Summer 2021

An Extended Analysis of Risk Management Concepts in IT Management Frameworks

Maksim Goman

An Extended Analysis of Risk Management Concepts in IT Management Frameworks

Maksim Goman
Johannes Kepler University Linz, Austria
maksim.goman@jku.at

Abstract

This paper analyzes risk concepts and risk assessment practices in modern IT management frameworks. We evaluate consistency and suitability of their methods for practical business decision-making using system analysis method. The objective is to determine fundamental logical flaws in regard to risk management in well-known IT control frameworks, and this can help to identify how to fix them. It turned out that examined frameworks can produce highly doubtful output of risk assessment in both substantial meaning and significance for decision-making.

Keywords: IT management, risk assessment, security risk, IT control framework

1. Introduction

IT risk management (RM) is a central topic of every IT control framework. For efficient management, any risk should have an exposed stakeholder and uncertainty about the circumstances of decision-making (DM) (Goman, 2018). The decisions aim at achieving specific predetermined goals. Uncertainty, i.e. lack of complete certainty or knowledge (Hubbard, 2014), is a natural feature of decision circumstance in management. Uncertainties can be different: imprecise information about threats or competitors, unclear perspectives of a technology, absence of certain technological skills, resources deficit, unstable business environment, inaccurate estimations and foundational models in general, lack of internal control (may not be recognized), improper organization structure, etc.

It seems that an intuitive course of action for a practitioner in respect of IT RM is to adhere to existing IT risk control methodologies from known IT management frameworks. Such frameworks are also called “best practices”, meaning “a proven activity or process that has been successfully used by multiple enterprises and has been shown to produce reliable results” (ISACA, 2012). Existence of multiple “good practices” means that their user is self-accountable for proper choice of the “best practice” and proper realization of its lower level techniques.

An interested reader grasps that the most known frameworks like IT Infrastructure Library (ITIL) (TSO, 2011) or Control Objectives for Information and related Technology (COBIT) (ISACA, 2012), consider IT RM as an important issue. However, their methods of risk analysis for IT function or enterprise level control are limited. An apparent question is whether they have a feedback control? That is, is there a measure of how well a “best practice” that works well “most of the time” behaves in a given company with specific environment “most of the time”? Hubbard (2009) formulated it as a risk paradox: The higher abstraction level of management, the less risk analysis is employed on regular basis and the simpler methods are used. Moreover, it is routinely taken for granted to evaluate business and technical risks with qualitative methods and scales. Quantitative methods of risk analysis are not even well referenced in frameworks COBIT and ISO 27000.

The primary goal of the paper is to highlight fundamental problems with reference to RM that popular IT related frameworks have. That can enable to propose directions for improvement to risk control practices in the future. Systems approach, observation and generalization are used to decide on consistency and validity of framework's vision towards IT RM. As a secondary objective, we call for debate on the modern problems of risk analysis in IT and business control. We analyze four aspects of IT RM in each framework. As the frameworks support specific parts of business management (projects, security, higher benefits through better services, strategic competitiveness, etc.), these four aspects should be coherent within each framework and serve the goal of risk control in a company. The four aspects were chosen following Goman (2019):

- Concept of risk, i.e. the very definition of the subject of control;
- Methods of risk measurement and assessment. Wherever possible, methods or algorithms should be provided for measurement;
- Relation between IT and business risk. Each framework promotes IT to business connection. Therefore, risk analysts and managers on the lower IT level should understand the connectivity of IT risk to the higher level business risks; and
- Criteria of IT RM effectiveness (related to overall corporate risk change) and special aspects of its evaluation in the risk control process or higher-level management processes. This is interesting because all standards under review consider RM as a stabilized process with a feedback.

The paper is organized as follows: A review of conditions of today's high-level IT RM principles is given in Section 2. Risk terminology and classification issues are considered in Section 3. Analysis of frameworks in the context of the four aspects is carried out in Section 4. The final section concludes the paper.

