ICIC Express Letters
Volume **10**, Number **4**, April **2016**

ICIC International ©2016 ISSN 1881-803X
pp. 949–956

INFORMATION SYSTEM RISK CONTROL METHOD BASED ON OPERATION-FLOW

Hongyu Yang and Xiang Cheng

School of Computer Science and Technology
Civil Aviation University of China
No. 2898, Jinbei Road, Tianjin 300300, P. R. China
yhyxlx@hotmail.com; huozhai9527@126.com

Received September 2015; accepted December 2015

Abstract. *This paper proposes a risk control method based on operation-flow (ORCM) to effectively control the risk of operation-flow in information systems. This method consists of the risk quantification process and the risk control process. In the risk quantification process, 11 risk quantification parameters were defined and initialized. In the risk control process, through the control effect maximization operation, the minimum residual risk damage was used as an object function to obtain the risk damage minimization deployment scheme based on the linear programming method; through the control cost minimization operation, the minimum control cost was used as an object function to obtain the control cost minimization deployment scheme on the premise of not more than the minimum residual risk damage. The RAS experiment shows that the ORCM not only has better security risk control effect but also has lower control cost.*

Keywords: Risk control, Operation-flow, Linear programming method, Control cost

1. **Introduction.** Information security risk control which is regarded as an important part of the information system security engineering has become the foundation and precondition of establishing information system security [1]. At present, the classic information system risk control methods mainly include BS7799, NIST SP 800-53, AS/NZS 4360, OCTAVE and other standards [2]. The BS7799 provides a set of information security management and implementation rules which consists of information security management entries for industry and commerce information systems [3]. The NIST SP 800-53 provides a set of integrated information security controls selection process to prevent the organizations from different kinds of information security risks [4]. The AN/NZS provides universal methods that contained risk recognition, risk analysis, risk assessment, etc. [5].

The majority of above information security risk control methods are based on checklist strategy, and there are two obvious drawbacks. First, as operation-flows change over time in information systems as well as the information security risks, some plausible risk controls may not work. Second, as ignoring reciprocal influence between control practicable and operation-flows, the information risk control effect is poor and the control cost is high.

In the field of information system risk control method research, [6] proposed a heuristic risk control method (HRCM). In this method, control effect was regarded as the determinant to deploy controls. However, HRCM did not deploy and plan the controls in a comprehensive perspective. [7] proposed a decision model used for deploying risk controls, but it did not consider the influence factors of operation-flow. In addition, [8-15] proposed some information security risk control methods in the perspective of risk assessment index, risk assessment method and risk control strategy. However, most of the above research achievements have not considered the influence factors of operation-flow as well as the relationship between control cost and control effectiveness.

Aiming at these problems, we propose the Operation-flow based Risk Control Method (ORCM). Combining the risk controls analysis process with operation-flow we accomplish the ORCM which includes the risk quantification process and the risk control process.

In this paper, we firstly give the part of risk quantification with 11 risk quantification parameters defined and we show the detail processes of parameters initialization. Then, we present the method of risk control which has two steps of operations, control effect maximization operation and control cost minimization operation. Through the control effect maximization operation, the minimum residual risk damage is regarded as an object function to obtain the risk damage minimization deployment scheme based on the linear programming method; through the control cost minimization operation, the minimum control cost is regarded as an object function to obtain the control cost minimization deployment scheme on the premise of not more than the minimum residual risk damage. At last, we get the conclusion that ORCM not only has better security risk control effect but also has lower control cost through the RAS experiment.

2. Risk Quantification.

The core function of information system is providing information service based on operation-flow, while each operation-flow will face various information security risks. In order to guarantee the confidentiality, integrity and availability of information systems against information security risks, controls should be deployed at appropriate locations in the operation-flow. Information security risk quantification which includes risk quantification parameters definition and initialization is necessary for deploying risk controls.

2.1. Risk quantification parameters definition.

Firstly, we abstract a set of nodes $\mathbf{N}$ from the information assets in information system, and abstract a set of edges $\mathbf{S}$ from the topological relations of information assets in the operation-flow. Then, the information system operation-flow can be formalized by the sets of $\mathbf{N}$ and $\mathbf{S}$. Next, we assemble the information security risks to a set of risk $\mathbf{R}$ and assemble the risk controls to a set of controls $\mathbf{C}$. At last, we define the parameter D describing the control cost ceiling.

