Business Process-Based Resource Importance Determination

Stefan Fenz[1], Andreas Ekelhart[2], and Thomas Neubauer[2]

[1] Institute of Software Technology and Interactive Systems
Vienna University of Technology, A-1040 Vienna, Austria
fenz@ifs.tuwien.ac.at
http://www.ifs.tuwien.ac.at
[2] Secure Business Austria, A-1040 Vienna, Austria
{ekelhart,neubauer}@securityresearch.at
http://www.sba-research.org

Abstract. Information security risk management (ISRM) heavily depends on realistic impact values representing the resources' importance in the overall organizational context. Although a variety of ISRM approaches have been proposed, well-founded methods that provide an answer to the following question are still missing: How can business processes be used to determine resources' importance in the overall organizational context? We answer this question by measuring the actual importance level of resources based on business processes. Therefore, this paper presents our novel business process-based resource importance determination method which provides ISRM with an efficient and powerful tool for deriving realistic resource importance figures solely from existing business processes. The conducted evaluation has shown that the calculation results of the developed method comply to the results gained in traditional workshop-based assessments.

Classification: Static process analysis.

1 Introduction

As almost every business decision is based on data, reliable information technology (IT) is a prerequisite for business continuity and therefore crucial for the entire economy [1,2]. The importance of information technology brought up the urgent need to ensure its continuous and reliable operation and to protect the processed and stored information respectively. Recent research has shown the impact of security breaches on the market value of organizations. According to [3] organizations lost on average approximately 2.1% of their market value within two days surrounding security breaches. The interconnectedness of the global economic system enables information security threats such as computer viruses to proliferate in a very fast way. Due to the rising economic relevance of IT risks, organizations should strive for adequately managing these risks.

Information security risk management (ISRM) is a process which allows IT managers to balance the operational and economic costs of protective measures

U. Dayal et al. (Eds.): BPM 2009, LNCS 5701, pp. 113–127, 2009.

and achieve gains in mission capability by protecting the IT systems and data that support their organizations' mission [4]. The two main phases of this process are Risk Assessment, which focuses on risk identification and evaluation, and Risk Mitigation, which refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures. Continual evaluation and assessment are necessary to keep the required level of security and thus are cornerstones in successful risk management. As we focus in this work on the Impact Analysis, which is part of the Risk Assessment process, we will briefly state the theoretical groundwork. In the information security context risk is defined as a function of the probability of a given threat-source exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization [4]. According to NIST 800-30 the level of impact is determined by the potential mission impacts and in turn produces a value for affected IT assets and resources. This description points out the information necessary for a successful impact analysis, keen understanding and knowledge of the processes performed, and secondly, system and data criticality values of connected resources (*importance* to an organization). The importance indicates the organizational impact if the considered resource is not longer able to conduct its designated tasks (we focus on the availability aspect). Even though a great deal of research has been conducted and manifold ISRM approaches evolved in the past 30 years, gathering this data is still mostly a manual and work intensive process, relying on interviews and questionnaires with system and information owners. The following problems are connected with the determination of the importance of an organization's resources:

- Business processes are subject to constant change. While flexible workflow design is a key factor in keeping pace with modern market trends [5,6,7], it poses a major challenge for ISRM [8,9]. Changing or newly introducing business processes requires a reevaluation of the current risk situation. Resources could be used in a dangerous new context or new activities could introduce critical vulnerabilities. Considering time consuming risk assessments, companies often refrain from continuous risk evaluation.

- Detailed and correct knowledge about business processes and attached resources is required, otherwise gained risk values will be incorrect. A consistent and up-to-date documentation of processes and connected resources is often not available and time consuming and error prone to create.

- While system and information owners should have a grounded knowledge of the processes and resources in their domain, resources can be used by various processes. Aggregating the resource importance from the process- to the organization-wide level is, again, time consuming and error prone.

- Even if there are well defined rating criteria, due to the involvement of various system and information owners (e.g., multiple departments) an objective rating cannot be guaranteed.

Determining the resource importance, based on business processes, is an elemental and reoccurring step in ISRM. With regard to the identified problems our research aims at answering the following question:

– How can business processes be used to determine resources' importance in the overall organizational context?

First, we elaborate on the research question by analyzing existing approaches in the field of business process analysis (cf. Section 2). Second, we aim at developing concepts to determine the organization-wide importance of resources based on business processes and the corresponding activities (cf. Section 4). Third, the gathered research results are prototypical implemented (artifact-building) and evaluated by comparing its output to a traditional workshop-based assessment (cf. Section 5 and 6).

