools* - IT has a very significant part in formulating and supporting the strategy of the company. Another task for the systems analysts is to help coordinating the derivation of new goals.

Discussing enterprise - or sometimes - corporate governance, OECD (Organisation for Economic Co-Operation and Development) guidelines are stated to have been cited in the CRM. The probably most important reference is taken actually from the minutes of an International Corporate Governance Meeting, that of an OECD conference. According to this minutes corporate governance is “the system by which business corporations are directed and controlled” [OECD IFC 2004].

The OECD Principles of Corporate Governance itself is quite a long study by OECD. It intends to give guidance primarily to publicly traded companies by fixing the basic principles of corporate governance, defining the rights of the shareholders, the roles of the stakeholders, etc. For us the preamble is, perhaps, of immediate interest, stating: "Corporate governance" ... "provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined " and: "Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring." [OECD study]

Provision for strategic direction begins with provisioning for the *existence* of the enterprise strategy. The first step of building a strategy is the *identification* of the strategic goals. The *measures,* or, in other words, those activities, that are able to enforce the fulfillment of

these goals, have to be determined, too, without them the corporate will not be really governed.

This already shows, that to translate the responsibility of the top management into a series of purely top-level items would be rather difficult. Even so, *defining* goals seems to belong to the higher level tasks in an organizational hierarchy, than to invent measures suitable to fulfill them. The question arises, which is better, to add measures - actions - to the definition, or to refrain from them on this definitional level?

Another important question is the origin of the strategic goals. As this determines the experts' attitude to governance, a reference to this source has a place in the governance definition. The primary source of the goals of the enterprise is the success on the market, an utmost necessity, if the enterprise wants to stay alive. Every other things come from the strive for this success. A firm has to keep going always forward, surviving is not enough. Stopping in the development means immediately falling behind. Falling behind its own goals, and, of course, falling behind the competitors, and this would be fatal.

The strategic goals are on the *second* highest level, following the enterprise success. Those goals, that are able to contribute to the fulfillment of the strategic goals, are on a lower level.

An important item in the list of the *responsibilities* of the top management is the *maintenance* of the strategy, and thus the maintenance of the strategic goals. Extension / change of a strategic goal should, of course, be strongly related, among other factors, to market-, or to environmental changes. Environment means here society, nature, etc.

Following this line I will be able to stay to be faithful to the spirit of ISACA. Besides this, the other source of my proposals is my long practical working experience in information security - IT audit. The *usability* of the definitions in the everyday life should always belong to the quality requirements, when institutional practices are discussed.

Having defined the strategic goals, the management has to assign their specific responsibilities to the organizational roles. The *responsibility of the whole staff* in achieving these goals must also be explicitly declared in the definition. Of course, the *scope* of this responsibility has to be varied, and authority has to be assigned to the individual organizational roles, according to their place in the organizational hierarchy. This is why the new framework to be created for enterprise governance, for the enterprise governance of PCUBE-SEC, has to *support every member of the staff*, in fulfilling their operational

responsibilities. Top management has to bear the responsibility that stems from their position. However, to *support* the strategic goals is the duty of the *whole staff*. This obligation should also have a place in the definition.

Going back to the analysis of the second part of the ISACA CRM and COBIT enterprise governance definition, the tools themselves, that are needed to *perform* those tasks, that serve to achieve the goals, do not fit into a definitional level. An example for a *tool*, that could have been placed rather into the explanation part, than into a strategic-level definition, is risk management, even if there is no governance without taking the risks into consideration. The responsible use of resources is an absolutely necessary prerequisite, otherwise we would not know the strategic value of the assets, so we would not even be able to ensure the appropriate, cost-effective treatment of the resources, not mentioning an overall responsibility, but this is also a lower-level requirement.

The drawback of this mixing of different levels can be clearly seen here. This mix hides the difference between the problems, problem solving, and tools. On "problems" PCUBE-SEC means issues to be handled, in order to reach the strategic goals, and the "tools" can be used to handle them. The domains, *where* these tools are applied, are also to be separated from tools and from problems.

For example, from the viewpoint of governance, risk is always related to at least two things. One of them is those sets of objectives, derived from the strategic goals, that are assigned to different - usually hierarchic - levels of the company operations. If these objectives are "at risk", this means, that they will not be reached without managing the risks, that is without conducting a risk management process. The threats to these objectives are the problems to be handled. That is why one direction of extending risk management is towards strategy-driven goal and risk management.

Another aspect to be taken into consideration in risk management is the set of those resources, that are necessary to the operations of an enterprise. These belong to the domain of problem solving. My already mentioned three pillars of operations are able to help a lot in classifying the usually very different resources. Differentation between the resources according to pillars give a very practical classification possibility, when we actually want to do something, and want to find out, where to begin, and where to turn to proceed.

2.1.2 The ISO contribution to governance and IT governance

The International Standards organization also realized the importance of governance. In 2008 an irregular publication appeared on IT governance, a so-called "advisory standard", according to its foreword. It does not prescribe requirements, as usually the ISO standards do, but *advises*, how can corporates be compliant with the different regulations - the standard calls this compliance as "conformance", and how they can ensure, that "IT contributes positively to the performance of the organization" [ISO 38500].

The discussion of the principles, that are suggested for consideration is split to three parts, evaluation, direction, and monitoring, which is again not a usual construction for an ISO standard.

The already mentioned OECD principles of corporate governance, studied by the CRM contributors, are "adapted" here, again, as it is explicitly stated in the text of this material. It is even included into the referenced documents section, together with the predecessor of the 2009 ISO Guide 73, that had been prepared in 2002. (To this 2009 version of the ISO Guide 73 we will return discussing the PCUBE-SEC risk management, which is strategy-driven goal and risk management.)

Thus ISO 38500 defines corporate governance the same way, as it stands in the OECD 2004: "The system by which organizations are directed and controlled."

The 38500 IT governance aims at the *corporate* governance of IT, but omits the responsible actor: "The system by which the current and future use of IT is directed and controlled. Corporate governance of IT involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using IT within an organization."

Neither the responsible actors, nor the market success, which should be the goal of the mentioned direction and supervision is clarified. Both of these aspects are very important. The significance of corporate wellness, market success, and growth, the necessity of allocating rights and responsibilities I had emphasized aready in 2010, defining corporate governance [Szenes, 2010, GRC]. Here this definition will be further improved.

2.1.3 The PCUBE-SEC style of enterprise-, and IT governance

Summarizing the previous requirements, we have quite a lot of goals for our framework. Here is a collection of them, together with references to means to achieve them. These are those aspects, that the definition of the basic notions have to take into consideration.

The corporate governance framework has to support company growth, market success. This involves three immediate consequences, three requirements.

The first is continuous development - this is the only way to stay alive, if a firm stops developing, it will inevitably fall backwards, as we have already mentioned. Here development means development in business, and even innovation.

The trivial second consequence is the business support.

The third is compliance to any kind of external obligatory requirements. These can be either inherently, or regulationally obligatory. To the first type belong natural, social, and the like circumstances, while to the second the requirements of the government administration, those of the shareholders, or those of the mother company, etc.

These requirements will be handled by my excellence criteria, that will, besides helping to characterize the desired quality of the results of the actions of the staff, contribute to the provision of the promised receipts of best operational practice, Some of these practices have - even if sometimes remote - predecessors in information security - IT audit.

The probably most important excellence criteria, that will be introduced here, might be the already mentioned order. besides supporting every improving effort, it can be used to estimate the difference between the present, and the targeted future state.

To achieve any goals, first the goals themselves, thus the strategic directions have to be fixed. As for a beginning, this means the provisioning for the *existence* of the enterprise strategy, that should contain the *definition* of the strategic goals.

All this is useless, of course, without such *measures* or, in other words, *actions,* that are able to enforce the fulfillment of these goals, However, actions have no place in definitions. In identifying the numerous possible actions, the already mentioned pillars of operations will help, by providing facilities for the classification of the tasks, and that of the scope of the tasks, too.

Discussing my excellence criteria I will emphasize, that the strategy is useless without built-in maintenance obligations. These should require both a regularity, and a compliance to the changing inside / outside circumstances.

To the actions, and to the requirements, too, actors have to be assigned, who fulfill them. The tasks & responsibilities of the different actors at different hierarchical levels are, of course, different. At the first place, as it will be emhasized here more, than once, top management is responsible for everything. However, in order to implement the requirements in real life, everybody in the staff has to have his / her own responsibility delegated, assigned to them, according to their roles in the corporate organization & hierarchy.

Taking all these into consideration, and deleting the consequences from the definitional level at the same time, I formulated such a definition, that is simple enough to be applied in ordinary practice. In its entirety this definition has first been published in 2012 [Szenes, 2012, MM], but has its predecessors already in 2010 [Szenes, 2010, GRC]. In this early version I had explicitly required the management of the communications media, but now I think that this is one of the activities, necessary to direct a company. However, It must be noted, that this is an important requirement. Lots of harm can be done, if this is badly conducted. Doing it cleverly might be a little exhausting, but brings fruits immediately.

Another important novelty of my definition is the emphasizing of the *responsibilities* of those, who work at, and hopefully for the company, too.

I define
PCUBE-SEC enterprise governance,

as the responsibility of the whole staff, top management included. Top management has to direct the company the best possible way towards market success, taking every kind of environmental aspects into consideration as far, and in such a way, as it is in the interest of the enterprise, based on the strategy of the institution. To define and maintain this strategy belongs to the responsibility of the top management, while the staff is responsible for supporting the top management in these issues.

Note 1
II intentionally avoided using the word "involve", which is very popular in such definitions. I would like to work with such an "enterprise governance" notion, that leaves no doubts behind, if this is at all possible. That is, no hidden details are "involved".

Note 2
The double responsibility of the top management is very important, the strategy is actually the *document, how* are they to perform their work, in the given inside and outside circumstances.

Note 3
I pondered a lot about assigning responsibility already at definitional level to the staff, too. Then I decided to state explicitly, that everybody has work to do, auditors, business, auxiliary areas alike. I wanted to embrace, at the same time, every responsibility, that has already been identified by the predecessors, e.g. the direction and control system of OECD 2004, or ISO 38500, too.

Trying to take into consideration every idea, presented here, concerning such distinguished predecessors of my IT Governance interpretation, as ISACA CRM, COBIT, the advisory standard of ISO, I suggest the following definition.

The successful
IT governance
I define, as one of the *necessary conditions* of successful enterprise governance, by directing IT in such a way, that it serves enterprise governance according to the intentions of the top management. Every member of the IT staff is responsible for it. The weight of their responsibility is directly proportional to their weight in the company hierarchy. The top management of the company is responsible for the supervision of the IT governance.

Note 1:
By adding the prefix "successful" I would like to emphasize, that this is actually a requirement, that can be over-declared by the PCUBE-SEC user, just as all my suggestions here. However, placing "success" into the definition might help the improvement of the quality of enterprise governance, together with that of the IT governance, and might improve the relations between top management and IT.

Note 2:
To emphasize the obligation to prepare a separate IT strategy did not seem to be necessary, this depends on the way of operations.

2.2 The PCUBE-SEC operational objective - remodelling the definition of the control objective

2.2.1 "Gone, like the flowers of Marlene" - the control objectives from COBIT 5.0

Having finished our teamwork with COBIT 5 I could not guess, what novelties are waiting for us behind the corner. In my complimentary copies of the new COBIT 5 books ISACA sent me in July, 2012, I tried to find the definition of control objective, but in vain.
"Where Have All the Control Objectives Gone?" asks professor Erik Guldentops, in his Guest Editorial of the ISACA Journal in the end of 2011 [Guldentops].

His answer: the COBIT 4 developers could not separate objective from action that is why he proposed the substitution of control objectives by control requirements. However, this way he seems to try formulating such requirements that are to be taken into consideration *during* controlling activities. Instead of this, I offer to help in identifying *goals to be achieved by the whole staff* of the institution. This way the PCUBE-SEC successor of the control objective will be a company goal, instead of being restricted to the audit scope.

It is interesting to note, that the COBIT 98 - COBIT 4.1 information criteria Guldentops adds to his list of requirements, composing, this way, a kind of "starting list", that he offers to his readers as a list to be extended.

Already in 2011 I proposed such a generalization of these criteria, from IT to corporate operations that could be used as strategic subgoals for operational activities [Szenes, 2011, Hack.].

2.2.2 The predecessors

ISO standards on information security mostly belong to the 27000 family, with some exceptions (e.g. 24762, that discusses disaster recovery). This family begins with ISO 27000, which serves more or less as a "vocabulary" for the family [ISO 27000]. Quoting from this standard, control objective "is a statement describing what is to be achieved as a result of implementing controls", where "controls" mean the so-called control measures. These measures are actually activities, that is the reason why I will define them here as improving activities.

This definition illustrates some of the basic differences between the ISO approach, and that of mine. For me the kind of goal, that takes over the place of the control objective, the operational objective, is such a goal, that is explicitly related to the strategy of the company. Neither ISO, nor ISACA specifies the addressee of the activity, the actor, who has to perform it. PCUBE-SEC assigns these tasks explicitly to the staff.

The COBIT control objective, quoted from the Glossary of COBIT 4.1 is: "A statement of the desired result or purpose to be achieved by implementing control procedures in a particular process". Actually COBIT handles control objective as a *working concept*, for expressing such management objectives, that belong to the best practice, and have to be achieved by IT activities, at the same time, as it is stated in the Appendix VIII of COBIT 4.1: " Control objectives—Provide generic best practice management objectives for IT processes".

It is important to note, that no activities of other operational area are taken into consideration. The role of the control objectives in COBIT is to "provide a complete set of high-level requirements to be considered by management for effective control of each IT process" - a quotation from COBIT 4.1 [COBIT 4.1].

In COBIT the control objective has a very important and practical role. The COBIT basics valid from 1998 till COBIT 4.1 identifies four domains of IT processes, we could quote these same lists throughout these years:

- "Plan and Organise
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate".

There are 34 IT processes that belong to these domains:

Plan and Organise:

"PO1 Define a Strategic IT Plan
PO2 Define the Information Architecture
PO3 Determine Technological Direction
PO4 Define the IT Processes, Organization and Relationships
PO5 Manage the IT Investment
PO6 Communicate Management Aims and Direction

PO7 Manage IT Human Resources
PO8 Manage Quality
PO9 Assess and Manage IT Risks
PO10 Manage Projects"

Acquire and Implement:

"AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI3 Acquire and Maintain Technology Infrastructure
AI4 Enable Operation and Use
AI5 Procure IT Resources
AI6 Manage Changes
AI7 Install and Accredit Solutions and Changes"

Deliver and Support:

"DS1 Define and Manage Service Levels
DS2 Manage Third-party Services
DS3 Manage Performance and Capacity
DS4 Ensure Continuous Service
DS5 Ensure Systems Security
DS6 Identify and Allocate Costs
DS7 Educate and Train Users
DS8 Manage Service Desk and Incidents
DS9 Manage the Configuration
DS10 Manage Problems
DS11 Manage Data
DS12 Manage the Physical Environment
DS13 Manage Operations"

Monitor and Evaluate:

"ME1 Monitor and Evaluate IT Performance
ME2 Monitor and Evaluate Internal Control
ME3 Ensure Compliance With External Requirements
ME4 Provide IT Governance"

In the COBIT books, the discussion of these IT processes show, how important are the so-called control objectives in COBIT, thus it was not a good idea to eliminate them, as we have already mentioned the COBIT 5 case. To every one of the 34 IT process, control objectives are attached, with a comprehensive explanation of the activities to be done to achieve them, and with many other useful information. These control objectives are such "goals", that give advice, how to align IT activities to business goals. At this level they express requirements that help to manage, to supervise IT activities.

The COBIT overview, prepared for chief executives, uses the term control objective in a bit different way, or rather, on a higher level. It states, that the management needs "something", that helps to achieve the business goals, detects and prevents undesired events, and if this was not successful, then helps correcting the effect of these inconvenient events. This something is called as "control objective" but it is much more than the control objectives described in the narrative belonging to the individual IT processes. When the level of the discussion is set to the business goals, then the control objectives are required to define the "ultimate goal of implementing policies, plans and procedures, and organizational structures" [COBIT 4.1].

2.2.3 The Operational Objective of PCUBE-SEC

Of course, COBIT 98 - COBIT 4.1 can be used very well even now, in spite of the multiple meaning of control objectives for which the above are examples. However, for my research purposes, I need a direct, explicit relation between enterprise strategy and information security, together with IT audit tools and methods. Using this relation, these tools and methods will provide for such PCUBE-SEC operational objectives, that are on the practical level of the company life, but can be used to achieve higher, strategic-level goals.

This will hopefully yields as a positive side-effect, a closer understanding between top management, and information security officials.

Thus my proposal is to generalize the activities achieving the objectives towards such activities, that improve operations - these will be my operational activities, to be described later. In accordance with this, I *extend the scope* of the control objective towards the operational arena, and attach *strategy* to it explicitly:

I define the
operational objective,

as an objective of one or more operational area(s) or role(s) to be achieved, in order to *contribute* to the fulfillment of strategic goal(s) of the company.

Let's define the
"*distance of an operational objective from the strategy"*,
as its degree of importance related to enterprise strategy,
in other words, as its importance in achieving it.

Explanation:
This importance is a subjective thing in itself. However, PCUBE-SEC "assigns" concrete value to it. More precisely, it can not assign 1 concrete value to 1 distance, as the distance can not be expressed by one single number, *it has meaning only in comparisons*.

That is, this distance, just as the other qualifying parameters in PCUBE-SEC, can be measured "only" in a relative way, meaning, that distances of operational objectives has to be related to each other, expressing, this way, that one objective is "closer" to a strategic goal, than the other, or expressing, that it is "further" from this goal, than the other.

Thus this distance connects *directly, explicitly* the PCUBE-SEC operational objective to the strategy, or, more exactly, to a strategic goal. Of course, instead of a strategic goal any other important, lower level goal can be used, *this same way.*

Relating objectives either to the same, or to a different strategic goal can also be sensible. For example, using this relative measurement the evaluation of the risk connected to different assets is just as possible, as it would be with independent measuring numbers. Now, as this weighting means a relative distance, the values can be, for example, "little, medium and high" - characterizing importance, but 1,2, and 3 can be used just as well.

Using this distance feature is not obligatory, as it is not always known. However, the PCUBE-SEC user is advised to find as many relative comparison possibilities, like this, as it is possible, as these make any evaluation more expressive.

This operational objective definition shows, that fulfilling this objective *contributes* to the strategy, *instead of being sufficient* to fulfill a strategic level objective. From this follows, that any kind of advice in the PCUBE-SEC knowledge base, put there, e.g. by other users, *contributes* to our success, but *can not ensure* it. That is, we do not have to deal with the mathemathical completeness of the promised PCUBE-SEC derivation process. To accept

the result of this derivation is upon the PCUBE-SEC users' discretion. Should the objective be a necessary condition, then logical completeness would have to be proved.

A very important *consequence* of the definition of the operational objective is, that the *excellence criteria* can be *special* operational objectives. They can also be lower level goals on the "road" leading to strategic goals. Thus they can serve as examples, for using the PCUBE-SEC generalization of information security - IT audit ideas directly in corporate governance.

Now we explicitly substituted the control objectives with the more general operational ones. Using the control objectives in giving advice, how to serve the 34 IT processes, ISACA often goes towards this more general direction, too. Among the countless possible examples, let us quote from the advice on project management, given in the form of a control objective to the IT process "Manage Projects". This can be applied for non-IT projects, just as well.

One of the control objectives here is the "Project Management Framework" (PO10.2). It begins as: "Establish and maintain a project management framework that defines the scope and boundaries of managing projects", and continues with emphasizing the necessity of assigning checkpoints and approvals to the project phases one-by-one, the necessity to integrate the project to the enterpise project management portfolio, etc [COBIT 4.1].

The other remarkable thing to note is, that the ISACA control objective has never actually been the objective of an auditor, or that of anybody, who was specially interested in being compliant to a prescription, coming from an external source, but it could be the objective of any member of the staff.

And *how* to derive more and more concrete operational objectives from the strategy? This question of the PCUBE-SEC user can be translated as: how to identify the things to be done? This will be the point, where PCUBE-SEC will be able to help, by offering seemingly information security- or IT audit related activities and objectives to achieve business goals. Derivation here means finding such operational level objectives that *contribute* to the achievement of given strategic goals.

Top management will usually have higher level objectives, than those of the staff. Not only because their way of thinking is closer to the strategy, than that of the others, but as, usually, employee of lower ranks have to find out, how to fulfill these high-level goals, and then to execute the necessary tasks.

An operational objective of a top manager can be, for example, the availability of the strategic informations any time, when they are needed, while managers on a lower level of the hierarchy might suggest, as one of the precondition of this goal, the availability of application system X, every morning from 8 to 10, in order to pre-arrange the necessary data. There are lots of non-IT examples on the operational area, e.g. only products already available in the warehouses can be sold, but selling them, at the same time, commercial, marketing activities are needed.

In the ISACA or ISO materials the improving activities are almost always restricted to the IT staff. Here we deal with the *whole palette of operations,* where IT is one of the "colours", even if a very important one, affecting often heavily, by the means of its quality, the performance of the other activities.

The COBIT control objectives - from 1998 to 2007, at least - support business by the means of effective implementation, operation and supervision of IT processes, while the more general, operational objectives of PCUBE-SEC are directly related to the strategic goals. The ultimate goal is to give effective means to implement, operate, supervise, and later even to build such operational processes, that serve the market success of the institution the best way.

The reverse way of thinking is not forbidden, either. IT security and audit professionals familiar with their methodologies might find in the receipts, collected by PCUBE-SEC users such ideas that have already been useful for other companies. If they want to "sell" it to their management, then they will be eager to find enterprise-level goals that can be supported by the idea that they would like to implement. This will facilitate the cooperation between security, audit and business, yielding useful inspirations for business use.

3. IDENTIFYING THE BASIC PILLARS OF CORPORATE OPERATIONS

Due to the already mentioned opposite direction of the priorities, that PCUBE-SEC and BMIS (ISACA Business Modell for Information Security) represents, concerning the relations between corporate success, business goals, and information security, the building blocks of the two methodologies are also different. BMIS 2010 relies on four so-called *elements*: process, organization, people, and technology. In 2009 organization had been detailed as organization design and strategy [BMIS 2009, 2010].

The PCUBE-SEC pillars are: organization, regulation, and technics.

A kind of predecessor of the PCUBE-SEC pillars are the COBIT resources. It is interesting to notice the slight change of their list at the main milestones of COBIT development.

The five 1998 COBIT "information technology resources", Data, Application systems, Technology, Facilities, and People, and their definitions remain the same till COBIT 2000. In 2005 the COBIT 4 resources did not change much, they were: Applications, Information, Infrastructure, and People. The COBIT 4.1 IT resources are exactly the same, defined word by word the same way, as those of COBIT 4. Throughout these versions the resources are used in the description of the IT processes and control objectives suggested to be reached by these processes. [COBIT 1998, COBIT 2000, COBIT 4.0 - 2005, COBIT 4.1 - 2007]

PCUBE-SEC uses its pillars in a bit different way. The operational activity is a mapping between two subsets of pillars. From the operational scope of the improving activity, that is from the area, where the activity "works", to the possibly, but not necessarily different pillar, from which the goal of the activity is taken. A goal can be reached through a series of activities. One of the help, that PCUBE-SEC intends to give to its user is just to find such a series of activity, that *can* lead to a goal activity (that can contribute to achieving a given goal activity). The final goals can be of strategic level. This way the series of activities can be considered as a series of improving activities, that - hopefully - "leads" to this strategic goal. The activities of the series "step from pillar element to pillar element", improving corporate operations.

Even if the names of the BMIS elements are partially similar to those of the PCUBE-SEC pillars, and to the resource names in COBIT, their meaning is different. According to BMIS, information security programs have to take into consideration such interaction or rather - dynamic interconnections - of these elements, as, e.g. "governing", "culture". The PCUBE-SEC operational pillars are used very differently. Their union is the *domain* of the

PCUBE-SEC improving activities, and their *range* is a subset of this union. Thus PCUBE-SEC pillars help *classifying the improving activities* according to two viewpoints: the type of pillar elements they improve from the *domain* viewpoint, and according to the type of the effect of the activities, that is, according to the *range*.

The history of the pillars is quite long now. In 2002, when I began developing a risk management methodology, I defined them to facilitate the partitioning of the IT security architecture [Szenes, 2002, risk]. Having realized, that using them, as classification aspects, they *help in collecting information*, and support, this way, to establish *order* concerning IT assets, I used them again in 2010, for basic pillars of IT and IT security. They facilitated the identification of the scope of *responsibility*, and the identification of *problem domains*, too. This way it is easier to find, to whom the responsibilities and tasks are to be assigned [Szenes, 2010, GRC]. Using the pillars it turned out, that they are extendable towards the whole scope of enterprise operations [Szenes, 2011, Hack.].

In the Appendix I. will show an example to illustrate PCUBE-SEC technics, it will show, among others, the way of using the pillars for this identification and for collecting infomation.

Just as COBIT or BMIS "does" with their resources or elements, I will define here the three operational pillars through the set of their elements.

Let an *organizational element* be any of the followings, or any combination of the followings:

- the whole organizational structure
- any part of this structure
- their creation / modification.

Thus any combination of these parts belong here, too.

Let a *regulational element* be any of the followings, or any combination of the followings:

- any prescription, regulating the activities of the staff
- the tools available at the company for
    - producing,
    - maintaining and
    - processing the regulations.

Let a *technical element* be any of the followings, or any combination of the followings:

- any physical (concrete) element of the enterprise infrastructure (fixed and wasting assets just as well)
- together with the technical realization of the conditions for using them.

The reason of the complexity of the second clause is, that we want to exclude rulebooks from here, as they belong to the regulational pillar, but to include such technical conditions, as, e.g., the actual, or the adequate *way* of setting parameters.

It is not necessary to dwell upon defining, what is a sensible combination of the organizational, regulational or technical elements, as a non-sensible combination can very well be permitted, only it might not be worth the effort of working with it.

It should be noted, that the notion of "distance", introduced as an optional feature for other PCUBE-SEC terms, too, can be used here just as well. As always in this dissertation, it serves to show the *"importance"* of an operational pillar element. Importance is evaluated again in a subjective way, as a kind of *distance* from the enterprise strategy. It has no individual value, but the evaluators give two different values to two different elements, and the *relation* of these values will show, which is the "more important" element. The example of one of the Appendices will show, how does the systems analyst work with this.

Just as the ISACA methodologies do, we
define the pillars through enumerating their elements:

Organizational elements are:
the whole organizational structure, and its parts, that is the individual organizational units, together with the "building parts" of these units, that is the roles, that are assigned, as duties, to the employees, working in the unit. Let's put the people themselves into this category, too.

PCUBE-SEC classifies these, and the structures composed from them, as organizational elements, but these assignments themselves, that are part of the job descriptions of the employee - of the people - belong to another pillar, to the *regulationa*l one.

In addition, to the *regulational* pillar belong, besides the procedural rulebooks themselves, that regulate the activities of the staff, both the intended, and the undesigned relations of these rulebooks to each other. This involves the facilities to search for given terms or rules, the hierarchy of the rulebooks themselves, if any, the contradictions embedded, the structure of the whole system, all these belong to our regulational pillar.

