6

Construction of Effective Database System for Information Risk Mitigation

Kiyoshi Nagata
Faculty of Business Administration,
Daito Bunka University,
Takashimadaira Itabashi-ku, Tokyo,
Japan

1. Introduction

In the Information Technology Communication Society, the information system in any organization is always exposed to various kinds of risks, and they should prepare countermeasures against possible risks to protect their assets and secure their activities' continuity. For that purpose, several types of information risk evaluation and management systems, such as ISO/IEC 27002, MEHARIT, MAGERIT, SP800-30, OCTAVESM, etc., are proposed by institutions all over the world. Although each system has its own policy and characteristic, on the final stage after the risk evaluation was done and some serious risks were clarified, the system usually goes on the process of choosing effective and available mitigation controls against each of risks.

In our prior works, we proposed a method to choose a set of effective elements from a given database of properly valued mitigation controls and we also proposed a method of clustering these controls related to the threat path of OCTAVE's risk profile worksheet.

However we have not yet constructed any feasible database system for practical use, now the effort is in progress. For that sake, it is necessary to investigate several existent systems of mitigation controls, and to compare and analyse them.

The content of the chapter is as follows:

1. Overview and investigation of existent information risk management systems and their mitigation controls
2. Brief explanation of useful tools for the proposed total system of risk management, such as fuzzy outranking, fuzzy inference mechanism, modified structural modelling method, and c-mean clustering.
3. Review of our proposed method for choosing effective set of mitigation controls from a well-defined database of controls
4. Details of the process constructing database systems
5. Discussion and conclusion

2. Overview and investigation of existent information risk management systems and their mitigation controls

Throughout this chapter, we define a risk mitigation control to be a measure which could reduce the current or potential risk degree. However the risk degree is evaluated in various aspects and from different point of views, and each mitigation control has its own property, characteristic, and merit, the total process of risk mitigation can be summarized in several similar steps. In this section, we will see some risk evaluation and management methodologies.

2.1 Hand book of information security

According to D. Kaye, risk mitigation is a process aimed at limiting the likelihood of risks and the potential losses those risks can cause (Kaye, 2002, p.100).

The following step summarization is from the Hand Book of Information Security (Bidgoli, 2006, p.750).

- Avoid the causes

Risks are caused by many types of instances. If the risk is technological, we can avoid the risk by updating or replacing the related system by more robust and reliable one.

- Reduce the frequency

Risk is usually assessed by the frequency it occurs and the impact it may cause. By adopting a control which mainly reduces the occurrence frequency of the risk, the risk can be mitigated.

- Minimize the impact

Since the frequency of the risk can not be reduced to zero, we should consider the impact of the risk to the organization's activities as the other important factor of risk. The impact related to a risk has various aspects depending on the organization under mind, and try to minimize the impact not only from each aspects but also from the total point of view.

- Reduce the duration

The duration of the exposure to a risk may cause more serious risks. The recovery time of data or system, for instance, is important matter.

The risks are usually evaluated as the pair of two factors such as the frequency and the impact, then the second and the third steps are usual steps for risk evaluation. The cause avoidance and the duration reduction are sometimes treated as concrete measures of mitigation controls.

In the book, the risk transfer, such as insurance or outsourcing, is dealt as the different step from the risk mitigation.

2.2 OCTAVE-S

SEI (Software Engineering Institute) of Carnegie Melon University developed OCTAVE^{SM} (Operationally Critical Threat, Asset, and Vulnerability Evaluation System) (Alberts &

Dorofee, 2003) as a security evaluation system based on organizational assets. OCTAVE-S is a variation of the approach tailored to relatively small organizations (less than 100 people) which have the limited means and unique constraints.

In the implementation guide (Alberts et al., 2005), the key differences between OCTAVE and other traditional information risk evaluation and management approaches are described as in the table 1.

Ordinary risk assessment has three important aspects such as operational risk, security risk, and technology risk. OCTAVE developers say that other evaluation systems are tend to evaluate the organizational systems and to focus on the technology. In OCTAVE, the technology is examined as the part of security practice, and other two aspects mainly drive OCTAVE approach.

OCTAVE	**Other Evaluation systems**
Organization evaluation	System evaluation
Focus on security practices	Focus on technology
Strategic issues	Tactical issues
Self direction	Expert led

Table 1. The key Differences

OCTAVE aims to evaluate the organization itself in aspect of information assets, threats and vulnerabilities, and focus on their practices to obtain the information security, which eventually lead the organization to strategic protection issues rather than tactical ones. The expert led system is managed by a team of experts in risk analysis, or in information technologies from outside or inside. OCTAVE is self-directed system lead by a small interdisciplinary team, called the analysis team, consist of members in the organization.

OCTAVE(-S) has three phases in each of which the analysis team outputs the corresponding matters as follows.

Phase1. Build Asset-Based Threat Profiles

Outputs: Critical assets, security requirements for critical assets, threats to critical assets, and current security practices

Phase2. Identify Infrastructure Vulnerabilities

Outputs: Key components and current technology vulnerabilities

Phase3. Develop Security Strategy and Plans

Outputs: Risks to critical asset, risk measures, protection strategy, and risk mitigation plans

Each phase has some process consist of several steps, which we show in the table2 from the guide (Alberts et al., 2005).

In the series of our research project, we first proposed a method to identify the set of critical assets from huge number of possible information related assets in correspondence of the step S2.1 in the table (Nagata et al., 2007). In the method we used FSM (Fuzzy Structural Modelling) based the modified structural modelling method described in the following

section. Next we proposed a risk evaluation system for a chosen critical asset with fuzzy inference mechanism corresponding to the process S4 (Nagata, et al., 2008B).

One of important roles of any risk management system is to develop a mitigation plan in which effective and proper mitigation controls are set up. For this purpose, a method to select effective risk mitigation controls is proposed using fuzzy outranking in correspondence of the process S5 (Nagata, et al., 2009). This method works under the assumption that there is a database of mitigation controls with some kind of vector whose entries are numerical values assigned to the attributes in OCTAVE's threat path. We also proposed a method for constructing that kind of database (Nagata, 2011).

