Integrating Risk Representation at Strategic Level for IT Service Governance: A Comprehensive Framework

Aghakhani Ghazaleh, Yves Wautelet, Manuel Kolp, Samedi Heng

Integrating Risk Representation at Strategic Level for IT Service Governance: A Comprehensive Framework

Aghakhani Ghazaleh[1], Yves Wautelet[2], Manuel Kolp[1], and Samedi Heng[3]

[1] UCLouvain, Louvain-La-Neuve, Belgium
{ghazaleh.aghakhani, manuel.kolp}@uclouvain.be,
[2] KU Leuven, Leuven, Belgium
yves.wautelet@kuleuven.be,
[3] HEC Liège, Université de Liège, Liège, Belgium
samedi.heng@uliege.be

Abstract. Organizations tend to set and pursuit objectives against an environment which faces levels of uncertainty. The effect of these uncertainties on objectives can be positive (opportunity risk) or/and negative (hazard risk). With every decision made by people within a company, risks are created, modified, updated or deleted. Therefore, the way these decisions are made in terms of change management strategy as well as the information they are based on, influence how objectives are achieved and requirements fulfilled. Despite the importance of risk definition and risk taking at all organizational levels, organizations mostly consider risk at the management and operational levels. Risks nevertheless also need to be considered at the strategic (governance) level because they constitute what hampers an organization to achieve its strategy. This paper focuses on risk at the strategic level and for this purpose it enriches the *Model Driven IT Governance (MoDrIGo) framework*; the enriched framework allows to evaluate the alignment of business IT services with strategic objectives while balancing this alignment/support with the potential risk at governance level. All in all, the framework is applicable in broader governance scenarios. The relevance of MoDrIGo as starting point to build a risk-aware governance framework (compared to other similar methods) is mainly because of its service-orientation and its focus on software development issues. The enhanced framework thus provides a high-level risk overview that helps organizations to successfully perceive, detect and treat risks when pursuing their objectives.

Keywords: Strategic Risk; Risk Governance; Risk Appetite; Strategic Risk Modelling

1 Introduction

Organizations face an uncertain, increasingly complex and challenging environment. This has brought the concept of risk to a higher profile [22]. In an organizational context, risk is usually referred to as anything that can influence the fulfilment of corporate objectives [22]. Such risk may impede what the organization is seeking to achieve (hazard risk), cause uncertainty about the outcomes (control risk) or enhance their goal (opportunity risk) [22]. Being ultimately responsible for the organization's business performance, value creation and decision making (all associated with risk), the Board of Directors (BoD) is responsible for managing such risk by governing risk through overseeing, directing, as well as setting policies and monitoring performance [12].
On the other hand, every business decision involves risk [12]. Organizations deliberately take risks in order to gain a positive return in the context of gaining competitive

advantage. These risks can be considered as speculative risks or opportunities, and an organization has a specific appetite to invest in such risks [22]. Balancing risk with acceptable reward for creating value without jeopardizing the organization has been a challenge for boards and senior management [12]. Therefore, it is crucial to understand the corporate exposure to risk and govern it properly [12]. According to [14], "*a sound risk governance allows for the articulation of how, in the context of its risks, a company is able to achieve its business objectives, formulate its value proposition, assess its risk tolerance, and design its processes with respect to the reasonable expectations of stakeholders*"

Traditional risk management approaches do not necessarily detect future strategic risks or anticipate future performance. Hence, rather than creating value, they are more focused on its protection [33]. In previous approaches risk has been addressed rather at the operational and management levels; risk is often tackled well at the operational level by taking appropriate precautions and insurance against events such as fire, theft, vehicle damage, and employee accidents. More precisely, risks that are internal to the organization are usually identified from experience, brainstorming sessions or risk lists, registers and taxonomies. At the managerial level, risks tend to be less well-handled because they are not so obvious to recognize. Loss of profits following an incident, product liability, reputational loss, and failure of management information systems are examples of such risks. Risks at the strategic level, however, may not be identified at all, even by top management, which can lead to negative impacts on the achievement of the long term objectives leading to the failure of the overall strategy [12]. In order to address this gap, this paper aims to address different aspects of risk treatment at the governance level. For that, we will enhance the Model-Driven IT Governance (MoDrIGo) framework of Wautelet [37], an existing model driven strategic framework, with risk concepts in order to better identify what are the different aspects of risk at the strategic level and better taking this into account for decision making.

2 Research Positioning and Objectives

2.1 Research Questions

The complex and fast evolution of the business environment has led to the emergence of a growing focus on risk management [17]. The focus is expanded to the broader, enterprise-wide risks faced by companies [17]. This especially includes strategic risks as their identification is important for the successful achievement of a business strategy [12]. Being in the paradigm of Design Science Research, we aim to bring a solution/enhancement to the identified problem of strategic-level risk identification, representation and treatment. Subsequently, we will use the identified risks to balance business-IT service adaptation based on Business IT Alignment (BITA). For that, this paper aims to answer the following question: *How can we use the identified risk concepts at the strategic level to balance business IT service adoption decisions based on BITA?*

2.2 The Choice of MoDrIGo

The relevance of MoDrIGo for this research results from its internal qualities when compared to three other similar frameworks on the basis of five important criteria. We used google scholar to find these frameworks and narrowed the research by selecting frameworks that focus on BITA and that are goal-oriented or/and industry-adopted. We