2 Existing Approaches

This section provides an overview how existing approaches address ISRM with focus on the resource importance determination. Today, a collection of information security risk management methods, standards and best-practice guidelines, such as CRAMM [10], NIST SP 800-30 [4], CORAS [11], OCTAVE [12], EBIOS [13], and recently ISO 27005 [14] exist. High level standards such as NIST SP 800-30 and ISO 27005 address the step of determining the importance of an organization's resources by recommending the collection of information on business processes and system/data criticality and sensitivity. Should there be no existing documentation available, such as business impact analysis (BIA) reports, interviews should be conducted with system and information owners to determine the impact level of IT systems and data in case of loss or degradation of confidentiality, integrity, and/or availability. The magnitude of impact can be assessed quantitative or qualitative.

The reference model for process-oriented IT risk management by Sackmann [8,15] connects Business Processes, IT Applications and Infrastructure, Vulnerabilities, and Threats to model IT security relevant risks and their effects on each layer. Therefore, Sackmann's reference model can be used for modeling threat consequences on business processes. The main problem of the approach is that it is not possible to describe how the modeled business processes and IT applications/infrastructure interrelate in detail. IT applications and infrastructure are assigned on the process- and not on the activity-level. Therefore, it is not possible to determine realistic importance values of the required IT applications/infrastructure, leading to biased risk values for the business process.

Another approach described in [16] uses the Tropos Goal Risk framework in the context of business continuity management. Business objects are annotated with utility values for the organization. Those high level goals can be achieved by tasks which again can depend upon resources. Negative events affect resources and thereby threaten the business goals. Utility values for goals are assigned manually by business owners in advance. Resource utility can be calculated by

summing up the values generated by a resource. While this approach offers a possibility to determine resource utility the following open challenges remain: (i) no standardized business process modeling language has been used, (ii) path possibilities have not been taken into consideration, and (iii) multiple usage of a resource in one process is not addressed.

In 2003 van der Aalst et. al. [17] point out that for information-intensive products, such as insurances, loans, permits, and many other services, the relationship with the supporting workflow process is often neglected. They primary goal was to support users in designing efficient and effective workflows based on product information rather than on subjective interpretations of managers, consultants, and IT experts. Their work is insofar important for our research as they strive to provide a methodology to automatically calculate the value of process elements. A Product/Data Model with nodes representing end-products, raw materials, purchased products, and subassemblies, is the basis for their calculations. In this tree-like structure various paths lead to the top element. Costs and required throughput times of child elements define the parent's characteristics. After node characteristics (costs, flow time, probability, and constraints) have been quantitatively defined, it is possible to provide insights, such as cost or flow time, on paths to reach the top level product.

Important to mention is the approach in [18] which explicitly focuses on business process-oriented resource evaluation. To improve accuracy of risk analysis results, they argue that resources have different values according to their business contribution, department utilization and user position, and are not sufficiently defined by purchase costs or maintenance expenses. Delphi teams apply weights for the 'business process-oriented classification factors' for each resource and thereby the resource value is calculated. While this approach offers categories and a methodology to evaluate resource values it still depends on Delphi teams to analyze business processes and resources, and to assign values accordingly to their cognition and experience.

Our paper makes a first step towards addressing the shortcomings of existing approaches and provides a business process-based resource importance determination method. Based on the organization's business processes, their overall organizational importance, and the resources required by their activities, the proposed method automatically determines the organization-wide importance of the involved resources. The advantages of the proposed solution are: (i) the necessary input data is restricted to machine-interpretable business process representations including required resources and the importance of the business process, and (ii) assuming that the required input data is already available our approach provides ISRM with fast results regarding resource importance, which are based on the business processes' structure and resource involvement.

3 Preliminaries

In this paper we use Petri nets to model business processes (cf. [19,20,21]). For the purpose of this paper, places represent the current state and causal dependencies of the business process whereas transitions represent the activities involved

in the considered business process. According to [20] we use the building blocks AND-split, AND-join, OR-split, and OR-join to model sequential, conditional, and parallel routing. Sequential routing deals with casual relationships between activities. Compare *A1* - *P2* - *A2* in Figure 1 for an example. Parallel routing uses AND-split and AND-join to model parallel activities (see the AND-split at *A4* and the AND-join at *A12* in Figure 1). Conditional routing is modeled by OR-split and OR-join building blocks to allow for routing which may vary between cases [20]. Place *P3* and *P15* in Figure 1 show a typical OR-split and OR-join. With regard to the stated research questions it is required that these typical business process building blocks are supported by our contribution.