2. Background of RM in IT Control Frameworks

Our focus in frameworks for this paper is on their concept of risk and risk methodology. Publications on IT management usually employ a single pattern regarding RM. They provide a system of practical advice or heuristics based on common sense or practical experience including certain assumptions. Customarily, no proofs of effectiveness or empirical success rate is provided, including effectiveness of risk analysis practices. IT management frameworks aggregate the information from the relevant body of knowledge, so we consider them as an established source of RM guidance for IT management.

As a brief summary, the definitions of IT risk concepts are not critically reevaluated; methodology is considered completed, proven, and unanimously understood; and any referred methods as reliable. The main goal of the books and frameworks in the area is to give solutions to certain typical problematic IT control scenarios or situations, and to perform exploratory and empirical risk analysis. IT risk is considered as mainly operational risk: only losses from inadequate or failed internal processes and systems, and human errors are assumed under operational risk. Accordingly, IT risk is referred to in a typical information security (IS) interpretation as "any threat to the integrity, confidentiality, or availability of data or IT assets" (Betz, 2011), i.e., a threat to IT assets, not to business. Nevertheless, impact to business presents in frameworks to some extent starting from purely IS objectives (e.g. prevention of unauthorized enterprise information access or its loss, etc.) (ISO, 2011) up to the goal of full-scale business support in the IT governance domain (ISACA, 2012).

There is no need to cite papers and books that agree on rules from frameworks like COBIT. Our objective is to analyze the underlying rules. The reader is referred to the couple of

examples of independent analysis, namely Betz (2011) reveals problems with process approach in ITIL (TSO, 2011), and Hubbard (2009) that criticizes modern management practices towards risk management. The latter author devoted another book to problems of IS risk analysis (Hubbard, 2016).

Insufficient data about the scale of practical application of any IT RM methodology may indicate that its effectiveness for IT risk evaluation was not proven. On the other hand, there is no proof in the IT frameworks that their methods shall produce accurate and repeatable result. They give no references to external sources with such information. Besides, the reviewed frameworks do not consider validation of its methods of risk assessment as well as verification of results obtained with the analysis.

3. Importance of Risk Concept and Classification

Definition of risk drastically differs in frameworks. Sometimes it is derived from one another (e.g. in (ISO, 2011; ISACA, 2012)). Each framework has risk treatment measures and control metrics. However, no evaluation of effectiveness of proposed measures or references to it are supplied. But the problem of measurement of risk level change after risk treatment as per framework's guidance is important in accordance with system approach. This is a feedback control in the RM activity. This control depends on risk definition and helps to assure RM effectiveness. Should frameworks have very different risk definitions, how can we assure that the feedback controls are compatible and appropriate?

We found that papers (Holton, 2004) (about philosophical basics) and (Goman, 2018) (about generic IT risk definition) are vital for understanding the nature of the risk concept. We believe that a consistent risk definition for IT RM is Goman (2018): "Risk is a state of uncertainty, such that there is a possibility that involves loss or other undesirable outcome for an exposed actor". Put it otherwise, risk is a *condition* when an actor is exposed to a problem and uncertain about its consequences.

Risk is usually categorized. Most of classifications include market, business, operational, strategic, reputation risks. Each framework applies a different approach to risk categorization and classification. This classification is subjective (i.e., performed by an expert) and not unique. Risks may belong to several classes. We found neither comprehensive database nor uniform scheme for such a database of IT risk classes and their business effects.

Some frameworks, e.g. COBIT, assume that IT risks are connected to non-operational business risks. But in most cases, the regulations and frameworks suppose that technology is a source of only operational risk. Legal regulations, like Sarbanes-Oxley Act and Basel Advanced measurement approach, include minor statements on IT risk control in their scope. Nevertheless, some IT great failures that originate from errors in business DM, in IT governance or failures in strategic technology implementation, mean strategic business risk (see example in (Goldstein et al., 2008; Nelson, 2005; Nelson, 2007; Widman, 2008)).

