Security of Information System in View of Business Continuity Management

Kiyoshi Nagata
Faculty of Business Administration
Daito Bunka University
Tokyo, Japan
Email: nagata@ic.daito.ac.jp

Dieter Hertweck
Electronic Business Institute
Heilbronn University
Heilbronn, Germany
Email: dieter.hertweck@hs-heilbronn.de

***Abstract*—In any type of company, the information system is one of the core systems in order to accomplish their business objectives. Exposure of its malfunction or defect sometimes causes critical damages to the company in view of business continuity, and the company should form a plan consist of several measures to prevent, to reduce, to transfer, to avoid risks and also to recover the system. Since the company's information system is closely related to their business type and strategy, the plan should be laid considering them. In this paper, we propose a methodology to ameliorate the present state of the company's information system in business continuity perspective.**

***Keywords*-IT system; business continuity; security controls; business process management**

I. INTRODUCTION

As a core system of a company, the information system and its management system is critical, and their malfunction directly affects the business performance. There are several systems proposed for evaluation and management of the information related system, and some companies acquired a kind of certificates of the information security, such as ISO/IEC27001 or BS7799-2. These certificates may give companies a guarantee on their information management system. However, the approaches of these certification sometimes tend to formal and stereotype, and does not reflect the companies characteristics. Especially in Small or Medium-size company, the information system and its management system should be evaluated based on their own assets, activities, and strategy. Thus a self-directed, business oriented, and assets based evaluation is recommended, and some systems such as OCTAVE [2] [10], ENISA's Information Package for SMEs (Small or Medium-size Enterprise) [13], and MEHARI [12] can be applied to SMEs.

Although the business oriented, self-directed evaluation system matches the company's characteristics and strategic goal, it sometimes requires to compose a relatively small team, called an analysis team, whose members are from several important sections of the company. The analysis team leads the evaluation process by acquiring information on their system all over the company. So the top managements should be in sympathy with the importance of information security evaluation, then consensus of staff members are necessary. SMEs neither have sufficient human resources nor have diligent intention to assign them to such a job, even if they know the malfunction of their information system causes serious problem on their business performance.

In this paper, we propose a methodology for information security evaluation and management which reduces company's workload by adopting evaluation process in ENISA's Information Package for SMEs, and by referencing their security measures which are actually in OCTAVE. In order to reflect company's characteristic or business objectives, the consensus with company staffs on the evaluation values are made in several steps.

Since our methodology is business oriented, essentially asset based, we need to find out from 3 to 5 critical assets. After the specification, we propose to describe the internal process related to each of asset using business process management tool such as ADONIS. This type of system has performance indicators, and we can see the bottle neck in the total process related to the asset. Then comparing the measures should be implemented with those of the output from ENISA, we can suggest a risk mitigation plan.

The rest of this paper is organized as follows; we refer to the ENISA's Information Package for SMEs in the next section, some methods to choose critical assets are described, some references on ADONIS as a business process management tool, then the total process of our proposed methodology comes up.

II. ENISA'S INFORMATION PACKAGE FOR SMES

ENISA (European Network and Information Security Agency) developed and delivered the Information Package for SMEs. The method is highly structured and one can obtain a set of several controls considered to be effective to solve the organization's information security problem or to improve their current condition.

The system procedure includes four phases as follows:

Phase1. Select Risk Profile
Output: Identified risk area, risk profile table with risk level labels, organizational risk profile

Phase2. Identify Critical Assets
Output: Five most critical assets, security requirement selection table with rationales for selection

 ISBN: 978-1-61208-254-7

Phase3. Select Control Cards
Output: Organizational controls, asset based controls
Phase4. Implementation and Management
Output: Gaps between recommended controls and current status, risk management plans

The risk profile table in Phase1 includes only four risk area which roughly correspond to the impact classification of OCTAVE, whose details are coming up in Section V. The risk should be evaluated for each of these areas, however the evaluation is very simple and automatically performed. Here we notice that the evaluation of "legal and regulatory" is dependent on the handling level of customers' personal information defined in the EU Data Protection Law [4, pp.104-105].