Phase	Process	Group of Steps
Phase1	S1: Identify Organizational Information	S1.1:Establish impact evaluation criteria S1.2: Identify organizational assets S1.3: Evaluate organizational security practices
	S2: Create Threat Profiles	S2.1: Select Critical Assets S2.2: Identify security requirements for critical assets S2.3: Identify threats to critical assets
Phase2	S3: Examine the Computing infrastructure in Relation to Critical Assets	S3.1: Examine access path S3.2: Analyze technology-related process
Phase3	S4: Identify and Analyse Risks	S4.1: Evaluate impact of threats S4.2: Establish probability evaluation criteria S4.3: Evaluate probabilities of threats
	S5: Develop Protection Strategy and Mitigation Plans	S5.1: Describe current protection strategy S5.2: Select mitigation approaches S5.3: Develop risk mitigation plans S5.4: Identify changes to protection strategy S5.5: Identify next steps

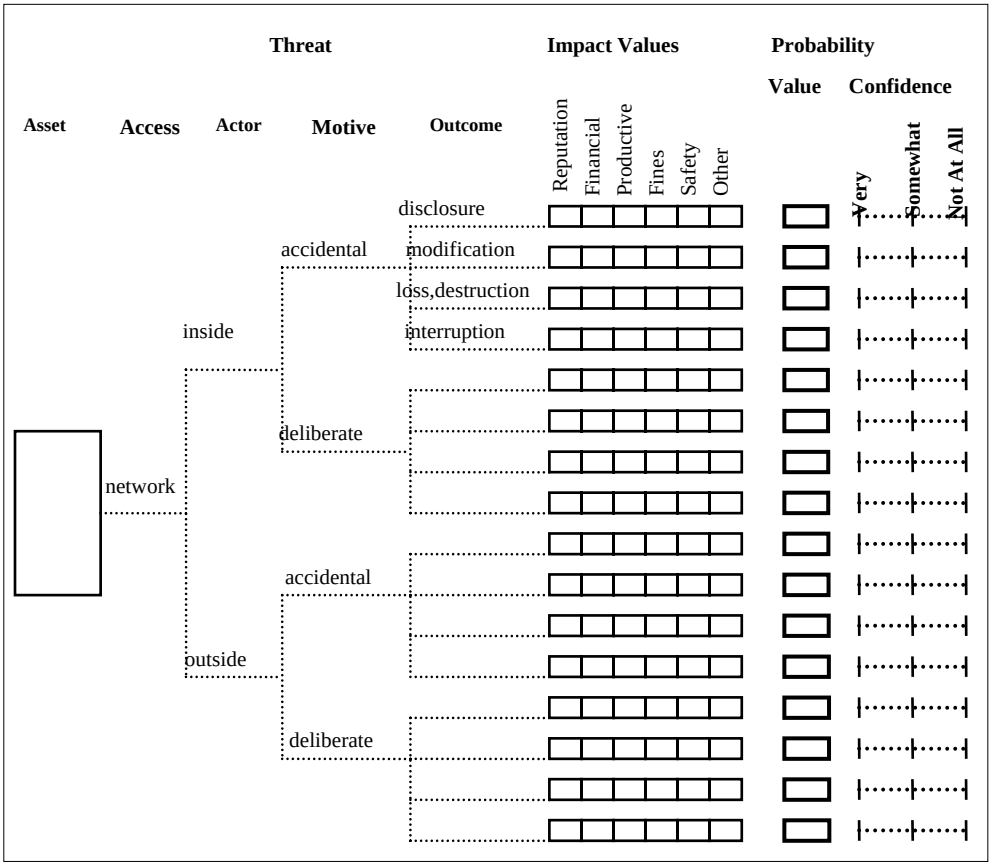
Table 2. Phase, Process, and Group of Steps in OCTAVE-S

When proceeding in risk evaluation steps, the risk profile worksheet plays a big role in order to recognize the information related threat, and to evaluate the impact and the frequency the threat may cause.

In the worksheet shown in Fig. 1, threats are classified into three types such as "Human actors", "System problems", and "Other problems" in the first place. For the human actors causing threats, the access path (network or physical), actors (inside or outside), motive (accidental or deliberate), and outcome (disclosure or modification or loss and destruction or interruption) are examined in this order. For the System problems causing threats, actors (software defects or system crashes or hardware defects or malicious code), and outcome are examined. For the "Other problems", various actors (e.g. problems related to power supply, telecommunication, third-party, natural disasters, physical configuration etc.) are examined. Each impact area of Reputation, Financial, Productivity, Fines/legal penalties, Safety and

Other (facilities) are considered for the non-negligible threats as the result of examination. According to the volume 3 of the OCTAVE-S Implementation Guide (Alberts, et al., 2005), the three impact measure (High, Medium, or Low) are adopted, and probability values are also measured as one of them (H, M, or L) by considering a frequencies such as daily, weekly, monthly, 4 times per year, 2 times per year, once per year, once very 2 years, and so on. Fig1 is an example of the risk profile worksheet for the Human Actors Using Network Access.

At first, put one of critical assets in the left-hand side box, and trace the dotted line considering the possibility of access, actor, motive, and outcome. Then, for each threat on the possible path, the impact values related to given subjects and the probability value are determined with confidence level.



(source: the Volume 5 of OCTAVE-S Implementation Guide, Version1)

Fig. 1. Risk profile worksheet for human actors with network access

We use the worksheet, but we adopt much more numerical evaluation method without loss of human related, consensus based, and organizational strategic concept. Our proposed total

system for evaluation of threat is based on Modified Structural Modeling Method (MSMM), fuzzy integral, and fuzzy inference mechanism. In our system, the input values for impact values and for probability which should be marked in the box or on the scale bar as linguistic values in the OCTAVE are all numerical crisp values between 0 and 1, and the human related, consensus based, and organizational strategic concept are mounted and integrated with them in the process of fuzzification.

In the final process, selection of mitigation plans comes up, and listed up in the OCTAVE's catalogue of practices (Alberts & Dorofee, 2003, pp. 443—454).

The followings are classified groups of them.