System approach tells us that legal and other non-operational risks can emerge from IT risk realizations together with them or following them as a consequence of a common mode failure. IT project failures can be spectacular too (Nelson, 2005; Nelson, 2007). While the losses can originate from operational failures, they can have eventually strategic outcomes. Such cases were revealed during our own work in IT audit and risk analysis. Because a company is a large system of sub-systems, even seemingly operational decisions on technology change may reveal

strategic influence due to its high importance for business change. Such decisions can fall into several risk categories. For instance, in (Goldstein et al., 2008), operational IT faults were not only IT concern, but were cases of business risk. Likewise, the mean loss seems large for any type of risk event classes in (Goldstein et al., 2008).

Furthermore, according to popular frameworks, threats, assets, vulnerabilities, impacts, existing controls, actors, scenarios, etc. are classified and documented. Risk registers should be maintained. For example, risk classification is a part of risk assessment task of repeatable Deming's IS RM process (ISO, 2011): Context establishment, Risk assessment, Risk treatment, Risk acceptance. This is applied for every known risk and is well documented. Someone should do that continuously. Analyst's imagination can conceive an almost infinite number of risk scenarios taking into consideration operational risk, IT complexity, and human actors in a business or IT process. An addition of a single change in asset or threat registers produces exponential growth of analysis overhead and the need of register maintenance. What resources does a large corporation having business in highly volatile business environment need for that? Some frameworks (e.g. COBIT (ISACA, 2014)) admit that, and recommend to restrict the number of artifacts in registers and the number of scenarios for them, but without details of how to differentiate between a critical scenario and one that is not worth consideration.

RM based on risk classification requires resources and creates management overhead. It helps to understand the firm, its problems, details of risky decisions, actors, ambiance, etc. How can we make it effectively? Which constraints should one apply to threats, assets, vulnerabilities, and their myriad combinations to have manageable registers? Frameworks do not provide a single answer.

4. Analysis

The following frameworks were studied: COBIT 5 (ISACA, 2012, 2013, 2014;), COBIT 2019 (ISACA, 2018a, 2018b), ITIL v.3 (TSO, 2011), ITIL v.4 (AXELOS, 2019), PMBOK 5th ed. (PMI, 2013), PMBOK 6th ed. (PMI, 2017), ISO 31000 (ISO, 2009a, 2009b), ISO 27005 (ISO, 2011), and NIST Special Publication 800-30 Revision 1 (NIST) (NIST, 2012). These frameworks were available to us.

Concepts of risk are very different in the frameworks (some have several distinct definitions). Results of risk concept analysis are summarized below:

1. COBIT: Risk is
   a) "the combination of the probability of an event and its consequence" (ISACA, 2012);
   b) "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" (ISACA, 2013);
   c) "the potential of business objectives not being met" (ISACA, 2013);
   d) Business risk is "a probable situation with uncertain frequency and magnitude of loss (or gain)" (ISACA, 2012);
   e) IT risk is "a business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise" (Goldstein et al., 2008).
2. ITIL: Risk is
   a) "a possible event that could cause harm or loss, or affect the ability to achieve objectives. A risk is measured by the probability of a threat, the vulnerability of the asset to that threat, and the impact it would have if it occurred" (TSO, 2011);
   b) "a possible event that could cause harm or loss, or make it more difficult to achieve objectives. Can also be defined as uncertainty of outcome, and can be used in the

context of measuring the probability of positive outcomes as well as negative outcomes" (AXELOS, 2019).

3. PMBOK:
   a) "Project risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives such as scope, schedule, cost, and quality" (PMI, 2013);
   b) "Individual project risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on one or more project objectives." (PMI, 2017) (this is also a definition of risk in the PMI glossary);
   c) "Overall project risk is the effect of uncertainty on the project as a whole, arising from all sources of uncertainty including individual risks, representing the exposure of stakeholders to the implications of variations in project outcome, both positive and negative" (PMI, 2017);
   d) "Secondary Risk. A risk that arises as a direct result of implementing a risk response" (PMI, 2017).
4. ISO 27005:2011 (ISO, 2011), ISO 31000:2009 (ISO, 2009a): Risk is:
   a) "an effect of uncertainty on objectives";
   b) "a combination of the probability of an event ... and its consequence";
   c) Information security risk is "potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to the organization".
5. NIST (NIST, 2012): "Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence." "Information security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts ...".