The personal data means any information relating to an identified or identifiable narural person, and the details are slightly different in countries. For example, according to the German Federal Data Protection Act, the definition of the sensitive personal data are as follows;

- Racial or ethnic,
- Political opinions,
- Religious or philosophical beliefs,
- Trade union membership,
- Health or sex life.

The assets are classified into four categories, System, Network, People, and Applications. In this phase, the analysis team, a team of small number of personnel from various sectors of organization also introduced in OCTAVE, has to choose five critical assets from many of possible assets. Evaluation is done by considering the impact to the organization when "Disclosure" or "Modification" or "Loss and Destruction" or "Interrupted Access" occurs. These scenarios are just the set of outcomes appears in OCTAVE's threat profile worksheet.

Like as many other security evaluation systems recommend, assets are evaluated in the usual three perspectives, that is Confidentiality, Integrity, and Availability (CIA). In the process of choosing five critical assets, we need to evaluate each assets from each perspective, then aggregate the resulted values or establish a method for giving priorities to each of the assets according to their values. We always have this kind of problem when performing an asset-based evaluation system, also in OCTAVE, and several methods can be applied to solve this kind of problem. For instance, AHP and FSM are very popular, where pair-wise comparisons of alternatives are performed and the priority value is expressed as the weight of each alternative. By identifying five critical assets with references of security requirement in three perspectives, the security requirements selection table is completed.

The control cards choosing phase, the Phase3, has two processes. One is for the organizational control cards corresponding to the Strategic practice in OCTAVE, and the selection of controls depends only on the risk levels of each risk area described in Phase1. In TableI, SP1, SP2, SP3, SP4, SP5, and SP6 are sets of controls related to "Security Awareness and Training", "Security Strategy", "Security Management", "Security Policies and Regulations", "Collaborative Security Management", and "Contingency Planning/Disaster Recovery", respectively, [13].

The other is for the asset based control cards corresponding to the Operational practice in OCTAVE, and possible and effective controls are listed in the asset control card whose selection depends on the level of total risk profile, the asset category, and the asset's risk level. Once selecting a card, one can find out controls to be adopted according to three perspectives and security requirements of "Physical security", "System and network management", "System authentication", "Monitoring and auditing IT security", "Authentication and authorization", "Vulnerability management", "Encryption", "Security architecture and design", "Incident management", and "General staff practices".

Table I
ORGANIZATIONAL CONTROL CARDS

Risk Area	High	Medium	Low
Legal and Regulatory	(SP1) (SP4)	(SP1) (SP4)	SP1.1
Productivity	(SP3), (SP4) (SP6), (SP5)	(SP4) (SP6)	SP4.1
Financial Loss	(SP2), (SP1), (SP4)	(SP4)	SP4.1
Productivity	(SP1) (SP5)	(SP4) (SP1)	SP4.1

The last phase consists of Gap analysis and planning the risk management. From the previous phase, recommended controls are proposed and one can see the gap from currently performed controls. Then make a plan in order to fill in the gap to compromise the present risk.

III. METHOD FOR FINDING CRITICAL ASSETS

In any decision making process, choosing one or a few critical alternatives from a large set of them is an important and difficult task. There are many methods proposed from theoretical point of view, and some are applied to practical cases. Here we refer to pairwise comparison based methods, like as AHP(Analytic Hierarchy Process), FSM(Fuzzy Structural Modeling). In AHP [8] or FSM [9], weights are obtained by computing the principal eigenvector of a subordination matrix with pairwise comparison values entries. The Perron-Frobenuis theorem guarantees the principal eigenvector to be considered as the importance weight vector. In order to apply the theorem to the matrix obtained by pairwise comparison, the (j, i)-entry value should be set as the inverse value of the corresponding (i, j)-entry in AHP, and the reachability matrix should be computed in FSM. Instead of

 ISBN: 978-1-61208-254-7

computing the principal eigenvector of reachability matrix in FSM, we have more simplified method by which the weight of evaluation factors can be found on the basis of the ratio calculation [1] [7]. The relationships between evaluation factors are transitive regarding the contextual relation "Importance degree".