Table 1. A comparative analysis of MoDrIGo and other competing methods

	Criteria				
Model or Framework	*Stakeholder-oriented*	*Support for BITA*	*(Strategy and goal)-oriented*	*Service-driven*	*Focus of software development issues*
MoDrIGo [37]	✓	✓	✓	✓	✓
B-SCP [7]	✓	✓	✓	-	✓
ArchiMate [32]	✓	✓	✓	-	-
SOARE [6]	-	-	✓	-	-

compared these frameworks based on five criteria that we assume crucial for a framework to embrace the strategic risk aspects:
Stakeholder-oriented refers to the consideration of all parties that are impacted by the future success or failure of an organization. This is especially important for us as we should identify the stakeholders who are affected by risk (i.e. who are responsible to take risk, perceive risk, mitigate risk, treat risk, etc.).
(Strategy and goal)-oriented refers to the focus on the strategies pursued by an organization. It allows to model strategic goals desired by some stakeholders and aimed to lead the organization to an enhanced competitive position. Having such characteristic is crucial for a risk aware framework as it allows to capture the impact of risks on a strategic goal as well as the amount of risk that the organization is willing to take in order to achieve such goal.
Service-driven refers to the delimitation of a software system entities into coarse-grained elements called services. The latter do have a seamless and tightly integrated interaction [11]. Services are well suited elements for software governance on one side [37] but also for forward engineering (i.e. transformation) and traceability on the other side [39]. Being service-oriented, a framework thus allows to (i) use identified risk elements for (strategic) decision (acquisition of services in the infrastructure) and/or (ii) to take actions to mitigate risk within the service adoption/development [19].
Support for BITA refers to the correspondence between business and IT objectives. This is especially important here because we are interested in how to trace the strategic risk at the tactical and operational levels.
Focus on Software Development Issues refers to the fact that rather than addressing problems at the enterprise architecture level, as mentioned earlier, we are focusing on services and functions with respect to the defined strategies and risk criteria.

Table 1 shows a comparative analysis of MoDrIGo with other frameworks. We can see that MoDrIGo outperforms the competing frameworks because it supports all the aforementioned criteria. For example, MoDrIGo supports BITA by making an explicit link between strategic and tactical levels. Therefore, enriching MoDrIGo helps understand the involvement of strategic risks in governance decisions of the BoD and the way the c-suite perceives and handles these risks.

3 Research Background

Mostly organizations develop a vision statement, or mission statement where they identify their functional goals and targets. This identification must be coupled by determining the minimum required risk that needs to be taken in order to achieve such goals and

targets. In case of unrealistic required risk (i.e., too high), the goals should be adjusted or the company will automatically undergo an exceeding level of risk [16].

3.1 Risk Is A Strategic Issue

Business risks are uncertainties that negatively (failing to achieve or delayed objectives) or positively (leading to exceed or early achievement of objectives) influence the ability of an organization to achieve its objectives and goals. They relate to business objectives as risk-taking is a prerequisite to success. For that, it is necessary to exploit some risks to take advantage of strategic opportunities and mitigate the ones that threaten success. The threatening risks include threats of problems occurring (e.g., misappropriation of assets) or opportunities not occurring (e.g., failure to achieve strategic goals) [34].
Different sources provide different definitions of risk. The key definitions are:

- ISO Guide 73 [35]: "*Effect of uncertainty on objectives. Note that an effect may be positive, negative, or a deviation from the expected. Also, risk is often described by an event, a change in circumstances or a consequence.*"
- Institute of Risk Management (IRM) [24]: "*Risk is the combination of an event and its consequences. Consequences can range from positive to negative.*"
- Orange Book from HM Technology [8]: "*Uncertainty of outcome, within a range of exposure, arising from a combination of the impact and the probability of potential events.*"
- Institute of Internal Auditors (IIA) [23]: "*The uncertainty of an event occurring that could have an impact on the objectives. Risk is measured in terms of consequences and likelihood.*"

More risk definitions are provided in other studies such as [22], [17], [30] and [15]. Given the large number of available definitions, organizations should be able to choose the definition that is most appropriate for their purposes [22]. We essentially refer to the definition provided by ISO Guide 73 as the most relevant to our research because we believe that other than being positive or negative, risk can also refer to the deviation from the expected objectives.

3.2 Enterprise Risk Governance and Management

To study risk at the governance level, it is important to distinguish classical risk management activities from risk treatment undertaken at the governance level. According to the ISACA COBIT 5 framework [26], there is indeed a clear distinction between governance and management:
*"Governance ensures that enterprise objectives are achieved by **evaluating** stakeholder needs, conditions and opinions; setting **direction** through prioritisation and decision making; and **monitoring** performance, compliance and progress against agreed-on direction and objectives (EDM)"*
*"Management **plans, builds, runs and monitors** activities in alignment with the direction set by the governance body to achieve the enterprise objectives (PBRM)"*

Organizations are more and more interested in risk and risk management [22]. At the board level, Strategic Risk treatment is a necessary core competency [17]. According to Charan [10], the BoD need to concentrate on the inherent risk that lies in the

strategy and strategy execution: "*Risk is an integral part of every company's strategy; when boards review strategy, they have to be forceful in asking the CEO what risks are inherent in the strategy. They need to explore [what ifs] with management in order to stress-test against external conditions such as recession or currency exchange movements*". Business decisions and strategy both carry risk. Managing risk is thus an integral part of board's corporate governance [12] but BoD is not directly in charge of risk management. However, its governance activities make a significant contribution to effective Enterprise Risk Management. This includes *defining and communicating risk tolerance thresholds to senior management, which will guide them in their decisions*, and *making sure that the management's performance indicators together with the associated key risks are properly aligned with the organization's strategy and appropriately linked to stakeholder value* [34]. More precisely, the attitude of an organization towards risk can be implied from the leadership which can be determined by its BoD as well as from its corporate objectives and strategies. This allows the organization to set out the objectives it is trying to achieve, and the strategies it is adopting to achieve these objectives. The harder to attain the objectives and ambitions of a company are, the greater the risks it should take to achieve them [15].