Each framework connects IT risk to business risk in some way. Proposed measures of RM effectiveness always presume analysis by some external party to RM or DM process with certain time delay. In this way, RM problems would be revealed with latency and their communication can be delayed. The measures can be as vague as "maturity levels" in COBIT, post-analysis of risk methodology by audit or "lessons learned" activity in PMBOK. ITIL has no explicit position in this regard and refers to other frameworks.

All the frameworks considered advise application of subjective ordinal scores as *numerical scales* for risk analysis and give examples. Methods of risk measurement and assessment in the frameworks are the following:

- COBIT 5 (ISACA, 2012): qualitative risk analysis using heat maps, ordinal scales for risk (low, med., high, very high), risk frequency and risk impact (0 to 5).
- ITIL v3 (TSO, 2011): refers to other frameworks on this matter.
- PMBOK (PMI, 2013): qualitative risk analysis as in item 1, quantitative risk analysis.
- ISO 27005:2011 (ISO, 2011), ISO 31000:2009 (ISO, 2009a): qualitative risk analysis, quantitative risk analysis, but with examples of qualitative analysis.
- NIST (NIST, 2012): qualitative risk analysis using heat maps, ordinal scales for risk, impact, likelihood, etc. (very low,..., very high), (0 to 10), or (0 to 100).

An important controversial point is a "positive" meaning of risk in all frameworks. The meaning of "positive" risk is confusing because it includes a desired outcome beyond unwanted ones. A usual meaning of the term "risk" is something negative, undesired, inadmissible, or inappropriate. A failure or loss suits this meaning in many languages (Holton, 2004; Hubbard,

2009, 2016), and this is the case of practical usage of the term "risk". Some other related issues of the "positive risk" are discussed in Goman (2019).

The positive quality of any risk is dispelled with the typical questions of RM: What is risk treatment for a "good" risk? What is the residual risk after the treatment measures? Finally, what is risk tolerance to this kind of risk? Consequently, the term "risk" is meaningful in only negative context.

Risks are classified by diverse properties and this is a resource demanding activity. All frameworks refer to risk registers, but give no advice on classification overhead reduction. Simple qualitative assessment methods based on subjective ordinal scores like "high", "medium", "low" or ordinal scales such as {0, 1, 2, 3, 4, 5} are recommended in each framework directly or indirectly (sometimes with respective examples). Existence of quantitative methods of analysis is only mentioned in passing. Instead, "heat maps" are promoted for management DM. Nevertheless, it is known that mathematical calculus for scores does not exist and application of such scores is problematic (Hubbard, 2009, ch. 7, 2014; Thomas, et al., 2013). The result of arithmetical operations on these subjective scores and any other ordinal values is not defined and meaningless.

Relevant findings will be shown in the following subsections. The descriptions of the selected frameworks add evidence to our discussion of problems in the IT risk control domain and generalizations in the conclusion.

4.1. COBIT

COBIT promises to be the most objective convolution of IT control practices that ensures achievement of the best possible business benefits while treating risks and optimizing use of resources. It calls success factors "enablers", namely "factors that, individually and collectively, influence whether something will work" (ISACA, 2012). COBIT classifies many goals, risks, success factors, etc. Then it defines finite sets of predefined IT processes, sets of IT goals with relations between them, and relations from IT goals to a set of business (enterprise) goals (Betz, 2011, ISACA, 2012). COBIT's concept is that IT processes ensure IT goals and IT goals support business goals realization. The processes "Manage risk" and "Ensure risk optimization" are among them.