At first, put all the alternatives in sequential oder, then give values $f_{i,i+1}$ $(i = 1, 2, \ldots, n-1)$ as the importance degree of i-th alternative compared with $(i+1)$-st one, where n is the number of all the alternatives. The corresponding symmetrical value of $f_{i,i+1}$, can be calculated by $f_{i+1,i} = 1 - f_{i,i+1}$ $(i = 1, 2, \ldots, n-1)$. These values are carefully given on the basis of experience and knowledge of the decision makers and/or specialists.

From these relative comparison values, we compute the evaluation value E_i of i-th alternative so as to satisfy following ratio equations:

$$E_k : E_{k+1} = f_{k,k+1} : f_{k+1,k} \qquad (1 \leq k \leq n). \quad (1)$$

A set of answer values of the simultaneous ratio equations is given by following formulae:

$$E_k = \prod_{i=1}^{k-1}(1 - f_{i,i+1}) \prod_{i=k}^{n-1} f_{i,i+1} \quad (1 \leq k \leq n), \quad (2)$$

where the empty product is set to be 1 for $k = 1$ or $k = n$.

If the values for each $f_{i,i+1}$ are carefully chosen to satisfy the transitivity, we actually do not need other comparison value $f_{i,j}$ $(i < j)$. We have only to evaluate each alternative to the adjacent one, and the total number of essential values is just $n - 1$.

In other words, we need to be careful that the set of values $\{f_{i,i+1}\}_{i=1,\ldots,n-1}$ should be transitive, which means that the importance degree of i-th alternative to j-th one $(i < j)$ should be approximately equal to the value calculated from $\{E_i\}$ in a certain degree of error. However in some practical applications, it is not so easy to guarantee that condition, and we will propose some modified pragmatic methods.

A. Checking system to guarantee the transitivity

Supposing that $\{E_i\}$ is the set of importance weights, the relative important degree of i-the alternative to j-th alternative should satisfies a ratio equation $E_i : E_j = f_{i,j} : f_{j,i}$, which is solved to have the following formula for $i < j$;

$$\frac{E_i}{E_i + E_j} = \frac{\prod_{k=i}^{j-1} f_{k,k+1}}{\prod_{k=i}^{j-1} f_{k,k+1} + \prod_{k=i}^{j-1}(1 - f_{k,k+1})}. \quad (3)$$

When this value seems to be considerably different from the value evaluated directly, we need to reconsider initial comparison values. If we notice that the directly given value should be modified, it will be all right.

B. Averaging over All or Some of Sequences

Sometimes it may happen that values given by formulae (2) widely vary depending on the way of setting alternatives in order, and an adjustment seems to be difficult. We can take the average of the evaluation values corresponding to each sequence given by a permutation of $\{1, \ldots, n\}$. When several principal sequences can be distinguished, the average can be taken only over them. For a subset S of the permutation group S_n, the formula for the normalized averaged weight are given by the followings:

$$\begin{aligned} E_i &= \sum_{\sigma \in S} \frac{1}{t_{\sigma^{-1}}} e_{\sigma(i)\sigma^{-1}} \\ &= \sum_{j=1}^{n} \left(\sum_{\sigma^{-1} \in S, \sigma(j)=i} \frac{1}{t_\sigma} e_{j\sigma} \right), \end{aligned} \quad (4)$$

where $e_{j\sigma} = \prod_{l=1}^{j-1} f_{\sigma(l+1),\sigma(l)} \prod_{l=j}^{n-1} f_{\sigma(l),\sigma(l+1)}$, $t_\sigma = \sum_{j=1}^{n} e_{j\sigma}$, and $S^{-1} = \{\sigma : \sigma^{-1} \in S\}$.