3.3 Modelling Risk and Risk Related Concepts: Related Work

Risk and security models help companies develop guidance and take action in order to embrace opportunity and manage risk [3]. Prior researches have discussed risk modelling. Asnar and Giorgini [2] model risk at the organizational level by extending the Tropos goal model. Likewise, Band et al. [3] make use of the ArchiMate standard to incorporate risk and security concepts at all levels. Mayer and Feltus [28] also analyse security and risk overlay of the ArchiMate language. Other studies rather propose a set of guidelines to model risk concepts. For example, Giannoulis [21] propose a set of guidelines that help refine i* models based on risk. However, despite the importance of considering risk at the governance level, all the aforementioned models only focus on risk at the management level. We believe that, to the best of our knowledge, Wautelet (2020) [38] is the only framework that also considers governance level aspects (in a meta-model) but it does not represent it graphically nor illustrate it.

4 Running Example: Risk Governance in Healthcare

In recent years, biomedical, normative, and technological changes have led healthcare organizations to implement clinical governance as a way to make sure that they can provide the best quality of care and thus increase efficiency in an increasingly complex environment. One of the most relevant aspects of clinical governance is risk management [9]. The latter is particularly crucial in the healthcare industry as mismanaging risks may result in dire consequences such as fatalities [36]. The aim is to decrease the probabilities and impacts of adverse events while increasing the probabilities and impacts of positive events [9].

The recent evolution in healthcare systems regarding the digitization of patient medical records, healthcare provider collaborative workflows, improved regulation requirements, along with increasing healthcare data records, has motivated the healthcare industry to adopt innovative technologies [20]. Technology contributes greatly to enhance safety in healthcare processes. However, without a well-structured organization, it may add more complication to the existing working practices, resulting in fewer benefits

than expected [9]. Adopting new technologies in the healthcare industry is usually a slow process. This is because medical informatics take-off involve uncertainties and risks. For that, it is necessary to first identify and make a realistic evaluation of business risk and then develop strategies to manage these risks [36].

As an innovative technology, cloud computing provides opportunities to boost healthcare services from the perspective of legality, management, technology, and security. However, it is crucial to assess the risks that arise from cloud computing before its adoption in healthcare projects [20]. When a health organization decides to move its services into the cloud, it should develop strategic planning to evaluate the new model's benefits and risks. Moreover, the organization should assess the capabilities of the model to achieve the objective and identify strategies designed for the implementation [27].

To illustrate risk and risk taking within the healthcare industry, we consider an evolution of the Saint-Romain hospital previously presented in [40]. Let's now consider that its governance board is interested in adopting a new strategy, which is moving its services into the cloud. Besides presenting significant opportunities, use of cloud also involves uncertainties. As such, the more educated Saint-Romain executives and boards become about the benefits and risks of adopting cloud, the more effectively they can prepare their organization for the future.

The utmost goal of Saint-Romain is to remain timely, efficient, and cost effective, and to provide high-quality services. For that, Saint-Romain requires to invest in continuous and systematic innovation. The aim of adopting cloud computing is to improve healthcare services within Saint-Romain. Some of these improvements are listed below:

- putting in place an on-demand, self-service Internet infrastructure that provides Saint-Romain users with seven-days-a-week, real-time data collecting and access to computing resources anytime from anywhere;
- reducing the setup expenses of the electronic health record, such as software, hardware, networking, licensing fees, and personnel;
- possessing a cost-effective and on-premise IT solution without the need to purchase or examine software or hardware, or to employ internal IT staff to service and maintain in-house infrastructure;
- overcoming major issues and difficulties in biomedical research data management such as data-handling problems, and unavailable or expensive computational solutions to research problems;
- automating the process of collecting patients' sensitive data through a network of sensors that are connected to legacy medical devices, and then storing, processing and distributing the data in a medical center's cloud;
- eliminating manual collection work as well as the possibility of typing errors.

Despite the aforementioned benefits associated with adopting cloud computing, Saint-Romain encounters three key areas of risks: *misalignment of cloud initiatives with business strategies, over-reliance on cloud service providers, and loss of control over high-value information*. For Saint-Romain, avoiding such clinical risk is of high importance since if something goes wrong, this may lead to patient harm or possibly even death. Therefore, with respect to challenges and opportunities, the clinical governance of Saint-Romain should decide on how much clinical risk it is willing to accept so that the adopted cloud projects stay aligned with their strategies. In other words, the