COBIT 5 and COBIT 2019 are very close in relation to RM. According to them, risk should be managed through its identification, assessment, and design of an appropriate "enabler" to mitigate the risk. Risk optimization has become a major part of governance and management objectives in the COBIT core model. In the areas "Evaluate, Direct and Monitor" (EDM) and "Align, Plan and Organize" (APO), there are dedicated sub processes EDM03 – Ensured Risk Optimization (risk governance process), and APO12 – Managed risk (risk management process) for risk management (ISACA, 2012; ISACA, 2013; ISACA, 2018a; ISACA, 2018b). IT RM also presents in enterprise goals. Moreover, COBIT 5 has a special book devoted to risk management (ISACA, 2013). Risk is regarded from two different points: Risk function and Risk management perspectives (ISACA, 2013). The former describes *what* is needed to establish efficient risk governance *and* management activities. The latter relates, *how* the core risk management processes are assisted by COBIT enablers. COBIT refers a user to ISO 27000 and ISO 31000 for guidelines on RM and risk control. COBIT 2019 further integrates overall business risk governance and management with IT governance and management.

There is a clear vision in COBIT that IT risk may refer not only to operational risk, but to any component of enterprise risk, including market, credit, and even strategic risk where IT component exists (e.g. IT is required for a new strategic business initiative). In addition to generic risk concept, COBIT defines business and IT risks. Regrettably, these two definitions are too different. Moreover, both of them allow "positive" risk that is unfortunate as well. However, they recognize IT risk as a subset of business risks. COBIT 2019 refines: "The management of IT-related risk should be integrated within the enterprise risk management approach..." (ISACA, 2018b). COBIT 2019 also specifies a term "Risk optimization" that splits value creation and value preservation. The latter is a designated objective of RM. COBIT itself "Helps to ensure the identification and management of all IT-related risk" (ISACA, 2018b) for risk management stakeholders.

COBIT 5 for risk (ISACA, 2014) gives an example of IT risk assessment. It suggests further IT risk classification: Primary (of high degree) and Secondary (of low degree) risks. This is an oversimplification. To decision-makers, does it mean that primary risks should be considered now, and secondary may be resolved later? Furthermore, it suggests aggregation of risks on a plot to cluster similar risks, e.g. a cluster contains risks that may cause a prohibitive impact and must be prevented at all cost. From engineering and mathematical points of view, aggregating two scored ordinal values for risks of completely different nature and measures is not as trivial as COBIT supposes. COBIT 2019 suggests further ways of risk and risk factors classification.

Basic example risk scenarios are shown in (ISACA, 2013). More than 100 sample risk scenarios are given in a special COBIT issue (ISACA, 2014). Without any doubt, the examples represent the view of COBIT on a good risk assessment practice. The major downside is usage of ordinal scales. For instance, is a certain enabler's "Low" effect on frequency enough for a case where combination of the frequency of risk is 3 and the impact is 2 (on a scale from 0 to 5)? Problems of such scales were analyzed in (Hubbard, 2009, 2014), and further references can be found in the books.

COBIT regards qualitative methods to be better for the initial risk assessment, but admits "high level of subjectivity, great variance in human judgments and lack of standardized approach" (ISACA, 2012). Problems of subjective qualitative estimations were well described by Hubbard (2009, 2014). COBIT suggests, that risk assessment methodology should be chosen by every company according to their needs, but does not tell anything about the principles of how to do it properly.

COBIT insists that organizational controls, well-built IT processes with defined and understood roles, inputs and outputs, company culture and so on will produce good RM. But after that, they propose to measure RM effectiveness as maturity levels, which are a kind of subjective ordinal scale. Taking into consideration information from this section, COBIT can not assist effective RM.

4.2. ITIL

The framework aims at organizing an optimized set of processes for a service provider. Risk is considered mainly in the context of risk for the supplier, not for the client. An exception is a service provider inside the company – IT function. It is implicated that, with adherence to process approach, risks are minimized. Metrics showing benefit for business, such as total cost of ownership and return on investment are supported. ITIL (TSO, 2011) advises, that processes should be measurable and performance-driven. Measurement methods and metrics are strongly propagated and proposed metrics are more reasonable for their objectives, than those in

COBIT. Unfortunately, examples in ITIL books show, that its authors prefer simplified trivial techniques for risk assessment and evaluation.

