View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by AIS Electronic Library (AISeL)

Bus Inf Syst Eng 63(2):129–143 (2021)
https://doi.org/10.1007/s12599-020-00634-3

RESEARCH PAPER

Quantifying Risk Propagation Within a Network of Business Processes and IT Services

Oscar González-Rojas · Nicolás Castro · Sebastian Lesmes

Received: 21 December 2018 / Accepted: 27 January 2020 / Published online: 18 March 2020
© Springer Fachmedien Wiesbaden GmbH, ein Teil von Springer Nature 2020

Abstract Nowadays, the organic nature of business processes and the increasingly complex and dynamic business environment make organizations face severe operational risks. However, current risk analysis methods of Information Technology (IT) resources ignore inter-process correlation and thus inter-process risk propagation. This gap needs a solution since the rigid alignment of organizations cause the risks which propagate throughout the whole organization to be the most serious operational risks. This paper presents a holistic approach for quantifying risk propagation in business processes based on the risk analysis of their underlying IT and human resources. This approach adapts financial techniques to quantify the level of risk that average and severe events on IT resources generate on individual business processes, and to quantify the risk propagation impact among dependent processes. This approach was applied to an enterprise modeling case study to quantify risk propagation for different risk epicenter scenarios. The results show that the proposed approach is capable of finding and quantifying both direct and indirect dependencies among operational assets within an organization. A high level of accuracy was observed when comparing the actual value of the process risk and the projected value considering risk propagation.

Keywords Risk quantification · Propagation analysis · Spillover effects · Business processes · IT resources · Event-based systems

1 Introduction

Nowadays, most organizations adopt a process-oriented organizational structure enabled by IT and human resources. The systematic nature of this structure usually implies a greater dependency between operational assets since a single process or resource could be supporting many other assets within the organization. Consequently, a risk materialization tends to exploit these dependencies in order to spread and cause a greater impact throughout the organization. Therefore, risk management becomes a critical discipline to control the organizational behaviour. In particular, quantitative risk analysis methods prove a useful and necessary functionality to measure and understand, in business terms, the true impact of a risk.

Current approaches quantify the risk for an individual business process (Bai et al. 2012; Fenz 2010; Conforti et al. 2016) by taking into account the correlation of events between its underlying resources. However, they ignore intra-process correlation which avoids quantifying the propagation of risk among business processes. Analyzing the correlation between the underlying resources supporting the business processes is fundamental to understand those processes that must be controlled and protected against contingencies due to their high vulnerability to risk propagation. Identifying the propagation path of risk is necessary to discover its real impact and to enable the mitigating or softening of its occurrence before it ends up spreading and causing a greater impact in the organization.

Accepted after two revisions by Jelena Zdravkovic.

O. González-Rojas (✉) · N. Castro · S. Lesmes
Systems and Computing Engineering Department, School of Engineering, Universidad de los Andes, Bogotá, Colombia
e-mail: o-gonza1@uniandes.edu.co

N. Castro
e-mail: n.castro15@uniandes.edu.co

S. Lesmes
e-mail: s.lesmes798@uniandes.edu.co

We define the following research question to address the aforementioned gaps.

RQ How to quantify risk propagation among dependent business processes and their underlying IT and human resources?

In a previous work we have defined the BP-VAR method to quantify the level of risk that events of IT resources generate for individual business processes (González-Rojas and Lesmes 2016). In this article, we have extended this work with two risk analysis capabilities: quantifying risk propagation among enterprise's operational assets, and quantifying process risk in severe IT resources' events. We used the β coefficient, typically applied in the context of finance theory, to measure the volatility of a business process in comparison with other operational assets of the enterprise (cf. the market value in a financial context). The β of a business process changes when more historical events that generate volatility are analyzed. These events correspond to variations of the expected value of quality attributes for IT resources and to variations of the expected amount of human resources required to execute process tasks. Although β changes cannot be predicted, they quantify the risk value of interdependent operational assets. We defined an algorithm with a set of propagation rules to quantify risk propagation depending on the epicenter of an undesired event. This algorithm uses the Value at Risk (VAR) and the Conditional Value at Risk (CVAR) financial techniques to quantify risks in average and severe events on IT resources respectively. These techniques and algorithms are automated in a web application allowing decision-makers to support risk impact analysis for real and simulated scenarios, and to plan business continuity.

This approach was applied within a Latin American University to analyze risks regarding the interoperability of operational assets. In this experiment we found that risk propagates mostly across processes since IT resources normally do not have a high dependency of each other. The results show a high level of accuracy in quantifying risk propagation among business processes and IT resources, when comparing historical data until date_t and the real data of date_{t+1}. For example, an error rate between 4% and 15% was found in the value of the dependent assets for a risk propagation scenario for one IT resource with $\text{CVAR}_{\phi} = 5\%$.

This paper is organized as follows. Section 2 presents the core concepts, requirements, and propagation scenarios for risk analysis within a network of processes. Section 3 discusses gaps and challenges found in related work. Section 4 presents the instantiation of the adopted financial techniques to the context of information systems and business processes. Section 5 briefly describes the functionalities of a tool we developed to simulate events that generate volatility and to quantify and predict risks. Section 6 presents the results of applying our risk analysis method to a case study. Finally, conclusions and future work are presented in Sect. 7.

2 Preliminaries and Motivation

2.1 Core Concepts

Enterprise modeling approaches create and analyze business and IT models to describe complex organizations (a network of dependent assets). Business modeling involves strategy, activities' decomposition (value chain activities, process groups, business processes, tasks), stakeholders, functions, services, products, etc. IT modeling decomposes IT services at different levels: application services, application components (information systems), and infrastructure components (system software, hardware). Our approach is aimed at quantification and propagation analysis of risks among enterprise models describing operational assets.

Operational assets refer to the set of business processes, IT resources (aka IT services at the level of application components), and human resources that implement the business model of an organization. Two assets are directly correlated if a positive or negative variation in the business value of one of them would affect the business value of the other asset in the same direction. Meanwhile, two operational assets are inversely correlated if for example the fall of one asset's value results in an increase of the other's value (e.g., if an IT resource is not available, the value of the resource and its supported processes decrease whereas the value of a human resource task increases). Operational assets can have direct dependencies explicitly represented by enterprise modeling architectures or methodologies but also indirect or implicit dependencies that have to be discovered to identify spillover effects.

Risk quantification is the estimation of the business impact (business value in monetary terms) expected from the volatility of the value of operational assets due to disruptive events. For example, external events such as exchange rate fluctuations may generate an increase in IT operation costs, lower prices from market suppliers may cause changes in IT resources, late support from suppliers may cause performance degradation of IT resources, and so on. The events that are internal to the organization but external to the business unit that is accountable for an operational asset are also considered as disruptive events

(e.g., performance degradation of internal IT resources) since both generate volatility of operational assets.

Risk propagation is the impact on business value spread across operational assets that results from the occurrence of a disruptive event. Risk propagation has two main factors that need to be taken into account: the *propagation path* across operational assets, and the *impact* that this propagation has on other assets different to the risk epicenter. Thus, the risk propagation should be directly related to the level and types of correlations that exist between the operational assets. Therefore, a risk epicenter refers to the operational asset that is directly affected by a disruptive event.

2.2 Requirements for Quantifying Risk Propagation

Nowadays, the organic nature of business processes and the ever more complex and dynamic business environment make organizations face severe operational risks (Conforti et al. 2016). Figure 1 illustrates in the archimate language a simplified view of the enterprise modeling of a Latin American University, which was analyzed as case study to validate the proposed risk analysis method. This enterprise model illustrates the dependencies between two critical business processes (i.e., Admission, Course inscription) and critical IT resources supporting them (i.e., Banner system, Authentication manager, and Database manager).