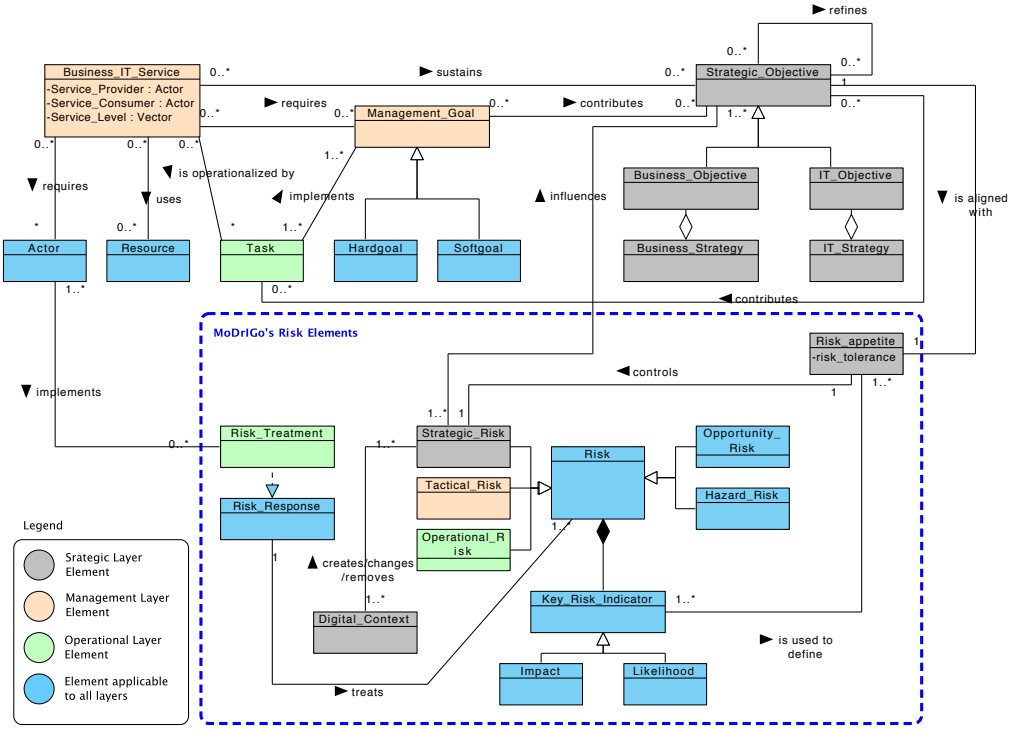

Fig. 1. Risk-aware MoDrIGo Meta-Model.

board of Saint-Romain should determine the cloud services that are appropriate to their healthcare based on their goals, risk appetite and tolerance.

The first step towards determining the risk appetite is to identify the assets that can incur risk such as *healthcare reputation, patient trust, staff loyalty and personal experience, service delivery, cloud service management interface, network (connections, etc.), personal data, etc.* The second step involves identifying *likelihood* and *impact* of events that could happen in case these assets are exposed to risk. Obviously, Saint-Romain does not consider to accept risks that exceed a certain level (i.e., risk tolerance).

5 The Risk-Aware MoDrIGo Framework

5.1 Risk-Aware MoDrIGo Meta-Model

Based on the literature study, some of the important concepts with regards to strategic risk modelling are identified and listed below. Each concept is illustrated on the case described in Section 4:

1. ***Strategic risk***
   Description: According to Frigo and Anderson [18], strategic risks refer to both external and internal events and scenarios that prevent organizations to achieve their strategic objectives. Moreover, it is generally accepted that the best risk definition

is the one that concentrates on risks as events (see definitions provided by ISO 31000 and IIA). Upon the occurrence of an event, the risk is materialized. Thus, a risk can be referred to as "*an unplanned event with unexpected consequences*". Based on the type of consequence, it is common to classify risks into two types: opportunity (or speculative) risks, and hazard (or pure) risks. Organizations seek to embrace opportunity risks and mitigate hazard risks [22]. Risks are often taken by organization to achieve a reward. In order to launch a new product, an organization decides to accept a certain level of risk by putting some of its resources at risk [22]. ISACA [25] emphasises that "*taking on more risk means grabbing potential opportunities*".
Illustration: In Figure 1, the strategic risk is demonstrated as class `Strategic_Risk`, a subclass of class `Risk`, and based on inheritance, it is either a `Hazard_Risk` or an `Opportunity_Risk`. Other types of risks such as operational (i.e., `Operational_Risk`) and tactical (i.e., `Tactical_Risk`) are also demonstrated in the meta-model but their detailed representation stays out of the scope of this paper.
Example: *For Saint-Romain, misinformation, losing patient data, developing an undesirable reputation, not being able to offer high patient care, etc. are all strategic hazard risks that will negatively impact the strategic objectives of Saint-Romain. On the other hand, personalised and responsive service, keeping wait time to minimum, real time information sharing between doctors and patients are examples of opportunity risks that could have a positive impact on the strategic objectives of Saint-Romain.*

2. ***Digital context***
Description: Today organizations are facing a fast paced, ever-changing world where digitization has been considerably changing individual, organizational and societal behaviour. The BoD plays a key role within the company to adapt to the changing strategic context. The growing momentum of digital transformation continues to influence society and organizations and thus continuously changes the strategic context of organizations. This shows the need for organizations to react to opportunities and threats of the changing context in order to strengthen or maintain their sustained competitive advantage [4]. Therefore, it is necessary to include digital context within the meta-model to address this issue. Here, digital context refers to different technological enablers such as big data, machine learning, IoT, algorithm-driven data analytical and processing capabilities, blockchain, artificial intelligence, crowd/sensor approaches, cloud, etc. through which information flows increase.
Illustration: In the meta-model, digital context is demonstrated as `Digital_Context` class in grey color.
Example: *In the case of Saint-Romain, adoption of cloud computing and integrating it with the healthcare activities, objectives, etc. not only impacts strategic objectives (formulating new objectives, modifying and eliminate some), it also creates, eliminates, or changes risks and opportunities. In case of other emerging digital contexts, such as mobile technologies and big data analytics, Saint-Romain would have different risks, opportunities, and strategic objectives.*

3. ***Key Risk Indicators (KRI)***
It is hard to measure the effectiveness of risk policy without considering KRIs and

comparing them over time [29]. According to Coleman [13], KRIs are measurements or statistics that can yield a perspective of an organization's risk position. The effective development of these KRIs has the goal to identify the relevant metrics that result in useful insights regarding potential risks that may influence the organization's objectives [5].
Illustration: In the meta-model, KRI is demonstrated as `Key Risk Indicator` class in blue color.
Example By considering the impact and likelihood of a risk (as two examples of KRI), Saint-Romain is able to oversee possible risk.