4 Business Process-Based Determination of the Resource Importance

Based on any given business process structure, we developed a method to determine the importance of a resource in the given organizational context. The importance indicates the organizational impact if the considered resource is not longer able to conduct its designated tasks (we focus on the availability aspect). The unit which is used to express the resource importance depends on the unit used to describe the importance of the overall business process. Monetary (e.g., Euros per hour) or qualitative (e.g., high, medium, and low) ratings are amongst others an option to express the importance of the business processes and the required resources. Assigning a value for the overall business process importance is usually done by the process owner in collaboration with the management. While various factors, such as business process profit, reputation or service level agreements, can influence the decision, the final figures depend on the organization's focus. Likewise, a decision for quantitative or qualitative ratings is based on the focus and available information. This high level of flexibility allows organizations to target their individual requirements. Despite this flexibility, once an organization has made a decision, it is necessary to follow a consistent rating process throughout the organization over all processes to guarantee consistent results. Our approach expects consistent process ratings, and calculates resource importance values, dependent on the resources' business process involvement and the business process structure.

4.1 Assumptions

Before going into the details of the proposed calculation model, we have to state some requirements: the considered business process has to (i) indicate which resources are required by the included activities, (ii) be correctly modeled so that it can be mapped to a valid Petri net, and (iii) provide an importance value for the considered organizational context. Each resource has (i) a business process-wide, local importance value $I_L(R_i)$, and (ii) an organization-wide, global importance value $I_G(R_i)$. The calculation model for these variables is described in the following subsections.

4.2 Determining the Resource's Local Importance

Let A_i be Activity i, P_i Place i, R_i Resource i, $E_{P_iA_j}$ the Edge which connects Place i and Activity j, and $E_{A_iP_j}$ the Edge which connects Activity i and Place j. The local resource importance $I_L(R_i)$ refers to the resource's importance in the context of the analyzed business process. While $I_L(R_i)$ is expressed in either quantitative or qualitative values, the local importance of an activity $I_L(A_i)$ is always expressed by a value between 0 and 1. $I_L(A_i)$ is calculated by summing up the local importance values of its ingoing edges E_{PA_i} and dividing it by the amount of ingoing edges $|E_{PA_i}|$:

$$I_L(A_i) = \frac{\sum_{j=1}^{|E_{PA_i}|} I_L(E_{P_jA_i})}{|E_{PA_i}|} \tag{1}$$

Similar to $I_L(A_i)$, the local importance I_L of place P_i is determined by summing up the local importance values of its ingoing edges (how we calculate the local importance values of edges is described in Equations 3, 4, and 5). Set E_{AP_i} includes the ingoing edges E of place P_i. If $|E_{AP_i}|$ is empty, $I_L(P_i)$ is set to one (this would be the first place in the Petri net).

$$I_L(P_i) = \begin{cases} 1 & , E_{AP_i} = \emptyset \\ \sum_{j=1}^{|E_{AP_i}|} I_L(E_{A_jP_i}) & , E_{AP_i} \neq \emptyset \end{cases} \tag{2}$$

According to the previous equations, we need the local importance of all ingoing edges E of place P_i and activity A_i to calculate their local importance value $I_L(P_i)$ and $I_L(A_i)$. If edge E connects an activity and a place (potential AND-split) the local importance $I_L(E_{A_iP_j})$ equals the importance of the edge origin element A_i:

$$I_L(E_{A_iP_j}) = I_L(A_i) \tag{3}$$

If edge E connects a place and an activity (potential OR-split) the local importance $I_L(E_{P_iA_j})$ is calculated by dividing the importance of the edge origin element P_i by the amount of outgoing edges $|E_{P_iA}|$:

$$I_L(E_{P_iA_j}) = \frac{I_L(P_i)}{|E_{P_iA}|} \tag{4}$$

The developed calculation model assigns each activity, place, and edge within the considered business process a local importance value ($I_L(A_i)$, $I_L(P_i)$, $I_L(P_iA_j)$, and $I_L(A_iP_j)$). Basically these values reflect the probability that the process passes through these elements. Currently, the model assumes an uniform distribution regarding potential process execution flows at conditional routing (OR-split) elements. Example: if there is an OR-split element with two outgoing edges, each edge has a 50% chance of being used (compare Place *P3* in Figure 1).

