

Evaluation of Assurance Case Description Method using ISO 27001 for Merger and Acquisition

Nobuyuki Kobayashi ^{*}, Aki Nakamoto [†], Maki Kawase [‡],
Makoto Ioki [†], Seiko Shirasaka [†]

Abstract

This study proposes an assurance case description method based on the framework of Information Security Management System (ISMS; ISO 27001). The method agrees to information security policies through co-creation of values between a parent company and its merged and acquired subsidiary. Information security policy varies among companies. Parent companies need to agree with their merged or acquired companies on the information security policies. The purpose is to maintain the existing business of the subsidiaries while the parent companies continue to use the current IT infrastructure and network.

This study first structuralizes ISO 27001 by using an assurance case. As a result, this study will: 1) Clarify the range of agreement and disagreement between the two companies' information security policies; and 2) show how two companies mutually conclude a final agreement for the entire range using the assurance case created. We also present the quantitatively evaluated results from Goal Structuring Notation (GSN) users' ability to structuralize systems with multiple viewpoints by using GSN. This evaluates the proposed description method. We asked three experts in information security to evaluate the understanding, utility and effectiveness of the proposed assurance case description method. The study participants used the method to create an assurance case.

Keywords: M&A, Co-creation, Information security policy, Assurance Case, Dependability Case.

1 Introduction

Against the backdrop of an increase in the number of global merger and acquisitions (M&A), including those by Japanese companies, some previous studies have seized cooperative activities through M&A among two or more companies as co-creation of value. For instance, Alves et al. [1] pointed out that one of the fields of co-creation of value involves the development of business

^{*} The System Design and Management Research Institute of Graduate School of System Design and Management, Keio University, Kanagawa, Japan

[†] Graduate School of System Design and Management, Keio University, Kanagawa, Japan

[‡] Center for Collaborative Research and Community Cooperation, Hiroshima University, Hiroshima, Japan

logic in which co-creation features as a source of innovative ideas among companies. For the development of business logic, infrastructure development is necessary. Infrastructure includes information security policy because infrastructure is developed abiding by the information security policy. In addition, Mitleton-Kelly [2] stated that coevolutionary integration may be facilitated through the co-creation of an enabling infrastructure. Information security policy is considered in the literature as key in the post-M&A business.

This study therefore intends to demonstrate how two companies co-create as values the business logic pointed out by Alves et al. [1]. Specifically, since information security policy varies among companies, parent companies need to agree with its merged or acquired companies on the information security policies. They can maintain the existing business of the subsidiaries while continuing to use the IT infrastructure and network. There are two reasons for the difficulty. First, the differences and similarities of the information security policies established by each company are not visible within the policy documented internally. Second, the third party who does not belong to those companies finds it extremely hard to find consistency in the information security policies of parent companies and its subsidiaries.

We thus propose a description method for agreeing to information security policies between a parent company and its subsidiary or subsidiaries merged or acquired, based on the framework of Information Security Management System (ISMS; ISO 27001) [3] by using the assurance case [4] proposed by Kelly [5].


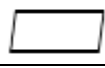




This study first structuralizes ISO 27001 by using an assurance case. We then show the items that a parent company and the subsidiary do not agree to based on each company's information security policy, and describe concrete responses for each item. As a result, this study will: (1) Clarify the range of agreement and disagreement between the two companies' information security policies; (2) Show how two companies mutually achieve a final agreement for the entire range using the assurance case created. The proposed method in this study is evaluated using three kinds of data. The first is the assurance case that the studied participants created using the proposed description method. The second uses interviews to three experts in information security (two who are in charge of information security management, and another who is in charge of marketing strategy for information security software) asking them how they evaluate the Understanding, Utility and Effectiveness of the proposed assurance case description method which the studied participants used to create the assurance case. The third is to present the quantitatively evaluated results from Goal Structuring Notation (GSN) users' ability to structuralize systems with multiple viewpoints by using GSN. This evaluates the proposed description method. The assurance case description results in this study were results described according to the procedure of the description method. Therefore, the outcomes were less dependent on the user's ability to create an assurance case. This study concludes with future research topics.

2 Literature Review

Goal Structuring Notation (GSN) of a safety case description method has been proposed by Kelly [5] in 1998 as a means for performing clear, complete and reasonable discussion. Using the safety case helps the operation reach an acceptable level in terms of safety between stakeholders. An assurance case [6] extends the discussion area to the whole quality of the discussed system including the "safety" proposed in the safety case. An assurance case is mainly an assurance method using six nodes, including Goal, Context, Strategy, Evidence, Monitoring and Undeveloped. [7] [8] These six nodes are shown in Table 1.

Previous research has made two proposals similar to this study in relation to application of assurance cases in information security policy. First, Ying [9] proposed templates applicable to information security management systems in healthcare. Ying's study, however, is focused on the healthcare field and does not propose a method for agreement among multiple companies. Second, Kaneko et al. [10] proposed Common Criteria Case (CC-Case; the same as ISO/IEC15408) as the procedures to analyze requirements systematically based on assurance cases as well as Common Criteria, which is an evaluation standard for information security. The study of Kaneko et al. is also focused on a specific field of system development and does not refer to a method of agreement among multiple companies.