4. ***Risk impact and the consequence***
Description: One of the important KRIs considered by risk managers, is the impact or the consequence that a risk can incur if materialized. The impact is considered as the way a risk affects the organization and its objectives. It represents the residual, net or current level of the risk. The impact of an event is reduced via the controls that are in place [22].
Illustration: In the meta-model, the risk impact and the consequence is demonstrated as `Impact` class in blue color.
Example: *In Saint-Romain, losing patient's vital data (i.e., risk) may result in losing patient's confidence in health service (i.e. impact of the risk).*
5. ***Likelihood***
Description: Another important KRI, is the likelihood or the probability of risk occurrence. According to Hopkin [22] likelihood is a broader word than, but includes frequency. It refers to the possibilities of an unlikely event happening.
Illustration: In the meta-model, the likelihood is demonstrated as `Likelihood` class in blue color.
Example: *In Saint-Romain, losing patient's vital data (i.e., risk) may result in losing patient's confidence in health service (i.e. impact of the risk). The likelihood of losing patient data will be low (high) if the staff are (not) well trained with in using new systems in place.*
6. ***Risk response and treatment***
Description: For each identified risk within the risk profile, a decision must be made – within risk tolerance limit – on the way this risk needs to be treated [1]. Treating a risk changes the likelihood, impact and the magnitude of consequences, both negative and positive, to achieve a net increase in profit [31]. There are several treatment options or more precisely risk responses: risk avoidance, risk acceptance, risk transfer/sharing and risk mitigation [1,25]. ISO 31000 also defines other options to deal with both risks that have upside and/or downside consequences. It includes: "removing risk source", "taking or increasing the risk in order to pursue an opportunity", "changing the likelihood", "changing the consequences" [31]. The treatment plans are then based on these treatment options [1,25] (i.e., link between risk response and risk treatment and risk). Defining risk response has the goal of aligning risk with the defined risk appetite [25].
Illustration: In the meta-model, the risk response is demonstrated as `Risk_Response` class in blue color. The realization of this response is done through risk treatment illustrated as `Risk_Treatment` class in green color.

Example: *In the case of Saint-Romain, when the healthcare realizes that there are cyber-attack risks involved with cloud adoption, as possible responses, it can only host the non sensitive and nonessential data of its patients on Cloud Service Provider, or deploy encryption over these data.*

7. ***Risk appetite***
   Description: Risk appetite refers to the amount and type of risk that a company is willing to take or more precisely managers are willing to 'bet' to meet their strategic goals [16,15]. The tolerable deviation from the level determined by the risk appetite and business objectives is referred to as risk tolerance [25]. The more severe the business impact of an event – resulting from an asset being exposed to risk - the less the risk appetite.
   Illustration: In the meta-model, the risk appetite is demonstrated as `Risk_Appetite` class in grey color. Its main attribute is `risk_tolerance`.
   Example: *For Saint-Romain, patient safety is a top priority. As such, it is not willing to accept any risk that comprises the safety of patients in the pursuit of its strategic objectives (eg. when patient experience indicators show a decrease in quality or when poor bed management or poor clinical records management impact patient safety). On the other hand, the hospital has a greater appetite when it comes to risks that may have impact on organizational issues (eg. failure to maintain the development of the organizational culture). Finally, Saint-Romain will accept highest risk level when it comes to pursuing innovation and challenging current working practices. Likewise, Saint-Romain has greatest appetite for reputational risks in terms of its desire to take opportunities where positive gains are anticipated (eg. failure to acquire share of new market). Risks that score outside of risk appetite (based on risk type, likelihood, impact, etc.) will be registered and reported to be reviewed at the clinical board.*

Within Figure 1, the MoDrIGo meta-model is enriched with the constituting elements described above. Note that different colors are applied on this meta-model to better distinguish different levels (of decision-making, goals, plans, etc.) within an organization. The elements that are associated with the governance/strategic level are colored in grey while the ones that are at the tactical level are colored in orange. To show the activities that are considered at the operational level, the green color is chosen. Finally, the color blue indicates the elements that can be associated to all three levels.