The applicability of the risk controls should be determined, that is choosing risk controls which can effectively detect and control the information security risks. Therefore, we define a parameter β_{rnc} ($r \in \mathbf{R}$, $n \in \mathbf{N}$, $c \in \mathbf{C}$) in the risk quantification process describing whether the control c can effectively control the damage which is caused by risk r when deployed at the node n. The β_{rnc} are formally defined as follows:

$$\beta_{rnc} = \begin{cases} 1 & \text{the control } c \in \mathbf{C} \text{ can effectively control the damage} \\ & \text{caused by risk } r \in \mathbf{R} \text{ when deployed at the node } n \in \mathbf{N} \\ 0 & \text{otherwise} \end{cases} \tag{1}$$

Deploying controls in the operation-flow will bring some control cost which is synthetically determined by economic investment, labor force consumption, system resource consumption, operation-flow delay and other factors. For each risk control c, control cost will fluctuate with the location changing. Therefore, we define a parameter θ_{nc} ($n \in \mathbf{N}$, $c \in \mathbf{C}$) describing the control cost of deploying control c at node n.

For each information security risk, if it has not been detected, the damage caused by it should be defined as F_r ($r \in \mathbf{R}$). If deploying control c at node n the damage would be reduced by f_{rnc} ($r \in \mathbf{R}$, $n \in \mathbf{N}$, $c \in \mathbf{C}$). As we use spanning-tree method to construct the operation-flow, the information security risk transmit paths should be stored in a parameter P_r ($r \in \mathbf{R}$). To solve the problem of deploying multiple controls in the operation-flow, we should accomplish multi-coverage of the controls. Therefore, the parameters W_{nc} ($n \in \mathbf{N}$, $c \in \mathbf{C}$) and Q_{rnc} ($r \in \mathbf{R}$, $n \in \mathbf{N}$, $c \in \mathbf{C}$) should be formally defined as follows:

$$W_{nc} = \begin{cases} 1 & \text{place control } c \in \mathbf{C} \text{ at node } n \in \mathbf{N} \\ 0 & \text{otherwise} \end{cases} \tag{2}$$

$$Q_{rnc} = \begin{cases} 1 & \text{placing control } c \in \mathbf{C} \text{ at node } n \in \mathbf{N} \text{ effectively controls the risk } r \in \mathbf{R} \\ 0 & \text{otherwise} \end{cases} \tag{3}$$

Note that, for every information security risk the damage is always nonnegative even though controls are deployed. We make the limiting criterion as follows:

$$\sum_{n \in N} \sum_{c \in C} f_{rnc} \leq F_r \tag{4}$$

The detailed parameters description is shown in Table 1.

Table 1. Parameters definition and description

Parameter	Parameters description
$\mathbf{N}$	Set of nodes in the operation-flow
$\mathbf{R}$	Set of risks faced by the operation-flow
$\mathbf{C}$	Set of controls in the operation-flow
D	Control cost ceiling
β_{rnc}	Whether the control c can effectively control the damage caused by risk r at node n
θ_{nc}	Control cost of deploying control c at node n
F_r	Presumptive damage of the risk r
f_{rnc}	Damage reduction when deploy control c at the node n for preventing risk r
P_r	The transmit path of risk r
W_{nc}	Deploying parameter
Q_{rnc}	Deploying parameter

2.2. **Risk quantification parameters initialization.** In the practical information security risk control process, there are various information assets, and it is necessary to ascertain the location of them in the operation-flow according to operation requirement. However, in order to facilitate the description and calculation we randomly allocate the nodes which represent the information assets in a limited range of right angle coordinate system. The initialization of any risk quantification parameter is based on its location in the coordinate system. The 7 prime parameters in the information security risk control process include: node, risk, applicability of the risk controls, control cost, impact of the risk controls, presumptive risk damage and control cost ceiling. The processes of the risk quantification parameters initialization are shown as follows.

(1) **Nodes Initialization**

We randomly allocate the nodes which represent the information assets in a limited range of right angle coordinate system, and calculate the distance between any two nodes.

(2) **Information Security Risk Initialization**

a) For each risk, randomly select nodes to include. Ascertain each node whether it can be included by risk r on the probability of ψ. For a risk, if there are no nodes to include, randomly choose a node.

b) Based on the Prim algorithm [16] and the distance between any two nodes calculated in node initialization, calculate the minimum spanning tree which consists of the included nodes, get the transmit path P_r of each risk.

(3) **Risk Controls Applicability Initialization**

For each node n included to the risk r ($n \in P_r$, $r \in \mathbf{R}$), using a uniform distribution randomly decides whether the control c can be applicable at this node. If it is applicable, set β_{rnc} as 1. Otherwise, set β_{rnc} as 0.