Table 1: Six nodes in assurance cases.

Node	Figure	Explanation
Goal		Goal describes what to assure, with a combination of a subject and predicate.
Strategy		Strategy describes how to break down the Goal into sub-goals leading to the lower layer.
Context		Context describes the state, or environment and conditions of the System, and shows ways to lead to the Goal and Strategy.
Evidence		Evidence eventually assures that we can reach the Goal, and shows ways to lead to the Goal.
Monitoring		Monitoring is intended to represent Evidence available at runtime, corresponding to the target values of in-operation ranges.
Undeveloped		Undeveloped shows the status that there is no Evidence or Monitoring, or discussion supporting the Goal.

Next, this study shows previous researches focused in fields of management and business. Kobayashi et al. [11] proposed four-layered assurance case description method for solving communication challenges in business. Kobayashi et al. [12] also showed that using assurance cases increases the feasibility of accomplishing management vision and management strategy. The other previous study has proposed an assurance case description method to reduce misunderstanding caused by the difference of grasping the objects managed in various departments as a monolithic system or a System of Systems. [13] In addition, the other previous study has proposed an assurance case description method which allows considering simultaneously the inside of a system and the assumed changes outside the system. [14] The previous study [15] evaluated whether GSN is a notation method structuralizing with multiple viewpoints. The previous study [16] based on the above study [15] proposed a quantitative evaluation method for evaluating the ability to structuralize systems with multiple viewpoints of users describing GSN. This study therefore evaluated whether the assurance case description method acquires the ability to structuralize systems with multiple viewpoints by using the quantitative evaluation method [16]. The novelty of this study therefore is to propose a description method for assurance cases to be used for agreeing to information security policies between a parent company and its subsidiary or subsidiaries merged or acquired.

Yamamoto and Matsuno stated that setting the following three factors in the description method is effective in solving the existing issues [17] related to the description method of assurance cases [18]: (1) A limited field of application, (2) A specific hierarchical structure for assurance case,

and (3) Description rules for nodes. The relationship of these three will be described in section 3. Thus what makes this study unique is the combination of the following points:

- Uses assurance cases (Dependability Cases).
- Taking account of agreement among multiple companies.
- Setting three factors in the proposed description method of assurance cases.
- Uses ISO 27001 as a framework.

Next, this study presented a method to quantitatively evaluate for both horizontal viewpoints and vertical viewpoints using GSN. Kobayashi et al. [15] stated that combining viewpoints is necessary for structuralization with multiple viewpoints. These viewpoints are: a viewpoint that is selected from multiple viewpoints aligned in the horizontal direction; and a viewpoint that is selected from multiple viewpoints aligned in the vertical direction. Kobayashi et al. [16] therefore proposed a method using GSN to quantitatively evaluate the results from horizontal viewpoints and vertical viewpoints separately. The previous study defined six evaluation formulas as follows, in the case where a certain “Strategy node” is set on the top level.

$$H(s)=G_d \quad (G_d>1) \quad (1)$$

$$H(s)=0 \quad (G_d=1) \quad (2)$$

$$V(s)=S_u \quad (G_d>1) \quad (3)$$

$$V(s)=0 \quad (G_d=1) \quad (4)$$

$$TH = \sum_{s=1}^{S_{max}} H(s) \quad (5)$$

$$TV = \sum_{s=1}^{S_{max}} V(s) \quad (6)$$

$H(s)$: $H(s)$ is the result evaluated from the viewpoints aligned in the horizontal direction [15].
 G_d : G_d represents the number of “Goal nodes” positioned directly under the “Strategy node” to be targeted. As an exception, when the number of “Goal node” is one, evaluation method evaluates that $H(s)$ equals zero.

$V(s)$: $V(s)$ is the result evaluated from the viewpoints aligned in the vertical direction [15].

S_u : This study counts from the top “Strategy node”, and S_u represents the numerical order of “Strategy nodes” to be targeted. As an exception, when the number of “Goal node” is one, evaluation method evaluates that $V(s)$ equals zero.

S_{max} : S_{max} is the total number of “Strategy nodes”.

TH : TH is the result of evaluating the total of the viewpoints aligned in the horizontal direction [15] lower than “Strategy node” to be targeted.

TV : TV is the result of evaluating the total of the viewpoints aligned in the vertical direction [2] lower than “Strategy node” to be targeted.

3 Assurance Case Description Method for Information Security Policy

The assurance case created using the proposed description method of assurance cases for information security policy is shown in Figure 1, where a specific hierarchical structure for an assurance case is created with a Logical Model, Logical Argument Model and a Concrete Model.

