Modeling of Risk Treatment Measurement Model under Four Clusters Standards (ISO 9001, 14001, 27001, OHSAS 18001)

Liu Qi¹*, Du Qingling¹, Shi Wei¹, Zhu Jine²

¹ Information Security Department, Henan Police College, Zhengzhou Henan 450002, China
² FujiElectric(Hangzhou) Software Co., Ltd., Hangzhou 310012, China

Abstract

A novel model to measure Risk Treatment ARME (Assets Risk Value & Control Measures Effectiveness) under four clusters standards (ISO 9001, 14001, 27001, OHSAS 18001) was firstly proposed in this paper. Establishment, computation, realization flow and applications were discussed in this paper. Correctness of the model was proved; the corresponding indicator system was given. The computation and implementation flow were developed. It was proposed the superiorities of some organization undertook this model. According to the theory study and the practical implementation, the model proposed in this paper was effective for measuring risk treatment plan.

© 2010 Published by Elsevier Ltd. Selection and/or peer-review under responsibility of Society for Resources, Environment and Engineering. Open access under CC BY-NC-ND license.

Keywords: risk treatment measurement; ARME; indicator system; risk treatment effectiveness

1. Introduction

Nomenclature

| A | Assets       | Su | Sufficiency |
|---|--------------|----|-------------|
| R | risk value   | U  | Usability   |
| S | security coefficient | La | Laxity |
| C | Control Measures | Sb | Suitability |
| T | Timeliness   | E  | Efficiency  |

* Supported By Henan Education Committee Project (12B620002); Corresponding author. Liu Qi (1978-), associate professor, Ph.D. Research Specialty. Risk Assessment. Mobile.15903667760. E-mail address: michellemini@yahoo.cn.
There exists different kind of risks in the process of organization operation, for example, quality risks, environmental risks, operational health and safety risks, information security risks, and etc. These risks present on different kinds of manifestation, and correlate with each other in organizations’ strategic planning, organizational management, production operation and service activity[1]. These may cause social responsibility risks and law risks eventually. Numerous organizations implement management system integrated quality, environmental, occupational health and safety, information security based on international standard Clusters ISO 9001[2], ISO 14001[3], OHSAS 18001[4], and ISO/IEC 27001[5] to manage risks[6-10], improve their general viabilities. However, there faces several problems in practical work when applying these four clusters of standards. One of the knotty problems is that it is difficult to measure the effectiveness after implement risk treatment plan. Seldom materials, standards could be found in published literatures at present.

A novel risk treatment plan measurement model (ARME) was proposed in this paper, based on the establishment of information security system in many organizations. The effectiveness of the model was proved in this paper, and it was applied in several organizations. Theory study and the practical implementation proved the effectiveness of ARME.

2. Modeling of ARME

2.1. Establishment of ARME

According to OHSAS 18001[4], risk means, “combination of likelihood of an occurrence of a hazardous event or exposure(s) and the severity of injury or ill health that can be caused by the event or exposure(s)”; risk assessment means, “process of evaluating the risk(s) arising from a hazard(s), taking into account the adequacy of any existing controls, and deciding whether or not he risk(s) is acceptable”. After assess risks, proper treatments should be implemented to guarantee organization’s security. These treatments are called risk treatments[11]. The purpose of establishing “risk treatment measurement model” is to measure the effectiveness of risk treatments. The evaluations are based on several corresponding parts: the sufficiency of risk treatment, if the execution could be undertake according to the plan, if the desired effect could be catered for, and etc.

Through the investigation, we think the following factors should be considered to measure risk treatment effectiveness: security coefficient; Timeliness (control measure effects could react organizations in time limitation); Sufficiency (control measures could be fully implemented); Usability (if control measures could be easily implemented); and etc. Based on the above, the effectiveness measurement model (ARME) and indicator system were firstly proposed in fig. 1.

![Fig.1 ARME Model](image-url)
2.2. Computation of ARME

The computation of ARME model was firstly proposed in this paper with definition, theorem, and corollary as follows.

**Definition:** Define ten tuples \( \sum = \{A, R, C, S, T, Su, U, La, Sb, E\} \) . \( R \rightarrow S \) satisfies \( S = (R_{\text{max}} + 1) - R \) . \( S, T \rightarrow La \) satisfies \( La = co_1 \times S + co_2 \times T \) . \( Su, U \rightarrow Sb \) satisfies \( Sb = co_3 \times Su + co_4 \times U \)  (co_1 , co_2 , co_3 , co_4 represent normalization coefficients) . Then \( Rl, Sb \rightarrow Ef \) satisfies \( E = La \times w_{rl} + Sb \times w_{sb} \) \( (w_{rl}, w_{sb} \) represent weights of \( La \) and \( Sb \).