Although IT risk is mostly considered as technical and technological operational risk, ITIL allows not only operational but any other kind of risk classes for both service provider and a customer, including strategic risk. Attention is paid to project risks too. Importance of understanding complexity of IT and processes is traced through all ITIL books.

ITIL introduces ambiguity to the risk concept: It is hard to conceive a risk (measured by probability, vulnerability, and impact) as an undesired event, and sometimes, as only an uncertainty about success or failure (measured by probability only) (TSO, 2011; AXELOS, 2019). Usage of the term "risk" either crosses with the meaning of "threat" or presumes that there exists imminent risk for intangible information assets, e.g. "...understanding and managing risks to the confidentiality, integrity, and availability of information..." (AXELOS, 2019, p. 114).

As risk is not a trivial topic, ITIL does not give any considerations on good methods of risk analysis and key factors or measuring techniques for both IT service provider and a client. Any details about RM are advised to see in other standards. Considering all above, ITIL does not incorporate RM well into its process paradigm.

4.3. PMBOK

The subject area of the framework is project management. The objectives of project RM are to increase the likelihood and impact of good events, and decrease the same characteristics for bad events in a project (PMI, 2013). In the 6th edition, project RM process has become even more complex, for it should address both levels of risk: individual risks and the overall risk (PMI, 2017). However, there is a discrepancy in the objective of the process, because at the same time "Project Risk Management aims to identify and manage risks that are not covered by other project management processes" (PMI, 2017, p. 677).

Ambiguity between terms "uncertainty" and "risk" increased in the latest edition with introduction of "non-event risks" (variability risk, ambiguity risk) (PMI, 2017, ch. 11). Multiple definitions of risk make the risk ontology complex and interrelations between the terms unclear. Moreover, the definition of a threat does mean another risk "event": "**Threat**. A risk that would have a negative effect on one or more project objectives" (emphasis in original) (PMI, 2017, p. 724).

Definition of risk assumes that a risk can be a "positive thing", e.g. individual and overall risks (if they occur) can have a positive or negative effect on project objectives (PMI, 2017, p. 677). Another innovation is "positive and negative risks are commonly referred to as opportunities and threats" (PMI, 2013). It is true for an opportunity, but a risk and a threat are hardly the same entity. Note, that these terms *are different* in ITIL, which considers PMBOK a framework supporting projects for ITIL processes.

The framework mentions the idea of simulation and modeling techniques. Regrettably, examples of probability and impact definitions show, that PMBOK prefers ordinal scales to mathematical numbers and conceals its mathematical rules for ordinal scoring values (see examples in (Snyder, 2013; Snyder, 2018)). There is no example of quantitative risk analysis for PM purposes in PMBOK. However, we know at least the book (Grey, 1995) that explained simple modeling for PM and had existed for more than a decade before the 5th PMBOK edition.

A good thing in the framework is lessons learned process, which aims at identifying things that fail and that should be improved in future projects. In spite of its retrospectives, this simple concept is very important in practice of RM, but the framework does not introduce it comprehensively.

4.4. Standards ISO 31000 and ISO 27000

Both standards are close in their terms. Standard ISO 31000 (ISO, 2009a) aims at managing any type of risk, and, for any decision-making activity. It is very abstract. ISO 27005 (ISO, 2011) targets on IS risks in the context of the organization's business risks. An essential idea through the standards is relation of risk to DM.

ISO 31000 standard defines principles for effective RM including extensive discussion of the human aspect, such as corporate culture. Recommendation is given to use quantitative methods whenever possible (ISO, 2009a). Both standards presume use of modeling techniques. At the same time, plenty of different methods are only shortly explained in the ISO book of risk assessment techniques (ISO, 2009b).

IS risk definition is defined with negative meaning, but introduces another ambiguous term "potential". These definition misses the decision-maker's involvement. According to ISO 27000 standard, a company should work out specific RM approach, then specific risk assessment methodology, and, in particular, assess the business impact. It is also suggested that analytical models and simulations should give meaningful results (ISO, 2011), and it is the only framework that mentions *refinement* of risk likelihood as a way of risk control.