In this case study, as presented in González-Rojas and Lesmes (2016), critical business processes are highly dependent on IT services for their execution and control. These services provide 11 application services that are supported by 26 software components. These services can be assumed as event-based systems when analyzing their behaviour in terms of events associated with the variance in the value of quality attributes such availability, performance, capacity, and integrity. The high volatility associated with these services generates volatility within business processes. For example, 10 disruptive events with 120 occurrences were identified for the aforementioned IT resources.

The following discusses the requirements we have identified in the case study to quantify the risk propagation for individual operational assets and for the interactions among assets. These requirements delimit the proposed methods and rules (see Sect. 4).

Req1. Quantify risk on average events We have found approaches that quantify the risk for an individual business process by analyzing average disruptive events of short time recovery and low impact on its underlying resources (Bai et al. 2012; Fenz 2010; Conforti et al. 2016) (see Sect. 3). However, we have not found formal methods (1) to quantify the risk of a business process based on IT performance variations, (2) to quantify the risk of an IT resource for a group of processes, and (3) to forecast the

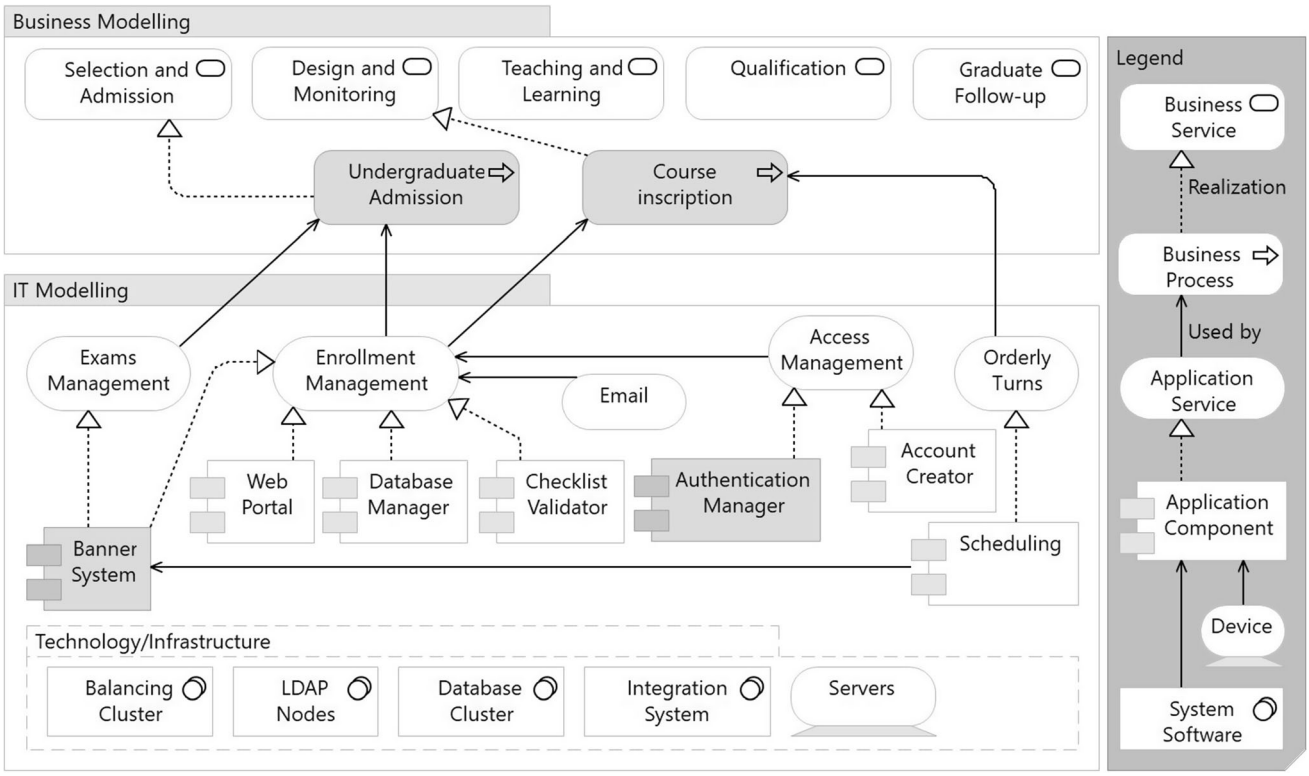

Fig. 1 Enterprise modeling of the interaction among operational assets

expected value for operational assets taking into account a daily time horizon. In general, typical disruption scenarios of operational assets are related to failures in applications, databases, and communications that do not involve physical damage of the computing and communications capabilities. These failures can generate process unavailability due to the unavailability of IT resources, integrity affectations by inconsistent data shared along process activities, and low performance and capacity to manage transactions.

Req2. Quantify risk on severe events Additional to the first requirement, there is a need to support risk quantification based on severe events that exceed the expected loss value identified for average events. A formal method is missing to quantify risk on operational assets based on severe events and to forecast the expected value for these assets taking into account a n-day time horizon. Most organizations endeavour to prepare against these shocking scenarios. Typical shocking scenarios of operational assets are related to data loss, physical damage or theft of isolated computing and communications capabilities, failures in the change controls of software and hardware, and breach of supplier contractual obligations.

Req3. Quantify risk propagation The materialization of risks usually impacts at first only one operational asset of an organization, but then also impacts other correlated operational assets. The lack of search for and quantification of risk propagation in joint processes is one of the main gaps found in risk-aware process management (Suriadi et al. 2014) (see Sect. 3), and thus, it is the main requirement tackled by our approach. Therefore, a risk quantification method must be able to find and take into account the level of direct and indirect dependencies, the risk propagation path, and the risk propagation impact. Risk propagation must consider the following analysis scenarios according to risk epicenters identified in the case study.

- *IT resource as risk epicenter* A risk materializes the occurrence of degradation events on quality attributes of the IT resource, causing a fall in their value and thus a fall in the resource value. The risk should propagate towards all those processes that have a significant correlation with the epicenter (cf. rule I in Sect. 4.3). For example, a risk concerning the *Exams Management* service must propagate to the *Undergraduate Admission* process (see Fig. 1). Then, the risk should propagate horizontally to other processes without affecting an asset more than once (cf. rule II in Sect. 4.3). Assuming that the risk propagates from the *Undergraduate Admission* process to the *Course Inscription* process, then the risk should be propagated from the second process without affecting the first process again. When propagating horizontally to multiple assets, the order of the propagation should be taken into account (cf. rule III and IV in Sect. 4.3).
- *Complementary human resources as risk epicenter* A risk materializes the lack of planned resources to perform process activities. A human resource is complementary if it has a direct correlation with the human and IT resources supporting the process. In this scenario, the propagation should occur the same way as the risk was propagated from an IT resource epicenter.
- *IT resource, with a supplementary resource, as risk epicenter* A supplementary resource has the ability of relieving another IT or human resource task. In a scenario where a degradation event impacts an IT resource which has a supplementary human resource (see *Enrollment Management* in Fig. 1), it would be expected that a significant inverse correlation arises between the human resource and other IT resources. In this case, a horizontal propagation at the resource level from the epicenter should be taken into account for significant correlated assets. Therefore, if an IT resource is impacted negatively, the risk will propagate to the human resource affecting it positively (transfer of work). Then a vertical propagation towards the process level should take place. In this case, the impacts should be aggregated before propagating, so that the positive impact caused by the human resource will reduce the negative impact caused by the degradation event in the IT resource (cf. rule V in Sect. 4.3). After propagating vertically, there should not be another horizontal propagation at the process level since one horizontal propagation has already taken place at the resource level (cf. rule II in Sect. 4.3).
- *Double risk epicenter* If multiple disruptive events occur which affect different resources, the former event must be identified. This is due to the fact that the risk propagated by the second event would have a lower impact since the value of the operational assets has already been affected. Once the risk generated for the first event has been established, then it is just a matter of propagating one risk after the other.
- *Process as risk epicenter* A process risk is generated by degradation events at the resource level. Since the risk should not propagate horizontally at the resource level (except for supplementary resources), the risk should propagate vertically towards the processes correlated with the process epicenter (cf. rule VI and VII in Sect. 4.3). In this vertical propagation, risks should be quantified for all dependent assets (cf. rule V in Sect. 4.3).