(4) **Control Cost Initialization**

In the practical information security risk control deployment process, control cost is comprehensively influenced by expenditures on economic part, labor cost, system resources consumption, operation-flow time delay and other factors. The final result is generally got by specialist discussion, experience summary, historical data analysis and other ways. In order to facilitate the further study, we randomly allocate an integer not more than the control cost ceiling as θ_{nc} ($n \in \mathbf{N}$, $c \in \mathbf{C}$), the control cost of deploying the control c at node n.

(5) **Risk Controls Impact Initialization**

If a node has more child nodes in a risk transmit path, deploying controls here could prevent more nodes from risk damage. Therefore, the method of calculating risk control impact is shown as follows:

a) Calculate the distances S between any two reachable nodes $n_1, n_2 \in P_r$ according to risk transmit paths.
b) For each node, calculate the total inflow to the node I which is calculated by the distance between the node and its father node plus the total distance from the node to each child node in the risk transmit path. Set I as the risk controls impact f_{rnc}. See Figure 1 for an illustration.

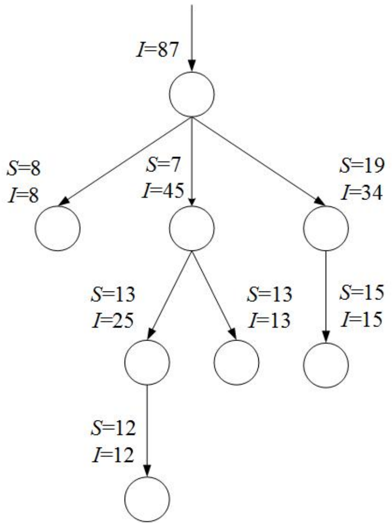

Figure 1. Risk control impact calculation process

(6) **Presumptive Risk Damage Initialization**

In the practical information security risk control deploying process, presumptive risk damage is determined by information security incidents summary and analysis, calculating the values using Probability Theory & Mathematical Statistics. To get the presumptive risk damage, we multiply the risk damage when no controls deployed T_r by the probability of risks occurrence λ_r:

$$F_r = \lambda_r * T_r \quad r \in \mathbf{R} \tag{5}$$

(7) **Control Cost Ceiling Initialization**

In the practical information security risk control deploying process, control cost ceiling is determined by information system management according to the actual criteria. In order to facilitate the further study, we calculate the control cost ceiling influenced by control scale Γ ($\Gamma \in (0, 1)$) and control cost θ_{nc}:

$$D = \Gamma \sum_{n \in N} \sum_{c \in C} \theta_{nc} \tag{6}$$

3. **Risk Control.** The risks usually initiate from one node in the operation-flow and spread through the operation-flow to other affected nodes. If deploying one or more controls at an affected node, the relevant risk could be detected and the risk damage could be controlled. The essence of deploying various controls at different nodes is a process of combinational optimization with control cost restriction. The purpose of information security risk control is deploying optimal controls at the nodes in the operation-flow conforming to the control cost restriction, and reduces the risk damage as much as possible. The ORCM includes the control effect maximization operation and the control cost minimization operation.

3.1. **Control effect maximization operation.** The mission of control effect maximization operation is developing appropriate and effective control deployment scheme to reduce the overall risk damage to the lowest level. According to the risk quantification process, define the parameter that minimum residual risk damage μ describing the minimum risk damage after deploying controls. The minimum residual risk damage is regarded as limiting criterion in the control cost minimization operation. It is formally defined as follows:

$$\mu = Min\left[\sum_{r\in R} F_r - \sum_{r\in R}\sum_{n\in N}\sum_{c\in C} f_{rnc}Q_{rnc}\right] \tag{7}$$

Similar to other linear programming methods, the minimum residual damage conforms to the following 4 limiting criteria:

(1) The risk can be controlled only if a control is deployed at a node as well as it is applicable there. Therefore, set the limiting criterion as follows:

$$Q_{rnc} \le \beta_{rnc}W_{nc} \quad \forall r \in R,\ n \in N,\ c \in C \tag{8}$$

(2) For each risk, at most one control can be effective in a risk transmit path. Therefore, set the limiting criterion as follows:

$$\sum_{n\in p}\sum_{c\in C} Q_{rnc} \le 1 \quad \forall r \in R,\ p \in P_r \tag{9}$$

(3) The total control cost of the control deployment scheme should not be more than the control cost ceiling D. Therefore, set the limiting criterion as follows:

$$\sum_{n\in N}\sum_{c\in C} \theta_{nc}W_{nc} \le D \tag{10}$$

(4) Set the limiting criterion of W_{nc} and Q_{rnc} as follows:

$$W_{nc} \in \{0,1\} \quad Q_{rnc} \in \{0,1\} \tag{11}$$

Conforming to the limiting criteria (8-11), we can formulate the suitable and effective control deployment scheme which can reduce the overall risk damage to the lowest level and get the minimum residual risk damage μ by multiple iterative calculations.