C. Hierarchical Block-wise Computing

If it seems that there are small set of invisible attributes behind alternatives, classify them according to these attribute. Then compute weights of alternatives in each class separately, and the weight of attribute class should be calculated. The aggregation process is done by multiplying the weight of super set to that of each attribute after normalization.

The merit of this option is that we may have small number of comparison candidates, and our weight computing method will effectively work. If the number of first blocks is large, we will try to find out some attribute factors which are common to several blocks.

IV. Business Process Management Tool

In this paper, as we are concerned about risks related to each of chosen critical assets, the management process on which the asset related process are mapped should be assessed carefully. Fortunately, there are some good computerized application of business process management tool. Here, we introduce ADONIS which is developed and provided by BOC Group [11].

ADONIS is composed of several model type such as "Company map", "Business process diagram", "Choreography diagram", "Conversation diagram", "Business process model", "Document model", "IT system model", "Product model", "Working environment model", "Risk model", "Control model", and "Use case diagram", and each model includes some objects with own attributes. Among them, here we refer to following models:

Business process model

This process model is essential model of this system containing several type of objects such as Activity, Subprocess, Decision, Performance Indicator, etc. which are combined with each other.

This can also contain Risk and its Control objects when an activity has a risk, and the risk and its control are described in each corresponding model. Figure 1 is a part of "Accept transfer model" in Example files down loadable from BOC group homepage, [11].

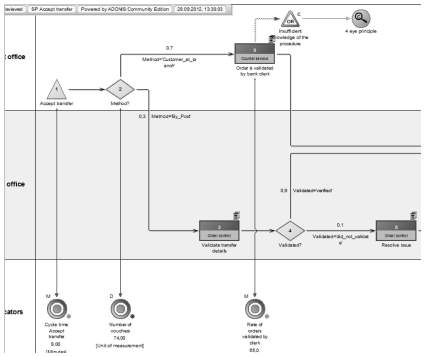

Figure 1. ADONIS Business Process Model

IT system model

This model contains Application, Service, Infrastructure element, and Operation. The model describes physical and logical relationship between objects by "has", "uses", "Is dependent on", "has note", and "has cross-reference" indicators.

Document model

This model is composed of several documents referred by personnel especially in case of emergency or trouble. The document's attribute has a reference link to a Word, or Excel, or PowerPoint file.

Working environment model

This model contains Organizational unit, Performer, Role, Position, etc. The position and primary roles of personnel, and their command structure is embedded in this model.

Risk model

The main object of this model is Risk whose attribute has several risk types such as "operational riks", "strategic risk", "market price and liquidity risk", "credit risk", "quality risk", and "other risk".

Control model

The main object is Control, and the control process is described as a business process model which is referred in the attribute of this object.

V. Proposed System

Before going on the detail of our proposed methodology, we just refer to the business performance in general. In the research area of evaluation of business performance, there are several models or methodologies proposed by many researchers or consultants. But most methodologies refer to "financial", "customer", "productive or internal process", and "learning and growth", which are emphasized especially in the Balanced Score Card (BSC) [3]. Of course, BSC insists that these four perspectives should be balanced and equally treated.

Although BSC and some other methodologies for business performance are tailored not only for evaluating the performance status but also for improve the future state of business, it seems that they do not consider any collapse caused in short span. Here we are interested in business continuity when some disasters occur or serious attacks, e.g. DDoS, are exposed. In most cases, problem seemed to be serious to the business continuity occurs in productive or internal process which causes big financial impact. Thus we explicitly focus on financial and internal process perspective among these perspectives.

Now we explain our proposed methodology for enforcing company's information system in view of business continuity. Figure 2 describes the total flow of our systematic methodology composed of four main phases.