These standards are the only frameworks (among all studied) that define terms "measure" and "measurement". It is important to admit that ISO 27005 warns: "Users of these methods should be aware that it might be invalid to perform further mathematical operations using the numbers that are qualitative results produced by qualitative risk assessment methods" (ISO, 2011). And in spite of that, several vague examples full of qualitative estimations follow. Unfortunately, in spite of some positive concepts, these standards repeat all ineffective approaches with subjective ordinal scores that we have seen above.

4.5. NIST

The framework defines risk principles and IS RM process for organizations and managers at all levels in the USA. The link between business and IT risk is clearly declared: "IS risk is associated with the operation and use of information systems that support the missions and business functions of their organizations" (NIST, 2012). It seems that risk basics are better developed in NIST than in other considered frameworks.

Although IT risk is mostly considered as technical and technological operational risk, its strategic influence is well defined in the text of the framework. Risk has only adverse meaning in the framework, and as in ITIL, risk is imminent for intangible information assets. An explanation of multiple risk interaction between different levels of an organization is provided. A generic risk model is given where risk to organizational operations or assets, individuals, and the Nation is a combination of impact and likelihood caused by interaction of threat sources, events, vulnerabilities, and actual conditions (including risk controls). However, subjective aspect of risk is missing.

There is a large effort to explain and illustrate importance to conceive IT and organizational complexity, and classification of threats and vulnerabilities in the framework. Uncertainty is well explained in relation to risk evaluation, but not as an inherent origin of risk. The framework introduces risk aggregation for a number of lower-level risks into a higher-level risk, and claims that risk is expressed better in the qualitative form or using ranges of values rather than single values. Quantitative analysis is well mentioned as well as difficulties of qualitative and semi-quantitative methods (methods using subjective qualitative range scores or scales akin (1-10)). As regards impact, the following statement is practically important and has no analogous in other frameworks: "In general, the risk level is typically not higher than the impact level, and likelihood can serve to reduce risk below that impact level. However, when addressing organization-wide ... impact as an upper bound on risk may not hold".

The risk management process includes risk assessment, result communication, and maintenance of risk assessment. The process should be applied on three main tiers of an organization and thoroughly communicated between the tiers. Nevertheless, as follows from Appendices D (threat sources), F (vulnerability severity), G (likelihoods), H (impacts), and I (level of risk as a combination of likelihood and impact), risk analysis is presumably should be based on usage of qualitative (semi-quantitative) values, and heat maps without theoretical background of their algebra and advised rules of their aggregation, combination, etc. Risk management process lacks measures of risk control effectiveness, except a single mentioning of "lessons learned" technique.

5. Conclusion

We considered today's IT management frameworks regarding their concepts of risk and methods of RM in the paper. We believe that there is an explicit criterion of effectiveness for any method: It should yield expected results in practical application. COBIT 2019 restates this explicitly: "It should also be measured in a way that shows the impact and contributions of optimizing IT-related business risk on preserving value" (ISACA, 2018a). Unfortunately, there is lack of empirical evidence that the application of "best practices" from the frameworks improves risk assessment, enhances related estimations and risk evaluations, reduce losses, and increases firms' efficiency and profits. However, we show that the frameworks contain so many serious problems that one needs a lot of consideration in order to effectively use RM methods in these frameworks.

Considering IT risk as a part of business risks, one needs to see IT RM effectiveness in the company's overall performance metrics and financial result. Current IT management frameworks have no means for that. Common metrics for that are still missing and practical validation of existing metrics is required. Feedback control systems for processes in frameworks leave to be better specified using unified concepts and notations from respective branches of science and engineering.

No objective evaluation were discovered about practical effectiveness of frameworks' risk control practices in companies and no tracks of post-analysis of popular frameworks' application were found. It means, that no systematic work is performed to link changes in IT function according to IT management frameworks and subsequently to overall change of business risk of companies.