5.2 Model-based Representation of Risk at the Strategic and Management Levels of MoDrIGo

Figure 2 shows an enhanced governance model of MoDrIGo's strategic level representation with (strategic) risk elements. The aim of modelling such representation is that first, it represents the elements that play a key role at the strategic level of an organization (here the Saint-Romain healthcare) and second, it represents the impact of the risk identification at the management level representation (here the *Bed Management service*) onto the business strategies. The blue arrow going from the service to the strategic objective represents the generation of an opportunity risk and the red arrow represents the generation of a hazard risk. Following is the explanation of each of the constructs in the Figure: **hazard risk** refers to the risks that negatively affect Saint-Romain's strategic objectives and is represented by an hexagon with letter "H". On the other hand,

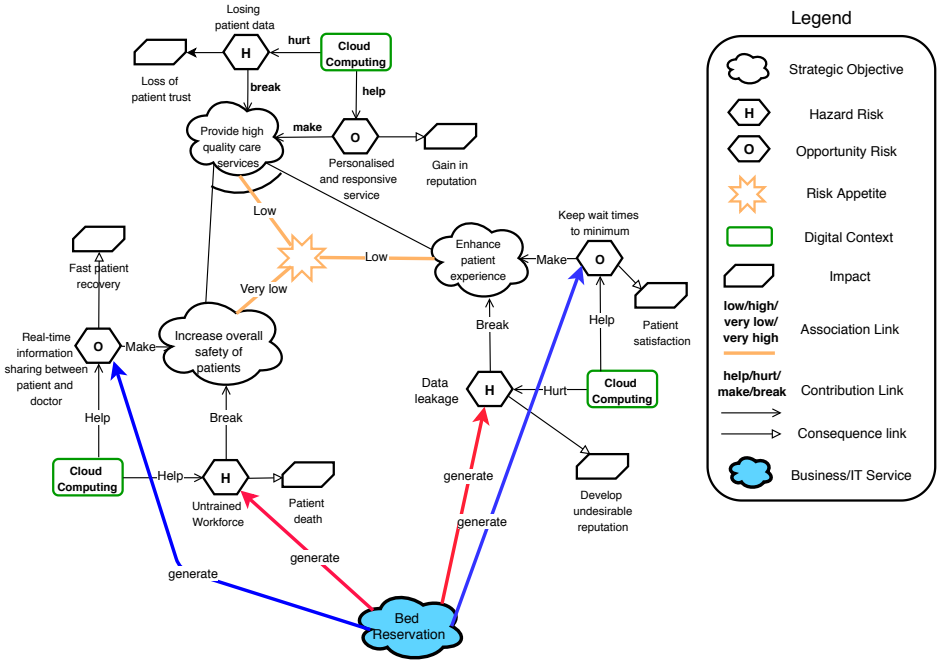

Fig. 2. Risk-aware Business Strategic-level Representation

opportunity risk refers to risks that positively affect the strategic objectives of Saint-Romain and is represented by an hexagon with letter "O". The interconnecting link between these risks and the strategic objective is shown by the contribution link, taken from i*, that can either represent a positive (opportunity risk) or a negative (hazard risk) influence. **Digital context**, represented by a rectangle, demonstrates new emerging technologies such as cloud computing, mobile technology, etc. The link between this construct and the risks is represented by the i* contribution link. The "help" link demonstrates how an opportunity risk or a hazard risk can be improved by adopting the digital context, while the "hurt" link shows how adopting the digital context aggravates the risk. This is especially important as today, organizations are more and more striving for digital transformation. The **consequence** of the hazard or opportunity risks, illustrated by a diagonal snip rectangle, represents the consequence that a particular hazard risk or opportunity can have if materialized. The relation between the risks and the consequence is illustrated by an open arrow. **Risk appetite**, represented by an eight point star or octagram, is one of the key concepts when it comes to board risk-taking and risk oversight. The association link from the risk appetite to the strategic objective shows the amount of risk that an organization is willing to take in the pursuit of such a strategic objective. Finally, the blue cloud in bold represents the bed management service (Figure 3) as an operationalization.

With the new added constructs at the governance level, we are able to model, first, the elements that affect the strategy such as risks and opportunities, and second, the

risk acceptance level of BoD regarding the achievement of a particular strategic objective. This is important as it helps organizations avoid taking too much risk with regards to the achievement of their objectives and thus to prioritise significant risks. Taking into account the strategic objective *"provide high quality care service"*, with the new constructs, it is now possible to first show the negative and positive risks that affect this strategic objective. *"A personalized and responsive service"* has a strong contribution (i.e. make) to satisfice this strategic objective while *"loss of patient data"* has a negative contribution sufficient enough to deny it. Moreover, providing high quality, effective and safe services with the aim to improve the well-being, health, and independence of the population served by Saint-Romain is its main strategy. We can discuss that the hospital is not willing to accept risks that limit its ability to fulfill such objective. Being the top priority, patient safety is associated with the lowest level of risk appetite. Regarding patient experience and quality care, Saint-Romain will accept a higher, yet low, level of risk (as long as it maintains patient safety as well as service improvements and quality care). Hence, the overall risk appetite of the hospital is quite low. As soon as these risks exceed a certain level that can result in jeopardising patient safety, poor quality care or non-compliance with standards, they are reported. Finally, considering cloud computing as digital context is important as it shows how this technology can aggravate or improve the existing risks and indirectly influence the strategy. In other words it can either put in place facilities that can help in achieving this strategic objective or hindering it by aggravating the existing risks or creating new ones. Here, cloud computing can aggravate data loss. This is because sensitive patient data might be stolen for fraudulent purposes. On the other hand, using cloud improves personalised and responsive services by providing real-time information sharing.

Figure 3 illustrates the management level representation of MoDrIGo (the bed management service) enhanced by relevant risk elements. The aim is to study the impact of the enhancement at the management level on the fulfillment of organizational strategies. At this level, we take into account the opportunity risk (represented with a blue hexagon) and the hazard risk (represented with a red hexagon) that are associated with each of the management level elements and can influence (represented by the threatening link) the strategic objectives. Following such representation, it is possible to see how risk can be escalated to the strategic layer and jeopardize the involved strategy. For example, the task *"stay planning"* is associated with the opportunity risk *keep waiting time to minimum*, which helps to the achievement of the strategic objective *"Enhance patient experience"*. On the other hand, the goal *record planning* is associated with hazard risk *data breach* which, has a negative influence on the fulfillment of both strategic objectives *increase overall safety of patients* and *enhance patient experience*. The ability to treat risks is another important enhancement brought to MoDrIGo's management-level representation. This is represented by a green hexagon as a *risk treatment* and is connected to the hazard risk via the *treatment link*.