3 Related Work: Gaps and Challenges for Quantifying Risk Propagation

Current approaches for risk analysis were assessed according to their scope (individual vs joint analysis) and according to their goal: identification and monitoring, quantification, correlation analysis, propagation in non-process contexts, and process-related propagation.

Approaches for risk propagation in joint processes The author in Tallon (2011) used a Delphi technique to identify spillover effects on business processes due to the miss-alignment with IT strategy. This author shows through match surveys that spillover effects propagate from the focal process through all the whole value chain. Therefore, indirect dependencies must be identified when propagating risk. Although this approach targets inter-process risk propagation, it lacks a formal and automated method to perform the risk quantification.

Approaches for risk propagation in individual processes The most complete approaches quantify risk propagation for individual processes. Bai et al. (2012) quantify risks due to data error propagation in the information flows along the process' activities. The authors use the VAR and CVAR to quantify business process risks taking into account the error propagation, the probability of error, and the availability of error-control resources. This technique calculates only direct correlations based on the amount of information that passes from one element to another. Therefore, risk is only propagated between preceding activities, ignoring indirect dependencies or spillover effects.

Mock and Corvo (2005) model and visualize how a failure (e.g., incorrect data, application failure, misread of data) is spread across process activities. An analyst has to identify the failure root cause, to represent the failure chain, and to link a failure with a resource (hardware, software, person of charge). The authors in Conforti et al. (2016) use a sensor-based architecture to share information about a risk detection among similar process instances. They provide each process instance with a sensor capable of measuring its conditions in order to identify important changes that act as risk contingencies. This propagation accelerates the detection of risks in other instances under the execution of the same process. The author in Fenz (2010) proposes a method to quantify risks by taking into account the specific importance and the probability of availability failure of each IT resource that composes a specific process. The importance of each resource is defined by the cost of process unavailability. This method lacks of capabilities to correlate risks within IT resources, whose impact quantification could also be extended by analyzing additional degradation events (e.g., performance, integrity).

Although these approaches allow to analyze and monitor individual business processes concerning risks, they are missing capabilities to quantify inter-process risk propagation. The propagation of events within in a business process (information flows, process instances) can be used to extend our approach to the analysis of the value and risk at the different stages of the process execution and not only as an absolute process value.

Approaches linking risk to business elements Shabnam et al. (2014) present a risk measurement methodology to find actors' dependency relationships across the whole organizational model. These dependencies are explicitly identified by analyzing the vulnerability and the criticality of each element based on their number of incoming and outgoing information flows. Nevertheless, this methodology ignores indirect dependencies. The authors in Caron et al. (2013) use the Chi squared test to find the correlation of events extracted with process mining and analyzed with the help of rule-based compliance checking. Chaudhuri et al. (2016) model and quantify the performance impact of risk on a supply chain by surveying expert opinions. The authors in Bergholtz et al. (2005) allow analysts to combine different business models (i.e., value webs, process models) to identify risks and to visualize them for mitigation purposes.

Although these methods find the type and level of dependency between business elements, they lack a method to quantify the impact that a change in one element has on another one. This requires identifying direct and indirect correlations among elements, filtering significant correlations, defining a propagation path, quantifying the risk value of individual elements, and quantifying the risk propagation.

Approaches for risk propagation in a non-related process context Some approaches propose methods and tools to make decisions for security risk treatment plans for information systems. Feng et al. (2014) use colony optimization algorithms to find the most probable propagation path in a Bayesian network that represent risk factors and their respective risk propagation probabilities. Konig et al. (2016) use percolation epidemiology theory as a visual risk propagation tool in a graph that represents risks and their propagation probabilities. These methods can be used in a process-related context to identify correlations between risk factors and also to identify the propagation path among elements. However, they lack capabilities for automating the identification and quantification of risks for individual elements and also for their propagation on a network of elements. This requires the identification of implicit dependencies among business elements and their linkage.

4 A Holistic Approach for Risk Analysis in a Network of Processes and Resources

Our holistic risk analysis approach offers three methods to tackle the identified quantification requirements: (1) to quantify risks of average disruptive events concerning individual assets, (2) to quantify risks of severe disruptive events concerning individual assets, and (3) to identify and quantify risk propagation among operational assets. Section 6 illustrates the quantification of risks using these methods for the case study.

4.1 Risk Quantification on Average Events

We created the BP-VAR method to quantify the current and expected values that a business process can deliver to the organization by analyzing the performance of the leveraging IT resources (cf. Req1 in Sect. 2.2).

The *current value* of a business process is quantified by aggregating a percentage of the current value of each IT resource according to the criticality of the resource to execute the process. The current value of an IT resource is quantified by adding the expected incomes of supported business processes, the penalties on level agreements violations, the costs associated with disruptive events, and the income losses due to performance degradation (González-Rojas 2015). A value fall depends on IT resources' volatility generated by degradation events of their quality attributes (i.e., availability, capacity, performance, integrity), by the continuous changes in the service providers' costs, and by the materialization of business threats. These discrete events and the resulting monetary values must be monitored and stored continuously through time for modeling the continuous behaviour of the operational assets.

The *expected value* quantifies a range of values within which the value of the process will be in the next unit of time (n-days). The BP-VAR adapted the VAR financial technique to quantify the total loss exposure, in monetary terms, that is generated on individual business processes by degradation events on their underlying IT resources (González-Rojas 2015). The VAR assumes that external events (i.e., Market Risk) brings a high volatility over enterprise incomes over time, and thus, the volatility of an *enterprise asset* must be measured by analyzing a series of *discrete events* (at least daily) to quantify its potential *Downside Risk* (e.g., losses in costs and incomes per downtime) or *Upside Risk* (e.g., winnings in incomes per efficiency).

The VAR can be calculated by different methods. The *historical method* assumes that the risk factor of an asset will behave as its historical values did. The *variance-covariance method* assumes that the risk factor follows a normal distribution and takes into account only the values that are above the chosen ϕ confidence level, therefore, ignoring severe events that are beyond the ϕ level (Yamai and Yoshiba 2005). The *monte-carlo method* generates random variables (disruptive events) for simulation of risk factors.

The BP-VAR uses the historical data of events generated by the volatility of quality attributes on IT resources (cf. discrete events) to quantify the current value of an individual process throughout time and then it uses a confidence level to quantify the expected resource and process risk values. For example, when calculating the VAR in days of a process (P) valued in dollars with a confidence level of $\phi\%$, the results indicate that there is a $\phi\%$ probability that P will lose VAR dollars or more of its value the next day.

4.2 Risk Quantification on Severe Events

We propose an extension to the aforementioned method to quantify risks on severe events (cf. Req2 in Sect. 2.2) by adopting the CVAR financial technique [also called expected shortfall (ES)]. The CVAR "is the conditional expectation of loss given that the loss is beyond the VAR level" (Yamai and Yoshiba 2005). The mathematical definition of this technique according to Yamai and Yoshiba (2005) is as follows, where X is a random variable that represents the loss of a given asset and α represents the confidence level used to calculate its VAR and CVAR:

$$CVAR_{\alpha}(X) = E[X|X \geqslant VAR_{\alpha}(X)] \quad (1)$$

The CVAR technique gives a range of values from the minimum expected loss to infinity (Yamai and Yoshiba 2005), whereas the VAR gives as a result a range of potential losses. For example, if a portfolio (group of assets) ρ had a $\mathrm{VAR}_{(\alpha=5\%)}(\mathrm{X}) = -20\%$ (highly deviated from the normal mean) working with periods of time of 1 day, then ρ has a 5% chance of losing 20% or more of its value the next day. Instead, the $\mathrm{CVAR}_{(\alpha=5\%)}$ gives an average expected loss for the worst 5% possible events, which is a much more useful and accurate result when quantifying severe events.