**Theorem:** For ten tuples \( \sum = \{A, R, C, S, T, Su, U, La, Sb, E\} \) , always holds equation 1.

\[
E = w_{rl} \left[ co_1 \times (R_{\text{max}} - R + 1) + co_2 \times T \right] + w_{sb} \left[ co_3 \times Su + co_4 \times U \right]
\]

**proof:**

\[
E = La \times w_{la} + Sb \times w_{sb} = \left[ co_1 \times S + co_2 \times T \right] \times w_{rl} + \left[ co_3 \times Su + co_4 \times U \right] \times w_{sb} = w_{rl} \left[ co_1 \times (R_{\text{max}} - R + 1) + co_2 \times T \right] + w_{sb} \left[ co_3 \times Su + co_4 \times U \right]
\]

**Corollary:** For arbitrary \( a_i \in A \) , \( e_{i,j} \in E \) , \( r_{i,j} \in R \) , \( s_{i,j} \in S \) , \( c_{i,j} \in C \) , \( t_{i,j} \in T \) , \( la_{i,j} \in La \) , \( su_{i,j} \in Su \) , \( u_{i,j} \in U \) , \( sb_{i,j} \in Sb \) , always holds equation 2.

\[
e_{i,j} = w_{rl} \left[ co_1 \times (\max(R) - r_{i,j} + 1) + co_2 \times t_{i,j} \right] + w_{sb} \left[ co_3 \times su_{i,j} + co_4 \times u_{i,j} \right]
\]

**Proof:** By the above definition, each set in ten tuples \( \sum = \{A, R, C, S, T, Su, U, La, Sb, E\} \) could be represented by matrix as follows. Input set Assets, output set Effectiveness could be represented by matrix as:

\[
A = \begin{bmatrix}
a_1 & \ldots & a_n \\
\end{bmatrix}, \\
S = \begin{bmatrix}
r_{11} & \ldots & r_{1m} \\
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
r_{nm} & \ldots & r_{nm} \\
\end{bmatrix}, \\
C = \begin{bmatrix}
s_{11} & \ldots & s_{1m} \\
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
s_{nm} & \ldots & s_{nm} \\
\end{bmatrix}, \\
T = \begin{bmatrix}
c_{11} & \ldots & c_{1m} \\
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
c_{nm} & \ldots & c_{nm} \\
\end{bmatrix}, \\
R = \begin{bmatrix}
r_{11} & \ldots & r_{1m} \\
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
r_{nm} & \ldots & r_{nm} \\
\end{bmatrix}, \\
U = \begin{bmatrix}
su_{11} & \ldots & su_{1m} \\
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
su_{nm} & \ldots & su_{nm} \\
\end{bmatrix}, \\
Su = \begin{bmatrix}
u_{11} & \ldots & u_{1m} \\
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
u_{nm} & \ldots & u_{nm} \\
\end{bmatrix}, \\
U = \begin{bmatrix}
t_{11} & \ldots & t_{1m} \\
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
t_{nm} & \ldots & t_{nm} \\
\end{bmatrix}, \\
Sb = \begin{bmatrix}
sb_{11} & \ldots & sb_{1m} \\
\ldots & \ldots & \ldots \\
\ldots & \ldots & \ldots \\
sb_{nm} & \ldots & sb_{nm} \\
\end{bmatrix}
\]

Use \( a_i \) , \( a_j \in A \) ; \( e_{i,j} \in E \) ; \( r_{i,j} \in R \) ; \( s_{i,j} \in S \) ; \( c_{i,j} \in C \) ; \( t_{i,j} \in T \) ; \( la_{i,j} \in La \) ; \( su_{i,j} \in Su \) ; \( u_{i,j} \in U \) ; \( sb_{i,j} \in Sb \) to represent arbitrary elements.
belongs to the set. (i = 1,2,...,n , j = 1,2,...,m ). Based on Definition, \( S = (R_{\text{max}} + 1) - R \), \( La = co_1 \times S + co_2 \times T \), \( Sb = co_3 \times Su + co_4 \times U \), \( E = La \times w_{La} + Sb \times w_{Sb} \), the corresponding equations could be obtained.

\[
s_{i,j} = (\max(R) + 1) - r_{i,j} \quad (3)
\]

\[
l_{a_{i,j}} = co_1 \times s_{i,j} + co_2 \times t_{i,j} \quad (4)
\]

\[
sb_{i,j} = co_3 \times su_{i,j} + co_4 \times u_{i,j} \quad (5)
\]

\[
e_{i,j} = la_{i,j} \times w_{La} + sb_{i,j} \times w_{Sb} \quad (6)
\]