To improve our business process-based resource importance results regarding their fit to the real world, we introduce two additional edge parameters at each OR-split: (i) pass probability for each outgoing edge $PP(E_{P_iA_j})$, and (ii) value-adding potential of each outgoing edge $VAP(E_{P_iA_j})$. $I_L(E_{P_iA_j})$ is determined by calculating the average of the pass probability $PP(E_{P_iA_j})$ and the value adding potential $VAP(E_{P_iA_j})$ of edge $E_{P_iA_j}$.

$$I_L(E_{P_iA_j}) = \frac{PP(E_{P_iA_j}) + VAP(E_{P_iA_j})}{2} \tag{5}$$

PP and VAP are expressed by a value between 0 and 1. The pass probability of all outgoing edges has to sum up to 1. The value-adding potential of all outgoing edges has to sum up to 1. By combining both values in $I_L(E_{P_iA_j})$ we are able to express besides the pass probability the value-adding potential of potential process execution flows. Each outgoing OR-split edge has to be assessed by the business process owner in a manual manner to determine (i) its pass probability based on historical process execution data, and (ii) its value-adding potential based on available relevant data and/or the business process owner's experience.

After determining the importance of each activity which is included in the considered business process we can calculate the importance of the involved resources. We assume that data about activities' resource usage is available in set M_{R_i} and that for each activity an ordered list L, containing all previous edges originating from an OR-split place, exists. For example: in the context of the business process shown in Figure 1, activity $A15$ would be associated with the list $L_{A_{15}} = \{E_{P_3A_3}, E_{P_3A_4}, E_{P_{16}A_{15}}\}$. For any activity combination A_x and A_y in M_{R_i} we check if L_{A_x} is included in L_{A_y} or if L_{A_y} is included in L_{A_x}. If L_{A_x} is a subset of L_{A_y} or L_{A_y} is a subset of L_{A_x} we further inspect the last element (edge) of the subset and keep the place P that it is connecting. If the superset contains exactly one edge that connects place P we can infer that the importance value of the superset is already included in the subset. Therefore, we exclude the activity that corresponds to the superset from M_{R_i}. In the next step we sum up in G_{R_i} the local importance values of those activities which share a common starting pattern and contain exactly one edge starting from the same place but differ in the targeted activity. Importance values of those activities which do not comply with the above rule (share a common starting pattern and contain exactly one edge starting from the same place but differ in the targeted activity), are also added to G_{R_i}. The local importance I_L of Resource R_i in context of Process p equals the highest importance value e included in G_{R_i}, times the overall importance I of the considered business process p.

$$I_{L_p}(R_i) = max\{e \in G_{R_i}\} * I(p) \tag{6}$$

Consider the following example in the context of the business process shown in Figure 1: $M_{R_i} = \{A3, A14, A15\}$, $L_{A_3} = \{E_{P_3A_3}\}$, $L_{A_{14}} = \{E_{P_3A_3}, E_{P_3A_4}, E_{P_{16}A_{14}}\}$, $L_{A_{15}} = \{E_{P_3A_3}, E_{P_3A_4}, E_{P_{16}A_{15}}\}$. According to the definition above, we search for subsets but cannot find any in M_{R_i}. In the second step we build new groups starting with L_{A_3}; L_{A_3} does not share an edge only differing in

its target activity and thus we create a new element in G_{R_i} with L_{A_3}'s importance value. Continuing with $L_{A_{14}}$, we find in $L_{A_{15}}$ an identical starting pattern ($E_{P_3A_3}, E_{P_3A_4}$) and the same place with a differing target activity ($E_{P_{16}A_{14}}$ and $E_{P_{16}A_{15}}$), thus we add a new element to G_{R_i} summarizing the local importance values of $L_{A_{14}}$ and $L_{A_{15}}$. As described in Section 4.1 the analyzed business process has to provide an importance value for the considered organizational context. This importance value can be quantitative (e.g. Euro per hour) or qualitative (e.g. high, medium, or low) and determines the way how the importance of the involved resources is represented. The business process owner and the management define the importance of the considered business process. Again, the importance indicates the organizational impact if the considered business process is not longer able to deliver the expected output (we focus again on the availability aspect).

4.3 Determining the Resource's Global Importance

Let P be the total number of business processes and $I_{L_p}(R_i)$ the local importance I_L of Resource R_i in context of Process p. The global importance I_G of resource R_i is calculated by summing up its local importance values $I_{L_p}(R_i)$ in the given organizational context:

$$I_G(R_i) = \sum_{p \leq P} I_{L_p}(R_i) \tag{7}$$

Finally, $I_G(R_i)$ provides a comprehensible figure on the resource's importance. The following section demonstrates the developed approach by applying it to three real-world business processes.