Should the management be committed to ethical values, a code of ethics defining the principles of staff behaviour can also be available [Belak, 2011]. This set of requirements is also a regulational element.

Technics covers all physical, infrastructural property assets, that are necessary to perform operational activities, together with the technical conditions, that determine their use.

Example for technical elements are the elements of the physical infrastructure, together with the buildings and other facilities, machines, actually the elements of the inventory belong here, together with their descriptive technical features, and the actual and best practice technical way of using them.
A special *subset* of the technical elements is the IT architecture of the institution.

IT architectural infrastructure elements, or, shortly, IT infrastructural elements are:
the computers themselves, their software (operating systems, utilities), the application systems serving the business processes, the database management systems, the network communication devices, the defense elements providing for the quality of the IT services. This quality, together with the non-IT type of operations, will be characterized here by so-called excellence criteria, to be introduced later. Actually every component of the IT infrastructure belongs here, even those, that have some computer system embedded into them, like the ATM-s of the financial institutions, or other kind of customer serving tools.

4. THE STRATEGY-DRIVEN OPERATIONAL RISK MANAGEMENT OF PCUBE-SEC

According to a research, for example, those banks survived the first economic crisis of our 21th century, that had "strong risk culture combined with an effective governance" [Oyemade, 2012]. It is well-known, that risk management belongs to one of the most important issues of information security. The most important *novelties* of my "risk management" approach are:

- the *extension* of the method to the whole corporate *operational arena*
- explicitly and methodically choosing *strategy as a base*, thus I named this method as strategy- driven goal and risk management, and even list the strategy-driven goal & operational risk management among my operations-improving *excellence criteria*.

In the followings we analyze the traditional definitions in detail. As we have already mentioned, their defensive approach, restricted more-or-less to the availability and confidentiality of information is a bit out of date in the current economical situation. They omit sometimes totally any reference to business relations. The fact, that the likelihood of being threatened, and the current vulnerability state of the objects both depend on the strategic importance of the object is neglected. The terminology is not always unambigous. Even the characterization of the risk notion is often chosen in random way. [ISO 27000, ISO 27001, ISO 27002, 27005, G73, CRM, COBIT 4.1]

These methods are restricted to IT problems, and deal with any operational aspects of the everyday corporate operations only occasionally, while PCUBE-SEC focuses on improving institutional operations, "on the road" towards the achievement of the strategic goals. The IT scope is an important, but special case.

A practically useful novelty of PCUBE-SEC is, that *the improving actions* of this best practice *can be classified according to the pillars of operations*. A set of "things" to be improved is the domain of these actions, while their range is the set of their possible results. Both the domain and range can be classified according to the pillars of operations, providing, this way, for more *explicit and practical advice*, and *to-do lists*.

Dealing with operations instead of being restricted to IT necessitated the other PCUBE-SEC specialty: the *assignment of processes to the owners, instead of assigning assets to*

asset owners, pulling, this way, the strategy-driven goal & operational risk management cycle down to earth, down to real life.

It should be noted, that every methodology from COBIT to the ISO standards requires to assign an owner to every asset. However, in the practice it is very difficult, if not impossible. Usually the best case is, that the companies begin building a data inventory, but they never finish it. The reason is, that to maintain it means too heavy burden for the participants besides their everyday work, and *for those, who have* actually *work with it*, not many benefit seems to come out of it. To identify the relevant processes and the responsible process owners is much easier. This does not mean, of course, that I suggest to give up data inventory forever. It would be great to have. Benefits should be offered for those "victims" in the staff, who have work with it, to make them interested.

Discussing the "Identifying improving actions" step of the strategy-driven goal & operational risk management cycle, we even give a short example for a part of a PCUBE-SEC knowledge base.

Beyond this operational-level handling of the issues, the PCUBE-SEC strategy-driven goal & operational risk management methodology yields other special benefits, too:

- raising both the scope and
- means of risk management from the traditional IT scope to the level of operations,
- the clarification of the mix to be found in the former definitions.

In the followings, having identified the defects of the traditional ISACA and ISO definitions, my novel risk definition, the asset risk will be introduced, which is used by the strategy-driven goal and risk management. The special importance of binding risk to the assets has already been emphasized as early, as in 2002. It was one of the basic ideas of my "RSDM", the abbreviation of Requirement / Steps Driven Method, which is a shorter version of "requirement specification system / activity steps driven evaluation / modelling method [Szenes, 2002, risk]. From then on I kept refining the method [Szenes, 2009, risk]. The name "asset risk" I introduced only in 2012 [Szenes, 2012, MM]. As it will be seen, this definition *explicitly* reflects the strategic importance of the resource or property in question, and *extends the risk domain* towards the corporate view.

Note:
Risk and threat are frequently synonyms in colloquial. Information security experts and information system auditors have always tried to be more precise, by taking instead of threat, its occurence into consideration. Risk is usually taken to be directly proportional

with simply two factors, these are: a kind of measure connected to the occurence of a threat, and the impact of the consequences.

Mixing probability and likelihood might not be such a big problem, even if it looks mathematically awkward. Quantitative risk assessment works with the probability, while in qualitative risk assessment likelihood should be used [Rameshkumar, 2010].

For the present we will stick to probability, as here we will want to give advice on ways of concrete measuring. In the ISACA materials probability is used, while the ISO standards use both, even if in some cases the actual choice looks quite random, as it will be seen in the followings.

This problem of likelihood versus probability is thoroughly discussed in ISO Guide 73, the Risk Management Vocabulary, in the same way. "Likelihood" is suggested to have the broader meaning, it is the "chance of something happening", probability is a concrete "measure of the chance of occurrence expressed as a number between 0 and 1, where 0 is impossibility and 1 is absolute certainty" [ISO G73, Section 3.6.1].

4.1 The ISO risk definition

ISO 27005, that deals with information security risk management, declares in its Scope section to accept the terminology of 27001 and 27002 [ISO 27005].

In the "Terms and definitions" section of 27001 there are lots of terms connected with risk, but neither standing alone "risk", nor "information security risk" is defined there [ISO 27001].

According to both, ISO 27000 and 27002, risk is a "combination of the probability of an event and its consequence". However, "event" can not be found in the definition section of either 27001 or 27001, but it is defined in 27000, as: "occurrence of a particular set of circumstances". [ISO 27000, ISO 27001, ISO 27002] The risk-oriented and, therefore, I think, much more precise ISO Guide 73 says, that risk is "effect of uncertainty on objectives". This definition is the closest to the one I will propose here, because of its second note, as it mentions the possibility of an aspect being on strategic level: "Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process)." [ISO G73]

The first note, attached to this definition, says: "An effect is a deviation from the expected — positive and/or negative." [ISO G73] This is very important for my research, even if its subject is not dealt with here. In a way it could be considered as one of the predecessors of my security definition, which - informally - says, that security is such a state of things, when the surprise can be forecasted with given value of probability.

Information security risk in ISO 27000 is a "potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization".

In ISO 27005 information security risk has the same definition as in ISO 27000, completed, in the former, by the "NOTE", that "It is measured in terms of a combination of the likelihood of an event and its consequence" - says ISO 27005. Should there be a possibility to measure risk somehow, which is very important, using probability is better, than "likelihood".

The risk definition of ISO 38500 uses "probability", and the note attached to it is very close to the approach proposed here: "Combination of the probability of an event and its consequence". The note explains, that the consequences, that can be either "negative", or "opportunities", are "impacts upon the organization". It does not go further to the position of the company, as I propose to do [ISO 38500]. Another important issue is, I think, to connect the consequence to a *desired result*.

We can only agree with this definition of risk management, which is point 1.6.15 in the ISO 38500, and point 2.1 in the ISO/IEC Guide 73:
"Coordinated activities to direct and control an organization with regard to risk".

It might be interesting to note, that Steven Ross, whose columns have been published practically at least in every second or third issues of the ISACA Journal, seriously criticizes the negligent wording of ISO 27005, using actually the word "loose" [Ross, 2009, risk]. He says, that the thing, that the standard defines as "risk", is, as a matter of fact, exposure. Unfortunately, he does not proceed either to 27001, nor to 27000. Had not he omitted the latter, the collection of those definitions, that are more or less valid in the 27000 family, he could have spotted the inconsistencies I described above. Ross misses the uncertainty from the risk of 27005. According to him the uncertainty is the most important factor of risk. With this I do not agree. There is, of course, an uncertainty factor in the nature of risk, as it is expressed with probabilities, and its value is not counted, but estimated. However, I still insist, that the connection of risk and strategy is the most important feature of risk.

For Ross, the reason of uncertainty is, that our defense is not worth 100%, as unexpected events, such as ""jet liners used as guided missiles, ... tsunamis" - that he enumerates as examples of environmental effects - can always come, as a surprise. While this can not be denied, I will show, that to some of this kind of uncertainties we can, and have to prepare. Such environmental accidents, as tornados, can only be handled in a limited way. We can mitigate the possible consequences by choosing the scene of our activity at such a place, where such weather phenomen rarely happen. But the intention of our rivals can, and have to be reconnoitred. This feature of managing risk will belong to my so-called strategy-driven goal & operational risk management excellence.

4.2 The ISACA risk definition and the asset risk of PCUBE-SEC

The two ISACA basics, the CISA Review Manual, and COBIT, work with the same risk definition, word by word, which, at the same time, is very similar to the ISO information security risk quoted above, but with the exception, that ISACA mentions "business".

According to the Glossary of both materials:
"Risk - in business is the potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss of/or damage to the assets. It usually is measured by a combination of impact and probability of occurrence" [CRM, COBIT 4.1 - Glossaries].

In all of these definitions the fact, that the business value has very important relation both with the impact, and with "the potential" of the occurence is totally overlooked, not mentioning the connections between vulnerability, and the other factors.

Thinking about how to adjust risk to the philosophy of PCUBE-SEC, and, what is more important, aligning theory to my practical experience collected in financial institutions and during audits of companies, I realized, that in the everyday practice we meet frequently with risk connected to the corporate assets, but we often have to deal with the risks of operations, too.

I solve this problem by introducing an asset risk definition, and by describing the handling of operational risk by a risk management cycle. The risk connected to the assets are the base of lots of important procedures, e.g. that of the business continuity plans, while handling the risks of operations we strive to reach an excellent operations level.

Thus my asset risk definition will help both in planning business continuity, and in communicating those issues to the management, that threaten it. Furthermore, the exactness

of the planning is increased by the exact values of weights, as the relation between these weights the management will be able to estimate much easier, than answer questions about probabilities of dangers and threats.

Asset risk is such a value, which

- is *assigned* to a pair of
  - corporate asset, and
  - operational objective (this can be a strategic goal, or an excellence criterium just as well)
- is supposed to be directly proportional to
  - the strategic / business value of this asset, in achieving this operational objective, as a goal
  - the probability of the occurence of an event threatening the business use of this asset (the duration of this usage is determined by the business process(es) needing this asset, in achieving this goal)
  - the vulnerability of this asset.

Where:
The strategic / business value is estimated in a subjective way by the top management or by the employee empowered by the top management to take on this business decision.
This estimation aims at the *comparison* of this asset to other assets, with respect to its importance in achieving this goal. The opinion of the estimator is expressed by the *relation* between the assigned values. The individual values assigned to the assets *one-by-one have no individual meaning*. In order to facilitate comparison and calculations integers are to be used as "values".

Formally:
business_value ($asset_i$, $goal_j$) := k_{ij}
where
$k_{ij} \in \{1, ... I\}$
$i= 1, ... n, j=1, ...m, l$ is an integer $< \infty$
(actually $l \leq 5$ is more, than enough)
(that is k_{ij} takes its value from a finite series of integers)
and
if
business_value ($asset_i$, $goal_j$) is estimated to be
< business_value ($asset_k$, $goal_j$)
then

$\forall$ j i= 1, ... m: k_{ij} (is chosen by the estimator to be) < k_{kj}

As instead of individual values we express the value of the assets in terms of relations, these *relations "offer" themselves to be weighted even further. Thus different composite classifications can be devised "on top of" this classification of assets according to their business value.* For example, classification of the given business according to its "hierarchical role" in the corporate strategy might be a useful refinement.

Different other refinement facilities can also be formulated, that the top management thinks to be relevant, e.g. classification by the process owner according to the importance of the asset in fulfilling given goals, or *according to other aspects, that the top management thinks to be relevant.*
As this fulfillment might require such *efforts, that hinder the achievement of other goals*, further weighting might be especially useful in the everyday practice.

Contrasting to the positive, goal-achieving approach of the preceeding paragraphs, we have to deal with the obstacles, too. In order to be able to take into consideration the effort of the staff to overcome them, we define
vulnerability of an asset or, shortly: asset-vulnerability
as the probability, that this asset fails to serve the fulfillment of any given operational objective, or, at least, fails to fulfill it to the required extent.

This probability depends on the choice of the asset, the goal, and the effort spent to improve the situation. This choice depends on the PCUBE-SEC user. PCUBE-SEC is not able to ensure, that every relevant factors are taken into consideration. As we often have to mention describing this methodology, completeness can not be achieved. The success of problem solving depends on the user. However, as it will be seen, there will even be advice given here on systems analysts' methods for exploring situations.

The above considerations can be formalized in the following way:

risk (asset, goal) ~ distance (asset, goal) *
probability (asset, goal, attack) *
vulnerability (asset, goal, effort)

Where:

/1 These **function notations** mean *here*, that the notion in the position "function name" is considered to depend *at least* on the notions listed in the position of parameters, between the parentheses.
The proportionality relations between right- and left-hand side, factor by factor are denoted by the "~" and the "*" signs.

/2 **"distance"**
serves comparison of assets the same way, as it is used in comparing other PCUBE-SEC notions, that is:
Let's define the
"*distance of an asset from any kind of goal*",
as its degree of importance in achieving the goal.
This goal can be any operational objective, as a special case, an excellence criterium, or a strategic goal just as well.
We work with the distance here, as in the other cases, that is the relation of the values assigned to the different values is taken into consideration, the individual values themselves are not meaningful.
The k_{ij} business values used in the formal description of the asset risk are just the distances of $asset_i$, from $goal_j$.

/3 **"probability"**
the only hypothesis we need on "probability" is the following:

if distance (asset1, goal) < distance (asset2, goal)
then
if attack_x, attack_y comes from a concurrency or from an enemy inside
then probability (asset1, goal, attack_x) > probability (asset2, goal, attack_y)

that is if asset1 is "closer" to the given "goal", then asset2,
then the "probability", that any kind of attack_x will be launched on asset1 is greater, then the "probability", that asset2 would be attacked by an attack_y.

else if
attack_x, attack_y comes from an outside intruder, then the benefit to be gained by the intruder will be the determinig factor, that is:

probability (asset1, goal_x, attack_x) ~ distance (asset1, goal_y)

where goal_y is a goal of the intruder.

On "vulnerability", the following hypothesis might be a good working one - or, at least, PCUBE-SEC suggests to "take better care" of the "more precious" assets:

if distance (asset1, goal) < distance (asset2, goal)
then
vulnerability (asset1, goal, effort1) > vulnerability (asset2, goal, effort2)
where usually effort1 < effort 2

Note: the case of a goal, without an identifiable asset
It is possible, that the asset is unknown, that is there is no concrete asset to which we can connect the risk, or at least it is difficult to specify exactly, what is actually threatened. In this case the PCUBE-SEC user needs the other parts of this asset risk notion, in describing the problem world. An example to this situation is the necessity to describe a risk management life-cycle, that has to deal with asset risks at the risk assessment phase of this life-cycle.

In this case a kind of "default asset" can be used, which is just a strategic goal, instead of being such a concrete asset, that has a concrete role in satisfying a concrete strategic goal. If no concrete strategic goal can be identified in a situation, then such a very high-level goal, as, e.g. the market success of the company is, or something as general, as that can be chosen. If the asset to be handled is that general, then its strategic value can be taken to be equal to the maximum value assigned to the chosen strategic goal. Probability and vulnerability will have to be shaped to this special case.

This "special case" of our definition gives back just one of the "old" definitions, which take the probability and the vulnerablitity into account, or sometimes omits even the vulnerability. The reason of this omission might be the practical experience, mentioned above, that the asset is maintained usually more thoroughly, if it is thought to be interesting to the external attackers.

An example of the use of a similar kind of default asset is a note of an ISACA member, proposing a differentiation between so-called "intentional", and "opportunistic" risk [Chapela, 2011]. The former is related to given data or functionality, so it is a kind of special case of my asset risk, while handling the latter, the opportunistic risk, seems to serve the improvement of a kind of general security level. However, I can not totally agree with Chapela. He assigns priorities to his intentional risks depending on the threats coming

from external sources. In order to evaluate external threats, he introduces three risk vectors. "Access" is determined by the easiness of accessing information. "Value" vector is the value of the threatened information. "Anonimity" vector is determined by the need of authentication to access the threatened information. Chapela states, that these vectors are independent form each other. I still insist, that the value of the information is not independent from the easiness to access it, as the more valuable is the information, the more effort is - or at least should be - spent to defend it. Besides, while priorities can be assigned based on a *feature* of external threat, internal threats, that are usually more dangerous, are also to be taken into consideration. Annyway, giving priorities based on any kind of danger is only a special case of strategic value-directed prioritizing.

4.3 The IT risk of PCUBE-SEC

My IT risk definition:
A special case of the asset risk is IT risk. I will define here *IT risk*, as such an asset risk, where the asset belongs to the corporate IT architecture, that is where the asset is an IT infrastructural element, as it was defined discussing the technical pillar.

4.4 The strategy-driven goal and risk management excellence

The place of the corporate assets on the scale of the strategic / business values can, and has to be estimated at the assessment phase of a risk processing cycle. The traditional name of this assessment is "risk assessment", but now we look for the possibilities of improvement, too, so this phase could be called as strategic goal-driven risk assessment. Exploiting the formulae introduced at the definition of risk we will be able to give even some concrete estimations on the costs.

The *operational* aspect of the asset risk, together with that of the problems in achieving strategy goals, will be listed among those excellence criteria, that describe the "good quality" operations. Among these criteria one is connected to the risk, it is the
strategy-driven goal & operational risk management excellence.
This will be another aspect of viewing risk.

The reason of defining it here, and not among the other excellence criteria is that this is the place of my proposal for such a best practice strategy-driven goal & operational risk management cycle, that can be followed in the practice.

I propose to define *strategy-driven goal and risk management excellence*

- based on the responsibility of the top management, concerning corporate strategy, as

- *the following system and the fulfillment of - at least - the following requirements to be satified by top management and staff:*

- the system is composed of a process and a requirement system, where the latter
  - is based on the top management's responsibility concerning
    - corporate strategy,
    - the definition and update regularly the strategic goals to be reached in order to ensure market success,
  - reflects management commitment to support, or even to initiate, the efforts of the staff, that has concrete tasks in the asset risk processing,

- these tasks of the staff include at least the followings:
  - devising methods to the *asset* risk processing
  - detecting points of *operations*, where concrete measures - activities are to be executed, in order to detect, prevent undesirable events, or correct their effect, if the decision had been to accept their occurence,

- and where predefined part of the steps of the process are to be repeated regularly.

These tasks are obligatory part of an "excellent" risk processing cycle.

There are at least five reasons why the the risk processing life-cycle I had defined first in 2002 and updated then in 2009 has to be remodelled now [Szenes, 2002, risk], [Szenes, 2009, risk].

The first reason is the positive, goal-oriented attitude, instead of the traditional negative one, the second is this *new asset risk* definition. The third, that is actually the base of these two is, that throughout this work I keep trying to align theory to a *fruitful and feasible everyday practice*. The forth is my personal practical experience on risk management that have been collected devising IT risk processing life-cycles working in financial institutions, that have to conduct risk assessments regularly [Szenes, 2009, törvények]. In the followings I generalize those methods, that I had already tried in the special - IT - case.

The fifth reason is *extending the scope* towards the operational risk arena. This involves the *extension of the domain of the assets* towards the corporate view. In the followings such a

feasible, and in the everyday practice usable series of steps follows, that could be used to non-IT asset types, just as well.

I propose to split the strategy-driven goal & operational risk management tasks into three parts. The *first part* is the initialization, that deals with the preconditions of a strategy-driven goal & risk processing. In this phase are they identified, and then they have to be checked regularly, and updated in case of need, so that their results, achievements, and benefits are sustained.

The operational pillars I defined are even more important, as classification aspects for assets or tasks, when we have to deal with operational risks instead of a restricted scope of risks, the IT risks. However, I used these pillars in my practice, too, in classifying IT-related knowledge.

The *preconditions* of the strategy-driven goal & risk processing can be organizational, regulational, and - a kind of - technical, so the preconditions can also be *classified* according to these three aspects, *according to the pillars of operations*. An important risk management *tool* will be a kind of organizational unit, that supports risk handling, this will be the committee of principals. Regulational tools will be used to fix the necessary conditions. Technics now will mean practices and auxiliaries, e.g. technical tools.

The actual cycle consists of the series of steps, that have to be regularly executed. This cycle begins with the *second part* of the strategy-driven goal & risk processing, the assessment. Here the guidelines and targets of the given review are identified. The *third part* derives the priorities based on the guidelines, and finds the most important defects, looks for improving activities, and performs them.

4.5 The steps of the PCUBE-SEC goal- and risk management

4.5.1 Preliminaries

In the followings we skip the details of those phases, that are not relevant to our subject. Every single strategy-driven goal & operational risk management effort should identify its *scope*, of course. Establishing the cooperation of those, who either can help, or are, in a way, subjects of the process, can depend on the scope, but there can be such situations, when an organizational unit, who has to conduct strategy-driven goal & operational risk management steps often, have more or less the same partners. So let us suppose, that the scope in general is already known, some further decreasing restrictions might be needed, of

course. In these cases the decisions of the Risk Management Committee have to be followed. This important body will soon be described.

An important and very practical feature of the PCUBE-SEC strategy-driven goal & operational risk management is the facitlity of collecting and processing receipts from either experts, or from other users. Those PCUBE-SEC basics, like the operational objective, operational activity, or the excellence criteria are my personal receipt, offered to the PCUBE-SEC users. The way of producing these receipts, and the technical background of their processing will be detailed here later. The goal is to make these suggestions available to the top management, and to the business staff, too, without asking them to learn any IT specialties. The receipts can be collected into the PCUBE-SEC knowledge base, and will have a role in the following strategy-driven goal & operational risk management cycle, too.

I. First part - INITIALIZATION

I./1 Establishing the cooperation of the actors - an IT experience

According to my experiences, *exploring and managing IT risks involves interfering into the affairs of the organizational units.* As usually IT and IT security is responsible for risk management, they have to initiate it. *This is impossible without a close cooperation between business, IT, and IT security throughout the whole processing cycle.*

If the assets belong to the scope of IT, then this cooperation is even more necessary, and other organizational units will also have to be invited.

For supporting *IT* risk processing, there is a technique, a trick, which I have used since 1998, when I had read about it in the CRM. This is the establishment of an IT Steering Committee. (its name had actually been IS Steering Committee, where IS stood for Information systems, but to our present terminology IT suits better.)

The members are the heads of the business areas, IT, and IT security. The mission of this committee is to provide for a cooperation platform between its members. Having realized, that by giving the information, that is necessary to build such applications, that support their business the best possible way, they usually become more than eager to cooperate. Business will bestow time and energy to inform the systems analysts on priorities, business roles and their needs.

These are just those facts and data, that have to determine the way of automatization of the processes, and help to estimate the dangers to be handled.

I./2 Identifying the "owners' role" for the processes & assets

When the business processes are already supported by IT application systems, then to every such application a responsible organizational unit have to be assigned. This will be the unit, that "owns" the application. In ideal case to every important business data a "data owner" can be assigned. Application & data owners help estimating the importance of "their" system and data. This is "only" a part of their responsibility for their "properties". They decide in everything concerning it, they have to give permission to authorize *any* member of the staff to access it, in such a way, that these rights are necessary, and sufficient to perform the work of the given employee, etc. The business user needs not know the technics of an actual technical task, but he / she has to be informed on the dangers of both kinds of result. He / she has to be told, that without testing the patch, it might turn out, that the application is not able to live together with it, and the dangers have also to be described, that might come, if, for example, a vulnerability of an operating system is not patched. The permission of the owner has to be available in any case.

The same identification of responsibility is required in the case of those applications, that support auxiliary processes, those processes, that support business, e.g. back-office, HR, and the like, or even the IT service, so the principals of these areas should also be invited in the IT Steering Committee.

I./3 Non-IT case: Risk Management Committee, owners' assignment

Managing risks of the wider, operational scope can, and have to be supported by a similar body. In this case *every organizational unit has to be represented* in the steering committee, as any kind of company asset can be the target of classification, and has to be assigned to somebody, who will be responsible for it.

The role of the moderator will be kept by the systems analyst, and due to IT risk management experience IT security will have special duties in supporting physical security when informations are to be offered on the assets belonging to the latter area. The name of this committee can be Risk Management Committee, or any other, that the participants are ready to accept. In the followings this name will be used.

Methodology PCUBE-SEC advises to submit to this Committee every planned change in the operations of the institution, when its opinion on the resulting risks is interesting to the top management. Otherwise a regular meeting schedule is to be kept, in order to facilitate the communication of the operational areas.
It might be interesting to note, that in the present editions of the CRM, "IS Security Steering Committee" appears, instead of the former Information Systems Steering Committee. In my 2012 contribution to CRM I advised the editors to return to the former name, as it might be more difficult to collect members if the declared goal is "IT security", instead of something, that they think to be closer to their everyday problems. Everybody will say, that I will help, when there is a concrete task, but I have no time for meetings. What is worse, the name IS Security Steering Committee does not express an overall type of responsibility.

Generalizing the scope has to mean the extension of the "owner" type of responsibility to those corporate assets, that are non-IT, and have to be taken into consideration. The first step of this committee will just has to be the identification of these assets.

The other extension, that seems to be necessary, is to *assign processes to the owners, instead of assets*. Every methodology from COBIT to the ISO standards requires the assignment of an owner to every IT asset. In the practice it is rarely feasible. What usually happens is, that the inventory of data - not the inventory of *every* IT asset - begins, and will never be finished, as it means too heavy burden for the participants beside their everyday work. What is more important perhaps, usually not many benefit seems coming out of it, at least *for those, who have work with it*. To identify the strategically relevant processes and the responsible process owners is much easier.

The owner of a process will, of course, own the assets "belonging to" the process. To choose the relevant assets among all the possible ones is not an easy task either, but if it has to be done process-by-process, then it is not impossible for the business users of the individual processes.

With the help of the Risk Management Committee the relations between organizational units / business processes / company assets have to be clarified and fixed. The correlations between these three factors are to be determined according to a "what is most important for this business process", and "which organizational unit has the most to do, with which business process" base.

In the following we will work with *process owners*.

I./4 The evergreen first "technical" step:
choosing the methodologies, practices to be used

The methods to be chosen have to support

- the collection of information
- its processing - in such a way, that this processing helps the user of the method in solving his / her problem,
- the user by good advice in solving the problem, e.g. by giving collections of information on similar problems,
- and / or by concrete advice, what is to be done, or what is a good idea to do in similar circumstances
- the fulfillment of the business /operational goals, that are finally to be accepted and set by the user:
    - by suggesting partial, lower-level goals aligned to the users' goals
    - by such plans, that, taking all these information and advice into consideration, help achieving the users' goals
- easiness of use!
- references
- etc. - there might be other aspests, depending on the industrial branch to which the given company belongs.