Other forecasting techniques such as time series models (e.g., averaging models, exponential smoothing) and linear regression were discarded since they not take into account those exceptional cases outside the trend and since they are not specific to risk analysis.

The proposed approach quantifies the CVAR of an operational asset by analyzing its historical values to calculate the VAR and then getting the expected value by calculating the average of all those values beyond the VAR. Despite this method can only forecast events

previously observed, the CVAR will analyze risk on severe events that are under the control of an organization.

Quantifying the risk for a business process ρ with a confidence level α by using the historical method of the CVAR, it is necessary to have a considerable amount of historical values of the given process with the same periodicity. Assuming the availability of n+1 historical daily values for ρ, it is possible to obtain n returns for ρ by calculating the perceptual difference between each historical value and its precursor. Afterwards, the n return must be arranged in ascending order and the values of the $\alpha \times n^{th}$ value will be the historical $VAR_{(\alpha)}$. Finally, the CVAR corresponds to the average value of those returns that are below the historical VAR.

4.3 Quantification of Risk Propagation

The aforementioned methods quantify risks for individual business processes without quantifying the risk propagation among a network of dependent operational assets. Risk propagation requires determining the type of correlation between operational assets, and also quantifying the impact that a change in one asset has on another (cf. Req3 in Sect. 2.2).

We specialized the beta coefficient (β) from financial risk to operational risk for a group of operational assets to find the type and level of correlation among processes, IT resources, and human resources. In finance, the beta coefficient is a measure of the volatility of a given asset value to the movements of the overall market (Choe 2016). For example, if an asset φ has a β of 1.2 with respect to the 10-year bonus (which normally represents the market because of its almost null risk), it would mean that φ would be 20% more volatile than the market. In other words, if the value of the 10-year bonus increases or decreases 10%, then the value of φ would increase or decrease 12% ($\beta \times 10\%$) respectively. Other correlation techniques such as the Spearman's and Pearson's coefficients (Hauke and Kossowski 2011) and the VAR with correlation, which uses Pearson's coefficient to calculate the value of a portfolio, were discarded since they do not quantify the impact that the movement of one asset has over another one.

Equation 2 presents the mathematical formula to calculate the β coefficient as defined by Choe (2016). In this formula, μ is the market, φ is the given asset, Cov is the covariance, ρ is the correlation coefficient, and $\beta_{(\varphi,\mu)}$ is the beta coefficient of φ with respect to μ. Notice that the order of the β factors φ and μ affects the result and its meaning.

$$[t]\beta_{(\varphi,\mu)} = \frac{Cov(\varphi,\mu)}{\sigma_{\mu}^{2}} = \frac{\sigma_{\varphi}}{\sigma_{\mu}} \times \rho_{\varphi,\mu} \quad (2)$$

We instantiated this formula for measuring the movement in value of an operational asset (business process or IT resource) with respect to the movements in value of the set of operational assets (cf. Market). The covariance, correlation coefficient and standard deviations between two operational assets is calculated from their historical values (see BP-VAR). We consider that a movement in the value of an operational asset can be originated from events that are external to the business unit that is accountable for the asset. For example, management decisions on investment and security policies that increase IT operation costs, changes in IT resources due to new IT tendencies or lower prices from market suppliers, volatility in the quality attributes of IT resources from suppliers, etc.

Figure 2 illustrates in the Archimate language some β coefficients that can be calculated between a subset of the operational assets presented in the case study. Two β coefficients are calculated for each duple of operational assets ($\beta_{(e1,e2)}$ and $\beta_{(e2,e1)}$), generating a matrix relating all operational assets. Explicit β coefficients are identified from direct dependencies specified in enterprise modeling initiatives, whereas implicit β coefficients are discovered from indirect dependencies by performing correlation analysis. Each β quantifies the impact that the materialization of a risk has on other operational asset.

We defined a set of rules to determine the correct path to propagate risk based on the epicenter of the value movement: in IT resources, in complementary resources, in an IT resource with a supplementary resource, in multiple resources, and in a process. These rules cover the scenarios identified in the presented case study (see Sect. 2.2) to avoid deadlocks and double impact quantification of the same operational asset.

R1 Only significant β coefficients should be taken into account. This rule discards all the β coefficients that have an absolute value below lower than a value of significance ς established depending on the user ideals. Afterwards, it would be expected to end

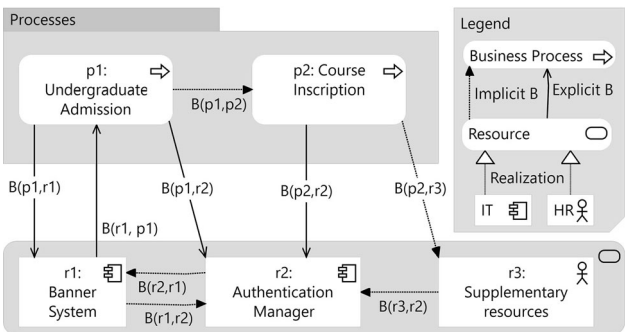

Fig. 2 β coefficients among operational assets

without significant β coefficient between the epicenter and any other assets.

R2 There should be only 1 horizontal propagation among assets of the same nature (process or resource) per disruptive event.

R3 An affected asset should try to propagate to all the assets that are significantly correlated to it without violating other rules.

R4 When propagating horizontally, each asset should be affected only once. An asset that is affected by the risk propagation from another asset must try to propagate the risk to a significantly correlated asset that has not yet propagated by ordering the affected assets from the most affected to the least affected. This process should be repeated until all the affected assets have tried propagating.

R5 When propagating vertically among assets of different nature, the impact caused by multiple processes to a resource or by multiple resources to a process should be aggregated before propagating, instead of only taking one of them. A horizontal propagation is required to capture all the impacts caused by the correlated assets of the same nature.

R6 The propagation should be done first horizontally from the epicenter in a resource level and then vertically to the processes level. If there are not significant correlated resources, then the risk should propagate vertically to the processes, then propagate horizontally in the process level and finally propagate back vertically to the resources.

R7 The propagation should not impact the resource that was the epicenter.

The risk propagation is quantified by analyzing three inputs: the matrix of β coefficients, the risk value of individual assets, and the risk epicenter. First, the standard deviation of all β coefficients, that were gathered automatically by correlating the operational assets, is calculated (e.g., 0.33). This value is multiplied for the number of deviations a business expert provides (e.g., 0.5) to discard non-significant β (i.e., β below 0.16). Then, degradation events on the performance of quality attributes of IT resources must be captured manually or automatically. When a degradation event is triggered over an operational asset (*i.e.* risk epicenter), the value fall rate of a correlated asset is computed by multiplying the value fall rate of the affected asset by their corresponding β. Finally, the risk of a correlated asset is quantified by multiplying its value fall rate and its individual risk value quantified with the BP-VAR method. For example, assume that a resource (r) has a value of 100, that a dependent process (p) has a value of 200, that their $\beta_{(p,r)} = 0.4$, and that the resource is expected a value fall rate of 10% due to degradation events (cf. CVAR). Then, if a degradation event is triggered on the resource, the risk is propagated to the process with a value fall rate of 4%. This change in value triggers a new risk epicenter in a dependent asset, and thus, the propagation rules must be applied to quantify risks for the network of processes and resources.