5 Proof of Concept

We use BOC's ADONIS tool to model the business processes for the proof of concept. ADONIS allows for attaching resource elements to business process activities and provides an export functionality which is capable of exporting the entire business process representation as an easily accessible XML file. After parsing the ADONIS business process representation into a valid Petri net, we were able to start the developed resource importance calculation. The business processes, overall importance values, and involved resources which are used in the course of the proof of concept are shown in Table 1. As an example Figure 1 shows a Petri net representation of the *Register Damage* business process. At each OR-split (Place *P3* and *P16*) we used equally distributed values for pass probability PP and value-adding potential VAP. Therefore the local importance of each outgoing edge at the places *P3* and *P16* is 0.5 (e.g., $I_L(P_3A_3) = \frac{PP(E_{P_3A_3}) + VAP(E_{P_3A_3})}{2} = \frac{0.5+0.5}{2} = 0.5$). The following activity/resource combinations exist in the *Register Damage* business process: M_{PCC} ={A6, A7, A8, A9, A11, A12, A16, A17, A18}, M_{NS} ={A16, A17}, M_{CD} ={A6, A7, A18}, M_{PD} ={A8}, M_{HD} ={A9}, and M_{ED} ={A16, A17}.

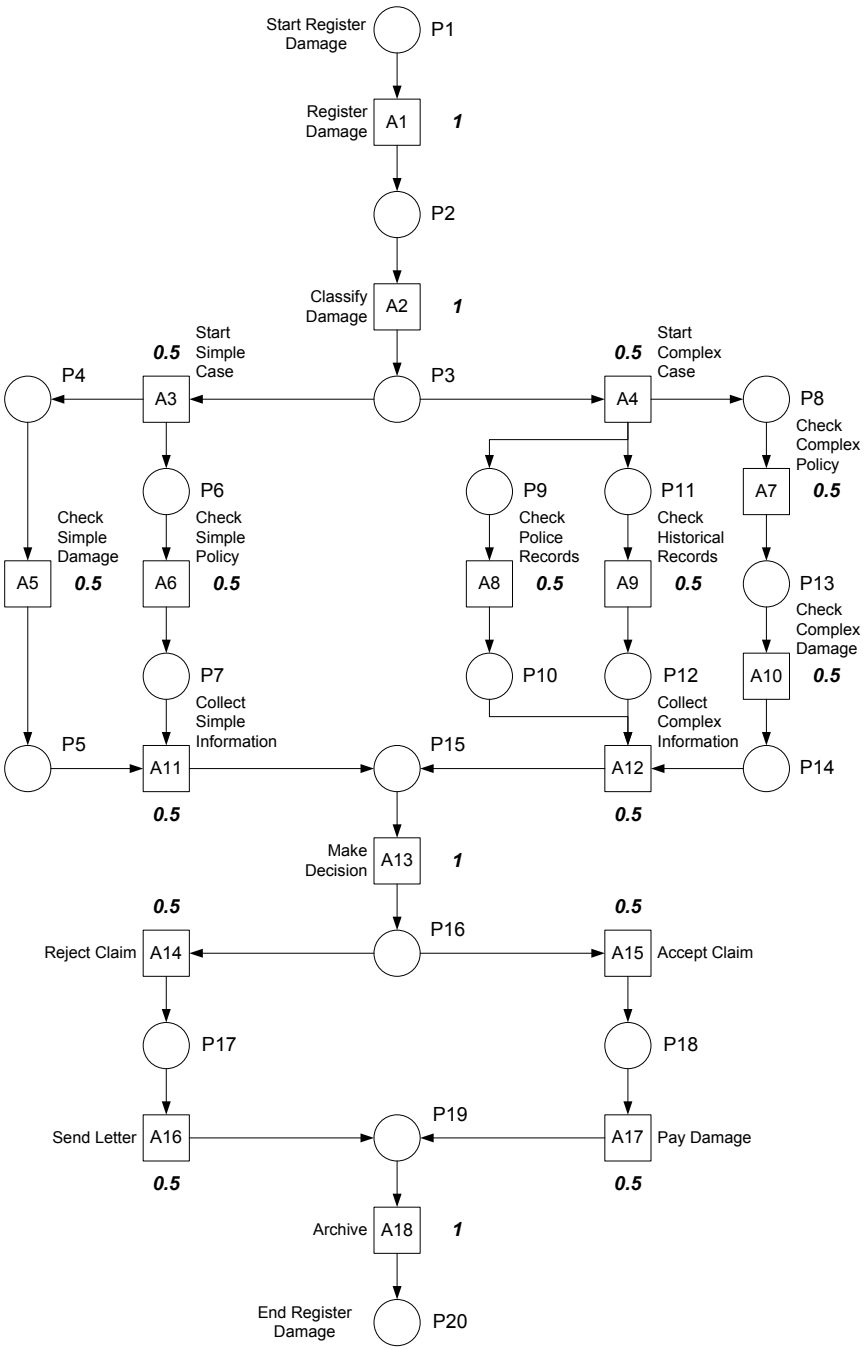

Fig. 1. Petri net representation of business process 'Register Damage' (taken from [21])