The choice is based, of course, on the declared focus areas of the candidate methods, requirements of their use - these can even be required characteristics of the institution, where it is to be introduced, and the expected difficulties arising during application. These difficulties are greatly affected by level of *documentation of the method*. The professional authority of the inventor / publisher / supplier is an important factor, too.

A usual approach is to construct an at least partially new method, using different best professional practices, as sources, exploiting those parts of the old ones, which is applicable to the given situation. In this research here, e.g., we rely mostly on the ISACA best practice, and on ISO standards. *Even the problems* of these well-known practices help us in building something new.

The method I improve here I began to develop more than 10 years ago. I presented its first version as a lecture on Risk Management, at an European ISACA conference in 2002 [Szenes, 2002, risk]. I named it as RSDM, Requirement / Steps Driven Method, a shorter

version of "requirement specification system / activity steps driven evaluation / modelling method.

I./5 The initialization & improvement of the PCUBE-SEC knowledge base

Having chosen the methods, one of the next decisions is to establish the formats, into which the data and the formerly collected knowledge will be *stored for an efficient futher use*. One of the novelties of PCUBE-SEC is the special emphasis on proposing such a format, that facilitates such a kind of *reuse* of formerly collected knowledge of either the members of the team, that conducts the risk management, or that of the experts, or that of other users. This "using again" is obviously more, than copying / pasting something, that had already been useful in another cases. This format is the same as that of a PCUBE world description, that will be described later.

The knowledge is collected from the COBIT and ISO ideas, and another important source is intended to be the personal experience of previous PCUBE-SEC users.

Another important plan is to facilitate the possibility of a kind of processing of the knowledge base. This means here supporting the *retrieval of information* from the already collected pool. This retrieval means here derivations of new facts form already known ones. This will be solved by the PCUBE "part" of PCUBE-SEC. This provides for a kind of automatized derivation of already known goals, from those, usually new goals, that are just to be fulfilled. This derivation is described in the chapter on the computerized facilities of PCUBE-SEC. Their base is PCUBE, the "ancestor".

Those goals are said to be "known" here, that the PCUBE user is able to handle from a previous experience, or using an advice of a methodology. The knowledge of handling a goal, as it will be seen, means, that the user knows those series of activities, that fulfill the goal. This had been the PCUBE help in problem solving, and this is to be extended by PCUBE-SEC.

PCUBE supported its user already in the problem specification phase. To extend this PCUBE facility for a strategy-driven goal & risk processing knowledge base, the assets have to be thoroughly documented, and the information has to be ordered.

Ordering *is important, if we want to have an easily to be updated, transparent information base. Without* ***documentation*** *everything will be once used and then thrown away. This is a vital precondition of a flexible* ***retrieval*** *facility, without which the information is of not much use.* Order, and one of its most important prerequisites, documentation, will be included into those excellence criteria, that characterize the quality of operations.

Of course, new formats for the storage of information can always be introduced to extend, replace, improve, etc., the already available ones, if the already existing information can easily be ***migrated*** into them.

The *goal of the PCUBE-SEC strategy-driven goal and risk processing* is to satisfy these requirements, together with the above support requirements.

If documents of procedures, and other, already proven knowledge is available, then it can be stored for further use.

Thus the data & knowledge base of RSDM is to be stored. Such kind of knowledge bases could be processed by PCUBE. PCUBE is my AI system for Planning Parallel and concurrent Process systems - P^3, that I have been developing from the eighties [Szenes, 1987]. PCUBE details will be given later.

One of the interesting features of PCUBE was, that besides ideas taken from best practice methodologies, the experience of previous users could also be stored in its knowledge base, helping this way its new user, even without any kind of automatic processing. Examples will show here, too, that the stored information can be used without pre-planned processing methods just as well, if the knowledge base is not too big.

Thus every expert can be invited to enjoy the benefits of this PCUBE-SEC collection, and to share his / her knowledge here, with others. The PCUBE-SEC way to support the "publication" of such "receipts" will be seen later. This will be one of the novelties in the methodology.

The database is advised to contain at least:

- external experts' knowledge on
  - threats,
  - such activities, that improve situations,
  - etc.
- internal information on the given situation, including

organizational - IT - operational dependencies

- descriptions of business / operational processes using the mutual relationships of
  - requirements
  - tasks / activities
  - organizational units
  - actors / roles
  - information - data
- descriptions of requirements using the mutual relationships between
  - specifications
  - organizational units
  - rulebooks
- any other factors of interest

as it had already been described in [Szenes, 2002, risk].

An important extension of the old RSDM will be here the aspects, provided by the pillars, that can be used for ordering knowledge and its processing. Using the pillars this way had first been introduced for IT case in [Szenes, 2010, GRC], and now this method is extended to operational pillars. This is an important PCUBE-SEC contribution to my former risk processing practice, as it can be used as *classification aspect*, both for the assets, and for the ways of their handling.

Using all these, an experienced systems analyst will be able to conduct a relevant goal & risk assessment, especially, when readily applicable ways will be suggested on executing strategy-driven goal & risk processing tasks. Useful receipts can be, for example, such preprocessed auxiliaries, that are ready to use, and had already been used in similar situations, e.g. questionnaires, or matrices for collecting information. The source of these auxiliaries can be either best practice methods, or former experiences.

Collecting information in the form of questionnaires or matrices have a considerable past in the practice of systems analysis. Answering the former the interviewee is able to speak his / her mind. This is important, when the analyst wants to fish out such information, that is not bound to already known facts. People usually think more freely, when they are not led by prearranged forms. Collecting complaints or suggestions this approach can be very useful.

The matrices serve directed questions. Example can be such a situation, that is shown by the quite complex, but easily to be understood diagram of Figure 1.

This had first been published in [Szenes, 2002, risk], as an example for the step 1 of RSDM, as a process – operation / organization matrix, with IT support information. Such matrices can be used very well, among others, in the risk assessment phase of a business continuity plan, or tailoring an identity management system to a given organization.

who what	role 1 - dept. 1	role 2 - dept. 2
activity 1	system 11	system 12
activity 2	system 21	system 22

Figure 1. Process - operation / organization - IT support matrix

4.5.2 Regularly executed management tasks

4.5.2.1 Assessing the advantageous / disadvantageous current facts

II. Second part - ASSESSMENT

II./1 Identifying the guidelines and targets of the current review

The review is one of the "triggers" of the current risk assessment procedure. Such a trigger can be such a government directive, that companies of different economical branches have to obey, and prescribes a periodical risk assessment. For example, financial institutions in Hungary are obliged to repeat it every year.

Another important reason might be a plan to accomplish a significant change in the technical, or in the organizational pillar. Before administering, and then completing this change by the adequate series of operations, that are finished e.g. by writing procedural rulebooks, the possible risks associated with the planned change have to be identified.

Thus the first task is to describe the trigger thoroughly, and to derive from it the actual guidelines to be followed.

II./2 Identification of the scope of the strategy-driven goal & risk management

The target and the guidelines have to identify, together, *where is the place* of the current review in the "company life". This means, that the first step is to find those business and operational processes, that will have the highest priority in the current strategy-driven goal & risk processing cycle.

This choice will probably depend on the currently valid *strategic issue*s, too.

All these belong to the responsibility and tasks of the Risk Management Committee, established above.

The whole committee has to agree in this issue. Then those assets are to be identified, that are the most important for these processes, with the help of the owners of these processes. The assets chosen at this phase will constitute the subject of this strategy-driven goal & risk processing cycle. First those risks have to be assessed, that can be connected to these assets.

To illustrate the advantages of my asset risk definition in the everyday practice, we remind those, who have already participated in risk evaluation, and had to work with the results afterwards, that to know the *relation* between those risk values, that characterize the individual assets, would have made their work much more comfortable.

Had the risk assessment team got some individual values assigned to individual assets, they could have very quicky converted this information into comparisons. These comparisons are very valuable, as they determine the "share" of the assets from the common, usually limited resource pool. Limited, because the "size" of this pool of improving activities, materials, human resources, etc., is always predefined by the management, and very good arguments have to be presented to ask for more. That is why those, who are responsible for the strategy, have to be induced somehow to *compare* the importance of the assets to each other.

Thus, when those business- and operational processes, that are to be handled in the current phase, are identified, then *"their" assets* are to be *classified* by their users. They know the best, how long would they be able to work without them. The users to be questioned are those members of the staff, who are responsible for that operation, in which the given asset has an important role. This user is either the head of the business or operations or supporting area, or his / her boss delegated this responsibility to him / her.

It can happen, that more, than one process, so more, than one responsible user needs the same asset. The first problem is to identify the business area that needs the asset *the most:* As a refinement of the results gained this way, the users themselves will also have to be classified according to the strategic importance of their tasks. This classification has to determine the share of the assets from the resource pool. Another solution could be first to prioritize the processes according to their strategic importance, and have then the assets inherit these priorities, but, in this case, the possibility to give those assets a better priority, that are important for one process, and not so important for another, might be lost. The Risk Management Committe has to choose, which way is to be followed in such a case.

In the special case of IT risk processing, or strategy-driven goal and risk processing, from the priorities of the processes such a classification of the process supporting applications can be derived, that will show, which one of them are worth to be taken into consideration, and what "mark of importance" can be given to them, compared to the other chosen ones.

In the above described formula

risk (asset, goal) ~ distance (asset, goal) *
probability (asset, goal, attack) *
vulnerability (asset, goal, effort)

now we have the first factor of the asset risk, the strategic / business value. We have already described the hypotheses on the relations between these probability, vulnerability, and the effort spent - worth to be spent - on the maintenance of the asset.

As we have already mentioned, other considerations can become also important. The vulnerability, e.g., might even depend on the history of the procurement of the asset - how much care was taken to choose it, for example, but might also depend on the type of its components, too. Based on such informations, revisiting the three factors might facilitate a more exact estimation of the probability of the occurence of undesired events, which is a benefit of this PCUBE-SEC approach, as this way of thinking helps us estimating the probabilities of an attack.

Besides intentional attacks other undesired events can also take place, but the possible damage, the level of threatening the continuity of business, caused by such incidents, again depends on the level of maintenance.

An important benefit of my approach can be seen at this point. The business and operations users, who are not computer experts, and do not intend to become one for the sake of strategy-driven goal & risk processing, will answer much more readily to questions on

required availability values and features related to those assets, that they use in their work, than to such questions, that require them to estimate such kind of probabilities, that seems to be totally out of their scope. As for availability is concerned, besides the advantage of getting exact values, that we can use in the business or operations continuity planning, we will get to know those relations, that determine, which asset has advantage over another.

This way I transformed the information to be collected from technical type to such, that are of business, or of operational nature, depending on the speciality of the end-user.

Due to the already mentioned novelty of the three factors of our asset risk definition, a more sophisticated, composite weighting is available. This can be very useful in communicating with the top management. The possibility of the classification of the business processes to which the assets "belong", had already been mentioned. There is a further classification possibility, that is able to reflect the weights of other aspects, too.

As instead of individual values we express the value of the assets in terms of relations, these relations "offer" themselves to be weighted even further, according to different characteristics, that describe the required compliance level to, for example, such excellence criteria, that the "owner" of the process - the owner of the asset thinks to be relevant in his "business case". This can be called as a business case in the case of any kind of operational process, just as well. My advice is to use the excellence criteria, but other aspects can be used just as well.

4.5.2.2 Strategy-driven goal and risk processing

III. Third part - PROCESSING

III./1 Collection of requirements

To the targets, guidelines, and priorities of the current strategy-driven goal & risk processing cycle, the Risk Management Committee has to determine those requirements, that are to be applied this time.

The owners of the processes have to mark those goals, that they think to be relevant. As it will be seen, PCUBE-SEC gives practical advice to choose goals. These are the so-called excellence criteria, that describe predefined excellence requirements. The criteria are practical goals, but any other kind of requirements can also be defined.

It is worth to assign weights to the desired level of the satisfaction of the goals.

The requirements of identifying goals, and then classifying them, support the management *to explore,* and also *to evaluate*, *those points* of the business and operations structure, that are *to be improved*, for the sake of fulfilling strategic goals.

For identifying those *assets*, that are relevant in achieving the goals, and the most sensitive possible weak points, taking the current strategic issues into consideration, the owner of the relevant process is responsible. Systems analysts' methods are able to find the relevant asset - goal - business process relations.

This is how the tasks can be found, that are to be executed. Taking all the above considerations on weights and priorities into consideration, the Risk Management Committee will be able to decide, based on the expected *identified* result, if the tasks are worth to be executed, ot not.

A great number of other information can, and have to be also collected. Using the three pillars for classification it is easier to ensure, that neither information nor its sources will be forgotten. The staff to be interviewed, the assets to be characterized, belong to at least one of the pillars, together, even, with the parameters of the assets.

For example, the records of the working time belong to the organizational pillar, so HR is to be questioned, if these records are to serve discipline. However, other organizational units might also be involved. If IT helps to match these records to the also logged failed login attempts, then these records are technical assets, working with them is a technical task, and the results have to be forwarded to information- and physical security, supporting reconnassaince, by tracking illegal behaviour. This shows the variety of pillars in the case of the same asset, and a variety from the viewpoint of the actors.

For logging and analyzing access to operating systems or to applications, always such tools are to be chosen, that serve the strategy of the firm the best possible way. From this strategy has to be derived those practical-level regulations, that determine the weight of consequences, should any trace of non-regular behaviour be found. This involves the regulational pillar.

It must be noted here, that in the PCUBE-SEC knowledge base some practical advice might be found in the form of those lower-level, or, in other words, more practical objectives, that, in the end lead to the fulfillment of strategic-level goals ("lead" means here, that they

are necessary conditions to the achievement of strategic - level goals). The information of a frequently maintained knowledge base can come handy even for the next step, for identifying inproving actions, just as well.

III./2 Identifying improving actions - determining the strategy-driven goal and risk management processes

Now, as a result of the previous RSDM steps, we have the list of those business / operational processes, that are currently most important, together with the assets, that these processes need the most, with the organizational units, responsible for these processes, and the requirements, that these assets have to fulfill, in order to serve "their" processes best, in fulfilling the already identified strategic goals.

This is the point, where the to-do lists are to be prepared by the groups, that are to be formed to handle the individual business processes. The head of the group will be the employee, who is responsible for the given business / operational process, the members are those, who have tasks "with the assets of the process". The group has to implement the derived requirements.

Using PCUBE, for deriving concrete activities from general-level operations, examples, taken from one of my lectures on risk management, can be described in the following way [Szenes, 2002, risk]:

adequate_operation:
 organized_operation - transparent_operation - effective_IS_support .

This is to be read as:
the conditions of "adequate_operation" are standing after the colon (":").
The conditions are separated by the minus sign ("-").
The end of the list of conditions is denoted by a dot (".").

As it will be seen, this is a statement from the PCUBE-SEC knowledge base that expresses the necessity of operating in an organized, transparent way, and the necessity of an effective IT support, if we want to operate in an adequate way. Of course, organized_operation, and the rest should also be explained, e.g.:
effective_IS_support:
  centralized_support_and_maintenance - helpdesk

- centralized_licence_management_and_download.

Another statements on this "adequate_operation" might also appear in the knowledge base.

It is necessary to emphasize again, that the knowledge base contains necessary conditons, but will never provide for sufficiency. PCUBE-SEC can not ensure "adequate_operation", as always new requirements might arise. However, its advice take us closer to it.

The technics behind these "knowledge base statements" will be explained later.

III./3 Advice on the execution of the strategy-driven goal and risk management processes

We are still in the strategy-driven goal & operational risk management part of the processing. The task in this phase is the planning of the improving actions, comprising those processes, that will improve the individual business / operational processes.

During this planning such excellence criteria, as, e.g. the efficiency can again be taken into consideration. To efficiency belongs. among others, the requirement of cost / effectivity. Taking this into consideration, some of the risks might be accepted, as handling them would have been too expensive, taking the expected benefits into consideration. Risk acceptance has to be documented, the excellence criteria "order" has always to be fulfilled. Documentation will be defined as a part of order, as it will be seen.

When everybody thinks, that those criteria will be satisfied - excellence or other criteria - that the working group defined, then the planned steps are to be executed, *if they are worth the effort.* For example, some estimations on the related cost factors can also be given. The hypotheses supporting the risk assessment phase of the PCUBE-SEC strategy-driven goal & operational risk management can be expressed by the following formulae.

We have to note again,
that unexpected problems might arise any time, thus we can not aim at any kind of completeness.
The formulae appearing here are based on practical experience, together with the restrictions below.

cost (achievement (goal_x)) ≥

$$\sum_{i=1}^{n}\sum_{j=1}^{m}\sum_{k=1}^{o}\sum_{f=1}^{3}\sum_{g=1}^{3}\text{cost}\,(g_i, a_j, e_k, p\_d_f, p\_r_g)$$

where:

cost (achievement (goal_x)) means the cost of achieving goal goal_x

g_i : subgoals, that contribute to the fulfillment of the goal goal_x
a_j: assets, *necessary* to the fulfillment of goal g_i, j=1, ... m
e_k: staff efforts, related to a_j, k=1, ...o

p_d_f : pillar domain of effort e_k f=1, ...3
(the domain of the activity comprising the effort)
p_r_g : pillar range of effort e_k g=1, ...3
(the range of the activity comprising the effort, that is the activity affects something in pillar p_d_g).

Restrictions concerning validity:
The benefit of achieving goal_x should, of course, be also taken into account.
If this can be expressed by concrete values, and if it is less, then this lower limit estimated above, then it might be worth to delete goal_x from those, that the company wants to reach.

To evaluate the individual cost (g_i, a_j, e_k, p_d_f, p_r_g,) might be worth if the dependence of some of the individual goals on each other is to be taken into consideration.

III./4 Investigation of the effect of the performed steps

This means, that the groups, who made the plans, have to check, what happened to the requirements, are they now satisfied? Then the conclusions have to be drawn. It is worth to formulate that part of the experience, that may come handy in the knowledge base for the next strategy-driven goal & operational risk management cycle, or perhaps for another strategy-driven goal & operational risk management effort.

Having documented the results and conclusions, the management groups might prescribe new activities, belonging to different pillars of operations.

IV. Fourth part - Scheduling the NEXT review

According to the compliance requirement (also an excellence criterium), the date of the next review has to be determined. Of course, in the case of a change in the organizational pillars, this date can, and has to be modified.

Now the cycle goes back to the Initialization phase, to check, if the strategic choices made there are still all right, or not. Then the next regularly executed strategy-driven goal & operational risk management cycle can begin.

5. CRITERIA OF EXCELLENCE

The fulfillment of the requirements of the PCUBE-SEC excellence criteria help shaping operations & management towards the here earlier defined PCUBE-SEC style of enterprise governance, by *suggesting* such operational and management practice, that serve the strategic goals of the company.

Some of these criteria are new, others are a kind of generalization of the COBIT information criteria. Three of these COBIT information criteria - availability, confidentiality and integrity of the data in IT systems - are ISO requirements, too.

It must be noted, that methodology PCUBE-SEC, and its way of program execution allows the user to redefine every PCUBE-SEC advice, this criteria, too, according to his / her needs. These users' definitions will overwrite the built-in ones in the users' world description.

The base of the following proposals is taken partly from the information security - IT audit best practice, and partly from my working experience, drawing enterprise governance and information security - IT audit nearer to each other. The COBIT information criteria have already been proved useful many times in setting the direction to improve corporate IT [COBIT]. The target of the PCUBE-SEC excellence criteria is the whole corporate operations arena, generalizing a *basically information security - IT audit best practice towards operations*.

IT is only one of the auxiliary operational activity areas, but there are a lot of others, too, finance, controlling, logistics, HR, etc. Every one of these has to support corporate operations. Enterprise strategy focuses on the business processes, these other areas are "only auxiliary" from strategical viewpoint.

Another *novelty* is, that the definitions of my excellence criteria support the differentiation between goals, and the means to achieve them. One of the examples can be my compliance criterium, and the way it handles the legal world.

Presently I have two groups of the criteria: one serves operational excellence, and the other contributes to the asset handling excellence [Szenes, 2012, MM].

Criteria characterizing *excellent* operations are: effectivity, efficiency, compliance, reliability, strategy-driven goal & operational risk management excellence, functionality,

and order. The first four have the same name, as their COBIT predecessors, but their activity scope have been generalized from IT to the whole operations arena. The importance of both functionality, and that of order, I had already identified in 2010 [Szenes, 2010, GRC], but their meaning have been considerably changed from then. Quite a lot of conditions required by the present strategy-driven goal & operational risk management excellence has already been available in 2002 [Szenes, 2002, risk], but I decided to include these new aspects of risk management into the list of my excellence criteria only in 2012 [Szenes, 2012, MM].

The old ISO/IEC requirements, availability, confidentiality and integrity, belong, at the same time, to the longer list of in the COBIT information criteria. These I generalized to *asset handling excellence criteria*, taking, as a base, their COBIT interpretation. The special importance of the asset risk has already been emphasized in [Szenes, 2002, risk], but this "asset risk" name I introduced only in 2012 [Szenes, 2012, MM].

5.1 Excellence criteria without predecessors

5.1.1 Strategy-driven goal & operational risk management excellence

From the special, positive approach of PCUBE-SEC, that focuses to the fulfillment of strategic goals instead of problem mitigation follows that this kind of "risk management" is fundamental in enterprise governance, and, vice versa, at the same time, this risk management is based on the corporate strategy.

One of the consequences is, that this risk management is closely dependent on the strategy of the enterprise. This is reflected in the PCUBE-SEC asset risk definition, decribed in the risk management section, giving a qualitative comparison facility, according to the strategic importance of the asset [Szenes, 2009, risk].

The other direction can be illustrated by choosing the actual *targets* of this risk management *according to* the actual *strategic goals*. E.g. data confidentiality is important, when important interest of the customers, for example their property is bound to it, like in the banking sector.

As already such a seemingly special framework, as that of the IT security framework of a corporate, strongly depends on the corporate strategy, the broader security management, the management of the operational risks also has to be based on the strategy of the company. A

possible solution has been shown in a lecture at an ISACA conference [Szenes, 2002, risk], and had been detailed in a book chapter [Szenes, 2009, risk].

5.1.2 Functionality

As an excellence criterium, functionality can not be defined by itself, without binding it to something, that it characterizes. However, I can determine, when I consider the *functionality of something* to be adequate.

In 2010 I had defined the adequacy of the *functionality* of an IT product, as the level of support, that it gives to the business processes. As a special case, the functionality of an application system can be considered to be as good, as the business support it offers [Szenes, 2010, GRC].

Even if, at the first glance, this requirement does not seem to be related to the fulfillment of the users' requirements, its practical fulfillment involves a strong relation between the two.

In the design phase of an application, the systems analysts have (at least) two problems to solve. One is to ensure, that the new system supports the business goals to be served *by just that* business *process*, that is to be supported by the application. Should it be not the case, then at first the related operational process has to be reorganized, but this does not belong to our present subject.

Other problem to be solved is, to understand the users' needs, and to align to them the applications system, both from functional, and algorithmic point of view. This has to be started already at the planning phase. The otherwise best application is able to fail, if these needs are not taken into consideration. Thus these two issues: serving company strategy, and doing it in such a way, that is acceptable to the business users, are not at all independent from each other. Involving the business users into every phase of the development is a must to solve this problem.

My proposal for the IT case:
The *functionality of the information system* of a company is *adequate*, if it serves the staff in such a way, that they can fulfill their job requirements in the best possible way. This "best" means compliance to given goals defined by the PCUBE-SEC user [Szenes, 2011, Hack.]

Note: This means, that besides supporting the user of the application - actually the user, who is the owner of the application - I intentionally require the provision of support for any other *involved* staff members.

Two notions are used here, that might need to be clarified, the information system of a company, and the staff. I suggest to use here the following interpretations.

The information system of a company, or, in other words,
enterprise information system
comprises, besides its computer-based part, a - preferably determined - way of any kind of information from its provider to its receiver, the underlying processes, and the activities concerning information maintenance, that should, of course, be an organized process, not an accidental one.

To the *staff* belongs every employee, from the top of the company hierarchy to the bottom, from the top management to the lowest level.

It should be noted, that this criterium is also dependent from most of the others. The reason probably is, what my experience has also proven: proper operations can not be maintained without the proper functionality of the results of every activity.

Thus it is worth to *extend the scop*e of this criterium towards the evaluation of the results of the activity of the whole staff, that is, towards operations.

The *functionality* of an *operation* is said to be *as adequate*,
as the strategic support is, that it offers to the staff.

As a consequence, every member of the staff, from the top of the hierarchy to the bottom, taking them either individually, or by organizational units, has to serve the business goals, should *they* function well.

Note:
All this - processes, requirements, their fulfillment, etc. - has to be *documented*, otherwise no evaluation is possible.

5.1.3 Order

With this we arrived to another excellence criterium: this is the *order*. This is also an extension of one of my formerly defined excellence criteria, namely *documentation,* or rather, documentation is one of its very much necessary conditions [Szenes, 2010, GRC].

Just as in the case of functionality, order, as an excellence criterium, can also not be defined by itself, but I can determine, when I *consider the order of something* to be *adequate*.

Let us begin with the generalization of *"documentation"*. My proposal for it had been in 2011:
"Every activity should be preliminarily planned, and documented at every phase of its lifecycle. The phases are those parts of the lifecycle, that are separated from each other by concrete deliveries, as milestones" [Szenes, 2011, Hack.].

This can also be considered to be the requirement of *adequate documentation of operations*. So let us accept it for this scope, too.

A six years long research of Melancon, described in the journal of ISACA proved, that some of those characteristics, that I take to be components of criterium "order", e.g. change management and configuration management, taking them with a scope restricted to IT, have been proved to contribute considerably to the *market success of the corporates* [Melancon, 2007].

Thus it seemed to be worth to extend documentation, which can greatly contribute to the effort of setting things right in an institution, towards a more general, composite "order" requirement, for which the above "operational" documentation is "only" a special case, or a component. I chose "order" to be this composite excellence criterium. Quite a lot of important criteria can be considered as one of its components, besides "documentation", e.g. business continuity management - BCM - and incident management. This latter is not at all independent from change management.

BCM is a composite criterium by itself, containing, e.g., regular, or, preferably, continuous monitoring of the state of the assets, and the processing of the results by the means of an incident management tool, that has to have other capabilities, and so on.

IT documentation has also special cases, or, in other words, components, for example change management, release management, and configuration management. Melancon

found, that the benefit of the improving activities also complies with the Pareto Principle, 20 percent of the activities provide for the 80 of the benefits, and among these activities IT configuration management and IT change management had outstanding positions.