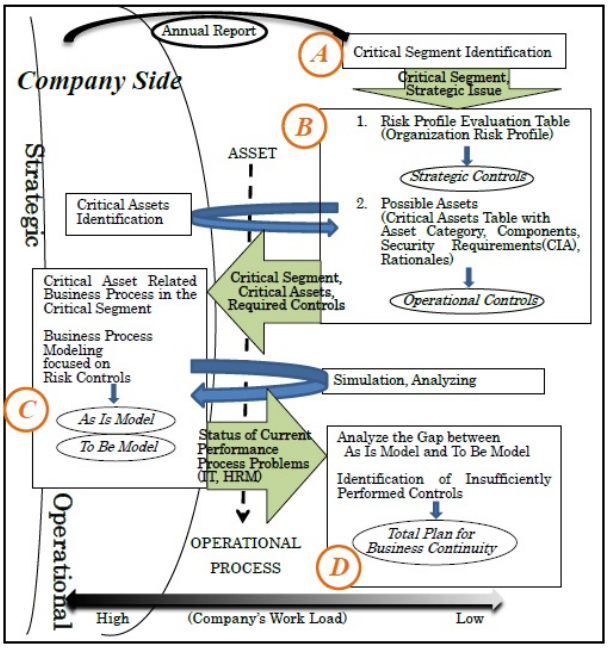

Figure 2. Flow of Total System

In the figure, the region on the left side is the company's region where workload by the company's personnel is high. The workload set in the right side region should be done by researcher's group.

The total work flow proceeds in the following way. First of all, find out the most important and critical business segment from financial perspective and the company's strategy referring the annual report. Next, apply ENISA system to evaluate company's information related property which lead to strategic practices required for the company. We also need

 ISBN: 978-1-61208-254-7

to identify a small set of critical assets which would lead a set of necessary operational practices. In the third phase, business process modeling related to each of critical asset is constructed using application software like as ADONIS. Then try to find out serious problems in the process by performing recursive simulation, considering suggestive operational and strategic practices. The final phase is a phase for making up a total risk control plan.

A. Critical Business Segment

If the company is very small and/or there is unique business segment, the critical segment might be clear. Even if the company has several segments, the critical business segment might be trivial just from the company's strategy. In these cases, this phase is seemed be unnecessary. However, we recommend to perform the total evaluation of segments in financial perspective in case that some disastrous incidents cause serious impact on the business continuity.

From the pyramid of financial ratios, ROCE(Return On Capital Employed; $= \frac{\text{“}NetProfit\text{”}}{\text{“}Capital\ employed\text{”}}$) is the starting point, then it is initially decomposed into the product of the net profit margin ($= \frac{\text{“}NetProfit\text{”}}{\text{“}Sales\text{”}}$) and the sales on capital employed ($= \frac{\text{“}Sales\text{”}}{\text{“}Capital\ employed\text{”}}$). The former index is on profitability, and the later one is again expressed as the product of the turnover of total assets ($= \frac{\text{“}Sales\text{”}}{\text{“}Total\ assets\text{”}}$) and the inverse value of the capital employed ratio($= \frac{\text{“}Total\ assets\text{”}}{\text{“}Capital\ employed\text{”}}$).

Focusing on the net profit margin derives other indices such as the break-even point ration, EBIT, EBITDA and their margins. The turnover of total assets is an index on investment effectiveness, and the CCC (Cash Conversion Cycle;$= 365 \times (\frac{\text{“}Receivable\text{”}}{\text{“}Sales\text{”}} + \frac{\text{“}Inventory\text{”}}{\text{“}Cost\ of\ sales\text{”}} - \frac{\text{“}Accounts\ payable\text{”}}{\text{“}Cost\ of\ sales\text{”}})$ is one of serious index for business continuity. The capital employed ration is an index on financial leverage, which derives DE ratio (Debt Equity ratio;$= \frac{\text{“}Debt(with\ interest)\text{”}}{\text{“}Equity\text{”}}$), and ICR (Instance Coverage Ratio; $= \frac{\text{“}Operating\ profit\text{”} + \text{“}Financial\ income\text{”}}{\text{“}Interest\ expense\text{”}}$) for example.