Table 1. Business processes, their organization-wide importance and involved resources

Business Process	Importance	Resources
Register Damage	300 €/h	PC-Consultant (PCC) Notification-Server (NS) Client-Data (CD), Police-Data (PD), Historical-Data (HD), Employee-Data (ED)
Consultant Assignment	100 €/h	PC-Reception (PCR) Notification-Server (NS) Client-Data (CD), Employee-Data (ED), Appointment-Data (AD), Historical-Data (HD)
Conclusion of Contract	200 €/h	PC-Consultant (PCC) Notification-Server (NS) Client-Data (CD)

The XML-representation of each business process has been used as input data for the prototype. According to the developed calculation schemes the local importance of each resource is calculated. As an example we will show how the importance of the Police-Data (PD) resource in the context of the Register Damage business process is calculated.

1. **Context Determination:** According to Table 1 and M_{PD}, the Police-Data resource is used in activity A8 of the Register Damage process.
2. **Local activity importance determination:** The local importance of A8 is determined by its incoming edge $I_L(E_{P_9A_8}) = \frac{I_L(P_9)}{|E_{P_9A}|} = \frac{0.5}{1} = 0.5$. The importance of place P9 has been calculated based on the importance of activity A4, which has been calculated based on the importance of place P3 and so on. As described in the previous paragraphs the outgoing edge importance of P3 has been calculated based on equally distributed values for pass probability and value-adding potential.
3. **Local resource importance determination:** After creating G_{PD} on basis of M_{PD} (cf. Section 4.2) the local, i.e. business process wide, importance I_L of the Police-Data resource PD in context of the Register Damage process equals the highest importance value included in G_{PD}, times the overall importance I of the Register Damage process p: $I_{L_{RD}}(PD) = max\{e \in G_{PD}\} * I(p) = 0.5 * 300$€/h= 150€/h.
4. **Global resource importance determination:** The global importance of the Police-Data resource is calculated by summing up its local importance values $I_{L_p}(PD)$ in the given organizational context. Since the Police-Data resource is only used in the Register Damage process the global importance equals its local importance in the context of the Register Damage process: $I_G(PD) = \sum_{p \leq P} I_{L_p}(PD) = 150$€/h.

Table 2. Local Resource Importance Results

Business Process	**Local Resource Importance**
Register Damage	PC-Consultant (1) Notification-Server (1) Client-Data (1), Police-Data (0.5), Historical-Data (0.5), Employee-Data (1)
Consultant Assignment	PC-Reception (1) Notification-Server (1) Client-Data (1), Employee-Data (1), Appointment-Data (0.5), Historical-Data (0.25)
Conclusion of Contract	PC-Consultant (1) Notification-Server (1) Client-Data (1)

Table 3. Global Resource Importance Results

Resource	**Global Resource Importance**
PC-Consultant	300€/h + 200€/h = **500€/h**
PC-Reception	100€/h = **100€/h**
Notification-Server	300€/h + 100€/h + 200€/h = **600€/h**
Client-Data	300€/h + 100€/h + 200€/h = **600€/h**
Police-Data	**150€/h**
Historical-Data	150€/h + 25€/h = **175€/h**
Employee-Data	300€/h + 100€/h = **400€/h**
Appointment-Data	**50€/h**

Table 2 shows the local resource importance value results in the context of the given business processes. Each value (potential range: 0 - 1) is derived, as shown in the previous example, from the business process activity involving the considered resource and having the maximum activity local importance value.

The local importance values of each resource are used to aggregate them to an organization-wide global resource importance value. Table 3 shows the calculation results. Based on the structure and importance of the considered business processes the results show the organization-wide impact if one of the involved resources is not longer available to the organization.

According to the results, the notification server, client data, and consultant PC are the most valuable resources in the organization (600€/h and 500€/h). The unavailability of appointment data would cause the least impact on the organization (50€/h).