5 A Tool for Quantifying Risk Propagation

The aforementioned quantification methods were implemented into a web application to validate and simulate scenarios of risk propagation. This application follows two architectural styles: Model-View-Controller (MVC) and component-based. Functionalities, models, and even data are encapsulated in an isolated process-specific component to ease its evolution. The process-specific component provides the following services:

- Daily risk value quantification: Fig. 3 illustrates the next-day risk value for the *Banner System* IT resource when simulating a degradation event of its availability (up to 15%). This value exceeds the desired limits (70–99.999%) degrading the IT resource. With this event a downside risk of 50.000 USD can be quantified by the tool when comparing the current and simulated values. The volatility of the resource value is quantified by expected losses due to incomes and agreements penalties.

- N-Day risk value quantification: Using series of historical events of the values variation of the quality attributes affecting an IT resource, a simulation of the

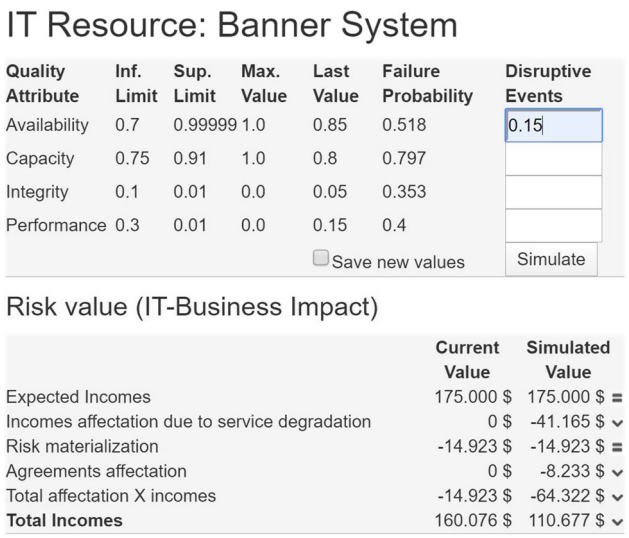

Fig. 3 Daily risk value simulation for an IT resource

n-day resource value is performed, with a defined confidence level.
- Daily risk value quantification with correlation: From series of historical resource values, a simulation of the next-day resource value is performed, and a comparative report is presented, now taking into account the resource's correlation.
- Quality attributes risk-correlation quantification: From an event of an alteration of one or multiple values of a risk level related to a quality attribute affecting an IT resource, a simulation of the new correlation value and therefore the next-day resource value is performed and a comparative report is presented. The variation of the resource value is generated by a degradation event.
- Quantification of risk propagation: From an event of a value alteration in one or more IT resources, the value propagation analysis is performed, generating a propagation graph that clearly indicates the direction and magnitude of the propagation effect across the whole operational assets.

The next section illustrates these functionalities in terms of the identified risk quantification scenarios.

6 Validation

6.1 Subjects, Design, and Variables

We designed three experiments that compare historical data of risk quantified until $date_t$ and the real data of $date_{t+1}$. The error rate and accuracy measures are calculated in these experiments.

Dataset description We used the historical data of the operational assets described in the case study (see Sect. 2.2) to validate the proposed method. The direct dependencies between processes and IT resources have been quantified in a previous work (González-Rojas 2015). The result of that empirical study is an enterprise modeling dataset[1] that contains approximately 13,500 elements with analysis data for the identified dependencies. The expected daily incomes represent the average of the actual incomes for final business processes received in 1 year. Costs are characterized by the associated IT resource, a concept related to the total cost of ownership (acquisition, support, communications, etc.), and the corresponding amount of money. Agreements on IT resources are represented by its type (service, operational, underpinning contract), the client or beneficiary (e.g., a customer, a business unit), the provider or whoever is responsible for the resource, the validity time, the related quality attribute if it this applies, the different service levels with lower and higher expected values, and the monetary penalty for agreement violation. Risks concerning IT resources are characterized by the risk factor, the impact (measured from 1-Very low to 5-Catastrophic), the frequency of occurrence (measured from 1-Exceptional to 5-Frequent), and the associated threats. Events degrading IT resources are represented by a quality attribute (i.e., capacity, availability, performance, integrity), the ideal value (the limit), an expected minimum value, an expected maximum value, and the current value stored with a timestamp.

This dataset contains a thousand records of values for quality attributes (i.e., availability, integrity, capacity, and performance) that were captured for each related IT resource during 12 months. The value of these quality attributes was gathered by the coordinator of the IT operation area of the enterprise by monitoring almost daily. Then the value of the processes was valuated individually (González-Rojas and Lesmes 2016) and additional data of IT resources' performance regarding quality attributes was gathered during 6 months.

The historical data series of values obtained for quality attributes were used to quantify the volatility of the IT resources' value. These values were used as input for statistical tools to obtain the mean and standard deviation (σ) parameters that fit the normal distributions assumed for each quality attribute. For example, the Authentication Manger resource in terms of integrity behave with a $mean = 0.332$ and $\sigma = 0.161$. Then a weighted deviation was calculated for each IT resource. We assume that an IT resource behaves without a specific tendency since the risk value quantified by $date_t$ is probably going to be the same (its mean) for $date_{t+1}$. In the case of a degradation in a quality attribute, the value of the IT resource is assumed to change within a belt distribution around the value of $date_t$.

6.2 First Experiment: Risk Analysis on Individual Assets

Setup This experiment compares the quantification of risk when using the VAR and CVAR instantiation for individual assets. We compare the current value of a process for a certain date, quantify the expected risk for the following day, and compare that forecasting with the actual value of the process on the next day. The same analysis is performed for an IT resource to understand the trigger of the risk.

Results Figure 4 illustrates the current value ($395.408 USD) for the Undergraduate Admission process at a particular date (2015-04-26). It also illustrates the expected downside risk for the next day (CVAR = $363.999 USD

[1] The risk quantification dataset can be found at: https://github.com/governit/EnterpriseModelling.

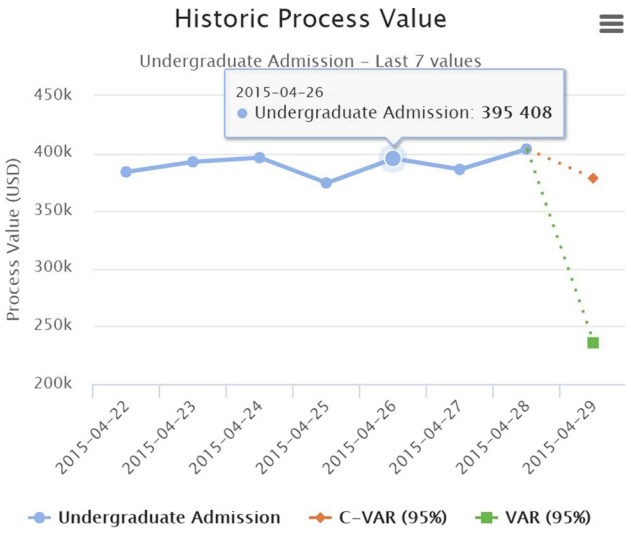

Fig. 4 Risk quantification with confidence level of 95%

and VAR = $235.858 USD) by assuming a confidence level of 95%. The results show a 61% of VAR accuracy and a 94% of CVAR accuracy when comparing these forecasting results with the actual process value ($385.966 USD) on the next day (2015-04-27).

The process value is obtained by aggregating the value of its three underlying IT resources for both date_t and date_{t+1}: Authentication ($\$_t$ 132.490 USD vs $\$_{t+1}$ 122.918 USD), Banner ($\$_t$ 105.419 USD vs $\$_{t+1}$ 105.549 USD), and Database ($\$_t$ 157.498 USD vs $\$_{t+1}$ 157.498 USD). This shows that the downside risk was quantified for a degradation of the leveraging IT Authentication resource, which was generated by a variation event on the quality attribute capacity.