The *generalization of change management* from IT to operations is trivial, the followings are to be registered in both cases:

- the subject, the current version number of the change, if the latter can be interpreted for the case,
- the date of the submission of the change issue, and
- the date, from which it is effective,
- the requestor's name, role, place in the organizational hierarchy,
- the same information about the executor,
- the place of the change in the thing to be changed, if this can be interpreted for the case,
- the reason, and the contents of the change request,
- the permitter's name, role, place in the organizational hierarchy,
- the acknowledger's name, role, place in the organizational hierarchy,

Configuration management, if it is at all introduced in the procedures of an institution, is restricted to the IT infrastructure, at least I have not seen it to be used for any other kind of assets. To have the staff keep configuration management alive is already a very difficult task, as to use the automatisms, if any such lightening is at all available, is usually uncomfortable, so this requirement meets the resistance of the systems engineers, who have to feed the data into the inventory. Unfortunately, configuration can not at all be managed without a precise, up-to-date inventory, no matter, what kind of things belong to the actual configuration.

To generalize the so-called IT resources of COBIT 4.1, that are application, information, infrastructure, and people, would be a natural way for us to follow, in generalizing the scope of configuration management from IT infrastructure towards operations. Following this line, I extend my scope from IT towards operations with the *management of HR, material, and immaterial resources*. To HR management belongs, in my interpretation, shaping organizational structures to business goals, and training, too.

The management of the assets satisfying my asset handling excellence criteria to be introduced here, can be considered as a special case of this generalization.

My goal had been to align the definition of order to the market success, but, at the same time, I wanted my "order" notion to comply with the everyday meaning of the word "order" [Szenes, 2012, MM].

The operations of an institution goes in so-called "order" - or, in other words,
the *order of operations is* called to be *adequate*, if
top management takes up the responsibility for the well-being of the institution. This involves, from the one hand, the determination of the strategy, aligning it to the market success, and its continuous maintenance, and, from the other hand, to have the firm fulfill the strategic goals.

Note 1:
To achieve success on the market is needed, at least, the followings:

- the identification of both the business goals and those requirements of the social and natural environment, that have to be fulfilled,
- the periodic update of the strategy,
- the provision for those institutional conditions, that serve the fulfillment of these goals and requirements.

Note 2:
Any of these tasks can be delegated to subordinates, but the responsibility stays at the top.

Note 3:
Every idea described here is intended for use for any kind of institutions. It can be either private enterprise, or any kind of organizations of the governmental sector, just as well. The market success of this sector depends on the satisfaction of the citizens besides preserving the fulfillment of such excellence criteria, e.g., that are introduced here. Another excellence criterium, cost / effectivity, for example, is a frequent requirement in government administration.

Note 4:
Provisioning for the institutional conditions involves preparing guidelines, choosing best practice to be followed, having organizational structure created, having procedural rulebooks be written according to these, etc.

Note 5:
However, I do not want to pretend to have enumerated all of the tasks to be done in order to achieve market success, nor do I think this to be possible.

With order, and its components, we have numerous examples for the dependence of the excellence criteria on each other. One of them can belong either to the scope or to the range of an other.

The scope of documentation - that belongs to criterium "order" - preferably has intersection with *every* other criteria - it should be obligatory to document the level of their fulfillment.

Business continuity management, change management, and incident handling have also trivial connections, e.g. the first is impossible without the other two.

Another example can be the relation between strategy-driven goal and risk management excellence, and more or less every other excellence criterium. For years now, in the everyday life of information security departments, *one of the most important goals of risk management* has always been *a special case* of the proposals discussed here. *This goal is to ensure* (to a reasonable extent, of course), *the fulfillment of just those the criteria, but restricted to IT scope only, that I generalized to asset handling excellence criteria, the availability, integrity, and confidentiality.* These three requirements have always been in the focus of the different best practice methods, even if my suggested criteria seem to be just as important, as they are, illustrating, hopefully, the significance of my extensions and generalizations.

5.2 Excellence criteria with predecessors

5.2.1 Predecessors

In the 1998 version of COBIT, ISACA suggested seven criteria to be satisfied by the company informations, that are handled in their IT systems, in order to serve the business goals. Their fulfillment is to support business requirements. These criteria remained almost the same till COBIT 4.1 in 2007. Two words were added to the definition of "availability", and "reliability" was changed a little bit. The extensions proposed here do not mean any kind of obsolescence. The COBIT criteria are still adequate, and they are very useful in qualifying the performance of IT - IT security - IT audit area, their responsibilities, and their business relations.

I think, that one of the predecessor ideas of the COBIT criteria could have been the COSO requirements. Abbreviation COSO stands for the of the Committee of Sponsoring Organizations of the Threadway Commission. They laid down the preconditions of fiduciary financial reporting. This Committee was founded in 1985, to support the National

Commission on Fraudulent Financial Reporting. As it has always been usual in the USA, the National Commission was named after his first chairman, James C. Treadway, Jr.

"COSO's mission is to provide thought leadership through the development of comprehensive frameworks and guidance on enterprise risk management, internal control and fraud deterrence designed to improve organizational performance and governance and to reduce the extent of fraud in organizations"
(cited from: www.coso.org).

COSO was founded by AICPA (American Institute of Certified Public Accountants), AAA (American Accounting Association), FEI (Financial Executives International), IIA (Institute of Internal Auditors), and IMA (Institute of Management Accountants).

According to COSO, internal control bodies have to ensure:

- effectiveness and efficiency of operations
- reliability of financial reporting
- compliance to the applicable laws and regulations.

This might have affected ISACA, as from the oldest materials almost till now this is repeated, usually as fiduciary requirements. Only the meaning of the word is changing a little bit. While, omitting the "applicable", this had exactly been the definition of "fiduciary" in 1998 COBIT, in CRM explains it as compliance and reliability, describing its IT audit and assurance standards framework [COBIT 1998, CRM 2011, 2012].

The COBIT information criteria till COBIT 4.1 are:

- effectiveness
- efficiency
- confidentiality
- integrity
- availability
- compliance
- reliability of information

In the followings these criteria will be extended beyond IT. We have criteria with predecessors from both of my groups: some of the COBIT information criteria had been extended to characterize operational excellence, while others describe asset handling excellence.

Describing these extended groups, the copies of the criteria interpretations taken from COBIT 4.1 will be cited between quotes, my new, hopefully improved versions are marked by the word "proposal".

In 2011 have these proposals been first introduced, for the special case of information processing [Szenes, 2011, Hack.].

5.2.2 New excellence criteria

Besides assigning a wider domain to the criteria, the advantage of my extensions is the clarification of the difference between subject, and operation on this subject.

In the COBIT definition of effectiveness, for example, binding the requirements more or less to the information, and to the quality of the provisioning process, seems a bit accidental. I think, that the target of the definitions should always explicitly be provisioning, as just this is the activity to be improved. This is the reason of shifting here the weight from the result of an action to the action itself, aiming at the excellence of operations, at the excellence of the so-called operational activities.

The notion of operational activity I will define in a succeeding chapter. The informal understanding of its meaning is more, than enough here.

5.2.2.1 Operational effectiveness

"*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." [COBIT 4.1]

My proposal for the IT case:
The information is *effective*, if
its correctness, relevancy and pertinency to the subject *is based on proofs acceptable to the customer* of the information, that is to those, who get it to use it, and it is delivered just at the point of time that was *agreed* upon by both parties, customer and supplier. [Szenes, 2011, Hack.]

Notes on the differences between the two definitions above:
The business area frequently plays the customers' role, but if we want to embrace the whole scope of enterprise operations, then the whole staff is affected. Employee of such auxiliary

areas, as human resource, security, or even IT itself, have also to be taken into consideration, for example.

An information is acceptable to its customer only if he / she agrees with its contents. This should involve agreement with the way of its production, too. The discussions between developer and end-user should start from this point. This emphasizes the necessity of the presence of systems analysis throughout the process of application systems development, from the beginning to the end of the life-cycle of the application system, as I had already pointed out discussing the security problems of a special, but even now very fashionable type of application, such an application, which is based on a service oriented architecture [Szenes, 2007, SOA].

My proposal for describing effective operations:
An operational activity is *effective*,
if its result(s) complies with the pre-planned requirements, that had been accepted by every relevant party.

Note:
Restricting this definition to IT, as special activities, we get back a more general set of requirements, than my original list of the above IT requirements.

This operational effectivity definition emphasizes two important phases: planning, and arriving to an agreement. This implies the requirement of the best effort in serving corporate strategy, if top management performs its duty, described in other criteria, too, e.g. in the strategy-driven goal & operational risk management excellence.

5.2.2.2 Operational efficiency

"*Efficiency* concerns the provision of information through the optimal (most productive and economical) use of resources." [COBIT 4.1]

My proposal for the IT case:
The information is efficient, if it is provided in a *pre-planned*, documented, and cost/ effective way, concerning the optimal use of human and material resources, and the way of problem solving. [Szenes, 2011, Hack.]

Notes on the differences between the two definitions above:

Here, and in the case of the other criteria just as well, emphasizing *preliminary* planning harmonizes with the intention of *setting the direction of the improvement*, before committing resources in vain, before running idle.

Even if documentation was said to "belong" to another criterium, its necessity must explicitly be emphasized here, too, otherwise it would be very difficult to judge the fulfillment of the other part of this definition.

The way of problem solving is also a new aspect. If this is not transparent, then to identify tha cause of the possible mistakes would really be difficult.

The IT case can be rewritten without any significant changes, to more general operations, too.

My proposal for describing efficient operations:
An operational activity is *efficient,*
if it is performed in a *pre-planned*, documented, and cost/ effective way, concerning the optimal use of human and material resources, and the way of problem solving.

5.2.2.3 Operational compliance

"*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." [COBIT 4.1]

My proposal for the IT case:
A company handles information in a compliant way, or, *shortly*, a company complies with the compliance criterium, if it complies, in a *documented* way, to any requirement of those authorities that have *authority* to regulate any aspect of the activities of the company.

To emphasize the necessity of documentation is very important again, so that providing for the proof of the adequate behaviour will not be forgotten. [Szenes, 2011, Hack.]

Notes on the differences between the two definitions above:
According to my practice, compliance might affect matters outside the scope of the business activity. There is a wide range of requestors available: different supervisory authorities supervising the given type of business, commissaries from government administration, or from mother companies, etc.

It is true, that if a company wants to stay in business, then it has to obey everybody, who has the power to give orders. Thus compliance can usually be considered to be a business goal. However, there are matters to be handled, that do not serve the interest of a given company, but are advantageous to its owner. Thus the COBIT requirements are a subset of mine.

Taking all these into consideration, the extended definition, that of operational compliance does not require too many replacements in my IT definition.

My proposal for describing operational compliance:
A company *operates* in a compliant way, or, *shortly*, the operations of a company complies with the compliance criterium, if it complies, in a *documented* way, to any requirement of those authorities that *have authority* to regulate any aspect of the activities of the company.

It will be seen, that in some traditional approaches, the goal to satisfy legal *aspects* will be mixed with that kind of activity, when a company uses legal *means*. Thus it is important to note here, that in PCUBE-SEC, to comply to the legal aspects, is a special case of the compliance defined the way above.

"Legal" area is quite often is considered - faultily - to be only a tool in achieving something else. In real life compliance to *different legal systems* is also a *business goal-related* criterium, this is why in PCUBE-SEC the "legal" aspect belongs to the compliance *criterium*.

5.2.2.4 Operational reliability

"*Reliability* relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities." [COBIT 4.1]

My proposal for the IT case:
An information system of a company is *reliable*,
if the information processing is organized in such a way, that it provides for the *preliminary agreed* data in such a manner, that supports the work of the *staff* according to the *best professional practice*. [Szenes, 2011, Hack.]

Notes on the differences between the two definitions above:

The proposed definition is stronger, than the COBIT one, from two viewpoints. The first is, that I set a quality level for the whole information system, *including* its built-in relations. The other viewpoint is, that the "customer" of the information can not be restricted to the management. Every member of the staff needs this kind of reliable support.

To require the fulfillment of a preliminary agreement involves to have a relevant agreement, by setting the direction of the improvement. It should be fixed at the planning phase of the information flow already, and then this direction is to be followed by the planning of the application system according to the also already determined invented information flow.

I think, that these details show a possible way to extend the scope from IT towards operations. This reliability criterium is certainly able to ensure a more organized way of operations.

Thus, generalizing the customer of information to customer of services my IT case can be extended to operations with really only few replacements of the involved parties.

My proposal for describing reliable operations:
The *operations* of a company is *reliable*,
if it is organized in such a way, that it provides for the *preliminary agreed* service(s) in such a manner, that supports the work of the staff according to the *best professional practice*.

5.2.3 Asset handling excellence criteria

The informal use of the notion "asset" is intentional throughout the whole discussion. Asset risk has been defined, and it dealt with such possible attributes of an asset, as its strategic / business value, or its vulnerablity, for example. In this dissertation we take asset, as an already existing resource / property of the institution, or as such a resource / property, that is "under construction".

I do not think, that we would need any punctuation, or further clarification here, as the suggested improving ideas are completely understandable without dwelling on defining asset some pages long.

Using "asset" this way, information is a special asset. Usually, no matter, how important is to provide for information, this is not the only product, this is not the only marketable result

of corporate operations. Thus it is worth to investigate, if the asset handling excellence criteria have at all meaning beyond the scope of information?

Confidentiality, I think, could only be formally extended to other kind of assets, as always the information on the product, or on any kind of asset is the thing, it seems, which is to be handled confidentially.

However, generalized integrity, generalized availability seem to be able to "live" in the real life, too.

5.2.3.1 Confidentiality

"Confidentiality concerns the protection of sensitive information from unauthorised disclosure." [COBIT 4.1]

My proposal for the IT case:
The information is *confidentially handled*,
if those, and only those have *access* to it, who have job to do with it. [Szenes, 2011, Hack.]

Notes on the differences between the two definitions above:
"My" confidentiality - instead of being just a protection requirement - refers to the *overall handling* of the information. I think, that a proper handling of information should require much more, that "simply" protecting it.

As a first step, those employee have to be identified, who have anything to do with a certain information. This involves sizing up, assessing, and classifying the information, then creating organizational roles according to the results, from which the job descriptions can be built, and which will be the base of lots of such important, not only protecting, but order - serving activities, as the identity management, or access right management are, for example.

Thus I have no other *proposal for describing confidential asset handling,*
then handling confidentially every information about it.

This requirement will trigger those conditions, that deal with the assets themselves.

5.2.3.2 Integrity

"Integrity relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations." [COBIT 4.1]

My proposal for the IT case:
The *integrity of the information* is preserved,
if its handling or processing *does not change it inadvertently*. [Szenes, 2011, Hack.]

Notes on the differences between the two definitions above:
To comply with the business' expectations suits better to another criterium, functionality. I think, that both accuracy and completeness relate also to the appropriate functionality of the information system. It can be noted, that both depend greatly on the adequacy of systems analysis.

I prefer to use the everyday meaning of integrity, which is: keeping intact those data, that are not operandi in an operation. This way this important requirement will be independent from the criteria.

Besides, binding this feature explicitly to the processing I hope, that the PCUBE-SEC users will not mix it with confidentiality, which is a frequent mistake.

The generalization is again very simple.
My proposal for describing such an asset handling, that satisfies criterium integrity:
The *integrity of an asset* is said to be preserved,
if its handling or processing *does not change it inadvertently*.

5.2.3.3 Availability

"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." [COBIT 4.1]

Compared to my already published definition [Szenes, 2011, Hack.], I have here a more exact
proposal for the IT case:
Availability of the information means, that
if it concerns a *given matter*,
then

it is available to every *competent* employee, who is competent in this matter,
in a *planned*, *predictable,* and *documented* way
according to the preliminary agreements on its availability.

Note 1:
The agreements can, and - if possible, have to - rule, first of all, to a measurable extent, the predictability of the availability. Other issues to be settled are, for example, the way of access, or the time interval for which the information is available.

Note 2:
This "competence" here above belongs actually to the domain of confidentiality, this is again an example of the dependence of some of the criteria on each other.

Notes on the differences between the two definitions above:
The explicit defense requirement "safeguarding" suits much better to, and is contained in confidentiality.
The importance of the requirements, that I added, are self-explanatory.

Extending availability to operations from information, it is worth to replace "measurable extent" with a set of "qualitative and quantitative prescriptions", that are relevant to the situation. Predictability can not be spared either. The predictions should be as exact and concrete, as possible.

My proposal for describing such an asset handling, that satisfies criterium availability:
Availability of an asset means, that
if it has a role in a *given matter*,
then
it is available to every *competent* employee, who is competent in this matter,
in a *planned*, *predictable,* and *documented* way, according to the preliminary agreements on its accessibility, that have to refer to every *qualitative and quantitative prescription*, that are *relevant* in the matter.

Finishing the description of my proposals, it is important to emphasize again, that the user of PCUBE-SEC can, and is able to redefine every criteria, described above.

6. THE SUCCESSOR OF THE AUDITORS' CONTROL MEASURE: THE PCUBE-SEC OPERATIONAL ACTIVITY

PCUBE-SEC operational activities will be defined here, those activities of the different actors inside and outside the companies - members of the staff, organizational units, external parties, etc. - who contribute to the market success of the company.

Beyond *extending* the traditional "control measures" from IT scope to the whole *operational arena*, an important novelty is affixing *attributes*, that help clarifying the *problem solving* activities by supporting the exploration of the details of the problem to be solved, and even the *identification of possible improvement* activities. The often *negative* traditional approach we *turn to positive*.

Using the importance of the goal of the operational activity, that of the operational objective, we identify the *distance of this operational activity from the enterprise strategy*, providing a useful classification aspect for these activities.

We begin with the predecessors of this notion, discussing their weaknesses, and the possible points of improvement. To these belong the so-called "control" and "action" of the ISO standards, and the so-called "control", "internal control" or "control measure" of the ISACA materials.

First we show the drawbacks, or, sometimes, even *inconsistencies and inaccuracies* of these definitions, then a more granulated view will be proposed, for expressing such actions, that *contribute to the achievement of a desired goal*, to *promote enterprise "wellness"*, or such actions, that *"handle" undesired events*.
Having found the cause of the problem, the user is supported in *drilling into* the information on *consequences*, too, in *documenting* them, using the *attributes* of the operational activities if appropriate, and even perhaps by concrete *receipts*, already proven problem-solving information.

My definitions, in general, support the user in solving the problems by emphasizing such important differences, that can be seen, e.g. in the case of the preventive attitude, between problems caused by a mistake of a staff member, or by an imperfect prescription concerning way of operations, and those inconvenient events, that are caused by intentional attacks, or accidents.

Another benefit of PCUBE-SEC is the *separation* of the scope of the actions from their desired effect, *the "inputs" from the "outputs"*. This is achieved by identifying the domain of the operational activities as the union of the three pillars, so this is the scope, this is the "input pool" here. The output is also well-known, it is a kind of contribution to an operational objective. This separation helps in identifying inconsistencies in the best practice definitions, and helps in extending the scope from IT towards operations.

6.1 The predecessors and their drawbacks

A basic problem of the traditional terminology is *mixing objective and action*, that contributes to its achievement, the already mentioned problem of Professor Guldentops. This is a result of the very frequent mixing of "what" and "how". I am sure, that the incosistent use of the word "control" to both makes it much worse.

Beyond *separating "what" and "how"*, operational objective and operational activity, PCUBE-SEC separates the *domain* of the activity from these, too.

This separation facilitates the solving of Guldentop's problem, the differentiation between action and objective, without omitting the notion of objectives, which is not a good solution, as I have already mentioned.

The capabilities of my operational activity serve as an important illustration of the difference between a traditional, and a PCUBE-SEC definition. I do not try to stuff everything that we want to achieve, into such a definition that has to serve *rather* as a definition of a type, with which we want to work, *than* the setting of some specific goals. *For the goals I have always reserved a distinct place in my research*, and I have taken care of *not mixing the "what" with the "how",* following the basic principle set by the researchers of artificial intelligency [Szenes, 1976-77] .

The *activity*, that is *necessary* to the achievement of a so-called IT "control objective" is often abbreviated, unfortunately, as "control" in the presently available information security - IT audit methodologies. At the same time, "control" itself often means a goal, a goal to be achieved, as an improvement. E.g. CRM 2011 lists "control" among the goals of some arrangements to be added to prototyping, among security, and auditability [CRM 2011].

This way objectives to be achieved and activities that achieve the objectives become synonyms, that is most unfortunate. Sometimes even a controlling system of an organization built to reach or avoid something is also "control" colloquially. For example,

even CRM 2011 splits the management level dimension of decision support systems framework into operational control, management control, and strategic planning [CRM 2011].

Quite naturally, the checking - monitoring activity is "control" everywhere, too.

In the COBIT 5 SME - Subject Matter Expert Group I proposed to correct this negligence in the next version of our valuable methodology. The organizer of the group effort supported me in a mail, we shall see.

I have to note, that the Quality Assurance Team, where I contributed to the refreshment of the CRM for 12 years, should have defined the "control measure" in the CRM Glossary, thus this is my fault just as that of the other members [CRM 1999-2011, 2013].

6.1.1 The ISO control definition

The ISO "control" definition is: "means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be administrative, technical, management, or legal in nature.
NOTE Control is also used as a synonym for safeguard or countermeasure."
[quoted from ISO 27000]
It should be noted, that this definition is the same in the version 2012 of this standard. There are two additional notes added, that are not related to our present discussion.

Beginning the analysis with the contents, both the definition and the note reflect a negative approach, that I will turn to positive by suggesting improvements, that is contribution to the strategy instead of taking only *counter*measures into consideration, that prevent undesirable events. Not even detective, or corrective possibilities are mentioned. However, at other places in the ISO 27000 standard, corrective action turns up abruptly, dealing only with the *cause* of the problem, and *neglecting the consequences*. Detective action is not defined, but the possibility of detecting something undesirable is mentioned. This is simply an example for inaccuracy.

In my present discussion legal compliance, just as other desired criteria, is to be satisfied by organizational, regulational or technical activities. Of course, to satisfy my criteria legal *means* might be useful, too. However, to mix legal means into the definition of an IT control measure is a mistake. Legal tools belong to the toolset available for every

enterprise, but their content is out of our scope, as it belongs to the jurisprudence. The legal tools, and the compliance to the legal requirements have to be separated.

As far, as the *composition* of this ISO definition is concerned, it gives a casual, mixed list of operations and subjects, on which operations can be performed. Structure, and procedural rulebook - if the procedure means this - are subjects, the activities of creating them are operations *on* these subjects. If procedure is practice, then both are materials to be created.

The difference and separation between method, action, and the subject of action is very important in this dissertation. My proposed generalized concept will not be subjected to such classification difficulties.

However, the main problem with this ISO definition is this casual listing of the methods, possible actions, mixed with their subjects.

We will show, that "policy" in the ISO 27000 family can mean both guideline or procedural rulebooks, while, in the everyday practice, it is often a certain security configuration, e.g., that of a firewall. If we do not want misunderstandings, then let us consider guideline as a general directive, while procedural rulebook is to describe the actual practice to be followed. Rules tell us, *how* we are obliged to do something, and *what* are our obligations. Thus the elements of the list "policies, procedures, guidelines, practices" are of quite different types.

On "organizational structure" is meant probably a result of an organizational procedure, e.g. an organizational unit created for a given purpose. However, to define a general type in which the organizational units and policies and others are of the same rank would be difficult and would not be worth the effort, either.

Going back to the problem of "policy", according to the prescriptions of the ISO 27000 family, this word has a double meaning: either guideline, or procedural rulebook. According to the ISO 27000 definition it is closer to a guideline, to a kind of management commitment: "overall intention and direction as formally expressed by management".

However, in ISO 27001, in its chapter 5, dealing with the responsibility of the management, the statement on management commitment is "policy", while in its section 4.2.1, that informs us, what kind of definition framework is necessary to establish an Information Security Management System, ISMS, policies are prescriptions of procedural rulebooks.

Contractual security obligations are here obligatory parts of a "policy". In the note at 4.2.1 b), that explains, that "ISMS policy is considered as a superset of information security policy" the latter "policy" clearly means procedural rulebook.

All these show, why is very important to specify, what does the "policy" under discussion means.

6.1.2 The COSO internal control

One of the most important predecessors of the ISACA "internal control" is probably the internal control of COSO, the Committee of Sponsoring Organisations of the Treadway Commission [COSO].

COSO interprets "internal control" as a process, in which every member of the company staff has to play its role, in order to provide reasonable assurance regarding the achievement of the (COSO) control objectives. Should the process "nature" have been added to this name, e.g., as "internal control process", the mixing of goal and activity to fulfill it could have been avoided.

Setting "control objectives" as goals for this "control" sounds general enough, but the COSO control objectives, besides the effectiveness and efficiency of the operations, and the compliance to laws and regulations focus mostly on the reliability and fiduciary of financial reporting, in order to facilitate the filtering of fraudulent activities.

One of the basic differences in attitude between PCUBE-SEC and the other discussed methodologies can be seen here. The prefix "reasonable" limits the "assurance" enough to let the reader know, that these "internal controls" lead us only as close to perfection, as our investments make it possible. However, there is no answer here to the question, when is an investment reasonable? Everybody knows, of course, or guesses at least, that the most important factor of this reasonability is cost / effectivity.

PCUBE-SEC openly emphasizes the dependence on strategy, and suggests its user some "ready-made" excellence criteria. Among these we have described such a one, too, that is related to cost / effectivity, too, but requires planning and documentation, as using resources optimally is not always enough to be efficient.

6.1.3 The COBIT internal control definition

Quoting the definition of internal control from COBIT:
"The policies, plans and procedures, and organisational structures designed to provide reasonable assurance that business objectives will be achieved and undesired events will be prevented or detected and corrected" [COBIT 4.1].

The tools suggested to improve a situation are partly the same, and just as mixed as those of the ISO definition. Managing risk, that is required in the ISO definition, is necessary to achieve business goals, but this kind of activity consists of a list of countermeasures, while this COBIT definition turns the view towards the positive side, enumerates things that are to give reasonable assurance to the fulfillment of *business* goals. Thus this definition takes us nearer to the success of the corporate, than the ISO version. Replacing the control objectives of the COSO definition by business objectives is also a step towards generalization. One of the problems is, that no reference is made to the possibility of a decomposition of higher level objectives to lower level ones that, if they are not directly fulfilled in our knowledge base, then could be also decomposed, either to already fulfilled goals, or to activities to be executed. Anyhow, this decomposition takes the users nearer to their final goals.

PCUBE-SEC not only permits, but encourages such derivation processes, that lead from more general operational objectives towards lower level ones. Thus already on the level of definitions, it will explicitly refer to the possibility of dealing with lower level objectives instead of higher level ones.

Another problem with the COBIT internal control is, that while regulational and organizational elements are present in it, technics seems to be left out - unless it is hidden in the "procedures".

Trying to find a name for the counterpart of the operational objective, for the improving activities, first I thought of using "measure", following ISACA CRM. Besides measuring the quality or quantity of something, " to measure" quite often means in the book such a kind of activity, or rather, such an arrangement, that serves objectives. An - in this book evergreen - example is the mandatory leave of conspicuous busybodies, who work day and night, and do not easily give information. The auditor wants, of course, to know, what is behind this activity, therefore he / she might prescribe to this colleague to take a vacation, and substitutes him / her for a time. CRM calls this arrangement as "control measure", to prevent fraud.

6.1.4 "Measure" in COBIT

Still, "measure" in COBIT is not an action. Among the many different meanings of the word "measure" COBIT chose the *characterization of the result* of an action - or, sometimes, the measuring activity itself. Quoting from the glossary of COBIT 4.1, "measure" is: "A standard used to evaluate and communicate performance against expected results."