Fortunately almost all the information necessary to calculate them are on the company's annual report, consisting of PL, BS, Cash flow statements. The annual report also contains information on the “strategy” which helps us to find out not only the critical segment but also critical assets.

B. Applying ENISA

This phase includes main two process. First one is the evaluation of company's, or segment's, proper condition by the risk profile evaluation table, then the process output a set of strategic practices from the organizational(Strategic) control cards. Second process is choosing a small set of critical assets in the assigned segment. Then the asset based(Operational) control card table is referred to have a set of controls according to the evaluation value of each asset from CIA points of view.

1) Risk Profile Evaluation Table: ENISA's risk profile evaluation table is very simple composed of four risk areas, and the evaluation is fairy automatically done as follows.

Legal and Regulatory
: “High” is marked if the company's business handles customer information of sensitive and personal nature including medical records and critical personal data as defined by the EU Data Protection Law. “Medium” if the handled customer information is not sensitive. “Low” if the business does not handle customer information.

Productivity
: “High” is marked if the business employs more than 100 employees having a daily need to access business applications and services. “Medium” if the number of such employees is between 50 and 100. “Low” if the number is less than 50.

Financial Stability
: “High” is marked if yearly revenues are of excess of 25 million Euros or/and financial transactions with 3rd parties or customers are taking place as part of the business as usual process. “Medium” if the yearly revenue are between 5 million and 25 million Euros. “Low” if the revenue are less than 5 million Euros.

Reputation and Loss of Customer Confidence
: “High” is marked if unavailability or service quality directly impact business profile or/and more than 70% of customer base have online access to business products and services. “Medium” if the impact is indirect and/or less than 5% of customer base have online access. “Low” if there are no impact on business profile or on loss of revenue.

According to the set of evaluation values, strategic controls are determined from the Table I in Section II.

2) Critical Assets: Task of choosing a few, at most five, critical assets is very important and difficult. As we mention in Section II, it is performed generally considering the case of “Disclosure” or “Modification” or “Loss and Destruction” or “Interrupted Access” from view point of each of CIA. When focusing on the business continuity, we should mainly consider the “Loss and Destruction”, and the “Interruption of Access” to assets.

First listing possible information related assets in the business segment, then choose any two of them and compare them as the important level with values in the open interval $(0, 1)$ from each of CIA point of view. If we apply the ratio based method, the number of pairs to be evaluated is just $n - 1$, but adjustment or modification process might be needed.

After calculating the set of three weight vectors, they are aggregated according to the importance degree of perspectives, CIA. Although the confidentiality has high degree in usual information evaluation activity because of nowadays

increasing concerns on personal data protection, the availability should be the highest from the business continuity point of view.

Once a few critical assets are distinguished, the asset base control card is assigned according to the asset category, "Application", or "System", or "Network", or "People", and the company's risk level ("High", "Medium", or "Low"). We also need to find out components related to each of critical asset and security requirement as confidentiality, and/or integrity, and/or availability.

C. Business Process Mapping

Before starting the business process mapping using an application soft ware, list up possible impacts on each of critical asset caused by any disaster or threats. Then map all the components to the application's model. For example, the total process for management or recovery of the asset related system is described by the Business Process Model whose activity is dependent on IT system and HRM system.

If the company has own model for this process, map it on the application and give the precise information on processing time, possibilities of decision, working time of each employee, and performance indicators should be carefully constructed. Once the process model is completed, several cases are simulated and results are stored for the next phase.