Figure 5 illustrates the current value of the degraded IT authentication resource ($167.710 USD) in terms of the group of processes at the same date (2015-04-26). The area under the curve (at the right side) represents the probability of the resource to increase or decrease its value to a value within this area. When comparing the expected downside risk for the next day (CVAR = $154.467 USD and VAR = $125.875 USD), by assuming a confidence level of 95%, with the actual resource value ($155.592 USD) on the next day (2015-04-27), the VAR obtained an 81% of accuracy whereas the CVAR metric had a 99% of forecasting accuracy.

The results of the $\text{CVAR}_{(\alpha=5\%)}$ denoted a better prediction than the $\text{VAR}_{(\alpha=5\%)}$. This is because the CVAR considers the 5% higher impact events faced by the resource, whereas the VAR considers a large range of events within the given probability.

6.3 Second Experiment: Risk Analysis on Joint Assets

Setup We calculated the β coefficient in both directions for every possible combination of two operational assets (processes and IT resources) based on their historical value data. Afterwards, a severe risk for any of the operational assets was quantified by using the historical CVAR technique. Then, we recreated each of the analysis scenarios according to the risk epicenter (see Sect. 2.2) by comparing the current value of operational assets at a specific date and the projected values of risk propagation when simulating disruptive events for those assets. To do this it was necessary to add a dummy human resource to the baseline case study in order to analyze risk propagation on scenarios with complementary and supplementary resources. Therefore, generic β coefficients between the operational assets and the human resource were added.

We validated the defined risk epicenters' scenarios (see Sect. 2.2) by applying the defined propagation rules to the operational assets of the case study (see Sect. 4.3). We used the $\text{CVAR}_{(\alpha=5\%)}$ to quantify the impact of the materialized risk for the three scenarios with IT resources as epicenter. For these scenarios, a degradation event in the Banner System (availability = 15%) was simulated for a particular date (2015-04-28). Then, direct and indirect dependencies were compared before and after risk propagation, and the quantified propagated value for each operational asset was compared with the actual value on next day.

Results for risk propagation with an IT resource as epicenter Figure 6 illustrates the propagation path used to quantify risk for a subset of the operational assets of the case study. There were no significantly correlated resources to propagate horizontally starting from the epicenter (Banner System). Therefore, risk propagated vertically towards both processes since they were both significantly correlated to the IT resource.

Since both processes were already affected, no other horizontal propagation was made at the process level. Instead, risk propagated vertically to the Authentication IT resources because of the negative variation in value of the Course Inscription process (a disruptive event at process level). Low error rates were obtained when comparing risk quantified on propagation with the actual value: 12% for the Banner System (actual value = $125.646 USD), 6% for the Authentication Manager resource (actual value = $146.744 USD), 7% for the Course Inscription process (actual value = $238.387 USD), and 15% for the Undergraduate Admission process (actual value = $359.398 USD).

Results for risk propagation with a human resource as epicenter Figure 7 illustrates the propagation path from a complementary human resource that degrades its

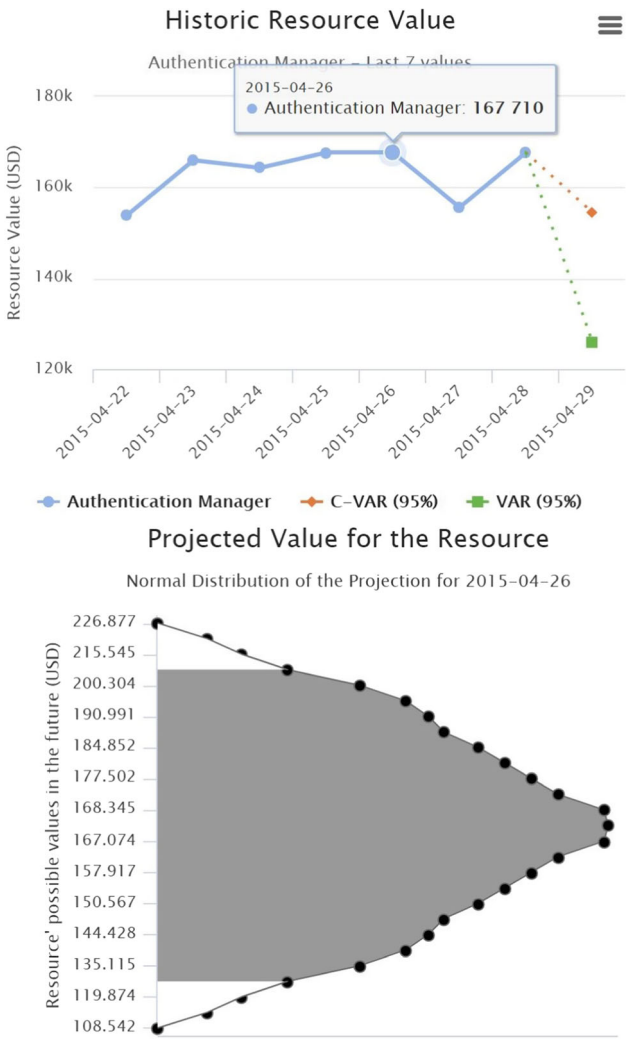

Fig. 5 VAR and CVAR quantification in an IT resource

availability of resources by 20%. For this scenario we assumed significant β coefficients among the simulated human resource and processes ($\beta_{(p1,s3)} = 0.23$ and $\beta_{(p2,s3)} = 0.4$) since we did not have the historical data of the resource required to use the CVAR technique. Lower error rates were obtained when comparing risk quantified on propagation with the actual value: 4% for the Banner System (actual value = \$125.646 USD), 8,3% for the Authentication Manager resource (actual value = \$146.744 USD), 1,4% for the Course Inscription process (actual value = \$238.387 USD), and 3,4% for the Undergraduate Admission process (actual value = \$359.398 USD). In this scenario risk propagated horizontally among business processes since the Undergraduate Admission process was not impacted previously. Although IT resources keep operating as expected, the lack of people to use them impact their value since the processes do not perform as expected.

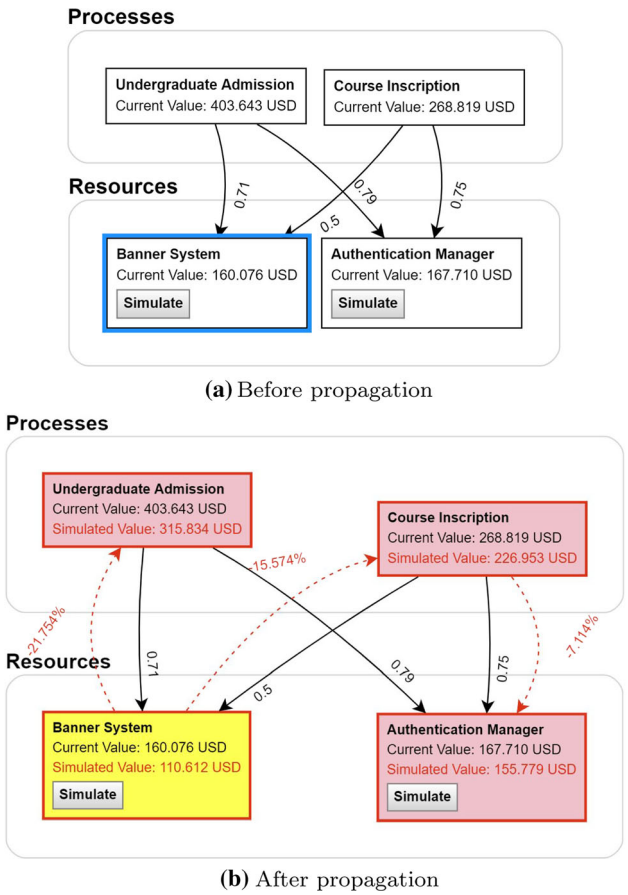

Fig. 6 Risk propagation for an IT resource epicenter

Results for risk propagation for an IT resource with a supplementary resource Figure 8 illustrates the propagation path to quantify risk in the absence of the Authentication IT resource and with the Banner System IT resource as the epicenter. We assumed that the β coefficients are inversely related between IT resources and human resources since they are supplementary resources (negative correlation). There were no correlated resources to propagate horizontally from the epicenter (Banner System). Therefore, risk propagated vertically to both processes since they were both significantly correlated to the IT resource. Since both processes were already affected, no other horizontal propagation was made at the process level. Instead, risk propagated vertically to a simulated human resource from both processes. The obtained error rates are the same as the ones obtained for the IT resource epicenter and for both processes of the first scenario. This is because the supplementary human resource reduced the negative impact caused by the missing IT resource. However, an additional method to quantify risk on human resources is still required.