- Strategic Practices (SP)
  - Security awareness and training (SP1)
  - Security strategy (SP2)
  - Security management (SP3)
  - Security policies and regulations (SP4)
  - Collaborative security management (SP5)
  - Contingency planning/disaster recovery (SP6)
- Operational Practices (OP)
  - Physical security (OP1): "Physical security plans and procedures (OP1.1)", "Physical access control (OP1.2)", "Monitoring and auditing physical security (OP1.3)"
  - Information technology security (OP2): "System and network management (OP2.1)", "System administration (OP2.2)", "Monitoring and auditing IT security (OP2.3)", "Authentication and authorization (OP2.4)", "Vulnerability management (OP2.5)", "Encryption (OP2.6)", "Security architecture and design (OP2.7)"
  - Staff security (OP3): "Incident management (OP3.1)", "General staff practice (OP3.2)"

In each subcategories listed above, there are several controls. For instance, SP1.1 of SP1 is "Staff members understand their security roles and responsibilities. This is documented and verified". OP2.1 contains 10 controls, e.g. OP2.1.3 is "Sensitive information is protected by secure storage such as…", OP2.1.4 is "The integrity of installed software is regularly refined", and OP2.1.6 is "There is a documented data backup plan that …".

2.3 ENISA

European Network and Information Security Agency, ENISA, provides risk management related documents in one of which risk mitigation is took up as a risk treatment. They define the risk treatment as a process of selecting and implementing measures to modify risk, and the process is composed of five steps such as, "Identification of Options", "Development of the Action Plan", "Approval of the Action Plan", "Implementation of the Action Plan" and "Identification of Residual Risks".

ENISA also provides a document named "Information Package for SMEs", where "SMEs" denotes "Small or Medium sized Enterprises". In the document, the risk management process is composed of four phases.

Phase1: Select Risk Profiles

The risk profiling is done using the risk evaluation matrix in which risk areas are specified as "Legal and Regulatory", "Productivity", "Financial Stability", and "Reputation and Loss of Customer Confidence". The possible risk levels are "High", "Medium", and "Low", and each level is clearly defined according to the risk area. For instance, if the organization's yearly revenue is of excess of 25 million Euros or/and financial transactions with third parties or customers are taking place as part of the business as usual process, then the risk area of financial stability is "High". If the yearly revenue exceeds 5 million Euros and not exceeds 25 million Euros, then the risk level is "Medium". Otherwise it is "Low". After identifying the risk levels for all the risk areas, the risk profile of the organization is defined as the highest level in the risk evaluation matrix overall the risk areas.

Phase2: Identify Critical Assets

In SME, the number of critical assets is fixed as five, and the analysis team choose them considering a large adverse impact on the organization caused by "disclosure" or "modification" or "loss and destruction" or "interruption" of the asset. These scenarios are same as the outcomes in OCTAVE's risk profile worksheet shown in Figure 1. The assets are categorised into "systems", "network", "people", and "applications", then the rationale and security requirement for selecting each critical asset are described. Here the security requirements are three ordinary information security aspects, i.e. Confidentiality, Integrity, and Availability.

Phase3: Select Control Cards

SME adopts OCTAVE's mitigation controls as their control cards. This phase proceeds in three steps such as "Step1: select organization control cards", "Step2: select asset base control cards", and "Step3: document list of selected controls and rationale". Here the organization control cards correspond to the mitigation controls of strategic practice (SP), and the asset base control cards correspond to those of operational practice (OP). The step1 is performed according to the risk profile in phase 1, and some control cards are selected beforehand. For instance, if the risk area "legal and regulatory" is low, then the control SP1.1 is adopted. The step2 is performed according to the critical asset category, and control card consist of security requirements and type of controls is prepared for each asset category and risk level. The table below is the list of control cards:

Critical Assets	High Risk Cards	Medium Risk Cards	Low Risk Cards
Application	CC-1A	CC-2A	CC-3A
System	CC-1S	CC-2S	CC-3S
Network	CC-1N	CC-2N	CC-3N
People	CC-1P	CC-2P	CC-3P

Table 3. Asset based control selection

For instance, CC-1A contains OP2.1.3, OP2.1.4, and OP2.1.6 for security requirement of confidentiality, integrity, and availability respectively as system and network management related controls.

Phase4: Implementation and Management

In this phase, the gap between the selected control cards and current security practice is analysed at first. Then create risk management plan, and the implementation is done.

The selection of mitigation controls is discussed both in the Phase3 and in the Phase4, and they classify controls into organizational controls shown in annex C, and asset based controls shown in annex D.

2.4 MEHARI

MEHARI, Method Harmonise d'Analyse de Risque, is developed by CLUSIF, Club de la Securite de L'Information Francais, aimed at providing a set of tools specifically designed for security management.

MEHARI uses a word of risk treatment measures or security services for mitigation controls, and classifies them into four categories, "Retention", "Reduction", "Transfer", and "Avoidance".

The standard scales of measures for likelihood reduction or for reduction of frequency factors are

- Efficiency of dissuasion measures
- Efficiency of prevention measures
- Efficiency of protective or confinement measures
- Efficiency of palliative measures

Each factor has four levels from level1, low or nul, to level4, very high (strong). The list of security services has more than 300 of sub-services classified into several service categories as follows.

1. Organization of security: "Roles and structures of security (01A)", "Security reference guide (01B)", "Human resource management (01C)", "Insurance (01D)", "Business continuity (01E)"
2. Sites security: "Physical access control to the site and the building (02A)", "Protection against miscellaneous environmental risks (02B)", "Control of access to office areas (02C)", "Protection of written information (02D)"
3. Security of Premises: "General maintenance (03A)", "Control of access to sensitive locations (except office zones) (03B)", "Security against water damage (03C)", "Fine security (03D)"
4. Extended Network (intersite): "Security of the extended network architectures and service continuity (04A)", "Control of connections on the extended network (04B)", "Security during data exchange and communication (04C)", "Control, detection and handling of incidents on the extended network (04D)"
5. Local Area Network (LAN): "Security of the architecture of the LAN (05A)", "Access control of the LAN (05B)", "Security of data exchange and communication on the LAN (05C)", "Control, detection and resolution of incidents on the LAN (05D)"
6. Network operations: "Security of operations procedures (06A)", "Parameters setting and control of hardware and software configurations (06B), "Control of administration rights (06C)", "Audit and network control procedures (06D)"