6 Evaluation

To evaluate the developed concepts we compare the results of the corresponding prototypical implementation to the results gained in the course of a

Table 4. Global Resource Importance Evaluation Results

Resource	Participant 1	Participant 2	Participant 3
PC-Consultant	500€/h (83%)	500€/h (83%)	114.55€/h (86%)
PC-Reception	100€/h (17%)	100€/h (17%)	19.3€/h (14%)
Notification-Server	600€/h (100%)	600€/h (100%)	133.85€/h (100%)
Client-Data	600€/h (100%)	600€/h (100%)	133.85€/h (100%)
Police-Data	150€/h (25%)	150€/h (25%)	22.5€/h (17%)
Historical-Data	175€/h (29%)	175€/h (29%)	23.6€/h (18%)
Employee-Data	400€/h (67%)	400€/h (67%)	75.55€/h (56%)
Appointment-Data	50€/h (8%)	50€/h (8%)	7.5€/h (6%)

traditional workshop-based assessment. Three business processes including their organization-wide importance and required resources (see Section 5) have been provided to the workshop participants. The following steps have been performed at the workshop-based assessment: (i) introduction and definition of the workshop goal → business process-based determination of resource importance values, (ii) definition of the *importance* term in the context of the workshop, (iii) manual process analysis by workshop participants → each participant is required to determine the importance of the resources involved in each business process, and (iv) determination of organization-wide resource importance values → the participants are required to aggregate the results of the previous step to organization-wide resource importance values.

Table 4 shows the global resource importance results of each workshop participant. Participant 1 and 2 intuitively use an approach similar to our proposed solution. Since Participant 3 used another calculation model to determine the global resource importance we related each global resource importance result to the most important one. Although Participant 3 used a different calculation model, the relative results differ only slightly from ours. It took every participant about 9 minutes to calculate the importance values of each resource in the local and global context. The subsequent discussion has been dominated by the limitations of our proposed calculation model: (i) the model does not incorporate down-time costs of activities; it ignores the fact that resource down-times of later activities are normally associated with less costs than resource down-times of early activities, (ii) the model does not incorporate the duration of activities; similar to Limitation (i) the model ignores that resources required by long activities are more crucial than resources required by short activities, and (iii) it is not guaranteed that the calculation results reflect the real world importance of the considered resources. Although, Limitation (i) and (ii) could be easily incorporated into the existing calculation model, we decided to accept these limitations at this stage of research since we want to keep the necessary input data at a minimum. Limitation (iii) reflects the fundamental problem of modeling the reality by business processes. As organizations and their work flows are dynamic, business processes have to be continuously adapted to match reality. Using business processes for the resource importance determination in the

ISRM context requires up-to-date and realistically modeled business processes to calculate realistic importance values for the involved resources.

7 Conclusions

ISRM heavily depends on realistic impact values representing the resources' importance in the overall organizational context. Business processes are widely used as a structured flow of organizational activities, which support business goals and are enabled by resources (cf. [22]). Therefore, the central research question of this paper was: How can business processes be used to determine resources' importance in the overall organizational context? Our paper makes a first step towards a business process-based resource importance determination. Based on the organization's business processes, their overall organizational importance, and the resources required by their activities, the proposed method automatically determines the organization-wide importance of the involved resources.

The *advantages* of the developed solution are: (i) the necessary input data is restricted to machine-interpretable business process representations including required resources and the importance of the business process, and (ii) assuming that the required input data is already available our approach provides ISRM with fast results regarding resource importance, which are based on the business processes' structure and resource involvement. The conducted evaluation reveals the following *limitations* of our contribution: (i) activity down-time costs are not incorporated, (ii) activity duration is not considered, and (iii) it is not guaranteed that the calculation results reflect the real-world resource importance, due to the fundamental problem of business process modeling: reflecting the dynamic reality by a model. Although, our model could be easily extended to address Limitation (i) and (ii) we decided to accept the limitations at the current stage of research to keep the necessary input data to a minimum.

Further research will empirically test our proposed solution by conducting case studies in the Austrian social security insurance sector. The gathered research results will be used to refine our approach for determining resource importance values in the ISRM context. Second, we will address the identified limitations and extend this approach to integrate the time factor (e.g., down-time costs and activity duration). Third, we will research on how to express the importance of business processes and resources. Although we used quantitative units in this paper, we do not want to exclude qualitative rating schemes. Fourth, we will extend our research from the availability to the confidentiality perspective. One of the next research questions will be: How can business processes be used to determine resources' confidentiality in the overall organizational context?