Results for risk propagation with double risk epicenter This scenario was already evidenced during the first and third

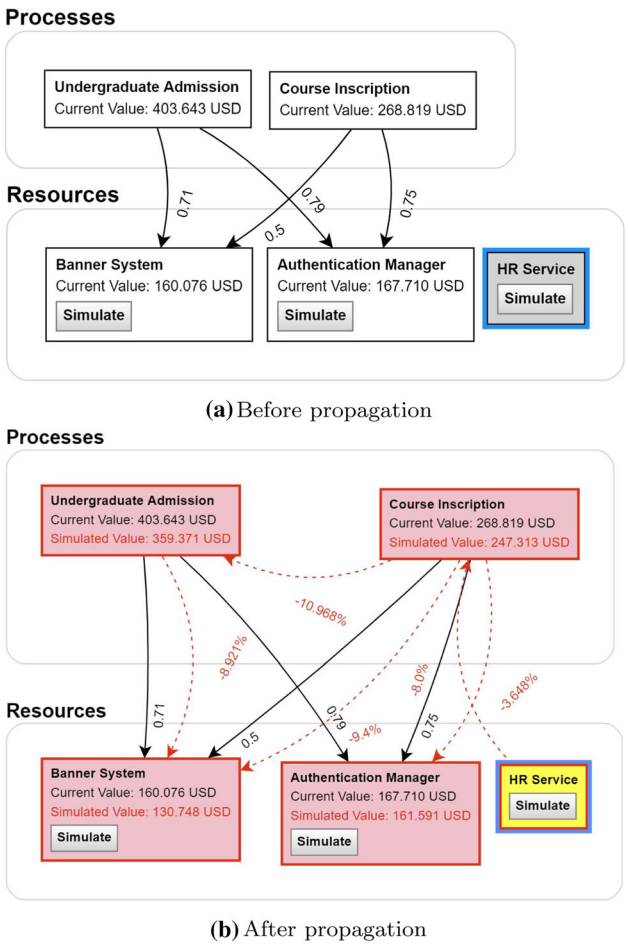

Fig. 7 Risk propagation for a complementary human resource epicenter

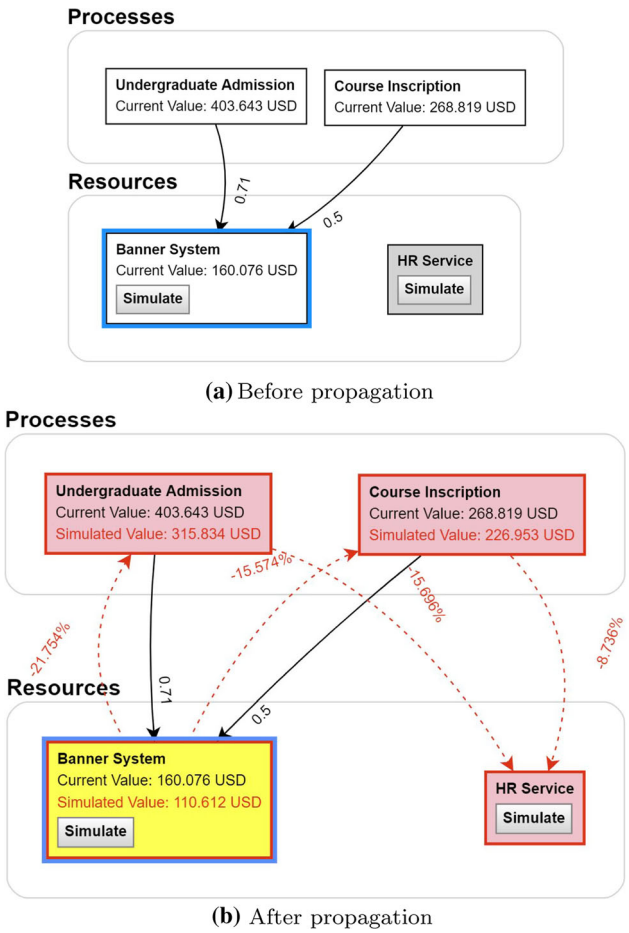

Fig. 8 Risk propagation for an IT resource with a supplementary resource

scenarios since a variation in the value of a process value, as a consequence of a risk propagated from an IT resource, propagates risk to underlying resources.

6.4 Third Experiment: Correlated Risk Analysis

Setup Three types of risk analysis scenarios performed on individual processes (stable, downside risk, and upside risk) are compared with and without the correlation component. The quantitative results without correlation were taken from González-Rojas and Lesmes (2016). The inter-process correlation presented in this paper enabled the inclusion of additional relationships and information to enrich the results. Given the fact that the quantification of the risk propagation does not provide a range of values, only one of the downside or upside risks is analyzed. A 1-day VAR projection with confidence value of 65% is analyzed for all scenarios.

Results for a stable scenario. Table 1 presents the accuracy results for a stable scenario that was identified from events in the time from 2015-04-20 to 2015-04-24. The set of recorded values of the processes experienced a low variation, mainly due to the constant behaviour of the quality attributes levels of their supporting IT resources.

The accuracy of quantifying the expected value for a stable scenario increased with the correlation. For example, the expected value without the propagation component was quantified within the 257.094 USD and 267.007 USD for the Course Inscription process, whereas the current value stored at 2015-04-24 was 263.784 USD. Similarly, the current value stored at 2015-04-24 for the Undergraduate Admission process (396.548 USD) is within the range of expected values (385.238 USD and 399.846 USD). In contrast, the risk quantified by the correlation predicted values with low variations from the actual value. A variation of 0,502% was obtained for the Course Inscription process (expected value = 263.365 USD), and a variation of 0.701% for the Undergraduate Admission process (expected value = 395.293 USD).

Results for a downside risk scenario Table 2 presents the accuracy results for a downside risk scenario that was identified from 2015-04-24 to 2015-04-25. During that

Table 1 Accuracy results for a stable scenario

	Course inscription		Undergraduate admission	
	Downside risk (%)	Upside risk (%)	Downside risk (%)	Upside risk (%)
Without β	97.5	98.78	97.15	99.17
With β	99.85	–	99.69	–

Table 2 Accuracy results for a downside risk scenario

	Course inscription		Undergraduate admission	
	Downside risk (%)	Upside risk (%)	Downside risk (%)	Upside risk (%)
Without β	96.66	92.67	96.11	92.17
With β	95.93	–	92.75	–

period of time the set of recorded values of the processes experienced a significant decreasing variation, mainly produced by the degradation of a leveraging IT resource (Banner System).

The analysis of risk propagation decreased the accuracy level when quantifying the expected value for a downside scenario. We assume this is because we are using the CVAR with the same VAR confidence level ($CVAR_{(\alpha=35\%)}$), which increases the potential impact. For example, the expected value without the propagation component was quantified within 258.796 USD and 268.778 USD for the Course Inscription process, whereas the current value stored on 2015-04-25 was 250.420 USD. Similarly, the expected value for the Undergraduate Admission process was quantified within 388.777 USD and 403.518 USD, whereas the current value stored on 2015-04-25 was 374.203 USD. For both processes a variation of 3,34% and 3,89% respectively were generated from the projection limits. In contrast, the risk quantified by the propagation component shows higher variations such as − 8.936% for the Course Inscription process (expected value = 240.213 USD), and − 12.478% for the Undergraduate Admission process (expected value = 347.067 USD).