7. Security and architecture of systems: "Control of access to systems (07A)", "Containment of environment (07B)", "Management and saving of logs (07C)", "Security of the architecture (07D)
8. IT Protection environment: "Security of operational procedures (08A)", "Control of hardware and software configurations (08B)", "Management of storage media for data and problems (08C)", "Service continuity (08D)", "Management and handling of incidents (08E)", "Control of administrative right (08F)", "Audits and control procedures relative to information systems (08G)", "Management of IT related archives (08H)"
9. Application security: "Application access control (09A)", "Control of data integrity (09B)", "Control of data confidentiality (09C)", "Data availability (09D)", "Service continuity (09E)", "Control of origin and receipt of data (09F)", "Detection and management of application incident and anomalies (09G)", "Security of the e-commerce sites (09H)"
10. Security of application projects and developments: "Security of application projects and developments (10A)", "Ensuring security in the development and maintenance processes (10B)"
11. Protection of users' work equipment: "Security of the operational procedures for the whole set of users' equipment (11A)", "Protection of workstations (11B)", "Protection of data on the workstation (11C)", "Service continuity of the work environment (11D)", "Control of administrative rights (11E)"
12. Telecommunications operations: "Security of operational procedures (12A)", "Control of hardware and software configurations (12B)", "Service continuity (12C)", "Use of end-user telecommunication equipment (12D)", "Control of administrative rights (12E)"
13. Management processes: "Protection of personal information (PPI; 13A)", "Communication of financial data (13B)", "Respect of regulations concerning the verification of computerized accounting (VCA; 13C)", "Protection of Intellectual property rights (IPR; 13D)", "Protection of computerized systems (13E)", "Human safety and protection of the environment (13F)", "Rules related to the use of encryption (13G)"
14. Information security management: "Establish the management system (14A)", "Implement the management system (14B)", "Monitor the management system (14C)", "Improve the management system (14D)", "Documentation (14E)"

We can see that the same or similar expressions appeared in different categories such as "security of operational procedure" is in 06A, 08A, 11A, and 12A, and "service continuity" is in 08D, 09E, 11D, and 12C. This suggests the possibility of different perspective for the classification of controls.

MEHARI describes threat by similar items in OCTAVE's risk profile worksheet as shown in Fig. 1.

- Events: "Accidents", "Errors", "Voluntary acts, whether malicious or not", etc. For each of the events, following aspects are described,
  - Whether the cause is internal to the entity,
  - Whether the event is material or immaterial,

  - Any other factor that may influence the probability of the event occurring.
- Actors: rights and privileges,
- Circumstances in which the risk occurs,
  - Process or process steps: modification of files during maintenance operations,
  - Location: theft of media from one location or another, inside or outside the organization,
  - Time: actions occurring during or outside working hours.

A risk scenario is created with the different element, and risk treatment measures effective to the scenario are selected.

2.5 ISO/IEC

BS7799 part1 based ISO/IEC 27002 defines a security control to be a control which should ensure risks are reduced to an acceptable level. The selection of appropriate controls is dependent on organizational decisions based on the criteria for risk acceptance and the general risk management approach. Thus the acceptance level for the organization should be discussed and determined previously.

The categorization of controls in the document is shown below with corresponding number of controls in MEHARIT.

- Security Policy: "Information security policy (14)"
- Organization of Information Security(01): "Internal organization", "External organization"
- Asset Management: "Responsibility for assets (11E)", "Information classification"
- Human Resources Security (01C): "Prior to employment", "During employment", "Termination or changes of employment"
- Physical and Environmental Security (02): "Secure areas", "Equipment security (03C)"
- Communications and Operations Management: "Operational procedures and responsibilities (08A)", "Third party services delivery management", "System planning and acceptance", "Protection against malicious and mobiles code", "Bach-up", "Network security management", "Media handling, Exchange of Information", "Electronic commerce services (09H)", "Monitoring"
- Access Control (05B): "Business requirement for access control", "User access management", "User responsibilities", "Network system access control (04B)", "Operating system access control", "Application and information access control", "Mobile computing and tele-working"
- Information Systems Acquisition, Development and Maintenance: "Security requirement", "Correct processing in application", "Cryptographic controls (13G)", "Security of system files", "Security in development and support processes", "Technical vulnerability management"
- Information Security Incident Management: "Reporting information security events and weakness", "Management of information security incidents and improvement"
- Business Continuity Management (01E, 01D): "Information security aspects of business continuity management"

- Compliance: “Compliance with legal requirements (03D, 13A, 13D)”, “Compliance with security policies and standards, and technical compliance”, “Information systems audits considerations”

These controls are selected by considering the possible options including:

- applying appropriate controls to reduce the risk
- knowingly and objectively accepting risks, providing they clearly satisfy the organization's policy and criteria for risk acceptance
- avoiding risks by not allowing actions that would cause the risks to occur
- transferring the associated risks to other parties, e.g. insurers or suppliers

2.6 NIST

We refer to NIST SP800--30, where the total process of risk mitigation is described in four phases such as “risk mitigation options”, “risk mitigation strategy”, “an approach for control implementation, control categories, the cost--benefit analysis", and "residual risk".

The followings are risk mitigation options.

- Risk Assumption: To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level
- Risk Avoidance: To avoid the risk by eliminating the risk cause and/or consequence
- Risk Limitation: To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability
- Risk Planning: To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.
- Research and Acknowledgement: To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability
- Risk Transference: To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

NIST also provides SP800--53, which includes a list of more than 170 recommended security controls for Federal Information Systems.

The classes of controls and their families are shown as follows.

- Management Class: “Certification, Accreditation, and Security Assessments (CA)”, “Planning (PL)”, “Risk Assessment (RA)”, “System and Services Acquisition (SA)”
- Operational Class: “Awareness and Training (AT)”, “Configuration Management (CM)”, “Contingency Planning (CP)”, “Incident Response (IR)”, “Maintenance (MA)”, “Media Protection (MP)”, “Physical and Environmental Protection (PE)”, “Personnel Security (PS)”, “System and Information Integrity (SI)”
- Technical Class: “Access Control (AC)”, “Audit and Accountability (AU)”, “Identification and Authentication (IA)”, “System and Communications Protection (SC)”

3. Brief explanation of useful tools

In this section, some tools based on fuzzy theory such as fuzzy outranking method, fuzzy inference mechanism, modified structural modelling method based on FSM, and fuzzy c-mean (clustering) are briefly described.