6 Discussion and Conclusion

In this paper we enriched the MoDrIGo framework with risk related concepts. The enhanced MoDrIGo framework sheds light on two important factors. The first one refers to the importance of considering risk at the strategic level of an organization and its influence on the strategic objectives. This allows the BoD to first perceive and iden-

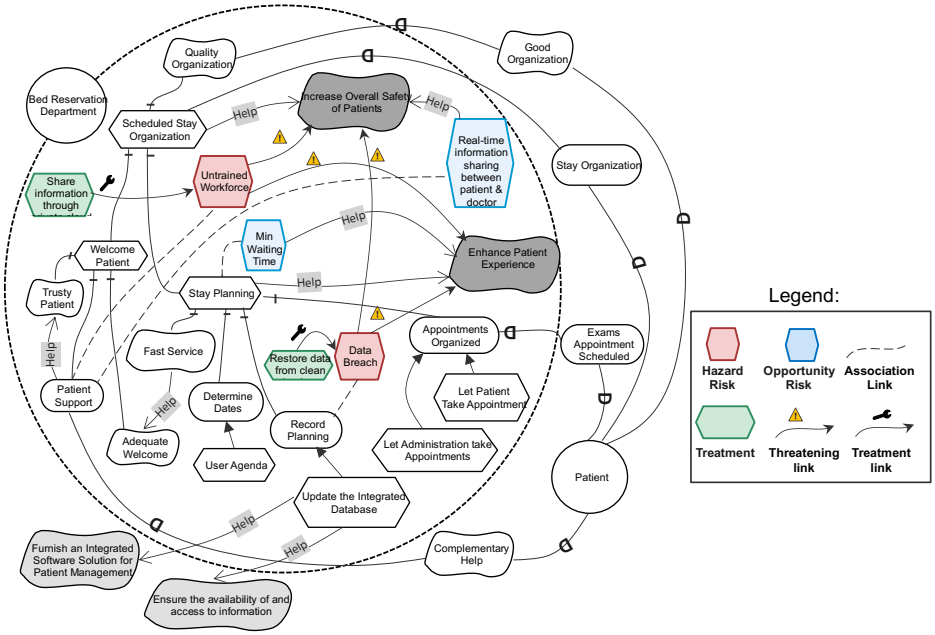

Fig. 3. The Bed Management Service's Impact on Strategy: Risk-Aware Management Level Rationale.

tify the negative and positive aspects of risks that could impact the achievement of objectives and second to determine the amount of risk they are willing to accept in order to achieve their strategic objectives. The second factor refers to the significance of recognizing risks at the managerial level and their impact on the fulfillment of their strategic objectives. The extension was first applied to the meta-model of MoDrIGo, then to its governance level representation and finally for the sake of traceability to the management-level representation. Based on the Saint-Romain example, we can discuss the main contributions provided by the resulting enhanced risk-aware governance framework:

- Risks are involved every time the BoD seeks to achieve its objectives. When instantiated, the risk-aware MoDrIGo framework allows C-level executives to understand the risk concerns of every decision in relation to strategic objectives.
- It is crucial that the BoD takes an adequate amount of risk that it assumes necessary to achieve a particular strategic objective. This is done by defining risk-taking elements such as risk-appetite and risk tolerance that control and mitigate risks. The higher the priority of an objective for an organization, the greater the risk it is willing to take for such objective.
- By enhancing the management level representation of MoDrIGo with the relevant risk concepts, we ensure the traceability between the governance and the management levels. This is done by studying the impact of the enhancement at the managerial level on the fulfillment of organizational strategies.

Despite the advantages of the resulting risk aware framework in recognizing risk at strategic and management level, the framework has the limitation to rapidly grow within large cases. Future work includes enhancing the framework to deal with scalability issues. This way we can fine-tune the framework and tackle the issues it faces such as scalability. The latter is one of the important issues that we consider to work on for the future improvement of the framework. We plan to overcome such problem by making use of modularity and separation of concerns (e.g. having different views). More precisely having a case tool that allows to roll up and drill down on the basis of strategic objectives.