Acknowledgment

The authors would like to thank Sigrun Goluch, Gernot Goluch, Stefan Jakoubi, and Simon Tjoa. This work was supported by grants of the Austrian Government's FIT-IT Research Initiative on Trust in IT Systems under the contract

813701 and was performed at the research center Secure Business Austria funded by the Federal Ministry of Economy, Family and Youth of the Republic of Austria and the City of Vienna.

References

1. Gerber, M., von Solms, R.: Management of risk in the information age. Computers & Security 24, 16–30 (2004)
2. Commission of the European Communities: Communication from the Commission to the Council, The European Parliament, The European Economic and Social Committee and the Committee of the Regions 'A strategy for a Secure Information Society - Dialogue, partnership and empowerment". COM (2006) 251 final (2006)
3. Cavusoglu, H., Mishra, B., Raghunathan, S.: The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce 9(1), 69–104 (2004)
4. Stoneburner, G., Goguen, A., Feringa, A.: Risk management guide for information technology systems. NIST Special Publication 800-30, National Institute of Standards and Technology (NIST), Gaithersburg, MD 20899-8930 (2002)
5. Voorhoeve, M., Van der Aalst, W.: Ad-hoc workflow: problems and solutions. In: Proceedings of the Eigth International Workshop on Database and Expert Systems Applications, pp. 36–40. IEEE Computer Society, Los Alamitos (1997)
6. van der Aalst, W.: Generic workflow models: How to handle dynamic change and capture management information? In: Conference on Cooperative Information Systems, pp. 115–126 (1999)
7. Mills, S.: The future of business - aligning business and it to create an enduring impact on industry. Technical report, IBM (2007)
8. Sackmann, S.: A reference model for process-oriented it risk management. In: 16th European Conference on Information Systems, ECIS 2008 (2008)
9. Al-Mashari, M.: Business process management - major challenges. Business Process Management Journal 8, 411–412 (2002)
10. Farquhar, B.: One approach to risk assessment. Computers and Security 10(10), 21–23 (1991)
11. Fredriksen, R., Kristiansen, M., Gran, B.A., Stølen, K., Opperud, T.A., Dimitrakos, T.: The CORAS framework for a model-based risk management process. In: Anderson, S., Bologna, S., Felici, M. (eds.) SAFECOMP 2002. LNCS, vol. 2434, pp. 94–105. Springer, Heidelberg (2002)
12. Alberts, C., Dorofee, A., Stevens, J., Woody, C.: Introduction to the OCTAVE approach. Technical report, Carnegie Mellon - Software Engineering Institute, Pittsburgh, PA 15213-3890 (2003)
13. DCSSI: Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) - Section 2 - Approach. General Secretariat of National Defence Central Information Systems Security Division, DCSSI (2004)
14. ISO/IEC: ISO/IEC 27005:2007, Information technology - Security techniques - Information security risk management (2007)
15. Sackmann, S.: Assessing the effects of it changes on it risk - a business process-oriented view. In: Multikonferenz Wirtschaftsinformatik (MKWI 2008), pp. 1137–1148. GITO-Verlag, Berlin (2008)

16. Asnar, Y., Giorgini, P.: Analyzing business continuity through a multi-layers model. In: Dumas, M., Reichert, M., Shan, M.-C. (eds.) BPM 2008. LNCS, vol. 5240, pp. 212–227. Springer, Heidelberg (2008)
17. Reijers, H.A., Limam, S., van der Aalst, W.M.P.: Product-based workflow design. J. Manage. Inf. Syst. 20(1), 229–262 (2003)
18. Eom, J.-H., Park, S.-H., Han, Y.-J., Chung, T.-M.: Risk assessment method based on business process-oriented asset evaluation for information system security. In: Shi, Y., van Albada, G.D., Dongarra, J., Sloot, P.M.A. (eds.) ICCS 2007. LNCS, vol. 4489, pp. 1024–1031. Springer, Heidelberg (2007)
19. van der Aalst, W., van Hee, K.: Business process redesign: a petri-net-based approach. Computers in Industry 29, 15–26 (1996)
20. van der Aalst, W.: The application of Petri nets to workflow management. The Journal of Circuits, Systems and Computers 8(1), 21–66 (1998)
21. van der Aalst, W.: Process-oriented architectures for electronic commerce and interorganizational workflow. Information Systems 24(8), 639–671 (1999)
22. zur Muehlen, M., Rosemann, M.: Integrating risks in business process models. In: ACIS 2005 Proceedings (2005)