3.1 Fuzzy outranking method

The method to roughly compare two alternatives a and a' through the adoption of loose relation is called outranking. When a is judged not to be inferior to a' at least, it is said that a outranks a'. When a' is more preferable than a or they are incomparable to each other, it is said that a doesn't outrank a'. While these relations are valued as 0 or 1 in the conventional outranking method, such as $\mu(a,a')=1$ if a outranks a' and $\mu(a,a')=0$ if a does not outranks a', the fuzzy outranking method access the outranking degree as a value between 0 and 1. More precisely, that degree is determined using a fuzzy membership function with lower threshold value q_i and upper one p_i, where "i" represents one of view points for evaluating these alternatives. Thus the corresponding value is denoted by $c_i(a,a')$ (i=1,…,n), and they are aggregated by taking the weighted average $\omega_1 c_1(a,a')+\ldots+\omega_n c_n(a, a')$ with a set of certain weight $\{\omega_1,\ldots,\omega_n\}$. This index is called the "concordance index" denoted by $C(a,a')$. Another index is "discordance index" denoted by $d_j(a,a')$, which is also calculated using a fuzzy set with lower threshold value p_j and upper one v_j. This index represents the degree of objection against the preferability to choose a then a'. Thus $d_j(a,a')=1$ implies that the condition "a outranks a'" is exclusively vetoed from the number j point of view.

If there are discordant points of view $j_1,\ldots, j_k$, whose index are greater than $C(a,a')$, then the total outranking index $\mu(a,a')$ is calculated by the following formula:

$$\mu(a,a') = C(a,a') \times \frac{1-d_{j_1}(a,a')}{1-C(a,a')} \times \cdots \times \frac{1-d_{j_k}(a,a')}{1-C(a,a')} \tag{1}$$

3.2 Fuzzy inference mechanism

Fuzzy inference (Kaufman, et al., 1975; Klir & Yuan, 1995) is originally the process of formulating the mapping from a given input to an output using fuzzy logic. Then the mapping provides a basis for which decisions can be made, or patterns distinguished.

The rule of fuzzy inference is generally expressed as follows:

"IF x is A_1 and y is B_1 THEN z is C_1, else IF x is A_2 and y is B_2 THEN z is C_2, else IF x is A_n and y is B_n THEN z is C_n , else x is A′ and y is B′ THEN z is C′ ", where $A_1,\ldots, A_n$, A′ are subsets of universe of discourse U, and B_1 ,…, B_n, B′ are fuzzy subsets of universe of discourse (V; C_1 , …, C_n, C′ are fuzzy subsets of universe of discourse W).

We have several types of fuzzy number such as triangular, trapezoidal, and Gaussian fuzzy numbers in mind (Inoue & Amagasa, 1998, pp. 57-66).

3.3 Modified structural modelling

The modified structural modelling method is developed by Cui, D. and Amagasa, M. for constructing a structural model with consensus of multi-participants (Amagasa, 2004, pp. 121-132, Nagata et al., 2008A). Here, assume that a decision group consists of several members (decision makers) with either equal or different knowledge background for a given problem.

Let GM_k (k=1,...,m) denote group members, and A_k (k=1,...,m) be fuzzy subordination matrices of data given by GM_k.

Then, mental model of GM_k is embedded into a fuzzy subordination matrix on the context on basis of the relaxation of transitivity, reflexivity and symmetry by each group member (Zadeh 1965; Klir & Yuan 1995; Tazaki & Amagasa 1979). Herein, NGT and automatic generation method of subordination matrix are applied to embed entries of the matrices efficiently and effectively. In order to formulate the individual fuzzy subordination matrix with the same establishment level, the entries of the matrix embedded by group individual are normalized statistically. Then, a representative subordination matrix is formulated by integrating the fuzzy subordination matrices of group members as follows:

Let $S = \{s_1, \ldots, s_i, \ldots, s_n\}$ denote a system with n elements, and let $A_k = [a_{ij}^k]_{n\times n}$ (k=1,2,…,m) denote the fuzzy subordination matrices in S, where $a_{ij}^k = f^k(s_i, s_j)$ ($0 \le a_{ij}^k \le 1$, i,j=1,2,…,n, k=1,2,…,m). a_{ij}^k is the grade of which s_i is subordinate to s_j and m is the number of group members. Let $NA_k = N^k(\bar{a}_k, (\sigma_a^k)^2) = [h_{ij}^k]_{n\times n}$ (k=1,2,…,m) denote the normalized fuzzy subordination matrices calculated by the given data $A_k = [a_{ij}^k]_{n\times n}$ from group members with

$$h_{ij}^k = \frac{1}{100}\left(\frac{a_{ij}^k - \bar{a}_k}{\sigma_a^k} \times 10 + 50\right) \quad (i,j=1,\ldots,n,\ \ k=1,\ldots,m), \quad \text{where} \quad \bar{a}_k = \frac{1}{n^2}\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^k \quad (k=1,\ldots,m) \quad \text{and}$$

$$\sigma_a^k = \frac{1}{n}\sqrt{\sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}^{k^2} - \bar{a}_k^2} \quad (k = 1, \ldots, m).$$

Now, the normalized subordination matrices are used to compute the representative subordination matrix which holds the data factor from group members. Let $NAR = [d_{ij}]$ (i,j=1,…,n) be a representative subordination matrix, which is computed by

$$d_{ij} = \frac{1}{m}\sum_{k=1}^{m} h_{ij}^k \quad (i,j=1,2,\ldots,n). \quad (2)$$

Next, the fuzzy reachability matrix is computed on the basis of NAR, and multi-level digraph is drawn as an interpretive structural model. In order to compare the structural model with mental model, a feedback for learning will be performed to group members. If an agreement among group members is obtained, the process goes ahead to documentation step. Otherwise, a threshold and fuzzy structure parameter will be modified and the process is iterated until a consenting model is derived. Here, let p be the threshold, specified by α-cut, which is defined by the modified z-value in standard normal distribution. The value of p is used for controlling the percentage of subordination relations among elements which exist in the structural model to be evaluated.