This COBIT measure interpretation is also very useful, weighting the extent of an achievement. A rich set of this kind of measures are suggested there, for evaluating results of IT processes, to measure the level of improvement. For example, to measure the performance of a process very useful metrics and performance indicators are proposed. Besides the evaluation of our IT investments we get help in optimizing these investments, in order to improve the current situation.

6.2 Definition of the PCUBE-SEC operational activity

It will be shown, that switching from the previously analyzed control and control measure notions to this new definition of the improving actions, to this so-called operational activity, some of the drawbacks mentioned above will be removed, and the new approach yields even advantages.

The PCUBE-SEC user will choose, which objective(s) will be served by the actual activity / activities, and how general are the objective(s), that is / are to be served by the given activity / activities. The PCUBE-SEC program will have a goal, an operational objective. As it will be seen, this program describes, with simple and complex "statements", how to contribute to its achievement. The granularity of this description is just as detailed, as it is made possible by the users' knowledge, or by the predefined receipts, that are available.

We try to provide for such guiding principles that can be used to any kind of operational objectives, let them be of strategic level, or very concrete ones. We have to be able to analyze activities dealing with high and low level objectives alike.

When an expert tries to solve a problem, if he / she specifies a general goal, then he / she either finds an activity, or series of activities, that at once satisfies it, or tries to decompose it to lower level goals. This way of thinking, this *way of derivation*, is to be supported by PCUBE-SEC, presently mostly with receipts, but later with some automatisms, too.

The *operational* activity is such an action, that

- *contributes* to the achievement of operational objective(s)
- operates on operational pillar element(s) as subjects.

Note:
The subjects here are meant to be elements of any of the three pillars.

The above definitions of "control", "internal control" are, in a way, special cases of this operational activity. The scope of the ISO definitions is restricted to activities handling risk. This is an important goal, but there are lots of other activities, too, e.g. those, that result in direct improvement of something. of course, the fulfillment of the strategic goals, and that of those goals, that can be derived from the strategic goals, could be reformulated involving risk in a forced way. This will be the risk of not fulfilling the objectives.

The countermeasures enumerated in the COBIT internal control definition do not clearly show, on which pillar they operate, and does not take the technical pillar into consideration, at least not explicitly.

The COSO definition can be interpreted in a general way, but the idea behind it is financial transparence and adequacy.

Our proposal *transparently separates* the goal of the activity - usually an operational objective - from the activity itself, and these two from the domain of the activity, which embraces the whole operations area, comprising the three pillars.

It will be seen, that these operational activities, just as their ISO and ISACA predecessors, can be detective, corrective and preventive, with respect to the damage - or event - they intend to handle, or cope with. These attitudes to the problem have to be described also more exactly, than before.

Now we build further the frame for characterizing the operational activity. The followings are advice only, that was not built into the definition, as the PCUBE-SEC services can be used without knowing these details.

However, as these considerations might support

- an ordered way of investigating a problem,
- identifying further important details, and
- help to identify improvement possibilities,

these belong to the benefits of our methodology.

Useful attributes, characterizing an operational activity *can* be:

- the operational objective, or set of operational objectives, that is / are to be served by this activity
- the scope of the activity, the set of its so-called subjects, and
- the range of the activity (both scope and range in terms of pillars of operations),
- the pillar(s), where the expected result(s) belong
- a list of "atomic" activities, comprising the operational activity
- the resources, either branches or roles, of course, different ones for each task, that is to provide for:
- identification of the goals, then
- the activities *possibly* contributing to its fulfillment,
- those of the executors,
- the acknowledgements of both the goal and activity,
- giving the necessary permissions,
- the executors, and their
- supervisors, etc.

This way PCUBE-SEC provides for such a goal - activity - domain - range - scope - resource complex, that ensures clear separation between these different roles, keeping the border between goal and the activity, that contributes to its fulfillment.

It is not compulsory to be able to identifying any of these attributes, but *if* they are known, it is worth to document them.

"Actor" can be either organizational unit, or role, but in the practice it is not worth to fix the kind of elements, that can be chosen.

It might be easier to explain current information to such colleagues, who are not interested in such details, that are not relevant to them, if we combine from them a more complex activity, which is the series, a list of these details. "Atomic" activities are here the elements of such a series. Examples for these elementary activities can, e.g., be technical tasks, that are irrelevant to those, to businessmen, who are not well-versed in the area.

According to the PCUBE-SEC philosophy it is always the user, who decides, what details are to be emphasized, how fine a granulation is to be used. The details usually lead to more

and more concrete information, meaning either a task, that can be directly executed, or an obejctive, that is a goal, that can be more easily fulfilled, or such a condition - either an activity, or an objective - that can be further decomposed more easily. To the already mentioned derivation capability of PCUBE-SEC will belong the facility, that if its user gives it a complex goal to be reached, then PCUBE-SEC will try to use those details, that the user - or a *previou*s user - has already put into its knowledge base. Based on these details, PCUBE-SEC might give an advice, what lower level goals are able to substitute the original, more complex one. When the operational activity is a more complex one, then the list of "atomic" activities shows a way of its decomposition to more and more "lower level" ones. In this decomposition excellence criteria can also function as "receipts", or parts of "receipts".

We had defined the importance of an operational objective in the corporate strategy as its distance from it, and used this distance later in risk assessment. If this distance of that operational objective is known, which is connected to our operational activity, then it can be considered, as the *distance of this operational activity from the enterprise strategy*. Thus this can be a classification aspect for operational activities. Dealing with more than one objectives a relation of these distances can also be useful.

This way the subjects of the activities, that are *actually pillar elements,* organizational structures, rules, technical tools, and the like, *can also be classified according their strategic importance.* It will be seen, how can be added to the knowledge base such a kind of information, that is used to solve a users' problem.

There can be other characteristics, too, that contribute to the description of an operational activity. They can be related to the subject of the activity, just as well. The user is, of course, encouraged to invent as many of these, as can be explored in the given situation, as, besides giving details on his / her problem, these can be predefined receipts to be used later by other users.

The following useful features are also suggested, in describing operational activities, and these might give ideas to invent others, too.

The set of *peliminary specified deliverables*, and the expectances connected to it, that can be preliminary specified parameters of these deliverables. If known, these are concrete, measurable, and they are able to take business requirements into consideration, and, what is very important, in a *documented* way.

The business requirements are those, that, with the help of the business areas, are determined for those given subject or subjects, on which the activity operates.

It is worth to note, that the requirement to explore and document the business criteria can be considered to be an operational *objective*, while exploring them is an operational *activity*, or rather, a series of operational activities. The suggestion, that such a series is to be executed if the company wants to satisfy its strategic goals, or some other operational objectives or some excellence criteria, is also an example for a receipt, that can be formulated for further use. These receipts will belong to the best professional practice of PCUBE-SEC.

Due to the special way of processing the PCUBE-SEC knowledge base, these are considered as *necessary, but not sufficient conditions*.

An important benefit of the excellence criteria is, that they can be pre-defined goals of PCUBE-SEC programs, if they relate with the users' problem. These criteria are able to characterize operational activities, as well.

The task, that the operational activity has to perform, is suggested to be characterized by at least the followings, if they are known:

why - the reason, the goal of the action

the actor
- who - the place of the actor in the corporate hierarchy
- he / she executes the task
- how - the way of performing it
- time factor

the supervisor
- who - the place of the supervisor in the corporate hierarchy
  - or outsider, then the connection to the company
- he / she supervises the result of the executed task

(reported to have been executed - this should be checked, too)
- how - the way of checking completion and its quality
- time factor

auditor (of both, "actor" and "supervisor")

who - the place of the auditor in the corporate hierarchy
or outsider, then the connection to the company
how - the way of checking the actor and the supervisor
if their work qualifies to the best professional practice
time factor
feedback - for improving the "how"-s

time factor here means any of these, according to the given situation:
when - start / end time or time interval
at what time - start time
regularly at every - point of time

One of the benefits of the three pillars proposed is another important classification of operational activities besides their relation to business importance. This is the scope of their action. Trying to solve a problem, ordering the search of possible solutions according to the pillars might come handy in finding tasks or conditions, that the user has not thought of yet. Methods related to organizations, regulations, or technics might have different sources, and probably will have different target audiences, too. However, improvements usually affect more, than one of the three pillars.

In spite of the trivial fact, that one activity can operate on more than one pillar, PCUBE-SEC ensures the clarity of the problem world description.

The user is permitted to define actions - operational activities - operating on more, than one pillar. These can be described by a complex statement, consisting of, besides tasks, operating on a single pillar, other, also complex operational activities, and operational objectives, too. As it will be seen, this way complex actions will be "decomposed" into more simple ones. Continuing this decomposition, in the end the resulting parts will correspond to simple statements. Simplicity means here only, that no further decomposition is needed from the view of solving the given problem, but otherwise these results can be quite complex.

PCUBE-SEC permits to assign executors to the tasks, if they are known. As the level of the definitions have been raised to the level of operations and strategy, any member of the staff, any organizational unit, or role in any unit can be thought of to be assigned, top management included.

6.3 Attitude to handling problems

To the most important benefits of these definitions belong again the clarification of the statements, removal of inconsistencies, and, which is equally important, raising the level of both the target and the scope of the definitions again to that of the operations from the IT-level, where this is needed. Those best practice definitions here, that has a scope already risen above IT, has flaws, so they had to be rewritten, too.

It is important to emphasize, that here the *attitude* to handling problems is discussed, this attitude *in itself has nothing to do with any improvement* of an already good thing to an even better one. This is, of course, the final goal of the operational activities with these attitudes, too, as always, but this final goal is not to be mixed into this "nature-like" attribute.

The PCUBE-SEC benefit of *separating* the scope of the actions from their desired effect, *the "inputs" from the "outputs"* have a special significance when we classify operational activities according to their way of handling problems. We will see here, how does this separation help in identifying incosistencies, and in extending the scope from IT towards operations.

Thus such a confusion can be avoided, as mentioning desired events in one definition, and forgetting about them in an other, as it will be seen in the COBIT 4.1 "control" definitions, where, in the detective control, desirability is mentioned, while in the preventive one it is omitted, as it should be - I think - everywhere.

Another important benefit is, that it will be easier to formulate the definiton of the three different attitudes in such a way, that the detective, preventive and corrective approach will not be mixed with each other, as they are in the ISO 27000 definition, as it will be seen. Thus the definitions will really correspond to the name of the given attitude.

Similarly to the discussion of the predecessors of the operational activity above, first the definitions taken from the ISO standards, and from the ISACA materials will be analyzed, justifying this way the necessity of the new definitions even for the IT case.

6.3.1 Correction

6.3.1.1 The ISO corrective action

The ISO 27000 corrective action is an "action to eliminate the cause of a detected nonconformity or other undesirable situation". [ISO 27000]

To require the handling of the cause of the problem is not corrective, but preventive from the viewpoint of a *current* situation, as dealing with the cause affects the future occurence of the mistake, but does not improve the current state of matters. Neither mitigating the consequences of a mistake committed, nor enlightening the consequences is mentioned. To define prevention such a way is not practical, either, as instead of a total elimination of a cause partial solutions could also have been accepted.

6.3.1.2 The CRM corrective control measure

According to the CISA Review Manual, it is: "designed to correct errors, omissions and unauthorized uses and intrusions once they are detected".

This measure is corrective, but sticks to IT, and, even in this domain, emphasizes some special type of mistakes.

6.3.1.3 Correction in COBIT

There is no corrective control measure mentioned in COBIT 4.1.

6.3.1.4 The proposed definition for the corrective attitude

An operational activity is corrective,
if it contributes to the elimination, or at least to the mitigation of the consequences of any kind of mistake that had not been recognized in time, so the mistake resulted in some unpleasant consequences, that need corrections.

6.3.2 Detection

6.3.2.1 Detection in the ISO standards

It is interesting to note, that the vocabulary to the ISO/IEC 27000 family, ISO 27000 does not define a detective type of "action". In the ISO/IEC 27001 the word "detective" was not found, but, interestingly enough, in ISO/IEC 27002, those, who intend to implement capacity management, are guided to apply "detective controls" in order to get timely notification on arising problems. This might be corrected in future versions, as 27001 deals with the information security management systems, while 27002 gives rather concrete advice on its practice. 27000 is a collection of definitions.

6.3.2.2 The CRM detective control measure

The scope of the CRM detective control measure is restricted to errors, and specific IT-, and physical security problems are emphasized. It says: it "exist(s) to detect and report when errors, omissions and unauthorized use or entry occur".

6.3.2.3 Detection in COBIT

The COBIT "detective control" definition in COBIT 4.1 is: "A control that is used to identify events (undesirable or desired), errors and other occurrences that an enterprise has determined to have a material effect on a process or end product".

This is quite close to my proposed definition, but "control" here means rather a control system, than a controlling activity.

6.3.2.4 The proposed definition for the detective attitude

I raise again the whole discussion above IT, and extend the things to be handled to any kind of problems besides events.

The role of a
detective operational activity
is to detect flaws in business and / or operations.
It should be noted,
that a best professional practice is to require the detection to be followed immediately with the *documentation* of the flaw, and the *authentic* collecting and storing of this

documentation, together with reporting the case to a specified problem solving unit, and / or to management level.

Note:
Some kind of means to document the flaws should be offered. The documentation process is to start first, with the definition of the processes, and both processes, that of the detection and that of reporting have to be defined in advance.

The authenticity of the documentation can often be vital. An example is the log management. Somebody can be accused with something only if the proof is authentic. If the proofs are logs, then they are authentic only if they are signed and time-stamped.

6.3.3 Prevention

6.3.3.1 The ISO preventive action

With its generality there is no problem, ISO 27000 says: "preventive action" is "to eliminate the cause of a potential nonconformity or other undesirable potential situation." The difference between this definition and mine is separating the possibility of committing a mistake from intentional damage and accidents.

6.3.3.2 The CRM preventive control measure

Unfortunately it had been left out from the Glossary of the CRM 2011, but a kind of explanation can be quoted, where the "controls" are classified by a kind of function description and examples. The function of "preventive control" is to:

- "Detect problems before they arise.
- Monitor both operation and inputs.
- Attempt to predict potential problems before they occur and make adjustments.
- Prevent an error, omission or malicious act from occurring."

Requirements, tasks, detection and prevention are mixed here. Making adjustments are corrective activities, monitoring is an example for a detective action.

6.3.3.3 Prevention in COBIT

The definition in COBIT 4.1 Glossary is quite close to mine, but it focuses on the effect of a negative event. I am sure, that the adequate behaviour of the staff is also important. COBIT 4.1 says: "Preventive control—An internal control that is used to prevent undesirable events, errors and other occurrences that an organisation has determined could have a negative material effect on a process or end product".

6.3.3.4 The proposed definition for the preventive attitude

Preventive operational activity:
I define an activity as preventive, if it prevents

- the occurence of undesired events and / or
- the possibility of committing a mistake.

The novelty of my definition compared to COBIT 4.1 is, that I separate "our" mistakes from attacks, and accidents. This can greatly help in finding the appropriate preventive action.

What might be considered in the future development of PCUBE-SEC is, if attacks and accidents should also be separated, or is it better to leave, as it is now?

The already mentioned PCUBE-SEC program complex "statements" can be built of different type of "simple" activities from the viewpoint of the attitude, too. That is, detective, corrective, and preventive activities at the same time can be parts of the same complex statement.

6.4 Other kind of attitudes

There are described other attitudes in the literature, too.
One of the *examples* is the *compensating control measure*.

Quoting from, e.g., CRM 2011, this measure "reduces the risk of an existing or potential control weakness resulting in errors and omissions".

Instead of mixing risk in a bit confused way into this "measure", that is, mixing it into an action, the target, the scope of the activity could have been clarified.

Compensating control measure might be needed in the control system of a company. If *corporate control system* is a cooperating set of improving activities, built to serve strategic goals by operational activities, then one weakness can result in errors to be found in an other part. Of course, lots of other scenes could also be invented, but the word "compensation" suggests, that a point is strenghtened in order to balance the weakness of another point.

I did not feel necessary to elaborate the definition of compensating attitude, as the scope of this measure seems to be rather the set of other measures than the operational area, and the goal of such a measure seems to be rather strenghtening the control system of a company, than to mitigate one specific weakness. The operational activities affect the quality of a corporate control system in a more concrete way, at specific - weak - points.

Another example for improving activities can be found in a neighbouring area, outside the area of information security - IT audit. This is a research of frameworks for business ethics implementation, where those measures, that support enterprise credibility strategy implementation, are divided into two groups. These groups are the so-called *support* measures, contributing to the credible behaviour, and the *preventive* measures, that prevent the non-credible behaviour. This grouping illustrates the benefits of classifications similar to those of ISACA in identifying those activities, that might affect the occurence of something that is desirable, or undesirable [Belak et al.].

7. THE BASES OF COMPUTERIZED GOVERNANCE SUPPORT IN PCUBE-SEC

In the followings we describe the automatized processing of the PCUBE-SEC knowledge base. The bases of computerization had been established in the seventies, and had then served as building blocks in such a process modelling system, that was able to solve the same problems, as the PROLOG-based tools did earlier [Szenes, 1976-77], [Szenes 1983, 1987, 1988].

The support to be provided by the new PCUBE-SEC methodology means actually suggesting such actions and lower-level goals, that serve corporate goals. The information security - IT audit notions, methodologies, generalized to the scope of corporate operations, and the excellence criteria together, give direct advice on the development of such operational practices, that promote operational excellence, thus contributing to the fulfillment of the corporate strategic goals.

As a side effect, besides operations, the security state of the companies will also be improved, especially, when excellence criteria are chosen as goals. Both of these improvements can be characterized using the pillars of operations [Szenes, 2013, ICCC].

It is important to note, that should there already be advice in the knowledge base available, coming from predecessor users, the new PCUBE-SEC user can start from scratch just as well, forgetting about any advice of others, and defining his / her own working concepts. All of the previously used names can be redefined, simply by putting the new definition before the old one. Should anybody detail a requirement in the knowledge base, describing its preconditions, its "parts" - its auxiliary requirements, with these a new decomposition can be declared anytime.

Here a formalism will be suggested that can be easily used to describe the users' problem world. This description consists of a - usually - high-level corporate goal to be achieved, and the information security - audit advice, together with the already explored dependencies. The description is aimed to support the identification of new dependencies, together with a future possibility of automatization this support. System PCUBE-SEC helps its user in improving a given concrete situation by providing this formalism, inherited from my predecessor system, PCUBE, in which already known solutions / derivations are described, as it will be seen. Analyzing the already known, described facts, the inference mechanism is to find new dependencies.

These dependencies come to light when, from the user's strategic goals, more and more concrete goals are derived. Solving the users' problem means, that, in the end, this derivation arrives to simple, practical goals, and concrete tasks, that can be executed. Of course, this is possible only, if every complex idea *has at least one decomposition* in the knowledge base to more and more simple ideas. This knowledge, that can be used for the decompositions, can come to the knowledge base from various sources, from receipts of previous users, etc., as it had already been mentioned. I defined the PCUBE-SEC concepts in such a way, that they can be possible building parts of the "receipts" in solving operational problems. The most important contribution to this public knowledge is probably the set of excellence criteria. Their fulfillment might positively affect the whole company life, by setting practical goals, as concrete examples will show it here.

In the followings the PCUBE-SEC knowledge base and its processing will be described. All this is supported - even if partly - by list processing mechanisms I put first together in the seventies, in my university doctor dissertation, then, in a different way, I used in the eighties, when I developed an expert system for the modelling and simulation of parallel and concurrent processes. This system I named as PCUBE, the system for modelling, **P**lanning and simulation of **P**arallel and concurrent **P**rocess systems [Szenes, 1987]. PCUBE is one of the predecessors of PCUBE-SEC, from the viewpoint of the way of both the construction and the processing of their knowledge base.

It should be noted, that in programming my robot controlling and automatic program generating system in 1975-1976, and devising the list processing layer of PCUBE and its process handling instructions I greatly relied on that kind of object orientation, that had been exceptionally well-developed in SIMULA 67. This object orientation style of SIMULA had been widely acknowledged [LNCS 54, 1977].

Before introducing PCUBE here, I describe the formalisms of the PCUBE-SEC knowledge base. Then the description of PCUBE follows, as all of the advantages of the way of its processing are due to a special concept of its implementation. PCUBE-SEC can be implemented the same way. This way the connection between the two systems, and the advantages resulting from this connection can be explained more easily.

7.1 The PCUBE-SEC problem world description and knowledge base

7.1.1 The problem world description

The users' *problem world description* in PCUBE-SEC is the union of the already available knowledge base, plus the knowledge of the user, concerning the given problem to be solved.

This union *need not be distinct*, as the user might over-declare anything, that is already available. This can be intentional, but not necessarily so. PCUBE-SEC *does not demand* the studying of the already available receipts.

Experts can build such parts, that can be used by other users. These others can also build their own knowledge into the PCUBE-SEC knowledge base. Every PCUBE-SEC user is welcome to share his / her knowledge with the others. Their contribution will also suggest always *necessary* conditions, that, according to their knowledge, contributes to the described goals. This knowledge is never stated to be sufficient to achieve anything. To preserve the knowledge of predecessor users is not compulsory, of course, but it might be useful, even if the next user does not always benefits from it. Preserving means not deleting it, a kind of over-declaration is possible. This actually means giving such a new series of conditions, that is not yet present in the knowledge base. It will be seen, that this over-declaration comes into effect only if it is encountered earlier during program execution, than the already available list.

In this research work the author also would like to offer ready-made receipts, beyond the excellence criteria, a kind of experts' knowledge concerning given special, practical problems. These will illustrate the PCUBE-SEC way of program processing. As an advice, these can be taken as results of the PCUBE-SEC research, illustrating, how to extend the information security - IT audit methodologies to operational level.

The knowledge base form of the already mentioned "receipt" is actually a PCUBE-SEC program. In the case of the predecessor, PCUBE, the program itself, and the *path,* that the program execution traverses, are equally important, as this path describes the suggested series of process steps. For PCUBE this was the solution of the user's problem.

For the PCUBE-SEC user this *path* gives the *order of the subgoals* / *activities* to be to be achieved / performed, "according to" PCUBE-SEC, as necessary preconditions of the users' goal. This path shows the order of processing those "statements", that are related to the

given problem, that is the order of those statements, that express those relations, that the user already knows.

PCUBE provides for the automatic derivation process, that actually "computes" the consequences of a given set of information. Applying the PCUBE solution in PCUBE-SEC, this set of information will be the PCUBE-SEC program, that is prepared "to solve a given case". During this "processing" of a program, PCUBE- or now: PCUBE-SEC, never looks into the meaning of the information comprising the program. This processing works almost like an interpreter, when it processes a source program. This formal processing provides for double help. From the one hand it *forces a coherent description, which is always good for documentation*. From the other hand it derives, in a kind of automatic way, the consequences of the information, comprising this description, new connections might also be exlored. Thus PCUBE-SEC *rewards documentations*.

The knowledge in the knowledge base is expressed basically in two forms. One is an objective - a kind of subgoal, and the other is a condition, or series of conditions, that can *contribute* to the fulfillment of the goals. These conditions can be activities, criteria, or any other thing, that is able to *help* to achieve a goals. They help only, as nobody is able to ensure, that they would be enough. Every methodology, just as PCUBE-SEC, gives advice on *necessary* conditions, but there is *no assurance*, that they were *sufficient*.

In formulating these goals and conditions all of the notions described in the previous chapters can be of use. As from the arena of information security - IT audit they are already extended to the scope of operations, corporate governance, they will hopefully also be applied in this context.

The excellence criteria can surely be offered to be chosen to be either subgoals, or preconditions to other goals, as the user prefers. They are short ready-made receipts by themselves. The definitions of these criteria are not necessarily part of the PCUBE-SEC knowledge base. These can be taken as - kind of - self-explanatory "atomic" expressions.

For example, "availability" need not be further decomposed in the knowledge base. Either the user accepts the PCUBE-SEC meaning, or chooses a completely different one, this notion will probably be considered to be a known one, requiring no further preconditions.
Such parts of the knowledge base, that are not detailed further, are called as the *atomic expressions* of the "programming language" of PCUBE. As they have no preconditions, their fulfillment *are outside of the scope of the PCUBE-SEC automatic reasoning*. In other words, these atomic expressions are taken by the user "as granted". However, formerly

atomic expressions can be "transformed" to composite ones, if preconditions are assigned to them.

Investigating the possibilities of the fulfillment of a goal corresponds in PCUBE-SEC to the processing of this goal as a "user's question". *Originally the user asks his /her final question, this is the final goal of the program, and answering it, PCUBE-SEC derives from this question other questions, other subgoals.*

PCUBE-SEC answers these questions using the information to be found on the given goal or subgoal in the current problem world description. From the original question lower and lower-level questions are derived, untill PCUBE-SEC is able to express the "answer" solely by atomic expressions.

PCUBE-SEC "takes the user's question in its one hand, the problem world description in its other hand", and tries to make something out of it, by matching the question to suitable elements in the knowledge base.

PCUBE produces the description of a possible successful process execution and cooperation in the form of series of process steps to be performed in order to achieve the given goal(s). The path itself is the important result. In the case of PCUBE-SEC the *derivation paths* will also be the most interesting part of the result, as they *show the road towards the goal*.

The way of processing the users' question explains, what is the meaning of *over-declaration* of something, that is already detailed in a certain way, that is by certain atomic expressions. Over-declaring simply means *another way of detailing this same thing*. This matching proceeds taking the statements of the knowledge base one-by-one, from the beginning of the knowledge base towards its end. Thus the explanation, that is the details, that PCUBE-SEC finds, will be those details, that stand *first* among the explanations of this same more complex thing. This is why the users' over-declaration "comes to live" only if it is encountered by the program execution.

An important advantage of the PCUBE-SEC way of implementation its users' knowledge is, among others, that it shows very well the *value of documenting* everything, that we know of. PCUBE-SEC, as any other tool, can use only the information, that it had been "told". Thus, if the user wants to benefit from the processing of his / her question, then he / she has to put everything into the knowledge base, what is already known about the problem. Concrete examples will show, how to formulate this knowledge.

Another advantage of PCUBE-SEC, and reward for the documentation, at the same time, will also be shown. This is the already mentioned *exploration of new connections* of the already known relations between the parts of the knowledge base, giving a chance to identify new dependencies, even without any further outside help. These dependencies between goals and conditions, beyond those, that the user has already described, will be the result of matching the user's question to the elements of the knowledge base.

This matching process corresponds to the special way of PCUBE program execution, that can be interpreted, as it will be seen, as the traversing of certain trees. This traversing utilizes the net of connections between the building blocks of the PCUBE-SEC problem world description. This traversing is a kind of derivation process, proceeding step-by-step, starting from the users' question, as if from a higher-, strategic level goal, towards more and more concrete information, which is either more simple goal, or executable tasks.

The user's goal, the "question" is to be answered using the knowledge base. This answering is made step-by-step, this is the so-called PCUBE derivation process, that PCUBE-SEC inherited from PCUBE.