D. Risk Control/Mitigation Plan

In the last phase, we make a plan for business continuity considering the result comes out of the previous phase. When the company has formalized plan and process against critical asset affecting exposure of risk, we will set up the total plan which reinforcing the process using the result from the simulation and controls as the output of ENISA system.

In case of no current effective process, we need to establish it considering the company's IT and HR condition which are already investigated in the previous phase.

The risk is usually treated in four types of way; retention, reduction, transfer, and avoidance. It is very important to investigate which activity has the key indicator mainly affect the business continuity, then determine controls in one or some of these types.

VI. Conclusion and Future Work

In this paper, we proposed a systematic methodology for evaluation of current status of critical business factor and for suggesting effective risk controls and mitigation plan. Since our main concern is the business continuity, we have considered the total business performance evaluation system, and try to incorporate the financial factor as the most critical business segment. As we mainly concern about the reduction of company's workload, a simple and systematical method, ENISA for SMEs, is adopted for the preliminary evaluation. Although usual security evaluation is essentially based on the asset based method, we also focus on the process against the exposure of risks, and propose to use a kind of business process management application whose simulation functions help us to review or compose an effective risk control/mitigation plan.

Instead of ENISA, we might use OCTAVE-S, a version for relatively small enterprises, if some method for extracting effective mitigation controls are established, see [5] [6]. We will apply our methodology to some of real company and see how it works.

References

[1] M. Amagasa, *Performance Measurement System for Value Improvement of Services*, Bulletin of The Australian Society for Operations Research Inc., Vol.29, No.1, pp.35-52, 2010.

[2] C. Alberts and A. Dorofee, *Management Information Security Risks*, Addison-Wesley, 2003.

[3] R. S. Kaplan, D. P. Norton,*The Balanced Scorecard-Measures that Drive Performance-*, Harvard Business Review. Vol. 70, No.1, pp.71-79. 1992.

[4] C. Kuner, *European Data Protection Law*, Oxford University Press, 2nd ed. 2007.

[5] K. Nagata, Y. Kigawa, D. Cui, and M. Amagasa, *Method to Select Effective Risk Mitigation Controls Using Fuzzy Outranking*, Proceedings of the 9th International Conference on Intelligent Systems Design and Applications, pp. 479-484, 2009.

[6] K. Nagata, *On Clustering of Risk Mitigation Controls*, Proceedings of 2011 International Conference on Network-Based Information Systems, pp. 148-155, 2011.

[7] K. Nagata, M. Amagasa, and H. Hirose, *Multi-attribute Decision Making Based on Fuzzy Outranking*,Proceedings of 13th IEEE International Symposium on Computational Intelligence and Informatics, pp.169-174, 2012.

[8] T. L. Saaty, *Decision Making for Leaders; the Analytical Hierarchy Process for Decisions in a Complex World*, Wadsworth, Belmont, Calif., 1982.

[9] E. Tazaki and M. Amagasa, *Structural Modelling in a Class of Systems Using Fuzzy Sets Theory*, International Journal of Fuzzy Sets and Systems, Vol.2, No.1, pp.87-103, 1979.

[10] C. Alberts, A. Dorofee, J. Stevens, and C. Woody,(2005). *OCTAVE-S Implementation Guide*, Version 1.0, CMU/SEI-2003-HB-003. Available from http://www.cert.org/octave/octaves.html, 18.12.2012.

[11] *ADONIS Community Edition: Taking BPMN 2.0 one step further*. Available from http://www.adonis-community.com/, 18.12.2012.

[12] *MEHARI 2010: Fundamental concepts and functional specifications*. Available from http://www.clusif.asso.fr/fr/zz production/ouvrages/type.asp?id=METHODES, 18.12.2012.

[13] *Risk Management: Information Package for SMEs*. Available from http://www.enisa.europa.eu/act/rm/cr/risk–management–inventory/downloads, 18.12.2012.

 ISBN: 978-1-61208-254-7