Fig. 2 illustrates a flowchart of the modified structural modeling method which begins with mental model of individual group member which is determined depending on their intuition to the given problem.

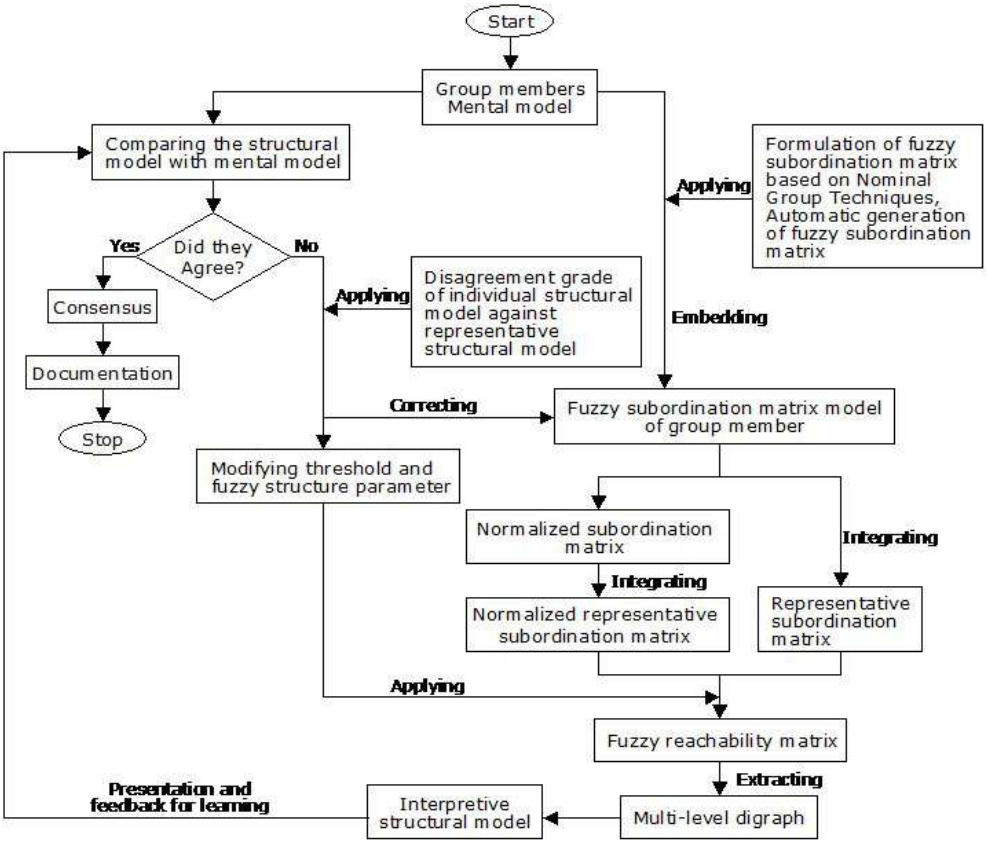


Fig. 2. The flowchart of modified structural modeling method

3.4 Fuzzy c-mean clustering

Data base of multi-attribute elements can be classified into several groups according to a fixed metric. This kind of process is call a clustering, and ordinary clustering is simply that defining a function,

$$\mu = \mu_d : D \times C \to \{0,1\}$$

satisfying the condition that for any $x \in D$ there is only one $c \in C$ such that $\mu(c,x) = 1$.

Here D is the set of all data, C is the set of clusters, and d represents a distance with some kind of metric e.g., Euclidean metric, maximum metric, etc. With the function above, each element has only one cluster and no overlapping of clusters.

Fuzzy c-mean clustering is represented by a function,

$$\mu = \mu_d : D \times C \to [0,1]$$

Here the value $\mu(c,x)$ between 0 and 1 indicates the degree of membership of a data $x \in D$ in a cluster $c \in C$, and clusters can be overlapped.

Now let n be the number of data with n_v attributes, and s be a number of clusters, and express each data x_i=(x_{i1},...,x_{in}) with values of j-th attribute x_{ij} where $D = \{x_1,...,x_n\}$.

When we put the set of all the cluster centers $V = \{v_1,...,v_s\}$, the objective function which should be minimized is defined as following.

$$J(D;U,V) = \sum_{j=1}^{s}\sum_{i=1}^{n} \mu^m{}_{ij}\, d^2(x_i, v_j) \,, \tag{2}$$

where $U = \{\mu_{ij} = \mu_d(c_j, x_i)\}$ satisfying trivial constraints in inequalities $0 \le \mu_{ij} \le 1$ (i=1,...,n, j=1,...,s) and only one non-trivial equation $\sum_{j=1}^{s} \mu_{ij} = 1$.

The exponential number m of μ reflects the fuzzyness of the clustering, such as setting m=1 implies the ordinary, not fuzzy, clustering, increasing the value of m means the widely overlapping of the resulted clusters.

By introducing the Lagrange multiplier λ, objective function is

$$W(D;U,V) = J(D;U,V) - \lambda(\sum_{j=1}^{s} \mu_{ij} - 1) \tag{3}$$

and optimal solutions are given at the saddle points, that is{ μ_{ij}} and v_j (j=1,...,s) satisfy

$$\begin{cases} \dfrac{\partial W}{\partial \mu_{ij}} &=& m\mu_{ij}^{m-1} d^2(x_i, v_j) - \lambda &=& 0 \\ \dfrac{\partial W}{\partial v_{jk}} &=& \displaystyle\sum_{i=1}^{n} 2(x_{ik} - v_{jk})\mu_{ji}^{m} &=& 0 \end{cases} \tag{4}$$

where v_{jk} represents the k coordinate of point v_j, and the distance function is the Euclidean distance $d(x_i, v_j) = \sum_{k=1}^{n_v} (x_{ik} - v_{jk})^2$.