3.2. **Control cost minimization operation.** The control cost will fluctuate with the location changing, and different control deployment scheme can also achieve the same or approximate control effect. Therefore, in the control cost minimization operation, minimum control cost is regarded as the object function to obtain the control cost minimization deployment scheme on the premise of not more than the minimum residual risk damage. Set the object function as follows:

$$Min\left[\sum_{n\in N}\sum_{c\in C} \theta_{nc}W_{nc}\right] \tag{12}$$

The control cost minimization operation also conforms to the limiting criteria (8-11). And residual risk damage should not be more than μ. Therefore, set the limiting criterion as follows:

$$\sum_{r\in R} F_r - \sum_{r\in R}\sum_{n\in N}\sum_{c\in C} f_{rnc}Q_{rnc} \leq \mu \tag{13}$$

Conforming to the limiting criteria (8-11) and (13), the control deployment scheme which is formulated by multiple iterative calculations is the optimal risk control deployment.

4. Experiment and Result Analysis.

4.1. Experiment environment build and attack scenario.

To verify the control effect of ORCM, we simulate the nodes and operation-flows in the information system at first. Then, implement the deployment scheme which was formulated by ORCM using LINGO. Majority of the current risk control processes use checklists or heuristic rules-of-thumb to implement the deployment of controls in operation-flow. Thus, we compare our method with two heuristic decision-making methods that are Heuristic Risk Control Method (HRCM) and Restrictive Heuristic Risk Control Method (RHRCM) which can be representative of typical risk control deployment method for information security through simulation attack.

Utilizing the risk quantification parameters initialization method, randomly build 150 data sets. Each data set randomly generates a set of risk quantification parameters including node, risk, risk control and other parameters which will be used in information security risk control operation.

Take the Random Attack Scenarios (RAS) which randomly select the risks can attack the operation-flow. Then attack the operation-flows which have been deployed controls. The details of attack are shown as follows:

(1) Randomly set an integer $\mathit{Num} \in (0, |\mathbf{R}|)$, $|\mathbf{R}|$ is the quantity of $\mathbf{R}$.
(2) Randomly select the amount of Num risks without replacement from the set of $\mathbf{R}$.
(3) Calculate the actual damage of the operation-flows which have been deployed controls by each method.

4.2. HRCM and RHRCM.

The HRCM iteratively selects controls and locations to reduce the information security risk damage of the operation-flows from an overall perspective. Once a control deployment operation exceeds the control cost ceiling, search the next control which can conform to the control cost ceiling. Do not stop deploying controls until there is no control to choose which can conform to the control cost ceiling. The detailed process is shown as follows:

(1) Calculate the entire risk damage reduction:

$$\sum_{r\in R} \beta_{rnc} f_{rnc} \quad \forall n \in N,\ c \in C \tag{14}$$

(2) Select the node that deployed controls can generate maximum risk control effect for all of the risks. That is on the premise of not exceeding the control cost ceiling, if deploying control c_0 at node n_0c, the value of $\sum_{r\in R} \beta_{rn_0c_0} f_{rn_0c_0}$ could reach the maximum value then set $W_{n_0c_0}$ as 1. If the selected deployment operation cannot conform to the control cost ceiling then select the next deploying operation.

(3) Do not stop execute step (1) and step (2) until there is no deployment operation to select which can conform to the control cost ceiling.

The RHRCM is improved from HRCM and its control cost ceiling is equal to the control cost of ORCM.

4.3. **RAS risk control contrast experiment.** We take simulation attacks to the operation-flows which have been respectively deployed by ORCM, HRCM and RHRCM to compare the risk control performance. Firstly, we calculate the risk damage reduction of the operation-flow which has been deployed controls. Then, we calculate the ratio between the risk damage reduction and the risk control cost. If a method's ratio is lower, we can conclude: On the premise of getting the same risk control effect, this method needs more control cost, and its performance is weaker. We define two control effect parameters RC and RCO to quantify the risk control performance:

$$RC = \text{Damage before deployed controls} - \text{Damage after deployed controls} \tag{15}$$

$$RCO = RC/\text{Control cost} \tag{16}$$

We set the RC and RCO of ORCM as a baseline (the value is 100) to facilitate the comparison of the risk control performance between ORCM and HRCM as well as RHRCM. If the RC of the other two methods are over 100, it would illustrate their control effects are superior to ORCM. If the RCO of the other two methods are over 100, it would illustrate their control performance is superior to ORCM. The RAS experiment results are shown in Table 2.