7.1.2 The PCUBE-SEC program

The simplicity of the PCUBE-SEC "programs" requires no IT knowledge, thus hopefully anybody will be able to understand it, or even to write statements into it, that is to document his/her knowledge on the necessary conditions of the goals.

The PCUBE-SEC problem world description is an ordered set of simple and complex statements. The ordering is simply the order of their occurence in the problem world description.

The *simple statement* is a series of characters, followed by a dot. For the PCUBE-SEC user this statement actually means either an operational objective, or an operational activity. For PCUBE-SEC itself it means just that series of charecters, which comprise it.

Thus these characters can be chosen in an arbitrary way, with the exception of the delimiters. Delimiters are the dot, the colon, the semicolon, the minus sign, and the brackets, "[", "]", these latter are used to denote comments in a PCUBE program.

It is important to note again, that it depends on the view and opinion of the PCUBE-SEC user, what action is *considered to be* "simple". These are the "atomic" expressions, that do

not need further detailing, do not need further explanations. This "simplicity" also depends on the users' view on the *current problem* to be described. *If* he / she does not want to bind the execution of an action, or the fulfillment of a goal to preconditions, *then* this action or goal is simple.

The goals - objectives - are handled the same way. Those goals are *simple*, that have *no preconditions*.

The *complex statement* is a list of such elements, that, individually, are "very similar" to a simple statement, without its finalizing dot. That is the head of the list is the first character series, and the tail consists of a series of such list elements, that are also series of characters, one-by-one.

The complex statement begins with "its" list head, then the elements of the tail follow, separated from each other by minus signs, by "-". The end of the complex statement is also denoted by a dot.

The derivation will be shown through examples. Now it is enough to say, that the elements of the list constituting the tail of a complex statement are in an "AND" relation with each other, and the simple or complex statements beginning with the same way, with the same head (complex statement), or with the same character series (simple statement), are in an "OR" relation with each other in the given knowledge base. They are alternatives of the same head or beginning. However, it is important to remember, that the elements of the tail of a complex statements are all *necessary*, but not *sufficient* conditions of the head.

Thus the elements of the list, comprising the "second part" of the complex statement are one-by-one *necessary*, but not *sufficient* conditions of the fulfillment of that (sub)goal, which is expressed in its head. Thus the "AND" of these elements is also necessary, but not sufficient conditions of the fulfillment of that (sub)goal.

This actually means, that the complex statement has a head, that - in a special way - is in itself "similar" to a simple statement, and this head is followed by a number of character series, the list elements. These themselves are also "similar" to simple statements, in their turn, one-by-one. That is the list elements could be simple statements by themselves, if they were terminated by a dot one-by-one.

These simple and complex statements constitute the knowledge base of PCUBE-SEC, that is used to answer the PCUBE-SEC question. There will be examples for this kind of program, and for its "execution".

For PROLOG experts it can very well be seen now, that what we want to avoid here, it is the details of the first-order predicate calculus, applying its theorems, together with their consequences. We do not need these proofs.

Having seen the PCUBE-SEC philosophy, the reader will hopefully agree, that we could manage this. To justify the construction of the problem world description from this kind of simple- and complex statements, and the way of deriving consequences from the problem world description does not require mathematical reasoning, as PCUBE-SEC rules out explicitly *any attempt at completeness. It promises* contribution *to finding such* advice*, that* might *help.*

Emphasizing the "contribution" to the achievement of anything has been very important throughout the whole methodology.

PCUBE-SEC - or rather, its predecessor, PCUBE - processes its problem world description in such a way, that it does not matter, if the simple statements corresponding to the members of the list are *necessary, or sufficient* conditions of this head. PCUBE-SEC takes the simple and complex statements as *usable,* that is, as *necessary* conditions, to achieve the goal, expressed by the user's question.

Information security - IT audit methodologies, anyway, never promise ideas or tools for finding such a set of activities, or any other kind of advice that would really be able to *ensure* the fulfillment of an objective.

Should the necessary conditons given in the problem world description be satisfied, this will always bring us *nearer* to a kind of completeness, to the absolute truth, which we can, of course, *never* reach. *That is why all the characterization and criteria here tries to provide for exact measures.* This is why it is so important to know, that the execution of actions, or the fulfillment of requirements *how near* takes us to the desired *perfection*.

This is again a proof for the importance of my *pillars*. Distinguishing between operational activities by subject domains makes to find exact measures much easier, as we are given a *hunch* at least, which direction to take. The exact measures will then facilitate the comparison of the effects of different activities.

From the above considerations, both from the philosophy, and from the way of implementation of PCUBE and thus from that of PCUBE-SEC, directly follows, that there might very well exist *other* version to the same head, or, in other words, other list of preconditions to its execution / fulfillment. These lists are then *alternatives of the same head*. The possibility of giving such alternatives were important advantages of PCUBE, as they permitted the specification of different ways to achieve the same goal. The PCUBE program describes the conditions of the execution of the systems of parallel, or even concurrent processes. The goals of the PCUBE program correspond to the goals of the individual processes, that comprise the process system. Actually these goals identify the processes. Thus the different ways to achieve the same goal correspond just to those different ways of process execution, that leads to the same goal. The steps of this process execution are the subgoals, that "have to be achieved". If there is such a step in a series of steps, that "has no way of achievement" in the PCUBE program, then PCUBE has to choose another alternative for the same head, if any. This processing of a complex statement, list element by list element, one-by-one, is directed, by the order of the elements in the list. If there is no other alternative, then PCUBE goes back to an earlier point, where another alternative could have been chosen.

In PCUBE-SEC the role of these alternatives is the same, they express different list of conditions.

It is important to note, that, just as PCUBE, PCUBE-SEC will choose the second, third, etc. alternative only if the processing of the first available alternative failed. This fail means, that PCUBE-SEC found such a condition, that had no simple statement counterpart in the knowledge base. However, this situation might be due to an incomplete documentation.

This way of processing alternatives PCUBE inherited from PROLOG, it even was suggested by the special way of PROLOG program execution [Kowalski]. However, it is important to note, that the PCUBE-, and, this way, the PCUBE-SEC programs, too, are interpreted and implemented in totally different way from that of PROLOG, as it will be seen. Thus the similarity is valid only till this point.

7.2 PCUBE, the ancestor

Parallel processes are, roughly speaking, such processes, that execute some of their steps at the same point of a kind of virtual time. Concurrent processes are such parallel processes, that compete for the same resources. The most important design goal of PCUBE - or shortly P^3 - was to support the modelling, **P**lanning and simulation of **P**arallel and

concurrent **P**rocess systems, to find such a scheduling, such a cooperation of these parallel, or even concurrent process systems, that satisfies the user-given goals [Szenes, 1987].

This modelling tool was later used in investigating the scheduling possibilities of such web services, that are the building blocks of service oriented architectures [Szenes, 2006, SOA].

The four layers of PCUBE are:

- a problem-friendly AI style users' problem description facility
- traversing trees corresponding to this problem world
- implementation the traversing + time maintenance + resources in list processing
- implementing the list processing level on base level.

The architecture of PCUBE is a hierarchy of these levels. To these levels different process modelling styles, implementation tools, type structures, and also different user problem description support belong.

The syntax of the top level, that of the user problem description is PROLOG-*like*, but this similarity exists only at the *top level* of the system. The overview of the PCUBE implementation layers will clearly show, that already the basic *architectural* concepts are totally different from those used generally by PROLOG experts.

This multi-layered architecture facilitates a rich process and process systems description, together with such a planning of process execution, that results in deadlock-free series of process steps.

This mixed diversity of positive characteristics is due, on the one hand, to the user-friendly problem description at the top level of PCUBE, that explicitly requires rather the knowledge of the problem to be solved, of the *"what"*, than programming skills, the *"how"*, and, on the other hand, to the multi-layered implementation.

My basic idea in developing PCUBE had been translating the users' problem world description, consisting of the preconditions of the execution of the individual steps of the users' processes first into a problem of traversing trees corresponding (more or less) to the individual processes.

As I had already had practice in using list processing for writing AI programs, from the time of writing my university doctor dissertation in 1976, it seemed to me quite natural to

implement this tree-traversing also in a list processing language, developed just for the purpose [Szenes, 1976-77], [Szenes, 1987, 1988].

The list processing language, could, in its turn, be implemented in a low-level, efficient code [Szenes, 1987]. This code had first been FORTH, [Forro], then, some years later, C [Palossy, Tempfli]. This way I could get rid of the disadvantages of the PROLOG-like interpreters, that had been a little slow, and required ample storage, that meant a drawback in the eighties.

This method of construction could even facilitate the concrete real time control of the execution of the user's process systems. In other words, the PCUBE process model is actually a time and / or execution table of the steps of the processes to be followed to achieve the user - given goal.

In the case of production processes this would mean the actual controlling of the machines themselves, according to the "successful" series of steps, that PCUBE had built - discarding, of course, those parts of the solutions, that lead to deadlocks. Of course, to perform this plan, machine-controlling facilities are to be added to PCUBE.

Both the knowledge bases of PCUBE and that of PCUBE-SEC contain facts known on the problem to be solved. The task of PCUBE was to find such solutions, using the knowledge base, that describes the different possible ways of the cooperation of the processes that reach the given goal(s). The task of PCUBE-SEC is to give back those parts of the receipts, those parts of the knowledge base, that lead to the users' goals, under the given preconditions.

On its top level PCUBE offers a wide scale of process interaction facilities, that I had learnt from such sources, as the basic article of Hoare on communicating processes, and the - I think - best modelling language with the already mentioned, remarkable object orientation, SIMULA [Dahl et al., SIMULA 67], [Hoare]. The SIMULA facilities gave the idea for the instructions, that described parallelism. The monitor concept, that I renamed as "resource", came from Hansen's Concurrent Pascal [Hansen]. This is the notion, that is needed to describe concurrency, as this is the resource, that is needed by the processes, but its use is exclusive. If one process uses it, then the others have to wait. The idea of the time-handling instructions, that express, that something happens BEFORE, AFTER, etc. some other event, or a process WAITs for a time interval, I took also from SIMULA.

My contribution to the T-PROLOG project had been just the description and specification of these SIMULA- and Concurrent Pascal-like features, in order to help the colleagues to include them into this PROLOG-based simulation language [Futó, Szeredi, J., Szenes]. The idea to extend PROLOG with time maintenance is due to Ivan Futo.

Due to the PROLOG base the T-PROLOG process handling was deadlock-free. PCUBE is also able to derive deadlock-free plans for process execution because of its tree-traversing layer.

On the list processing level of PCUBE and thus that of PCUBE-SEC, to a simple knowledge base statement such a list corresponds, that consists of the series of characters comprising the simple statement, this is such a list, that consists of a head only, and has no tail. To the complex statement corresponds a list composed from its head and tail.

Developing the list processing level of PCUBE, first I had to define the list traversing instructions. The lists have to be traversed forwards, and backwards, too. Composing new lists from existing lists had also to be described. All these instructions were based on the notion of successor and predecessor, as this is actually the notion, which is needed to describe the tree traversing.

To facilitate the time- and resource handling in PCUBE, I wrote a scheduler, in the list processing language, based on my experiences with job-scheduling on mainframes, and on the ways of processing the interrupts by the means of interrupt drivers, according to the customs of the old assembly "world". For the scheduler I got some ideas from the CDC 3300 job scheduler, too.

Having specified this scheduler, I gave it to my already mentioned students, who wanted to program the base level, as diplom theses first in FORTH [Forro], then in C [Palossy, Tempfli].

It must be noted, that the facilities of my list processing language also took after those of SIMULA 67, as I had written my AI system in 1976 in SIMULA, on a CDC 3300, exploiting the really very extensive, and, at the same time, exceptionally comfortable SIMULA list processing facilities. The AI feature was providing for such robots' thinking facilities, as those of WARPLAN, that had been written in PROLOG, by David Warren [Warren], [Szenes, 1976-77].

"Thinking" meant, that the robot had to compose at least one series of steps from a given set of possible steps, that led to a given goal. In other words, it had to find at least one way to achieve a given goal, under given preliminary conditions. In my doctor dissertation I had illustrated the deadlock handling capabilities of my system with some examples.

7.3 The PCUBE processes and their tree models

The base of PCUBE is the one-to-one correspondence between the process and the backtracking traversing of a tree. The nodes of this tree correspond to those conditions, that the process "could use" to reach its given goal. As it will be seen, these nodes are actually the simple statements, or the heads of the complex statements comprising the knowledge base, and the root corresponds to the goal, which is the user's question. T*his goal identifies the process to PCUBE.*

The user's process system is mapped to a kind of traversing of the non-distinct union of the trees corresponding to the individual processes, that is, to the current receipt available at the time of processing, in PCUBE-SEC terminology. This receipt is composed of the user's knowledge on the given problem, experiences of former users, and, in the case of PCUBE, the built-in process system description facilities. PCUBE takes this knowledge, and using it, tries to answer the user's question, that corresponds to a process goal in PCUBE. As it had already been described in the case of PCUBE-SEC, *PCUBE takes the user's goal or goals into its "one hand", the knowledge base into its "other hand", and tries to find statements in the knowledge base, that match the goal*, or, if the goal is complex, then to the head of the "goal-list". Having found a matching element, PCUBE begins "processing" the goal, that is PCUBE drops the head of the list comprising this matching composite statement, and adds the tail of this composite statement to the goal to be processed. Then proceeds with the remaining list elements of this tail. Having first processed these list elements that came from the matching knowledge base statement, PCUBE continues with the remaining part of the goal-list, list element by list element.

The "process steps" are actually these matching elements.

Thus the PCUBE process is actually considered to be a series of steps, where "step" means either the execution of an activity, or a subgoal. The activity is a unit one, that is it isn't to be splitted into further "activity particles". As it has been mentioned, it depends on the user, which conditions are "atomic" conditions, which are those "statements", goals or activities, that are not to be decomposed further.

Examples will show this "program execution", step-by-step.

In PCUBE we usually have more, than one processes, so we have more, than one trees. The communication - dependent traversing of these process trees is just the physical structure of the given process system in PCUBE. A certain part of this structure that corresponds to the successful execution of the processes is the solution of the given problem. This will be illustrated by a production scheduling example.

Every process has one and only one goal that it "has to achieve" by an appropriate series of the allowed possible steps, which are "taken" using the simple and complex statements of the knowledge base.

The chance of "fulfilling" - deriving - the user's goal depends on the world "sorrounding" the processes, described by the knowledge base. The step-by-step derivation of the goal comprise that "receipt", which the PCUBE program is to find. This receipt is such a series of steps, chosen from the possible series that achieve the given goal.

The procedure of finding this "succesful" series of steps corresponds to the already mentioned tree-traversing. The possible nodes of the tree correspond to the possible process steps. The root of the tree corresponds to the PCUBE goal. The successful series of steps corresponds to the successful execution of the given PCUBE process. The nodes corresponding to the elements of this successful series are those nodes, that are "to be followed" in order to reach the goal of the given process.

If we take the series of *every step that has been tried*, not only those, that lead to the successful solution, then this is the tree that had been traversed, this is the tree that *corresponds to the given process*. This is the "original" process, that "got" the goal, that it "has to" fulfill. This correspondence between tree traversing and users' process will be illustrated by examples, showing this step-by-step inference.

This structure and tree-traversing was exploited in the special handling of systems of parallel and concurrent processes. Because of the backtracking, if there is a solution of the given problem, under the given preconditions, then PCUBE will find it. If it reaches a deadlock situation, it backtracks and tries to reach the goals in an other way, if possible. This "other way" simply means going back to the latest point, when another matching alternative could have been chosen. Thus "PCUBE" tries every possible paths, to solve the users' problem.

The difference between PROLOG / T-PROLOG and PCUBE can now be clarified. PROLOG also wanted to find matching clauses to the goal (those statements, that are simple or complex statements in the PCUBE-SEC terminology, are the so-called clauses of PROLOG), but PROLOG is not prepared to handle a multiple-goal problem situation. One way of introducing such facilities was writing PROLOG programs - this was the T-PROLOG approach. Another way was the introduction of this four-layered PCUBE architecture, augmented by the scheduler. The scheduler is responsible for facilitating the maintenance of system time, and for resource handling. Thus it is possible to prescribe to a process to do something before or after a certain "point" system time, such time-related process communication is available, as, e.g. waiting for another process for a given time interval, resources can be taken and then released.

7.4 The PCUBE process communication

The PCUBE processes can interact either by messages, this is the direct process communication, or by implicit communication. This latter means substituting constant values into variables. It will be seen, why is this operation called as "communication", and what is the information, that it gives to the PCUBE user.

The time and resource handling PCUBE "instructions", might come handy in a later stage of PCUBE-SEC development, for describing real-life operational problems. We wrote programs to implement them in the list processing language. Thus in a PCUBE or PCUBE-SEC program these can be either simple statements, or conditions in a complex statements just as well.

The wide variety of the PCUBE process communication facilities provide for the connection that binds the processes together to be a *parallel system*, while the resource maintenance capability is the base of the description of concurrent problems. In order to fulfill the "task" expressed by the process goals, the process interact, they have to communicate, and compete for the resources.

The name of these facilities, that of these "instructions", are fixed. However, these can be over-declared just as any other PCUBE built-in facility, or PCUBE-SEC receipt, should the user want to "mean" something else on these names, on "AFTER", "RESOURCE", and the like, should he /she need just these character series to express something else.

From the user's point of view communication facilities have to handle the parallel / concurrent problems and the time maintenance. The following predefined system "instructions" serve this purpose:

Implicit interaction:

AFTER (point_of_time)
AT (point_of_time)
BEFORE (point_of_time)
HOLD (time_interval)
TIME (what_is_the_time)
TIME (point_of_time)

Explicit interaction:

Resource handling (concurrent problems):
resource declaration:
RESOURCE (resource_name ,
number_of_the_available_ones_of_this_type)
use of resources:
RELEASE (resource_name)
TAKE (resource_name)

Direct communication (messages):
SEND (message)
WAIT (message)

Those self-explanatory arguments that contain the term "time" refer to the system time of PCUBE. This is a common "variable" to every process in a given user's process system and is maintained by the scheduler. At the start of program execution the system time is set to zero. The above instructions increment its value according to the actual requirements of the state of the problem solving. This means, that these values, when they appear in the knowledge base, are usually variables at the start time, and get a constant value by matching the statements of the knowledge base to the process goals, and in the process goals they are constants, as the production scheduling example will show.

As we already mentioned, in the case of a deadlock situation PCUBE "goes back" to another possible alternative on the "road towards" solution. This might cause the

decrementation of the system time. Tracing the way of problem solving this decrease looks as if a "process went back in time in order to try doing something else then it had done before". This is the backtrack in time.

The "resource" is such an object of predefined type that can only be used exclusively. That is, if a process "TAKE"-s it then no other one can access it before the first process "RELEASE"-s it. The number of the available "RESOURCE"-s are, of course, decremented / incremented accordingly.

From these instructions composite expressions can be built. Such a requirement, as, e.g., a process only after a certain message may (but then should) try to TAKE a RESOURCE can be specified simply by writing the respective instructions (WAIT, TAKE) one after the other, into one complex statement. Dependence on time can be expressed the same way.

7.5 PCUBE example program

The following production scheduling program I wrote originally in order to introduce the facilities of T-PROLOG [Szenes, 1982], then I used it to illustrate the capabilities of PCUBE [Szenes, 1987, 1988].

Besides illustrating the use of these time- and resource-handling features, it shows a backtrack, too. The backtrack in the PCUBE derivation process is facilitated by the tree-traversing, as we will see here, following the execution step-by-step. The comments are marked by braces.

```
RESOURCE (M1, 1).
RESOURCE (M2, 1).       [and so an, M3, M4, M5, M6,
                         simple statements, declaring
                         the resources, the machines
                         "RESOURCE" is a PCUBE keyword]

[now comes the 1st  part
of the description of the production process,
how to produce something - it needs machine, that has to be "taken", then "held" for a given
time interval, and then it is to be given back to the resource pool, that is, it is "released";

the time limit is set to "22 ", as this choice is suitable to illustrate the deadlock situation,
with just one backtrack step]
```

PRODUCE (*P *M *T) : TAKE (*M) - HOLD (*T) - RELEASE (*M) - BEFORE (22) .

[*2nd part*
of the production description:
what are the *actual steps of producing* product P1, ... P3
to the production of product P_i,
some of the machines are needed for given time intervals]

FINPROD (P1) : PRODUCE (P1, M1, 2) - PRODUCE (P1, M2, 2)
- PRODUCE (P1, M3, 2) - PRODUCE (P1, M6, 2) .

[and so an, declarations of FINPROD (P2) and that of P3 are similar]

PROCESSES [this is a keyword of PCUBE,
for marking the beginning of the user's goals]

FINPROD (P1) .
FINPROD (P2) .
FINPROD (P3) .
END [keyword to denote the end of the program]

The execution of this kind of program begins, as it had already been mentioned, taking the user's goal in one hand, and the knowledge base in the other.

In order to process goal FINPROD (P1), a complex statement starting with the same expression has to be found in the knowledge base. Having "reduced" the goal with the head of the complex statement found, now we have the list elements PRODUCE (Pi, Mj, time interval) to handle, to eliminate, one-by-one. These can be processed "with" the "algorithm" PRODUCE (*P, *M, *T), where * denotes variables. In this algorithm these variables are "substituted" with the concrete, constant Pi, Mj, and time interval values, in order to facilitate the elimination of the individual list elements.

This is an example for the already mentioned *implicit communication*. If another process "finds" the constant in place of the variable, then this process will "get to know", what was the required value for the process, that "came earlier".

Having executed the substitutions, and merging the remaining lists, we have now to process the TAKE, HOLD, and RELEASE, one by one.

We do not follow this example to its very end, we will have examples instead, with such subjects, that are closer to governance, operations and security. However, the starting of one branch of the one tree can already be seen here. The root is FINPROD (P1), and the next node is the complex statement, resulting from matching this goal with the complex statement, that begins the same way, with head FINPROD. In the end of the example, we have, of course, as many non-distinct trees, as the number of process goals, in this example it was three.

The root of our first tree here is:
FINPROD (P1)
From this root a branch leads to the node following the root. This next node corresponds to the list, that remained without the condition, that had been just now processed. Now this "lost" condition was the FINPROD (P1).

This tail of the first list is:
PRODUCE (P1, M1, 2) - PRODUCE (P1, M2, 2)
- PRODUCE (P1, M3, 2) - PRODUCE (P1, M6, 2)
The third node following this, will again be the remaining list, preceeded by those conditions, that we "gained", having "lost" PRODUCE (P1, M1, 2):

TAKE (M1) - HOLD (2) - RELEASE (M1) - BEFORE (22)
- PRODUCE (P1, M2, 2) - PRODUCE (P1, M3, 2) - PRODUCE (P1, M6, 2)

7.6 Examples for the PCUBE-SEC technics

7.6.1 Decomposing excellence criteria

As we have already mentioned, the excellence criteria can very well be exploited in the knowledge base of a PCUBE-SEC program.

Let us take order, as goal. In the PCUBE-SEC practice, this usually will be a sub-goal, not a final goal, but now we deal only with "order", and its "constituents".

The trees, as we have already seen, follow the derivation process. It must be noted, that for such simple cases, as the one presented here, this automatic derivation could be thought

over without the aid of a machine. *This thinking is just that governance-conscious way of thinking, that PCUBE-SEC wants to advertise.*

Reviving the discussion of criterium order, we can construct at least two different PCUBE-SEC program Fragments:

[Fragment1:]

[we give 3 alternatives for order, these are in an "OR" connection:]

order: documentation.
order: business_continuity_management.
order: incident_management.

business_continuity_management:
asset_classification - asset_supervision.

[very important tasks are omitted here from business continuity;
PCUBE-SEC promises to list *necessary* conditions,
sufficiency does not belong to its targets]

asset_supervision:
continuous_monitoring of_the state_of_the assets - result_processing.
asset_supervision:
regular_monitoring_of_the_state_of_the_assets - result_processing.
[continuous monitoring is preferred, this is
why it is the first element of the list of conditions,

but, should it be not feasible,
regular monitoring is better, then nothing, if "continous..." fails,
then the "regular" alternative will be chosen

result_processing is a must, of course, in both cases]

documentation:
change_management - release_management - configuration_management.

Now we give a very different other Fragment, where those conditions, that had been in "OR" relation above, are in an "AND" relation:

[It is worth to note, that both documentation and change management are considered to be vital factors in corporate success [Melancon]. Here we declared the latter to be a necessary condition of the former.]

The second Fragment begins in a different way:
[Fragment2:]

[instead of the three alternatives for order above,
we require the three things *together:*]

order: documentation
- business_continuity_management - incident management.
[the rest is the same as Fragment1]

Thus the difference is, that Fragment1 requires only *one of the three conditions*: documentation, business_continuity_management, and incident management, while Fragment 2 requires them *together*.

If, in our PCUBE-SEC program, Fragment2 comes first, and then comes Fragment1, then it means, that we would prefer the fulfillment every single conditions of these three conditions, but should all of them not be available, we content ourselves with the fulfillment of at least one of them.

Depicting these considerations in the form of PCUBE trees, from root "order" we have four branches. The first leads to such a node, that has a longer name:
documentation - business_continuity_management - incident management.

The second, third, and fourth branch correspond to the three alternatives in the beginning of Fragment1, that is, the second branch leads to node documentation, the third to business_continuity_management, and the fourth leads to node incident_management.

Let the goal (between the PCUBE keywords PROCESSES and END) be:
order.

The processing goes the same way, as the execution of such a PCUBE program, that has only one goal.

7.6.2 Selling best practice to the top management

Order is obviously a basic factor of corporate success. Let's use it in an example for "selling" a best practice criterium to the top management.

The information security officer, and the IT auditor of our example would like to induce top management to enforce *order* in the corporate, according to *their* order definition.

To identify tasks, and actors, responsibles, and other attributes of the operational activities to be executed to contribute to order, PCUBE-SEC advises to classify these, according to the pillars of operations: organization, regulation, and technics.

The top management should be *regulated* to define the tasks of the *organizational* units, then the heads of units should be *regulated* to perform such *organizational* tasks, as the decomposition of these tasks of their unit into *job descriptions*, then to decompose further these job descriptions into *roles*, and assign tasks to these roles, etc. We used the regulational, and the organizational pillar.

The *technical* pillar is also needed. Tools, that help the staff in performing these tasks have to be available. Again job descriptions have to be written, regulating, which member (which role), in which organizational unit operates these tools, how, under what supervision, etc., that is organizational and regulational activities are needed again.