References

1. Al-Ahmad, W., Mohammed, B.: A code of practice for effective information security risk management using cobit 5. In: 2015 Second International Conference on Information Security and Cyber Forensics (InfoSec). pp. 145–151. IEEE (2015)
2. Asnar, Y., Giorgini, P.: Modelling risk and identifying countermeasure in organizations. In: Intl. Workshop on Critical Information Infrastructures Security. pp. 55–66. Springer (2006)
3. Band, I., Engelsman, W., Feltus, C., Paredes, S.G., Diligens, D.: Modeling enterprise risk management and security with the archimate®. Language, The Open Group (2015)
4. Bankewitz, M., Aberg, C., Teuchert, C.: Digitalization and boards of directors: A new era of corporate governance? Business and Management Research **5**(2), 58–69 (2016)
5. Beasley, M.S., Branson, B.C., Hancock, B.V.: Developing key risk indicators to strengthen enterprise risk management-how key risk indicators can sharpen focus on emerging risks. Research commissioned by the Committee of Sponsoring Organizations of the Treadway Commission (COSO) (2010)
6. Bleistein, S.J., Aurum, A., Cox, K., Ray, P.K., et al.: Strategy-oriented alignment in requirements engineering: linking business strategy to requirements of e-business systems using the soare approach. Journal of Research and Practice in Information Technology **36**(4), 259 (2004)
7. Bleistein, S.J., Cox, K., Verner, J., Phalp, K.T.: B-scp: A requirements analysis framework for validating strategic alignment of organizational it based on strategy, context, and process. Information and software technology **48**(9), 846–868 (2006)
8. Book, U.T.O.: Management of risk principles and concepts. HM Treasury, Crown, London (2004)
9. Cagliano, A.C., Grimaldi, S., Rafele, C.: A systemic methodology for risk management in healthcare sector. Safety Science **49**(5), 695–708 (2011)
10. Charan, R.: Owning up: The 14 questions every board member needs to ask. John Wiley & Sons (2009)
11. Cherbakov, L., Galambos, G., Harishankar, R., Kalyana, S., Rackham, G.: Impact of service orientation at the business level. IBM Systems Journal **44**(4), 653–668 (2005)
12. Choi, I.: When do companies need a board-level risk management committee? (2013)
13. Coleman, L.: Risk strategies: dialling up optimum firm risk. Routledge (2009)
14. Council, C.G.: Risk governance guidance for listed boards (2012)
15. Coyle, B.: Risk awareness and corporate governance. Global Professional Publishi (2004)
16. Duncan, B., Zhao, Y., Whittington, M.: Corporate governance, risk appetite and cloud security risk: A little known paradox. how do we square the circle? In: 8th International Conference on Cloud Computing, GRIDs, and Virtualization (CLOUD COMPUTING 2017). IARIA (2017)
17. Frigo, M.L., Anderson, R.J.: Strategic risk management: A foundation for improving erm and governance. Journal of Corporate Accounting & Finance **22**(3), 81–88 (2011)

18. Frigo, M.L., Anderson, R.J.: What is strategic risk management? Strategic Finance **92**(10), 21 (2011)
19. Fugini, M., Ramoni, F., Raibulet, C.: Service-oriented architecture for risk management. In: 2011 11th Annual International Conference on New Technologies of Distributed Systems. pp. 1–8. IEEE (2011)
20. Gbadeyan, A., Butakov, S., Aghili, S.: It governance and risk mitigation approach for private cloud adoption: case study of provincial healthcare provider. Annals of Telecommunications **72**(5-6), 347–357 (2017)
21. Giannoulis, C., Zdravkovic, J.: Exploring risk-awareness in i* models. In: iStar 2010–Proceedings of the 4 th International i* Workshop. p. 103 (2010)
22. Hopkin, P.: Fundamentals of risk management: understanding, evaluating and implementing effective risk management. Kogan Page Publishers (2018)
23. IIA, T.: The role of internal auditing in enterprise-wide risk management (2009)
24. IRM, A.: Risk management standard. The Institute of Risk Management, London (2002)
25. Isaca: The Risk IT Framework. ISACA (2009)
26. ISACA: Cobit 5: for Information Security. ISACA (2012)
27. Kuo, M.H.: Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research **13**(3), e67 (2011)
28. Mayer, N., Feltus, C.: Evaluation of the risk and security overlay of archimate to model information system security risks. In: 2017 IEEE 21st International Enterprise Distributed Object Computing Workshop (EDOCW). pp. 106–116. IEEE (2017)
29. Peček, B., Kovačič, A.: Methodology of monitoring key risk indicators. Economic Research-Ekonomska Istraživanja **32**(1), 3485–3501 (2019)
30. Porter, M.E., Advantage, C.: Creating and sustaining superior performance. Competitive advantage **167** (1985)
31. Purdy, G.: Iso 31000: 2009—setting a new standard for risk management. Risk Analysis: An International Journal **30**(6), 881–886 (2010)
32. Sales, T.P., Almeida, J.P.A., Santini, S., Baião, F., Guizzardi, G.: Ontological analysis and redesign of risk modeling in archimate. In: 2018 IEEE 22nd International Enterprise Distributed Object Computing Conference (EDOC). pp. 154–163. IEEE (2018)
33. Serafin, T.: Exploring strategic risk: 300 executives around the world say their view of strategic risk is changing (2013)
34. Sobel, P.J., Reding, K.F.: Aligning corporate governance with enterprise risk management. Management Accounting Quarterly **5**(2), 29 (2004)
35. for Standardization, I.O.: Risk Management: Principles and Guidelines. ISO (2009)
36. Teoh, S.Y., Cheong, C.: Implicit enterprise risk management: an it healthcare adoption case study. ACIS 2008 Proceedings p. 8 (2008)
37. Wautelet, Y.: A model-driven it governance process based on the strategic impact evaluation of services. Journal of Systems and Software **149**, 462–475 (2019)
38. Wautelet, Y.: Using the rup/uml business use case model for service development governance: A business and it alignment based approach. In: 2020 IEEE 22nd Conference on Business Informatics (CBI). vol. 2, pp. 121–130. IEEE (2020)
39. Wautelet, Y., Kolp, M.: Business and model-driven development of bdi multi-agent systems. Neurocomputing **182**, 304–321 (2016)
40. Wautelet, Y., Kolp, M., Heng, S., Poelmans, S.: Developing a multi-agent platform supporting patient hospital stays following a socio-technical approach: Management and governance benefits. Telematics and Informatics **35**(4), 854–882 (2018)