Solving the equations above, we have

$$\begin{cases} \mu_{ij} &=& \left(\displaystyle\sum_{k=1}^{s} \left(\frac{d(x_i, v_j)}{d(x_i, v_k)} \right)^{\frac{2}{m-1}} \right)^{-1} \\ v_{jk} &=& \dfrac{\displaystyle\sum_{i=1}^{n} \mu_{ij} x_{ik}}{\displaystyle\sum_{i=1}^{n} \mu_{ij}^{m}} \end{cases} \tag{5}$$

Thus the algorithm proceeds in the following steps;

1. Load a database D. Determine the number of clusters s, fuzzification value m, and the error evaluation threshold ε
2. Set t=1, and give certain initial values for $\{\mu_{ij}\}$ denoted by $\{\mu_{ij}{}^{(t-1)}\}$
3. Calculate $v_{jk}^{(t)} = \sum_{i=1}^{n} \mu_{ij}^{(t-1)} x_{ik} / \sum_{i=1}^{n} \mu_{ij}^{(t-1)m}$, and put

$$\mu_{ij}^{(t)} = \left(\sum_{k=1}^{s} \left(\frac{d(x_i, v_j^{(t)})}{d(x_i, v_k^{(t)})} \right)^{\frac{2}{m-1}} \right) \tag{6}$$

4. With the corresponding values for $\lambda = m\mu_{ij}^{m-1} d^2(x_i, v_j)$, evaluate the difference of two values $W(D;U^{(t)},V^{(t)})$ and $W(D;U^{(t-1)},V^{(t-1)})$ by ε
5. If the difference value is less than ε, then stop and output $\{\mu_{ij}^{(t)}\}$ and $\{v_j^{(t)}\}$ as the results for U and V. If not, increase t by 1 and go back to the step 3)

In the algorithm above, we need to be careful that the fuzzification exponent m=1 reduces the denominator of the exponent of each terms in Σ for $\mu_{ij}^{(t)}$ to 0.

Moreover, m is usually set a values between 1.4 and 2.6 (Celikyilmaz, & Turksen, 2009, p.57).

4. Method for choosing effective set of mitigation controls

For our proposed method for selecting set of mitigation controls from a database of controls, we assume the existence of an external database, D, of mitigation controls with mitigation degree, $\delta_m(T) \in [0,1]$ and $m \in D$, evaluated depending only on the type of threat path T. This mitigation degree should signify that adopting the control roughly mitigate the risk level from 1 to that degree.

We use the risk profile work sheet of OCATVE-S, and we suppose that determination of the set of critical assets are done, and all the possible threat path were distinguished with the risk value calculated from (v_R,v_F,v_P,v_{Fi},v_S,v_O,p), the vector of impacts and probability. This is the preliminary stage of our method.

Then the process is performed according to the following steps.

Step 1. Determine a threat path T.

Step 2. Select several controls as members of the candidate set, $M \subset D$, by evaluating their initial mitigation degree dependent on T. One simple way to determine M is setting $M=\{m \in D : \delta_m(T) < \delta\}$ for a definite value δ.

Step 3. Define the desirable, but dummy, mitigation control, a_0, as an acceptable impacts and probability vector (v_{R0},v_{F0},v_{P0},v_{Fi0},v_{S0},v_{O0},p_0).

Step 4. For each element $m_j \in M$, figure out its mitigation degree $d_*{}^j$ with respect to each of impacts and probability. For instance, $d_R{}^j$ represents the reduction degree with respect to the impact of reputation when m_j is performed. These degrees are calculated by considering the type of assets, threat path, and impact or probability in some criteria.

Step 5. Calculate a_j= ($v_R{}^j$,$v_F{}^j$,$v_P{}^j$,$v_{Fi}{}^j$,$v_S{}^j$,$v_O{}^j$,p^j) as the alternative vectors corresponds to m_j by $d_*{}^j \times v_*$.

Step 6. Apply the fuzzy outranking method with certain threshold values of concordance and discordance indices to each of (a_j,a_0) for j=1,…n, where n is the cardinality of M.

Step 7. Determine the set of effective mitigation controls E_T by referring the outranking relation values $\mu_j=\mu(a_j,a_0)$. We have two versions for this. One is to determine $E_T=\{m_j;\mu_j > a\}$ as the optimal set with fixed lower boundary value α. The other is to choose the definite number of m_is′ from the permutated mitigation controls in descending order.

5. Method for construction of effective database system

Now we propose a method composed of three phases to construct a database system with an effective clusters.

Phase I: Collecting Mitigation Controls

It seems to be patient and time-consuming works that we gather and examine all controls possible to mitigate information related risks, together with giving each of them a kind of classification index simultaneously. The classification is used to give each control a value vector of OCATVE's threat path attributes related entries in Phase II. Fortunately, we have some of existing database of controls referred in section 2 such as in ISO/IEC 27002, MEHARI, NIST SP-800, and in OCTAVE. They are already classified in view of various aspects.

Phase II: Evaluation of Controls

This phase is composed of two processes.

Process 1: Vector indication in a fixed set

Fix a set of mitigation controls with some classification. Indicate a vector whose entries are values between 0 and 1 corresponding to each of attributes in OCTAVE's threat paths to all the controls in the set. Concretely speaking, we have six possible attributes “access“ (“network“, “physical“), “actor“ (“inside“, “outside“), “motive“ (“accident“, “deliberate“) on the human actors worksheet, and four possible attributes “actor“ (“software defects“, “malicious code“, “system crashes“, “hardware defects“) on the system problems worksheet. We propose a method to indicate the values for each of attribute by applying the MSMM in the following steps,

Step 1. give a weight each of first level or second level classes
Step 2. give a weight all the controls in each class
Step 3. aggregate two weight values in step 1 and step2

Process 2: Evaluation and modification

In the previous process, we have controls with value vector according to each classified set. The same or similar control can be appear in some classified sets, and it could be possible that one control has more than one value vector. We need to identify those controls and examine the indicated vectors of each of them before going on the next phase. If the vectors corresponding to a control have only acceptable difference, then take a vector whose entries

are the average of each entries as the final value vector of the control. If not, go back to the value vector indication steps.

Phase III: Clustering Controls

Clustering all controls using fuzzy c-mean clustering method by means of attribute vectors. Make the correspondence between each of clusters and each of threat paths by looking at the center vectors of clusters. Selecting a small set of mitigation controls is performed using this correspondence and *U* defined in subsection 3.4.