The following receipt is to justify the worth of the security considerations for the top managers.

corp_success_on_market: corp_info_effective - operational_services_available
- [etc. here could come some other conditions, where
operational criteria, or other best practice wisdom is cited]

[to offer general security-improving measures to the top management might not arise too keen interest, but initiating the defense of such an applications system, that supports important business processes might ring a bell,
that is why we chose here this formulation -

let's substitute, of course, the favourite business-supporting application of the top management in place of " importantITsys":]

corp_info_effective: info_in_ImportantITsys_correct
- info_in_ITsys_delivered_at_time
- corp_info_relevant_pertinent.

info_in_ImportantITsys_correct: cant_be_tampered_with.
info_in_ImportantITsys_correct: [something else, another version for an alternative,
then this is a choice point, a fork in the tree].

cant_be_tampered_with: [to this head now
a list of such operational activities can be enumerated, that prevent tampering,
or, at least, to make it a bit more difficult, than usual;

trying to identify the sought activities according to the pillars makes easier to find them - this is a PCUBE-SEC advice to systems analysts:]
org_measures_tamper - regul_measures_tamper - tech_measures_tamper.
[all of these activities will serve the establishment of order in the company]

org_measures_tamper: role_def_in_job_descr - [etc.
role_def_in_job_descr: responsibility_def - relation_in_hier_def.

regul_measures_tamper: document_job_descr.

tech_measures_tamper: logging - log_analysing.
[these activities above are not independent, of course,
to this logging and analysis of the logs, for example, the respective job descriptions should be defined;

should there be no tool for log analysis available,
then this is the place in the receipt,
where its procurement could be inserted]

PROCESSES
corp_success_on_market.
END

7.6.3 The PCUBE-SEC practice in systems analysis and programming

Example for using some of the technical and systems analysts' tools of PCUBE-SEC:

step 1
Let the strategic goal be customer_satisfaction.
Let the only hit be in an already available PCUBE-SEC knowledge base:

customer_satisfaction:
- service_tuned_to_customers_requirements.

step 2
In order to collect further details, that is to collect such improving objectives / activities, that contribute to condition:
service_tuned_to_customers_requirements

the systems analyst turns to the IT Steering Committee
(communications forum between business and IT; it was described in the risk management chapter of the dissertation).
Its members are the heads of the business-, and business-supporting divisions.

Let's first explore, *which* excellence criteria do the business leaders consider to be relevant to the above quality of service related problem, by turning with the following matrix to the members of this Committee:

criteria	mark 1-5	notes of the interviewee, e.g. further characteristics - parameters - to the criteria
Confidentiality		
Integrity		
Availability		
Operational effectiveness		
Operational efficiency		
Operational compliance		
Operational reliability		
Strategy-driven goal & operational risk management excellence		
Functionality		
Order		
other important criterium		

step 3
Let's suppose, that the votes of the interviewees resulted in:
availability (product, flexible)
functionality (procedure, customer_care)

step 4

Using following matrix either with the same interviewees, or with their subordinates, a unique meaning of these requirements can be settled,
where
obj. denotes improving operational objectives,
such subgoals, that result in an improvement,

by the means of *act.,*
that *denotes improving activity,*
belonging to the pillar identified by the name of the column,

that has "*area*" as *domain*, that is

area denotes the domain, in this case the organizational units, or
the union of organizational units, *where* the activity is to be performed

exc. crit. \ pillar	organizational obj./ activity/ area	regulational obj./ activity/ area	technical obj./ activity/ area
availability (product, flexible)			
functionality (procedure, customer_care)			

step 5
A possible example result matrix can be:

denoting just in time delivery by JITd

exc. crit. \ pillar	organizational obj./ activity/ area	regulational obj./ activity/ area	technical obj./ activity/ area
availability (product, flexible)	JITd / assign responsible roles / logistics, production	JITd / rulebook of the process from order to delivery / logistics,production, finance	JITd / procurement of tools for flexible production & logistics / logistics,production, finance
functionality (procedure, customer_care)	customer-oriented service / assigning account managers / marketing (with scope or with defined contacts to other organizational units)	customer-oriented service / rulebook of customer service procedure; rulebook on collecting feedbacks / marketing	customer-oriented service / procurement of tools for collecting and analysing feedback / marketing, finance, IT

step 6
This matrix can be expressed by the following PCUBE-SEC knowledge base "program statements", that is, our starting condition can be decomposed by the following series:

service_tuned_to_customers_requirements:
    - availability (product, flexible) - functionality (procedure, customer_care).
availability (product, flexible):
    - just_in_time_delivery.
just_in_time_delivery:
    - assign_roles_production
    - assign_roles_logistics
    - write_process_rulebook
    - procu_of_flexibility_tools.
functionality (procedure, customer_care):
    - customer_oriented_service.
customer_oriented_service:
    - assign_acct_managers
    - write_procedure_rulebook
    - edit_feedbacks_into_rulebook
    - procu_of_collecting_analysis_tools.

Notes
It should be emphasized again, that PCUBE-SEC promises to support its user in finding *necessary* conditions to the starting complex statements, sufficiency can *not* be overtaken.

The example could have been more complex, adding classification of the interviewee, that is classifying the heads of organizational units, according to the business importance of their unit, or according to another relevant aspect.

Here only an example is given for using systems analysts' skills and expertise in

- identifying those business goals, that provide for a sustainable development of the business, and thus for continuous improvement,
- preparing such a detailed plan, that clarifies to every level of the corporate hierarchy, to every member of the staff, how to contribute to the achievement of *their part* of the strategic goals.

In order to align the employee roles to the tasks, the heads of the organizational units have to define these roles, and they have to add this to the job descriptions of their subordinates. Systems analysts can support the bosses first in deriving the subgoals of their organizational units from the company strategy, then in allocating the tasks to their subordinates. These *organizational* tasks belong to the organizational pillar.

8. PROVISIONING FOR MEASURABLE AND PREDICTABLE OPERATIONAL SECURITY AND INFORMATION SECURITY FOR COMPANIES

Based on the previous results, now we are able to define a *measurable* and *predictable* operational security and information security for enterprises.

The direction from security towards corporate governance, that is the way of improving the quality of corporate management by the means of such methods, that originally belong to the armoury of information security - IT audit, had been illustrated by our definitions for corporate governance, IT governance, pillars of operations, operational objective and activity, strategy-driven goal & operational risk management excellence, and the excellence criteria.

We have also seen example for the other way around, for serving security by governance, for devising governance issues from security requirements. Top management might accept security requirements as their own, if these requirements are derived from unquestionable governance requirements.

In order to establish the mutual dependence between governance and security, in order to serve both parties, top management and security - audit, let us define
operational security, as
such

- an organizational, regulational, and technical *system*,
  to be established in a company,
- by the means of
  - identifying
    - strategy-related operational objectives and
    - operational activities,
  - and by contributing to the fulfillment of these objectives,

that

- *satisfies* the excellence criteria
  - prioritized by the top management, or by their delegates in the business areas
  - in a predictable, measurable, and scalable way.

Notes:

For operational security target I could have chosen a special case, the strategy of the company. Choosing the PCUBE-SEC excellence criteria or other strategy-related, but everyday operational objectives keeps the required goals and activities at "ground" level.

The importance of the excellence criteria should always be evaluated with respect to each other, their *actual* fulfillment is not obligatory.

This operational security requires an overview of the present system according to the pillars, and suggests the user to find those operational objectives / activities, that lead towards the given strategic goals, together with those improvement facilities, that they involve.

The mutual connection between enterprise governance and information security - IT audit, the market success of the company set the stage, this way, for the introduction of the PCUBE-SEC style of enterprise governance.

Following the direction set by this operational-level security definition, the information security can be derived, through defining the security of an information system. The goal is to serve every actor in the best possible way, top management, business, and the supporting organizational units, just as well.

The *information system of a company*
is *secure*, if this information system supports the operational security in a measurable and predictable way.

8.1 Using PCUBE-SEC tools in example situations

8.1.1 Cloud

Cloud computing is one of the fashionable challenges nowadays, that triggers all those kind of doubt and fright in the customers, that prevented earlier the extensive use of internet banking. However, as the advances in automatization began facilitating such budget savings, that permitted the financial institutions to offer significant discounts to those customers, that were satisfied with using automatized features instead of the branch office, quite a lot of the people began turning to the internet connection.

What the public is afraid of, and rightly so, it is the dangers of the internet, the leakage of their data. People quite often mistrust both the service providers, and the financial

institutions. Cloud computing involves other kind of threats, besides communication via the internet. Can a remote service be reliable, is its provider able to separate us from its other, possibly careless users? Already the problems of a "simple" outsource case are difficult to handle, without internet connection [Szenes, 2011, Hack.].

To control the security of computers is easier, if their users and we work in the same company, otherwise we need permissions to control their machine, and this is not always cost-effective. We could, of course, distribute firewall clients all around the world, and then the firewall would not let to sign in insecure computers, but this would be a bit too expensive, even if most of the commercial firewalls are able to screen the state of the remote computers. Thus the exact specification of the duties of every participant in an outsource cooperation is even more vital if internet plays any role in a communications flow. The *specifications of obligations, when customer and supplier rely heavily on the reliability of each other*, have to be built very thoroughly, anyway [Szenes, 2010, outsource].

Cloud computing inherits the problems both from the outsource, and from the remote access at the same time, and the list of these problems can not simply be united, the difficulties reinforce each other. On top of stuffing every restriction, that we want to impose upon the service provider, into the contract on the cloud service, the same way, when we outsource a service, we have to choose carefully those parameters, that have to follow dynamically our current needs.

Optimal balance between costs, facilities, and other relevant factors can not be reached without an exact mapping of the business needs and their best possible IT support. Thus, before signing any contracts, the best compromise has to be found. These kind of assessments require the establishment of a mutual understanding between business and IT. To achieve this, is again a task, which is to be assigned to a system analyst.

Using systems analysts' tools it is possible to identify those needs in details, that are arisen by the *strategic goals*, or rather, by their fulfillment. To find these details usually such ready-formulated requirements, as my excellence criteria, come quite handy. Part of these criteria are actually generalizations of security criteria, so this is a relation directed *from governance towards security*.

A possible method is to take the excellence criteria, as one dimension of decision matrices. The systems analysts will be able to build a mapping between business needs and criteria,

and then, lots of different, useful third dimensions can be added. E.g. as a possible third aspect, the tasks, that contribute to the fulfillment of the excellence criteria might be used.

Lots of other variances can be invented, according to the needs of the given situation. Suitable coordinates for such a mapping can be, for example, the excellence criteria, another axis can represent the point of time, to show durations and deadlines, and another axis can correspond to the expectable amount of data. If the business users understand the excellence criteria, then they will be able to decompose them to such "prosaic" - e.g. to IT - characteristics, as bandwidth, percentage of availability, packet loss, checking requirements, and the like.

Exploiting the benefits of the excellence criteria by creating understanding between managers of different business-, and operational areas belongs to the best practice of PCUBE-SEC corporate governance, together with the *weighting* of the necessary level of fulfillment of the criteria. This weighting can then be inherited by those cloud services, that are necessary to achieve the criteria.

Another example can be the strategic-level goal to economize. In this case those security parameters, that can not be omitted, can be identified in the following way. We review the individual services, assign to them their value resulted from the goal & risk management cycle, and draw the matrix of services / security requirements. Those security requirements have to be maintained, that belong to important services, the others can be reconsidered. This way the set of those facilities can be identified, that are absolutely necessary to have. Having this governance support of risk management it would be less difficult to ask budget for all the lot of systems analysts' work it involves.

Every top-level executive will support the thought, that using higher level protection, than necessary, would eliminate the advantages of cloud computing.

It is worth to note, that there are research results, that can be used to refine the matrices I suggest to create. If the data have already been classified according, for example, to the PCUBE-SEC advice on excellence criteria, then "service-specific" security of the cloud computing services can be applied to further granulate the requirements [Chen, et al.]. Excellence criterium confidentiality can be further decomposed, using some of the requirements of Chen and the co-authors, offering an even more sophisticated data protection. They aim at a sparing use of resources, the easier way of using data, and faster data availability, if these data are not defended by complex security mechanisms. What they introduce, is a kind of service-specific security. The life-cycle of the data is split to

three stages: in transition, in process, and in storage. According to these, three security domains are proposed: network, service, and storage. This approach is called as on-demand security architecture.

It is interesting to remember, that a very similar partition had been published for the "lifecycle" of threatened data: in 2006, in the journal of ISACA, data on a storage, in motion, and in use [Ross, 2006].

It must be noted, that the above considerations are very far from covering cloud security problems. Even if we forget our operational generalizations, and restrict ourselves to the IT security of the cloud services, lots of important areas have to be dealt, and with special care. One of them is contracting cloud services. This is a special case of outsourcing, which is a very sensitive contracting problem anyway [Szenes, 2010, outsource].

The definitions of the service provider, e.g. what is meant on an x % of availability, are to be studied thoroughly. Then: what are the tasks of which of the contracting parties in providing for this level of availability? What will happen to the data of the customer after the contracted duration of the contract, and what, if the contract is to be terminated unexpectedly, because of one of the parties?

8.1.2 Data privacy, privacy by design

An important governance aspect, either in the government agencies, or in the private sector, is the necessity of collecting the citizens' or customers' data, or even their profile, for different reasons, challenging, this way, their privacy.

Looking at the European view of this issue from the USA, even our not very fresh 95/46/EC European Data Protection Directive seems to be a desirable regulation [Spiekermann]. However, even over there impressive solution to privacy problem can be noticed, requiring, at the same time, *involvement of systems analysis* in aligning data privacy and the necessary security. This has been invented by Ann Cavoukian, information and privacy commissioner of Ontario [Cavoukian].

She is concerned about the data privacy of customers in commerce, and that of the citizens, in general. Both of these data collectors, either trading companies or government administration, are to be restrained. According to Dr. Cavoukian, *the required privacy settings should be integrated into the information systems already in the systems design phase*. She named this process, as "Privacy by Design" - abbreviated as PbD.

This requirement is completely in tune with my basic requirement concerning application systems development: preliminary planning of the systems, and documenting the state of both the users' and the compliance requirements at every milestone of the *whole life-cycle* of the application [Szenes, 2006, SOA], [Szenes, 2011, Appls.].

All these *prove* again*, that systems analysis* is necessary *for satisfying high-, strategic level aspects.* Following the advice given in this discussion contributes to the *security of the application*. Privacy is one of the most important *business* aspects of data security, thus it is a strategic goal.

8.1.3 "Tighter specs." The importance of the systems analysis in the web revolution

The vital role of systems analysis comes to surface even in the HTML 5 web revolution, which promises to simplify the programmers' work, and to provide for a better cooperation between the physical and programmed products of different suppliers, than before, besides offering, of course, very interesting new features to the users of these products.

According to Gary Anthes, HTML 5 is an "umbrella term", embracing the markup language, and the technologies connected to it [Anthes]. In order to exploit the advantages of this evolution, the developers had to realize, that specifications of better quality are necessary to provide for compatibility between browsers. The need of more detailed - so-called "tighter" - specifications has even been emphasized by such very practical people, as Ian Hickson, software engineer at Google, founder of the Web Hypertext Application Technology Working Group, a complementary standards body of W3C [W3C].

At the first sight, to create such tighter specifications might not exactly seem to suit to those systems analysts, who have dealt with business requirements, instead of technics. However, their skill in exploring users' needs will come handy in creating such a standard, that can be supported by all the browsers, as this requires a capability to *coordinate different* facilities. Collecting the preferences of those vendors and standard groups, who demand more exact specifications will not be a novelty to the experienced colleagues.

The fulfillment of such lower-level, information security requirements, as, e.g. the detailed specification of the input / output of the devices, is necessary to the cooperation between vendors, which is a high-level, strategic goal, To require this specification belongs to two excellence criteria, to efficiency, especially to the pertinency to the given subject, and also to functionality.

These examples show, that experienced systems analysts are needed to set order in the business-, and operational life of the companies.

8.2 Example for PCUBE-SEC knowledge base statements: the IT excellence criteria in clouds

Should anybody attack our cloud successfully, besides possible data leaking, even the service itself can be either refabricated, or made simply unreachable. Reviving some of earlier suggested defense methods, and extending their requirements with criterium order, the following, far from comprehensive, but useful advice could be added to the knowledge base [Szenes, 2011, Hack.].

cloud_service_confidentiality:
network_confidentiality-application_confidentiality - storage_confidentiality.
[see above the on-demand cloud security]

network_confidentiality: network_security - network_maintenance.
network_security:
prot_man_in_the_middle - prot_DDOS - prot_traffic.
[even if using the expressive names makes the knowledge base more readable,
it is important to remind, that
PCUBE-SEC *"knows"* the knowledge base statements and their parts
only to the extent of the explanation to be *found in the database*]

prot_man_in_the_middle: TLS.
prot_man_in_the_middle: IPSEC.
[here the techical details are omitted]

application_confidentiality: application_sec_use - [etc.]
application_sec_use: authorized_use - client_sec.
authorized_use: order_in_ hierarchy - user_education
- intro_of_autho_techniques - [etc.]

[We got to "order" quite soon. Here order_in_hierarchy could be further decomposed by requirements on the organizational pillar. The requirement, that a company should be organized, is of governance level. Security here yielded a strategic-level requirement.]

intro_of_autho_techniques:
org_autho_tech - regul_autho_tech - tech_autho_tech.
[To introduce authorization techniques we need all the three pillars.]

[This is again an illustration for the classificational benefits of my pillars. For example, should we aim at introducing role-based access control, sorting the subjects and executors of the tasks to be done according to the pillars, help in identifying - and also in allocating! - the tasks to be executed.]

org_autho_tech: determine_sec_level_of_appl - [etc.]

The example has shown, how even the building of our PCUBE-SEC knowledge base help us in *collecting and ordering our thoughts* on a given subject.

9. POSSIBLE DIRECTIONS IN THE FUTURE DEVELOPMENTS OF PCUBE-SEC

Improving the knowledge base & problem description

In the future concrete knowledge base receipts derived from everyday practice, or from best practice can be developed [COBIT, COBIT 5, ISO standards].

A future PCUBE-SEC facility can be *taking into consideration the degree of fulfillment of the expectances.*
/1 This information means relations between preliminary specifications, and their results. Feeding it back in such a way, that these expectances could affect the conditions of the fulfillment of a goal, would greatly improve the exactness of the deliverable.
/2 This facility could be useful first in choosing problem-relevant goals. Having found them, the user will then be supported in choosing between these goals. This is also important, as the efforts aimed at fulfilling a given goal might hinder the achievement of others, as we have already mentioned.
/3 To decide such cases will also be supported, when the cost of an effort to reach a goal might be greater, than the cost of not fulfilling it.

Possible future facilities due to the PCUBE base

To describe real-life operational problems, such new kind of dependencies might be described using such PCUBE features, as the process communication "instructions", the time-, and the resource handling.

Constants also might appear in the PCUBE-SEC goals, together with variables in the corresponding places of the knowledge base, just as it had been shown in the PCUBE production secheduling example.

APPENDIX - 25 INDEPENDENT, AND 2 INSIDE REFERENCES TO THE PUBLICATIONS OF THE AUTHOR

[Futó, Szeredi, J., Szenes] Futó, I., Szeredi, J., Szenes, K.: A modelling tool based on mathematical logic – T-PROLOG; Acta Cybernetica, 1981., Szeged, Hungary, p. 363 - 375 references to this publication:

not independent reference No1:

Futó I., Szeredi J.
A Discrete Simulation System Based on Artificial Intelligence Methods, Discrete Simulation and Related Fields, ed. A. Javor, North Holland, Amsterdam, 1982 pp 135-150. (invited paper)

not independent reference No2:

Futo, Ivan, and Janos Szeredi. "System Simulation and Cooperative Problem-solving on a Prolog Basis." Implementations of PROLOG, ed. J.A.Campbell, Ellis Horwood, (1984): 163-174.

independent references to this publication:

T-PROLOG - 1:
Balbin, Isaac, and Koenraad Lecot. "Other Application Areas of Logic Programming." Logic Programming. Springer Netherlands, 1985. 178-218.

[Szenes, 1982] Szenes, K.: An application of a parallel systems planning language in decision support - production scheduling; Procds. of the IFIP W.G. 5.7 Working Conf. APMS (Advances in Production Management Systems), Bordeaux, France, 24 - 27 Aug., 1982. ed.: G. Doumeingts & W. A. Carter, North Holland, 1984., p. 241 - 249

references to this publication:
(an old reference in Computer Abstracts: No. 1827)

+ 6 references:

APMS-1:

Hatvany, J., and F. J. Lettner. "The efficient use of deficient knowledge." CIRP Annals-Manufacturing Technology 32.1 Elsevier (1983): 423-425.

APMS-2:
Tzafestas, Spyros. "Expert Systems in CIM Operations: Key to productivity and quality." Systems Analysis and Simulation I. Springer US, 1988. 378-386.

APMS-3:
Tzafestas, S. G., and G. Tsihrintzis. "ROBBAS: An expert system for choice or robots." Managerial Decision Support Systems and Knowledge-Based Systems (IMACS/IFORS Proc.) North-Holland, Amsterdam (1987).

APMS-4:
Eom, Sean B. "Expert system applications in production and operations management: A selected bibliography (1975–1989)." Expert Systems with Applications 5.1 Elsevier (1992): 167-183.

APMS-5:
Balbin, Isaac, and Koenraad Lecot. "Programming Concepts in Logic Programming." Logic Programming. Springer Netherlands, 1985. 101-119.

APMS-6:
Balbin, Isaac, and Koenraad Lecot. "Logic Programming - A Classified Bibliography" 1985.
WILDGRASS BOOKS Pty Ltd.
289A Smith St., Fitzroy, Victoria 3065, AUSTRALIA
NATIONAL LIBRARY OF AUSTRALIA; CATALOGUING-IN-PUBLICATION
Balbin, Isaax, 1959-Logic programming.
ISBN-13:978-0-908069-15-6 e-ISBN-13:978-94-009-5044-3
DOl: 10.1007/978-94-009-5044-3
APMS: on p. 117

[Szenes, 2010, GRC]: Szenes, K.: "IT GRC versus ? Enterprise GRC but: IT GRC is a Basis of Strategic Governance" EuroCACS 2010 - Conference on Computer Audit, Control and Security Copyright 2010 ISACA, Rolling Meadows, Illinois, USA ; 23-25 March 2010, Budapest, Hungary

references to this publication:

GRC1:
Kilic, N., B. Metin: Importance of Education in Information Technology Governance, Procds. of the 4th IEEE International Symposium on Logistics and Industrial Informatics - LINDI 2012 Sept. 5-7, 2012, Smolenice, Slovakia, E-ISBN: 978-1-4673-4518-7 Print ISBN: 978-1-4673-4520-0 INSPEC Accession Number: 13037502 DOI: 10.1109/LINDI.2012.6319463, p. 65-68

GRC2:
Yildirim, T., B. Metin: Critical information Systems Processes
ISACA Journal, vol. 2, 2014, editor: Information Systems Audit and Control Association, Rolling Meadows, Illinois, USA ©2014 ISACA p. 33-36

[Szenes, 2011, Appls.] Szenes, K.: Supporting Applications Development and Operation Using IT Security and Audit Measures in: e-Informatica Software Engineering Journal, Volume 6, Issue 1, 2012, DOI 10.5277/e-Inf120102, http://www.e-informatyka.pl/wiki/e-Informatica, p. 27–37

references to this publication:

APPLS-1:
Kilic, N., B. Metin: Importance of Education in Information Technology Governance, Procds. of the 4th IEEE International Symposium on Logistics and Industrial Informatics - LINDI 2012 Sept. 5-7, 2012, Smolenice, Slovakia, E-ISBN: 978-1-4673-4518-7 Print ISBN: 978-1-4673-4520-0 INSPEC Accession Number: 13037502 DOI: 10.1109/LINDI.2012.6319463, p. 65-68

APPLS-2:
Schubert T., Póser V., Ács S., Prém D., Márton J., Kozlovszky M.: Számítási felhö biztonsági kérdései; Műszaki Katonai Közlöny, XXII. évfolyam, 2012. 2. szám, ISSN 2063-4986; link:
http://hhk.uni-nke.hu/downloads/kiadvanyok/mkk.uni-nke.hu/pdfanyagok2012szeptember/2012.%202%20szam%20ossz.pdf

APPLS-3:
Otti Csaba, Rónaszéki Péter:
Információbiztonság: az ISO 27001 információbiztonsági irányítási rendszer 1. rész

Detektor Plusz Magazin, Kiadó: Typon International Kft, Budapest, ISSN 1217-9175, 2013/1, 10-11. old.

APPLS-4:
K. Erdélyi: Special factors of development of green software
supporting eco sustainability; in: Procds. of IEEE 11th International Symposium on Intelligent Systems and Informatics SISY 2013; September 26-28, 2013, Subotica, Serbia; ISBN 978-1-4799-0305-4 ©2013 IEEE p. 337-340

[Szenes, 2011, Hack.] Szenes, K.: Enterprise Governance Against Hacking. Procds. of the 3rd IEEE International Symposium on Logistics and Industrial Informatics - LINDI 2011 August 25–27, 2011, Budapest, Hungary, ISBN: 978-1-4577-1840 DOI: 10.1109/LINDI.2011.6031153 © 2011 IEEE, IEEE Catalog Number: CFP1185C-CDR [CD-ROM], http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6026102, p. 229-233

references to this publication:

HACK-1:
Kilic, N., B. Metin: Importance of Education in Information Technology Governance, Procds. of the 4th IEEE International Symposium on Logistics and Industrial Informatics - LINDI 2012 Sept. 5-7, 2012, Smolenice, Slovakia, E-ISBN: 978-1-4673-4518-7 Print ISBN: 978-1-4673-4520-0 INSPEC Accession Number: 13037502 DOI: 10.1109/LINDI.2012.6319463, p. 65-68

HACK-2:
Otti Csaba, Rónaszéki Péter:
Információbiztonság: az ISO 27001 információbiztonsági irányítási rendszer 1. rész
Detektor Plusz Magazin, Kiadó: Typon International Kft, Budapest, ISSN 1217-9175, 2013/1, 10-11. old.

HACK-3:
G. Nagy: An interpretation of the COBIT information criteria to operational criteria of voice controlled Ambient Assisted Living systems, Procds. of the 5th IEEE International Symposium on Logistics and Industrial Informatics, September 5–7, 2013, Wildau, Germany, pp. 49-53

HACK-4:
T. I. Nagy, J. Tick: Self-Organization Issues of Wireless Sensor Networks, Procds. of the 12th IEEE International Symposium on Applied Machine Intelligence and Informatics, Herl'any, Slovakia, January 23-25. 2014., p. 29-33

[Szenes, 2011, Gov.] Szenes, K.: Serving Strategy by Corporate Governance - Case Study: Outsourcing of Operational Activities in: Procds. of 17th International Business Information Management Association - IBIMA November 14-15, 2011, Milan, Italy, ed. Khalid S. Soliman, ISBN: 978-0-9821489-6-9, DOI: 10.5171/2011.903755, indexat BDI: Ebsco © 2011 IBIMA, [CD-ROM], p. 2387-2398

references - to this publication:

IBIMA-1:
Otti Csaba, Rónaszéki Péter:
Információbiztonság: az ISO 27001 információbiztonsági irányítási rendszer 1. rész
Detektor Plusz Magazin, Kiadó: Typon International Kft, Budapest, ISSN 1217-9175, 2013/1, 10-11. old.

IBIMA-2:
Yildirim, T., B. Metin: Critical information Systems Processes
ISACA Journal, vol. 2, 2014, editor: Information Systems Audit and Control Association, Rolling Meadows, Illinois, USA ©2014 ISACA p. 33-36

[Szenes, 2012, MM] Szenes Katalin: Informatikai biztonsági módszerek kiterjesztése a vállalatirányítás, a működés, és a kockázatkezelés támogatására Hungarian - Extending IT security methods to support enterprise management, operations and risk management in: Minőség és Megbízhatóság (Quality and Reliability); publisher: European Organization for Quality (EOQ) Hungarian National Committee
HU ISSN0580-4485 editor: Pal Molnar; XLVI., 2012. / No 5 p. 252-257

references to this publication:

MM-1:
Otti Csaba, Rónaszéki Péter:
Információbiztonság: az ISO 27001 információbiztonsági irányítási rendszer 1. rész
Detektor Plusz Magazin, Kiadó: Typon International Kft, Budapest, ISSN 1217-9175, 2013/1, 10-11. old.