Put equations (3)—(5) into equation (6), then

\[
e_{i,j} = \left[ (\max(R) + 1) - r_{i,j} \right] \times co_1 + \left[ co_3 \times su_{i,j} + co_4 \times u_{i,j} \right] \times w_{Sb}
\]

Equation (2) could be obtained:

\[
e_{i,j} = c_1 w_{RL} \left[ (\max(RV) - rv_{i,j} + 1) \times t_{i,j} \right] + c_2 w_{Sb} \left[ aq_{i,j} \times cv_{i,j} \right]
\]

2.3. Realization Flow of ARME

Effectiveness of model (ARME) could be computed by extracting parameters from risk treatment tables, control measurement implementation tables, then binding initial values input subjectively, as showed in figure 2.

3. Applications of ARME

We applied ARME in several organizations, to guarantee the effectiveness of risk treatment plan in the previous work. Take H organization for example, model ARME was used to measure its effectiveness of risk treatment. Every threat, vulnerability in all 59 risk treatment tables was evaluated as follows.

- Measure all risk treatment plans by ARME
- Compute the scores of each risk treatment plans
- Classify all the results into three levels
- Analyze the results and obtained the efficiency of ARME

A sample of ARME application is showed in table1. From table1, Treatment results of 100 classes risk treatment plans were 37% with excellent effect, 33% with good effect, 30% with average effect.
Table 1. Risk Treatment Plan Measurement by ARME (Incomplete)

| Assets Serial Numbers | Risk Value (normalized) | S | T | C | U | La | Sb | E |
|-----------------------|-------------------------|---|---|---|---|----|----|---|
| PD-MD-AD-BC           | xxx                     | 20| 85%| 2 | 2 | 7  | 2  | 5 |
| PD-MD-AD-TC           | xxx                     | 20| 80%| 2 | 2 | 2  | 2  | 2 |
| PD-MD-AD-EC           | xxx                     | 21| 100%| 3 | 5 | 8  | 6  | 7 |
| PD-DD-SD              | xxx                     | 5 | 80%| 2 | 2 | 7  | 2  | 5 |
| PD-DD-SD              | xxx                     | 20| 100%| 5 | 4 | 10 | 8  | 9 |

The analysis is as follows. Measurements with excellent effects focus on establishing corresponding management regulations, procuring necessary equipments, and etc. This result catered for actively working attitudes of top leaders and coordinate department. Measurements with good effects concentrate on staff implementing corresponding control measurements. This result catered for their busy working fuzzy regulations of reward and punishment. Measurements with average effects focus on IT department. This is accorded that there is no full-time staff in the department. All the results above catered for H organization’s actual situation, which shows the effectiveness of model ARME proposed in this paper.

4. Conclusion

A novel risk treatment measurement model –ARME for organizations established ISO 9001, ISO 14001, OHSAS 18001, and ISO/IEC 27001 four clusters standards management systems was firstly proposed in this paper. Besides, the corresponding indicator system was proposed. The computation equations was designed and proved theoretically. The realization flow was showed and one of the application cases of H organization was given. According to theoretically study and practical applications, the model ARME proposed in this paper is effectiveness for measuring risk treatments. Next research will focus on indicator system coefficients adjustment, organizations’ feed back about the model, and etc.

References

[1] Guang Yaohua, Xie Zongxiao, Cheng Yuqi. Quality/ Environnemental/ Operation and Health/ Information Security Four Clusters Standards Integrating Management System Course. China Standards Publishing House. 2009.9.
[2] ISO 9001, Quality management systems— Requirements.
[3] ISO 14001, Environmental management systems— Requirements with guidance for use.
[4] OHSAS 18001, Occupational health and safety management systems— Requirements.
[5] ISO/IEC 27001, Information technology-Security techniques-Information security management systems-Requirements.
[6] NIST Special Publication 800-30: Risk Management Guide for Information Technology Systems.
[7] Z. Predrag. Information risk and security modeling. Proceedings of SPIE — The International Society for Optical Engineering, Vol. 5812, Data Mining, Intrusion Detection, Information Assurance, and Data Networks Security 2005, 142-150.
[8] H. Olivers, Information modeling for automated risk analysis. Communications and Multimedia Security: CMS 2006, LNCS 4237, 2006, 228-239.
[9] V. Page, M. Dixon, I Choudhury. Security risk mitigation for information systems. BT TECHNOLOGY JOURNAL, 2007, 25(1), 118-127.
[10] Kevin J. Soo Hoo. How much is enough? [D] A Risk-Management Approach to Information Security, Doctoral dissertation, Stanford University, (20):69-78, 2000.
[11] NIST, ISO/IEC 27002, Information technology-Security techniques - Code of practice for information security management