Results for an upside risk scenario Table 3 presents the accuracy results for an upside risk scenario that was identified from 2015-04-16 to 2015-04-17. During that period of time the set of recorded values of the processes experienced a significant increase in their value, mainly produced by the optimal performance of their three underlying IT resources.

The analysis of risk propagation increased the accuracy level when quantifying the expected value for an upside risk scenario. For example, the quantification of risk without the propagation component was estimated within 247.501 USD and 257.088 USD for the Course Inscription process, whereas the current value stored on 2015-04-17 was 265.737 USD. Similarly, the expected value for the Undergraduate Admission process was estimated within 373.564 USD and 387.721 USD, whereas the current value stored on 2015-04-17 was 399.266 USD. For both processes a variation of 3.25% and 2.89% respectively were generated from the projection limits. In contrast, the risk quantification predicted by the propagation component presented a variation of 4.267% for the Course Inscription process (expected value = 263.033 USD), and a variation of 5.959% for the Undergraduate Admission process (expected value = 403.325 USD).

The propagation component proposed to quantify risk increased the accuracy of the analyzed scenarios and allowed to take into account a higher number of variables and dependencies among operational assets.

6.5 Threats to Validity

The proposed risk quantification method depends highly on the availability of historical analysis data regarding the operational assets. The lack of complete and consistent information can limit its adoption in enterprises. To guarantee a higher level of accuracy for risk quantification, the proposed method should be validated for the complete set of operational assets involved in the case study. However, this information is not yet gathered.

Table 3 Accuracy results for an upside risk scenario

	Course inscription		Undergraduate admission	
	Downside risk (%)	Upside risk (%)	Downside risk (%)	Upside risk (%)
Without β	93.14	96.75	93.57	97.11
With β	98.99	–	–	98.99

We instantiated the VAR and CVAR financial techniques by using the historical and variance-covariance methods. However, these methods assume that an operational asset will behave as it did in the past. This can limit the prediction results by considering only those event risks that have already been observed and registered. We assumed a 1-day recovery time when triggering average and severe disruptive events on IT assets. However, the impact for catastrophic events, those that go beyond the control of a mature organization and with an uncertain recovery time, exceed the prediction of the proposed method extensively. Some examples of catastrophic events are the loss of a data center, a cyber-attack which causes multiple utility and financial systems to collapse, the internet crash. Accordingly, temporal restrictions can be incorporated into the proposed approach to support a non-lineal analysis.

7 Conclusion

Our risk analysis proposal is capable to quantify the impact of a risk taking into account its propagation. Thanks to the functionality provided by the β coefficient our proposal quantifies risks by considering the correlation between all the different operational assets regardless whether they have a direct or indirect dependency. This is a very important functionality, since it enables to find and consider inter-process correlation and spillover effects. We successfully instantiated and integrated both the β coefficient's propagation capabilities and the CVAR risk quantification capabilities for analyzing a network of inter-dependent processes and IT resources.

Validation results show a low error rate over the performed estimations, which analyze particular behaviours of operational assets. However, further research is required to analyze the estimation error over an entire timeframe. The lack of public available datasets can be the main reason why current state of the art does not provide solutions for quantifying inter-processes risk propagation. Quantifying risk propagation requires an input model which represents the wide amount of process and IT assets, as well as the large amount of analysis data within their dependencies (e.g., risks, costs, incomes). The high complexity and effort required to empirically build the described dataset prevents our approach from being validated extensively with more case studies.

The paper assumes that risks originate only in IT resources and from there propagate to processes and other resources. The quantification of risk propagation should be extended to more dimensions involved in business operations. First, the validation of correlation scenarios with human resources needs further research since the results obtained were based on assumptions and generic data. Additional analysis dimensions such as time constraints for risk propagation and SLA violations in the performance of business processes must be modeled. Finally, further research is required to analyze propagation scenarios with multiple epicenters in order to carry out a synchronous risk quantification.

In addition, we plan to automate the identification of the metrics and events of IT resource's quality attributes to avoid manual and human dependent actions that limit the adoption of the proposed method. An enterprise-wide adoption of this approach will require the integration with enterprise modeling tools to automate the enriched specification of inter-dependent operational assets, and a standardized format to consolidate information from existing IT management processes and tools (configuration, service level, financial).

References

Bai X, Krishnan R, Padman R, Wang H (2012) On risk management with information flows in business processes. Inf Syst Res 24(3):731–749

Bergholtz M, Bertrand G, Paul J, Michael S, Petia W, Jelena Z (2005) Integrated methodology for linking business and process models with risk mitigation. In: 1st international workshop on requirements engineering for business need and IT alignment (REBNITA05)

Caron F, Vanthienen J, Baesens B (2013) A comprehensive investigation of the applicability of process mining techniques for enterprise risk management. Comput Ind 64(4):464–475

Chaudhuri A, Srivastava S, Srivastava RK, Parveen Z, Huang Z, Wang K (2016) Risk propagation and its impact on performance in food processing supply chain: a fuzzy interpretive structural modeling based approach. J Model Manag 11(2):660–693

Choe G (2016) Stochastic analysis for finance with simulations, chapter 20. Springer, Berlin, pp 273–274

Conforti R, Fink S, Manderscheid J, Roeglinger M (2016) PRISM – a predictive risk monitoring approach for business processes. In: International conference on business process management, Springer, Heidelberg, pp 383–400

Feng N, Wang HJ, Li M (2014) A security risk analysis model for information systems: causal relationships of risk factors and vulnerability propagation analysis. Inf Sci 256:57–73

Fenz S (2010) From the resource to the business process risk level. In: Proceedings of the South African information security multi-conference (SAISMC'2010), pp 100–109

González-Rojas O (2015) Governing IT services for quantifying business impact. In: Raimundas M, Marlon D (eds) BIR 2015: perspectives in business informatics research, vol 229. LNBIP. Springer, Cham, pp 97–112

González-Rojas O, Lesmes S (2016) Value at risk within business processes: an automated IT risk governance approach. In: La Rosa M, Peter L, Oscar P (eds) BPM 2016: business process management, vol 9850. LNCS. Springer, Cham, pp 365–380

Hauke J, Kossowski T (2011) Comparison of values of Pearson's and Spearman's correlation coefficients on the same sets of data. Quaest Geogr 30(2):87–93

Konig S, Rass S, Schauer S, Beck A (2016) Risk propagation analysis and visualization using percolation theory. Int J Adv Comput Sci Appl 7(1):694–701

Mock R, Corvo M (2005) Risk analysis of information systems by event process chains. Int J Crit Infrastruct 1(2–3):247–257

Shabnam L, Haque F, Bhuiyan M, Krishna A (2014) Risk measure propagation through organisational network. In: 2014 IEEE 38th international computer software and applications conference workshops (COMPSACW), IEEE, pp 217–222

Suriadi S, Weiß B, Winkelmann A, ter Hofstede AHM, Adams M, Conforti R, Fidge C, La Rosa M, Ouyang C, Rosemann M et al (2014) Current research in risk-aware business process management: overview, comparison, and gap analysis. Commun Assoc Inf Syst 34(1):933–984

Tallon PP (2011) Value chain linkages and the spillover effects of strategic information technology alignment: a process-level view. J Manag Inf Syst 28(3):9–44

Yamai Y, Yoshiba T (2005) Value-at-risk versus expected shortfall: a practical perspective. J Bank Finance 29(4):997–1015