To sum up, RM should be a proactive activity, not a reactive one: One needs better information about future bad events and their impact, not a "risk process" itself. Clear terminology is the basement: What is the decision, who is the decision-maker and what is risk for him. Next,

proven methods of analysis, probabilistic view and stochastic modeling are required. To manage IT risks efficiently, it is vital to understand systemically all relevant processes, projects and IT systems, maintain this knowledge, and constantly discover new insights from analysis of available data and history of events. Efficient RM is not possible without consideration of people in models and assigning responsibility to them. Meaningful KPI/KRI, reports and documentation in business and IT processes should help employees, but not produce overhead.

References

AXELOS (2019). *ITIL Foundation: ITIL 4 Edition*. TSO.

Betz, C. (2011). "Ongoing Confusion of Process and Function ITIL®, COBIT®, and ®CMMI: Ongoing Confusion of Process and Function." *BPTrends*.

Goldstein, J., M. Benaroch, and A. Chernobai (2008). "IS-Related Operational Risk: An Exploratory Analysis." *In: Proceedings of AMCIS 2008*.

Goman, M. (2018). "Towards Unambiguous IT Risk Definition." *In: Proceedings of CECC 2018*.

Goman, M. (2019). "Current State of IT Risk Analysis in Management Frameworks: Is it Enough?" *In: Proceedings of ITMS 2019*.

Grey, S. (1995). *Practical Risk Assessment for Project Management*. Wiley.

Holton, G. A. (2004). "Defining Risk." *Financial Analysts Journal 60*(6), 19-25.

Hubbard, D. (2009). *The Failure of Risk Management*. Wiley.

Hubbard, D. (2014). *How to Measure Anything, 3rd edition*, Wiley.

Hubbard, D. (2016). *How to Measure Anything in Cybersecurity Risk*. Wiley.

ISACA (2012). *COBIT 5*. ISACA.

ISACA (2013). *COBIT 5 for Risk*. ISACA.

ISACA (2014). *Risk Scenarios Using COBIT 5 for Risk*. ISACA.

ISACA (2018)a. *COBIT 2019 Framework: Introduction and Methodology*. ISACA.

ISACA (2018)b. *COBIT 2019 Framework: Governance and Management Objectives*. ISACA.

ISO (2009)a. *International standard IEC 31010:2009. Risk management – Risk assessment techniques*. ISO.

ISO (2009)b. *International standard ISO 31000:2009. Risk Management – Principles and guidelines*. ISO.

ISO (2011). *International Standard ISO/IEC 27005:2011. Information technology – Security techniques – Information security risk management*. ISO.

Nelson, R. R. (2005). "Project Retrospectives: Evaluating Project Success, Failure, and Everything in Between." *MIS Quarterly Executive 4*(3).

Nelson, R. R. (2005). "IT Project Management: Infamous Failures, Classic Mistakes, and Best Practices." *MIS Quarterly Executive 6*(2).

NIST (2012). *Guide for Conducting Risk Assessments*. Retrieved 10 January 2021, from https://doi.org/10.6028/NIST.SP.800-30r1

PMI (2013). *A Guide to the Project Management Body of Knowledge: PMBOK Guide, 5th edition*. PMI.

PMI (2017). *A Guide to the Project Management Body of Knowledge: PMBOK Guide, 6th edition*. PMI.

Snyder, C. S. (2013). *A Project Manager's Book of Forms.* Wiley.

Snyder, C. S. (2018). *A Project Managers Book of Tools and Techniques*. Wiley.

TSO (2011). *Information Technology Infrastructure Library: ITIL Framework (5 Volume Set)*. TSO.

Thomas, P., R. B. Bratvold, and J. E. Bickel (2013). “The Risk of Using Risk Matrices.” *SPE Economics & Management, 6*, 56-66.

Widman, J. (2008, October 9). *IT’s Biggest Project Failures – and what we can Learn from them.* Computerworld. Retrieved 10 January 2021, from https://www.computerworld.com/article/2533563/it-s-biggest-project-failures----and-what-we-can-learn-from-them.html