MM-2:
T. I. Nagy, J. Tick: Self-Organization Issues of Wireless Sensor Networks, Procds. of 12th IEEE International Symposium on Applied Machine Intelligence and Informatics, Herl'any, Slovakia, January 23-25. 2014. p. 29-33

[Szenes, 2013, ICCC] K. Szenes: Operational Security - Security Based Corporate Governance in: Procds. of IEEE 9th International Conference on Computational Cybernetics; July 8-10, 2013 Tihany, Hungary; IEEE Catalog Number: CFP13575-USB (pendrive); CFP13575-PRT (printed); ISBN: 978-1-4799-0061-9 (pendrive); 978-1-4799-0060-2 (printed) Copyright @2013 by IEEE. p. 375-378

references to this publication:

ICCC-1:
Póser V., Schubert T., Kozlovszky M., Prém D.: Security On-Demand megoldások az informatikai infrastruktúrákban in Hadmérnök, 2013. VIII. évf. 3. sz., Budapest, 2013, pp. 211-222., ISSN 1788-1919

ICCC-2:
G. Nagy, An interpretation of the COBIT information criteria to operational criteria of voice controlled Ambient Assisted Living systems, in Proc. 5th IEEE International Symposium on Logistics and Industrial Informatics, September 5–7, 2013, Wildau, Germany, pp. 49-53

ICCC-3:
T. I. Nagy, J. Tick: Self-Organization Issues of Wireless Sensor Networks, Procds. of 12th IEEE International Symposium on Applied Machine Intelligence and Informatics, Herl'any, Slovakia, January 23-25. 2014. p. 29-33

[Szenes, 2008, hálózatbiztonság] Szenes, K.: A számítógéphálózatok biztonságának felülvizsgálata
Hungarian - Reviewing the security of computer networks
in: Az Informatikai biztonság kézikönyve, 28. aktualizálás
Verlag Dashöfer, 2008. február, 5.3.1 1. old. - 5.3.1.18. old. - 18 oldal
p. 5.3.1.1. - 5.3.1.18. total: 18 pages

references to this publication:

Hálóbizt.1
Krisztina Erdélyi, "How Information Technology Helps to Mitigate Difficulties Occurred in Teaching Intercultural Groups", 10th IEEE International Conference on Emerging eLearning Technologies and Applications, November 8-9, 2012, StarAA LesnAA, The High Tatras, Slovakia, ISBN 978-1-4673-5122-5/12/$31.00, pp. 95-98 IEEE Catalog Number: CFP1238M-CDR

All together - összesen
T-PROLOG - 1 + 2 belső hivatkozás + APMS- 6 + 2010 GRC- 2 + 2011 Apps- 4 + 2011 Hack - 4 +
+ IBIMA - 2 + MM -2 + ICCC - 3 + 1 Hálózatbiztonság... (Network security...) book chapter

---

25 references +
2 not independent, that is from my former co-authors
(these refer to the publication on T-PROLOG)

References

Publications of the author

I. Book chapters
II. Publications in journals
III. Conference articles
IV. Panels
V. University Doctor Thesis

I. Book chapters - author, co-author, editor & reader
(only those, that are referenced in the dissertation)

[1] [Szenes, 1999, logisztika] Szenes, K.:
Ad-e ötleteket a logisztikai rendszerek auditálásához az informatikai ellenőrzés?
Hungarian - How to audit logistic systems?
in: Logisztikai Évkönyv, 1999.
publisher / kiadó: Magyar Logisztikai Egyesület, MagICS Holding, 121-127

The following chapters appeared in: Information Security Handbook
- Az Informatikai biztonság kézikönyve,
publisher: Verlag Dashöfer, Budapest, Hungary, ISBN: 963 9313 122
new materials to this book are published quarterly
I had been the editor and reader of this book in 2006-2012

The references to this book is *abbreviated* in the followings, as:
Verlag Dashöfer

[2] [Szenes, 2006, COBIT] Szenes, K:
Az ISACA auditálási alapelvei, és a COBIT® módszertan bemutatása
Hungarian - An introduction to the audit basics of ISACA and to methodology COBIT
in: Az Informatikai biztonság kézikönyve, 21. aktualizálás
Verlag Dashöfer, 2006. augusztus, 7.2.1. old. - 7.2.83. old. - 83 oldal
p. 7.2.1.- 7.2.83. total: 83 pages

[3] [Szenes, 2006, SOX] Szenes, K.: Informatikai biztonsági megfontolások a Sarbanes - Oxley törvény ürügyén

(A 2002-es Sarbanes - Oxley törvény hatásai az informatikai biztonsági rendszerekre és az informatikai ellenőrök feladataira. A jelentésszolgálat és a többi kulcsfontosságú alkalmazás felügyeletének kérdései)
Hungarian - IT security considerations triggered by SOX
in: Az Informatikai biztonság kézikönyve, 22. aktualizálás
Verlag Dashöfer, 2006. október, 2.2.1.1. old. - 2.2.8.8. old. - 96 oldal
p. 2.2.1.1. - 2.2.8.8. total: 96 pages

[4] [Szenes, 2007, SOA] Szenes, K.: A szolgáltatás - orientált architektúrák biztonsági kérdései
Hungarian - On the security of service-oriented architectures
in: Az Informatikai biztonság kézikönyve, 23. aktualizálás
Verlag Dashöfer, 2006. december, 2.5.1.1 old. - 2.5.14.14 old. - 134 oldal
p. 2.5.1.1. - 2.5.14.14. total: 134 pages

[5] [Szenes, 2007, COBIT] Szenes, K: A COBIT 4.0 és 4.1 újdonságai
Hungarian - Novelties in COBIT 4.0 and 4.1
in: Az Informatikai biztonság kézikönyve, 27. aktualizálás
Verlag Dashöfer, 2007. november, 7.3 1. old. - 7-3 64. old. - 54 oldal
p. 7.3 1. - 7.3.64. total: 54 pages

[6] [Szenes, 2008, hálózatbiztonság] Szenes, K.: A számítógéphálózatok biztonságának felülvizsgálata
Hungarian - Reviewing the security of computer networks
in: Az Informatikai biztonság kézikönyve, 28. aktualizálás
Verlag Dashöfer, 2008. február, 5.3.1 1. old. - 5.3.1.18. old. - 18 oldal
p. 5.3.1.1. - 5.3.1.18. total: 18 pages

[7] [Szenes, 2009, risk] Szenes, K.:
Kockázatkezelés szempontrendszerrel irányított értékelési módszerrel
Hungarian - Classification systems based evaluation in risk management
in: Az Informatikai biztonság kézikönyve, 32. aktualizálás
Verlag Dashöfer, 2009. február, 8.6.1. old. - 8.6.5.2.2.6 old. - 62 oldal
p. 8.6.1. old. - 8.6.5.2.2.6 total: 62 pages

[8] [Szenes, 2009, törvények] Szenes, K.:
Az informatikai biztonsággal kapcsolatos törvényekről és rendeletekről
Hungarian - On the Hungarian laws and regulations dealing with IT security

in: Az Informatikai biztonság kézikönyve, 33. aktualizálás
Verlag Dashöfer, 2009. május, 3.4.1. old. - 3.4.34. old. - 34 oldal
p. 3.4.1. - 3.4.34. total: 34 pages

[9] [Reusz, Höltz, Szenes, 2009, naplózás]:
Reusz, G, Höltz, P., Szenes, K.:
Adatfeldolgozási és biztonsági események naplózása
Hungarian - Logging data processing and security events
in: Az Informatikai biztonság kézikönyve, 34. aktualizálás
Verlag Dashöfer, 2009. szeptember, 4.3.1. old. - 4.3.4.4. old. - 32 oldal
p. 4.3.1. - 4.3.4.4. total: 32 pages

[10] [Szenes, 2010, outsource] Szenes, K.:
Az informatikai erőforrás-kihelyezés auditálási szempontjai, I., II. rész
Hungarian - Auditing outsourcing of IT resources, Part I., Part II.
in: Az Informatikai biztonság kézikönyve, Verlag Dashöfer,
I. rész: 36. aktualizálás, 2010. február, 8.10. 1. old. – 26. old. (26 oldal),
II. rész: 39. aktualizálás, 2010. december 8.10. 27. old. – 158. old. (132 oldal)
(összesen 158 oldal)
Part I. 36. aktualizálás, 2010. február, p. 8.10. 1. – 26. total: 26 pages,
Part II. 39. aktualizálás, 2010. december p. 8.10. 27. – 158. total: 132 pages
Part I.-II. total 158 pages

II. Publications in journals

[11] [Futó, Szeredi, J., Szenes] Futó, I., Szeredi, J., Szenes, K.: A modelling tool based on mathematical logic – T-PROLOG; Acta Cybernetica, 1981., Szeged, Hungary, p. 363 - 375

[12] [Szenes, 1985] Szenes, K.: A mesterséges intelligencia kutatás egyes módszereinek alkalmazása folyamatrendszerek modellezésében
Hungarian - On the application of AI research methods in modelling process systems
Felügyelet nélküli gyártás Szeminárium, Kecskemét
J. Automatizálás (PRODINFORM) vol. XIX., No. 8., 1985. Aug., p. 28 - 30,

(also available in the proceedings of the conference:
Felügyelet nélküli gyártás Szeminárium,
Kecskemét, 1985. okt. 17-18, p. 331 - 340)

[13] [Szenes, 2000] Szenes, K.: Az informatikai audit felhasználási területei
Hungarian - On the application areas of IT audit
Loginfo, 2000/2. szám, kiadó: Magyar Logisztikai Egyesület, p. 20

[14] [Szenes, 2011, Appls.] Szenes, K.:
Supporting Applications Development and Operation Using IT Security and Audit Measures
in: e-Informatica Software Engineering Journal, Volume 6, Issue 1, 2012, DOI 10.5277/e-Inf120102, http://www.e-informatyka.pl/wiki/e-Informatica, p. 27–37
Scopus: 84885130511

[15] [Szenes, 2012, MM] Szenes Katalin: Informatikai biztonsági módszerek kiterjesztése a vállalatirányítás, a működés, és a kockázatkezelés támogatására
Hungarian - Extending IT security methods to support enterprise management, operations and risk management
in: Minőség és Megbízhatóság (Quality and Reliability);
publisher:
European Organization for Quality (EOQ) Hungarian National Committee
HU ISSN0580-4485 editor: Pal Molnar
XLVI., 2012. / No 5 p. 252-257

Minőség és Megbízhatóság; nemzeti minőségpolitikai szakfolyóirat
kiadja: az European Organization for Quality (EOQ) Magyar Nemzeti Bizottsága
alapítási nyilvt.sz.: B/SZI/1993. HU ISSN0580-4485
a kiadásért felel: dr. Molnár Pál, az EOQ MNB elnöke
XLVI. évf. 2012. / 5. sz., p. 252-257

III. Conference articles

[16] [Szenes, 1982] Szenes, K.: An application of a parallel systems planning language in decision support - production scheduling
Procds. of the IFIP W.G. 5.7 Working Conf. APMS
(Advances in Production Management Systems), Bordeaux, France,
24 - 27 Aug., 1982. ed.: G. Doumeingts & W. A. Carter, North Holland,
1984, p. 241 - 249
reference in Computer Abstracts: No. 1827

[17] [Szenes, 1983] Szenes, K.: A comparison of the traditional and a new principle way of parallel systems description, simulation and planning,
Procds. of the 8th Winterschool on Operating Systems,
Visegrad, Hungary, 31 Jan.- 4 Feb., 1983

[18] [Szenes, 1987] Szenes, K.: PCUBE - an AI system for planning process systems;
Procds. of the 5th Symp. on Microcomputer and Microprocessor Applications, Budapest, Hungary,
29. Sept. - 1. Oct., 1987., ed.: OMIKK-TECHOINFORM, p. 551-562

[19] [Szenes, 1988] Szenes, K.: Planning the activity schedule of process systems by the means of an AI based system
Procds. of the 27th International MATADOR Conf., 20-21. Apr., 1988.,
Manchester,
ed.: B. J. Davies, UMIST, MACMILLAN Education Ltd.,1988., p. 139 - 144

[20] [Szenes, 1998, IT audit] Szenes,K.:
Informatikai rendszerek ellenőrzése és auditálása
Hungarian - Auditing and supervising IT systems
V. Vállalati Informatika Konferencia, Siófok, 1998. szeptember, p. 130-137

[21] [Szenes, Forró, 1989] Szenes, K., Forró, P.: Implementing the base level of a process maintenance system in FORTH
Procds. of the 6th Symp. on Microcomputer and Microprocessor Applications,
Budapest, Hungary, 17-19. Oct., 1989.,
ed.: Scientific Society for Telecommunication, Budapest, Hungary, p. 65-74

[22] [Szenes, 1999] Szenes, K.:
Informatikai biztonsági rendszer és ellenőrzése nagyvállalati környezetben
Hungarian - Auditing and supervising corporate IT security systems
VI. Vállalati Informatika Konferencia, Siófok, 1999. szeptember, p. 171-174

[23] [Szenes, 2006, SOA] Szenes, K.: On the Intelligent and Secure Scheduling of Web Services in Service Oriented Architectures - SOAs
Procds. of the 7th International Symposium of Hungarian Researchers on Computational Intelligence
Budapest, Hungary, 24-25 November, 2006, p. 473-482

[24] [Szenes, 2011, Hack.] Szenes, K.:
Enterprise Governance Against Hacking. Procds. of the 3rd IEEE International Symposium on Logistics and Industrial Informatics - LINDI 2011 August 25–27, 2011, Budapest, Hungary, ISBN: 978-1-4577-1840
DOI: 10.1109/LINDI.2011.6031153 © 2011 IEEE,
IEEE Catalog Number: CFP1185C-CDR [CD-ROM],
http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=6026102,
p. 229-233
Scopus: 80555154910

[25] [Szenes, 2011, Gov.] Szenes, K.:
Serving Strategy by Corporate Governance - Case Study: Outsourcing of Operational Activities
Procds. of 17th International Business Information Management Association - IBIMA November 14-15, 2011, Milan, Italy, ed. Khalid S. Soliman, ISBN: 978-0-9821489-6-9, DOI: 10.5171/2011.903755, indexat BDI: Ebsco © 2011 IBIMA, [CD-ROM], p. 2387-2398

[26] [Szenes, 2013, ICCC] K. Szenes: Operational Security - Security Based Corporate Governance
in: Procds. of IEEE 9th International Conference on Computational Cybernetics (ICCC); July 8-10, 2013 Tihany, Hungary
IEEE Catalog Number: CFP13575-USB (pendrive); CFP13575-PRT (printed)
ISBN: 978-1-4799-0061-9 (pendrive); 978-1-4799-0060-2 (printed)
Copyright @2013 by IEEE. p. 375-378
Scopus: 848868396260

IV. Panels

[27] [Szenes, 2002, risk] Szenes, K.: Building a Corporate Risk Management Methodology and Practice
EuroCACS 2002 - Conf. for IS Audit, Control and Security
Copyright 2002 ISACA, Rolling Meadows, Illinois, USA
24-27 March 2002, Budapest, Hungary

[28] Szenes, K.: Prevention of Fraud in Financial Institutions and in Other Corporations in Hungary
panel, ISSE (Independent European ICT Security Conference and Exhibition), Budapest, Hungary, 27-29 September, 2005

[29] [Szenes, 2010, GRC]: Szenes, K.:
"IT GRC versus ? Enterprise GRC
but: IT GRC is a Basis of Strategic Governance"
EuroCACS 2010 - Conference on Computer Audit, Control and Security
Copyright 2010 ISACA, Rolling Meadows, Illinois, USA
23-25 March 2010, Budapest, Hungary

V. University Doctor Thesis at the University Eotvos Lorand, Budapest, Hungary, Faculty Natural Sciences, Specialty: Mathematics:
[30] [Szenes, 1976-77] Szenes, K.:
Automatikus progamgenerálás és robotvezérlés a rezolúció elve alapján
Hungarian - Automatic program generation and robot control based on the resolution principle

Referenced publications of other authors

Abbreviation:

The frequently used:
editor: Information Systems Audit and Control Association
Rolling Meadows, Illinois, USA, © ISACA

will be abbreviated as: "editor: ISACA"

Note on the journal of ISACA:

the present title of the journal is: ISACA Journal

the former title had been:
IS Control Journal (Information Systems Control Journal)

[Anthes] Anthes, G.: HTML 5 Leads a Web Revolution

Communications of the ACM, July 2012, Vol. 55 No 7, p. 16-17

[1] [Belak et al.] Belak, J., Milfelner, B.: "Informal and Formal Institutional Measures of Business Ethics Implementation at Different Stages of Enterprise Life Cycle", Acta Polytechnica Hungarica, Journal of Applied Sciences, Hungary, Vol. 8, No. 1, 2011, p. 105-122

[2] [ISACA-BMIS, 2009] An Introduction to the Business Model for Information Security
Copyright © ISACA 2009, editor: ISACA

[3] [ISACA-BMIS, 2010] The Business Model for Information Security
Copyright © ISACA 2010, editor: ISACA

[4] [Cavoukian]
http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/
last visited: 3rd Sept., 2012

[5] [Chapela, 2011] Chapela, V.: Tips for Managing Intentional Risk
http://www.isaca.org/About-ISACA/-ISACA-Newsletter/Pages/at-ISACA-Volume-11-25-May-2011.aspx#2
last visited: 4th April, 2012 published: 25 May, 2011

[6] [Chen, et al.] Chen, J., Wang, J., Wang, X.: On-demand Security Architecture for Cloud Computing
Computer, July 2012, IEEE Computer Society, p. 73-78

[7] [COBIT 1998] COBIT Executive Summary
April 1998 2nd Edition
Released by the COBIT Steering Committee and the Information Systems Audit and Control Foundation, editor: ISACA

[8] [COBIT 2000] COBIT® 3rd Edition, July 2000
Released by the COBIT Steering Committee and the IT Governance Institute™
editor: ISACA

[9] [COBIT 4.0, 2005] COBIT® 4.0
Control Objectives, Management Guidelines, Maturity Models
Copyright © IT Governance Institute® , 2005

editor: ISACA

[10] [COBIT Map] COBIT Mapping
Overview of International IT Guidance, 2nd Edition
Copyright © IT Governance Institute®, 2006
editor: ISACA

[11] [COBIT 4.1, 2007] COBIT® 4.1
Framework, Management Guidelines, Maturity Models
Copyright © IT Governance Institute® , 2007
editor: ISACA

I have been member of SME - Subject Matter Experts to review the results of the COBIT 5 from 2010; having contributed to the review of the following two working papers:

[12] [COBIT 5, 2010]
COBIT® 5 Design Paper Exposure Draft
© 2010 ISACA, working paper

[13] [COBIT 5, 2011]
COBIT 5.0 Vol. I – The Framework" and "COBIT 5.0 Vol. IIa – Process Reference Guide
© 2011 ISACA, working paper

[14] [COBIT 5, 2012]
Enabling Processes - COBIT 5 An ISACA Framework
Copyright © 2012 ISACA. All rights reserved. For usage guidelines, see www.isaca.org/COBITuse
(As an Expert Reviewer of the Subject Matter Expert Team of ISACA COBIT 5
I had participated in the COBIT 5 effort in 2010 - 2011
my name in the list "Expert Reviewer", on p. 5)

[15] [COSO] http://www.coso.org
last visited: 20th December 2012

[16] [CRM] 1998 - 2014 CISA Review Technical Information Manual
published yearly
editor: ISACA

(from the year of 1999 Katalin Szenes contributes to the Manual as a member of the Quality Assurance Team, with the exception of CRM 2011
mostly to the chapters Protection of information assets, and Business continuity planning; Manual 2014 is under edition)

[18] [Dahl, et al., SIMULA 67] Dahl, J., Myhrhaug, B., Nygaard, K.: SIMULA 67 Common Base Language; Norwegian Computing Centre, Oslo, Norway, 1970

[19] [Forro] Forro, P.:
The IBM PC implementation of a list processing language in FORTH - Hungarian
Diplom Thesis, Technical University, Budapest, 1987.

[20] [Guldentops] Guldentops, E.:
Where Have All the Control Objectives Gone? They Have Picked Them Every One...
ISACA Journal Vol. 4, 2011, © 2012 ISACA
editor: ISACA, p. 1-4

[21] [Hansen] Hansen, P. B.: The architecture of concurrent programs
Prentice Hall, Englewood Cliffs, New Jersey, 1977

[22] [Hoare] Hoare, C. A. R.: Communicating sequential processes
Comm. of the ACM, Vol. 21, No. 8. Aug. 1978. 666-671

[23] [ISACA] http://www.isaca.org
last visited: 20th December 2012

[24] [Hungarian ISACA Chapter] http://www.isacahu.com
last visited: 20th December 2012

[25] [ISO 12207] Magyar Szabvány MSZ ISO/IEC 12207:2000
Informatika. Szoftveréletciklus-folyamatok
Hungarian version of the ISO/IEC 12207:1995
Information technology. Software life cycle processes

[26] [ISO 27000] International Standard ISO/IEC 27000 First edition 2009-05-01
Information technology — Security techniques — Information security management systems — Overview and vocabulary
Reference number: ISO/IEC 27000:2009(E)

[27] [ISO G73] ISO Guide 73:2009 (E/F) - First edition 2009 Première édition 2009
Risk management — Vocabulary
Management du risque — Vocabulaire
© ISO 2009

[28] [ISO 17799] International Standard ISO/IEC 17799 First edition 2000-12-01
Information technology — Code of practice for information security management
Reference number: ISO/IEC 17799:2000(E)
Copyright © ISO/IEC 2000

the new versions of 17799 are ISO 27001 és 27002:

[29] [ISO 27001] International Standard ISO/IEC 27001 First edition 2005-10-15
Information technology - Security techniques - Information security management systems - Requirements
Reference number: ISO/IEC 27001:2005 (E)
Copyright © ISO/IEC 2005

[30] [ISO 27002] International Standard ISO/IEC 17799 First edition 2005-06-15
Information technology — Security techniques — Code of practice for information security management
Reference number: ISO/IEC 27002:2005(E)
Copyright © ISO/IEC 2005

[31] [ISO 27005] International Standard First edition 2008-06-15
Information technology — Security techniques — Information security risk management
Reference number: ISO/IEC 27005:2008(E)
Copyright © ISO/IEC 2008

[32] [ISO 38500] International Standard First edition 2008-06-01
Corporate governance of information technology
Gouvernance des technologies de l'information par l'entreprise
Reference number: ISO/IEC 38500:2008(E)
Copyright © ISO/IEC 2008

[33] [ITGI] http://www.itgi.org

last visited: 20th December 2012

[34] [ITGI, Roundtable] an excerpt based on content provided by ITGI (IT Governance Institute) for reprint:
IT Governance Roundtable: Brisbane September 2008
ISACA Journal, Vol. 3, 2009
editor: ISACA, p. 25-26

[35] [ITGI - SOX - 2006]
IT Control Objectives for Sarbanes-Oxley, 2nd Edition (Exposure Draft)
The Importance of IT in the Design, Implementation and Sustainability of Internal Control over Financial Reporting and Disclosure
Copyright © 2006 IT Governance Institute

[36] [Kowalski] R. Kowalski: Predicate logic as a programming language
Memo No. 70, University of Edinborough, November, 1973

[37] [LNCS 54, 1977] Design and Implementation of Programming Languages
Procd. of a DoD Sponsored Workshop, Ithaca, Oct., 1976
Lecture Notes in Computer Science, No. 54.
ed.: G. Goos and J. Hartmanis
Springer-Verlag, Berlin Heidelberg New York, 1977
(DoD is the abbreviation of Department of Defense)

[38] [Melancon] Melancon, D.: Security Controls That Work
IS Control Journal, Vol. 4, 2007
editor: ISACA, p. 29-32

[39] [G. Nagy] G. Nagy: „An interpretation of the COBIT information criteria to operational criteria of voice controlled Ambient Assisted Living systems," in Proc. 5th IEEE International Symposium on Logistics and Industrial Informatics, September 5–7, 2013, Wildau, Germany, p. 49-53.

[40] [T. I. Nagy, J. Tick] T. I. Nagy, J. Tick: Self-Organization Issues of Wireless Sensor Networks, Procds. of the 12th IEEE International Symposium on Applied Machine Intelligence and Informatics (SAMI), Herl'any, Slovakia, January 23-25. 2014, p. 29-33.

[41] [OECD IFC 2004]

International Corporate Governance Meeting
Morning Session: Corporate Governance – A Working Definition
Teresa Barger, Director, IFC/ World Bank Corporate Governance Department
Hanoi, Vietnam, December 6, 2004
© OECD 2004
http://www.oecd.org/dataoecd/18/47/34080477.pdf
last visited: 13th June 2012
OECD: Organisation for Economic Cooperation & Development
IFC: International Finance Corporation

[42] [OECD study] OECD Principles of Corporate Governance
2004, © OECD, 2004
http://www.oecd.org/dataoecd/32/18/31557724.pdf
last visited: 13th June 2012

[43] [Oyemade, 2012] Oyemade, R.: Effective IT Governance Through the Three Lines of Defense, Risk IT and COBIT
ISACA Journal, Vol. 1, 2012
editor: ISACA, p. 24-29

[44] [Palossy, Tempfli] Palossy, L., Tempfli, L.:
The IBM PC implementation of the expert system PCUBE in C
Diplom Thesis, University of Natural Sciences "Eotvos Lorand", Budapest, 1993

[45] [Rameshkumar, 2010] Rameshkumar, A. V.: Looking at IT Risk Differently
ISACA Journal, 2010 Vol. 1
editor: ISACA, p. 42-51

[46] [Ross, 2006] Ross, S. J.: Falling Off the Truck
Journal Information Systems Control (later: ISACA Journal), 2006 Vol. 3
editor: ISACA, p. 9-10

[47] [Ross, 2009, risk] Ross, S.J.: Gang Aft Agley
ISACA Journal, 2009 Vol. 2
editor: ISACA, p. 9-10
("Gang Aft Agley"
- citation from a poem, and according to Ross, it means: go awry)

[48] [Spiekermann] Spiekermann, S.:The Challenges of Privacy by Design
Communications of the ACM, July, 2012, vol.55 p. 38-40

[49] [Szeredi, P., Futo]: Szeredi, P., Futo, I.: PROLOG Kézikönyv
(PROLOG Reference Manual - Hungarian),
Journal Számológép, No 3, 4; editor: NIMIGÜSZI, Budapest, 1977.

[50] [Warren]: Warren, D. H. D.: WARPLAN: A system for generating plans DCL Memo 76, Dept. of Artificial Intelligence, University of Edinburgh, Scotland, 1974

[51] [w3c] World Wide Web Consortium, http://www.w3.org/Consortium/
(2014. január)