Table 2. The value of RC and RCO in RAS experiment

Risk Control Methods	RC			RCO		
	Average	Average	Average	Average	Maximum	Minimum
ORCM	100	100	100	100	100	100
HRCM	96.7	4.5	4.5	4.5	48.6	0.5
RHRCM	82.6	79.3	79.3	79.3	98.9	29.6

The experiment results indicate that:

(1) The ORCM not only has better security risk control effect than others but also has lower control cost than others;

(2) In some occasional cases, the HRCM can get the control effect which is equal to the control effect of ORCM;

(3) When the RHRCM restricts the control cost ceiling which is equal to the control cost ceiling of ORCM, the risk damage reduction reduces sharply.

The causes of the results are:

(1) The HRCM and RHRCM merely take risk damage reduction into account without considering the factor of control cost;

(2) The HRCM cannot effectively select risk controls once deployment operation cannot conform to the control cost ceiling. It makes the stability of this method so poor;

(3) In some occasional cases, the HRCM can effectively control the information security risks. However, on the premise that the control cost of each method is equivalent the HRCM cannot get the same risk control effect as ORCM.

5. **Conclusion.** We proposed the ORCM to effectively control the information security risk of operation-flow in information systems. Firstly, we studied the method of risk quantification based on operation-flow. Then, we studied the method of risk control using linear programming method. The RAS experiment shows that the ORCM not only has better security risk control effect but also has lower control cost. In the future research, we plan to improve the time complexity of ORCM and increase the efficiency of decision-making.

Acknowledgement. This work is partially supported by the National Natural Science Foundation of China (NSFC). We would like to thank NSFC and people for their supports.

REFERENCES

[1] M. Zhang, Survey of information security risk assessment methods, *Information Security and Technology*, vol.25, no.1, pp.10-20, 2015.

[2] M. Qasem, Information technology risk assessment methodologies: Current status and future directions, *International Journal of Scientific & Engineering Research*, vol.12, no.4, pp.966-973, 2013.

[3] BS7799-2, *Information Security Management Specification for Information Security Management Systems*, 2002.

[4] NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, 2013.

[5] AS/NZS 4360, *Risk Analysis of Technological Systems – Application Guide*, 2004.

[6] D. Cernauskas and A. Tarantino, Operational risk management with process control and business process modeling, *Operation Risk*, vol.26, no.4, pp.3-17, 2009.

[7] S. Dzazali and A. Zolait, Assessment of information security maturity: An exploration study of Malaysian public service organization, *Journal of Systems and Information Technology*, vol.14, no.1, pp.23-57, 2012.

[8] B. Xue, G. Ram and N. Manuel, On the prevention of fraud and privacy exposure in process information flow, *Journal of Computers*, vol.24, no.3, pp.416-432, 2012.

[9] A. Hemanidhi, S. Chimmanee and C. Kimpan, Cyber risk evaluation framework based on risk environment of military operation, *Proc. of the Defense Technology*, Thailand, pp.42-47, 2015.

[10] A. Teixeira, C. Kin, H. Sandberg and K. Johansson, Secure control systems: A quantitative risk management approach, *Control System*, vol.35, no.1, pp.24-45, 2015.

[11] S. Mousavian, J. Valenzuela and J. Wang, A probabilistic risk mitigation model for cyber-attacks to PMU networks, *Power Systems*, vol.30, no.1, pp.156-165, 2015.

[12] M. Moyo, H. Abdullah and R. Nienaber, Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems, *Proc. of the Information Security for South Africa*, Johannesburg, pp.1-6, 2013.

[13] H. Orojloo and M. Azgomi, A method for modeling and evaluation of the security of cyber-physical systems, *Proc. of the Information Security and Cryptology*, Tehran, pp.131-136, 2014.

[14] I. Fray, M. Kurkowski and J. Pejaś, A new mathematical model for analytical risk assessment and prediction in IT systems, *Control and Cybernetics*, vol.41, no.2, pp.241-268, 2012.

[15] H. Yang, X. Liu and Y. Lu, A risk quantitative evaluating method based on related vulnerabilities, *ICIC Express Letters*, vol.5, no.9(A), pp.3081-3086, 2011.

[16] X. Sun, Algorithm of minimum spanning tree problem based on fuzzy structured element, *Journal of Chinese Computer Systems*, vol.36, no.4, pp.806-809, 2015.