6. Conclusion and discussion

As the final goal of the series of information security evaluation and management system, a system to propose a set of mitigation controls effective and efficient to reduce the organizational risk level is very important. For this purpose, the construction of a feasible database of mitigation controls is necessary. In this chapter, we look over several types of controls, and proposed a method for construct the database. The resulted consists of controls with a value vector whose entries are corresponding to some of attributes on the threat path in OCTAVE's risk profile worksheet. Our idea to apply the fuzzy c-mean clustering might be helpful to choose a small set of control candidates from a huge number of controls.

For the practical use, we need to construct a feasible and real database by applying our system and to verify the effectiveness of the total system.

In our future work, we intend to apply our system to some of classified set of mitigation controls, such as in OCTAVE, ENISA, NIST SP800 and in MEHARI, to obtain an example of effective database. We also intend to define a function from a set of threat path attributes to a set of clusters resulted from fuzzy c-mean clustering.

7. References

Alberts, C. & Dorofee, A. (2003). *Management Information Security Risks*, Addison-Wesley.

Amagasa, M. (2004). *Management Systems Engineering*, Institute of Business Research, Daito Bunka University

Bidgoli, H. (Editor-in-Chief) (2006). *Hand Book of Information Security*,Vol. III, John Wiley & Sons.

Inoue, H. & Amagasa, M., (1998), *Fundamentals of Fuzzy Theory*, (in Japanese), Asakura Shoten.

Celikyilmaz, A. & Turksen, I. B. (2009) *Modeling Uncertainty with Fuzzy Logic*, Springer.

Kaufman, A. et al. (1975). *Introduction to the Theory of Fuzzy Subsets*, NewYork: Academic Press.

Kaye, D. (2002) *Strategy for Web Hosting and Managed Services*, John Wiley & Sons.

Klir, G. J. & Yuan B. (1995) *Fuzzy Sets and Fuzzy Logic-Theory and Application*, Prentice Hall International Inc.

Nagata, K.; Kigawa, Y.; Cui, D. & Amagasa, M. (2007). Integrating Modified Structural Modeling Method with an Information Security Evaluation System, *Proceedings of*

the 8th Asia Pacific Industrial Engineering and Management Systems Conference 2007, T1-R02, ID68.

Nagata, K.; Umezawa, M.; Cui, D. & Amagasa, M. (2008A). Modified Structural Modeling Method and Its Application -Behavior Analysis of Passengers for East Japan Railway Company-, *Journal of Industrial Engineering and Management Systems*, Vol. 7, NO. 3, pp. 245-256.

Nagata, K.; Kigawa, Y.; Cui, D. & Amagasa, M. (2008B). Risk Evaluation for Critical Assets with Fuzzy Inference Mechanism in an Information Security Evaluation System, *Proceedings of the 9th Asia Pacific Industrial Engineering and Management Systems Conference 2008*, pp. 2630-2640.

Nagata, K.; Kigawa, Y.; Cui, D. & Amagasa, M. (2009). 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.

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

Tazaki, E. & Amagasa, M. (1979). Structural Modeling in a Class of Systems Using Fuzzy Sets Theory, *International Journal of Fuzzy Sets and Systems*, Vol.2, No.1, pp. 87-103.

Yu, Q. H. ; Liang, G. Y. & Nagata, K. (2010). Risk Scoring Method on Business Information Management System, *Proceedings of the 11th Asia Pacific Industrial Engineering and Management Systems Conference 2010*, DVD-ROM, ID117.

Zadeh, L. A. (1965). Fuzzy Set, *Information and Control*, Vol.8, pp. 338-353.

Alberts, C.; Dorofee, A.; Stevens, J. & Woody, C. (2005). OCTAVE-S Implementation Guide, Version 1.0, CMU/SEI-2003-HB-003. 28.02.2011,Available from http://www.cert.org/octave/octaves.html

Information technology--Security techniques--Code of practice for information security management, ISO/IEC 27002 Central, 28.02.2011, Available from http://www.17799central.com/

MEHARI 2010: Fundamental concepts and functional specifications, 28.02.2011, Available from http://www.clusif.asso.fr/fr/production/ouvrages/pdf/MEHARI--2010--Principles—Specifications.pdf

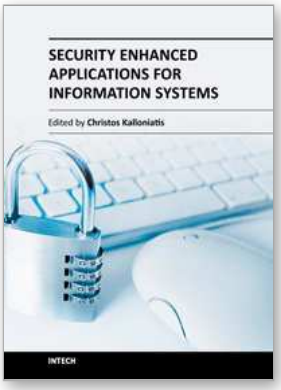
Recommended Security Controls for Federal Information Systems: 28.02.2011, Available from http://csrc.nist.gov/publications/nistpubs/800--53--Rev3/sp800--53--rev3--final/_updated--errata/_05--01--2010.pdf

Risk Management:Implementation principles and Inventories for Risk Management/Risk Assessment methods and tools, 28.02.2011, Available from http://www.enisa.europa.eu/act/rm/cr/risk--management--inventory/downloads.

Risk Management: Information Package for SMEs, 28.02.2011,Available from

http://www.enisa.europa.eu/act/rm/cr/risk--management--inventory/downloads

Risk Management Guide for Information Technology Systems, 28.02.2011,Available from http://csrc.nist.gov/publications/nistpubs/800--30/sp800 --30.pdf



Security Enhanced Applications for Information Systems

Edited by Dr. Christos Kalloniatis

ISBN 978-953-51-0643-2
Hard cover, 224 pages
Publisher InTech
Published online 30, May, 2012
Published in print edition May, 2012

Every day, more users access services and electronically transmit information which is usually disseminated over insecure networks and processed by websites and databases, which lack proper security protection mechanisms and tools. This may have an impact on both the users' trust as well as the reputation of the system's stakeholders. Designing and implementing security enhanced systems is of vital importance. Therefore, this book aims to present a number of innovative security enhanced applications. It is titled "Security Enhanced Applications for Information Systems" and includes 11 chapters. This book is a quality guide for teaching purposes as well as for young researchers since it presents leading innovative contributions on security enhanced applications on various Information Systems. It involves cases based on the standalone, network and Cloud environments.

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821