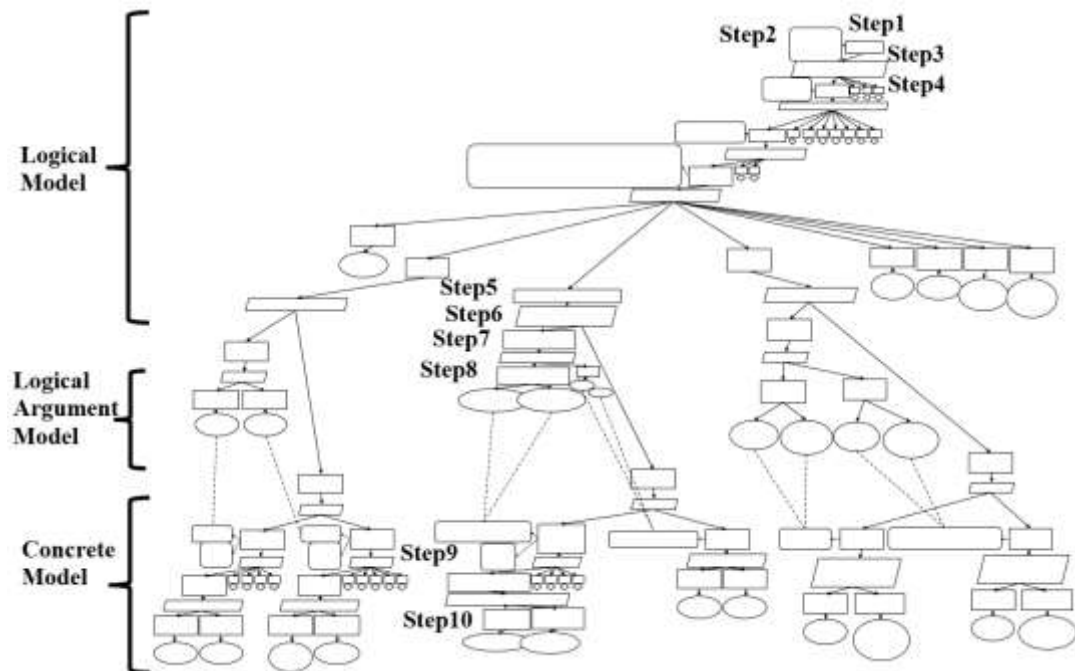


Figure 1: Assurance case created using the proposed description method.

The Logical Argument Model refers to: (1) The range that each company needs to discuss; (2) Goal nodes, and the corresponding Evidence nodes and Monitoring nodes. The Evidence nodes and Monitoring nodes set in the Logical Argument Model are a prerequisite for discussing the Concrete Model. In other words, the Argument Model is, as shown in Figure 1, set as Context nodes for the goals of the Concrete Model. The Concrete Model describes the actual countermeasures of each company against information leakage.

The description method is shown below by steps. The correspondent figures are Figure 2-Figure 4.

A. Description steps for Logical Model

Step 1: Set Goal node.

Step 2: Set Context node as sub-goals by dividing the Goal into sub-goals (called “objectives” in Figure 3-Figure 4). In addition, set priorities, if any, in the Context node when the priority of sub-goals is important.

Step 3: For Strategy node, divide the Goal into sub-goals (in prioritized order, if any).

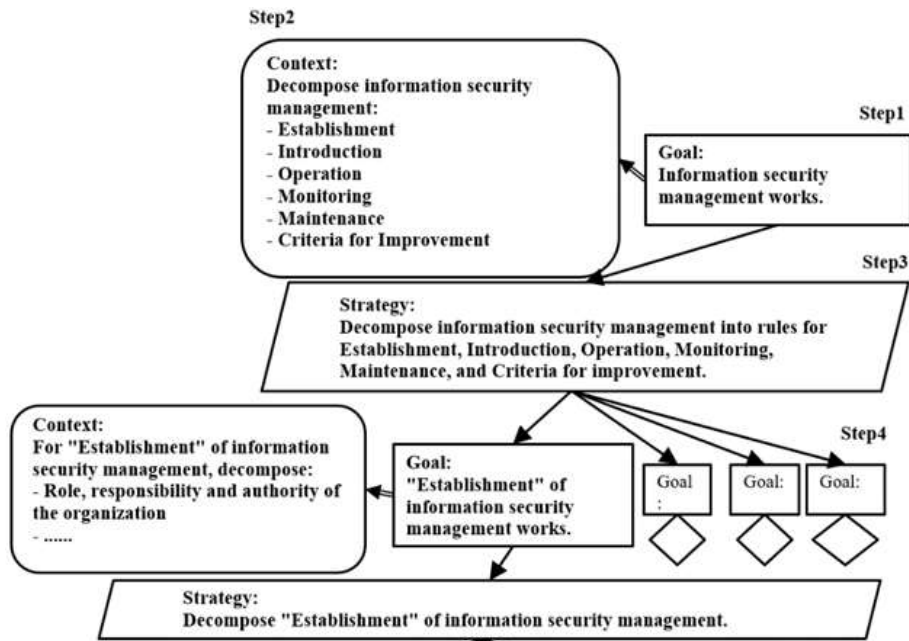


Figure 2: Description steps (1).

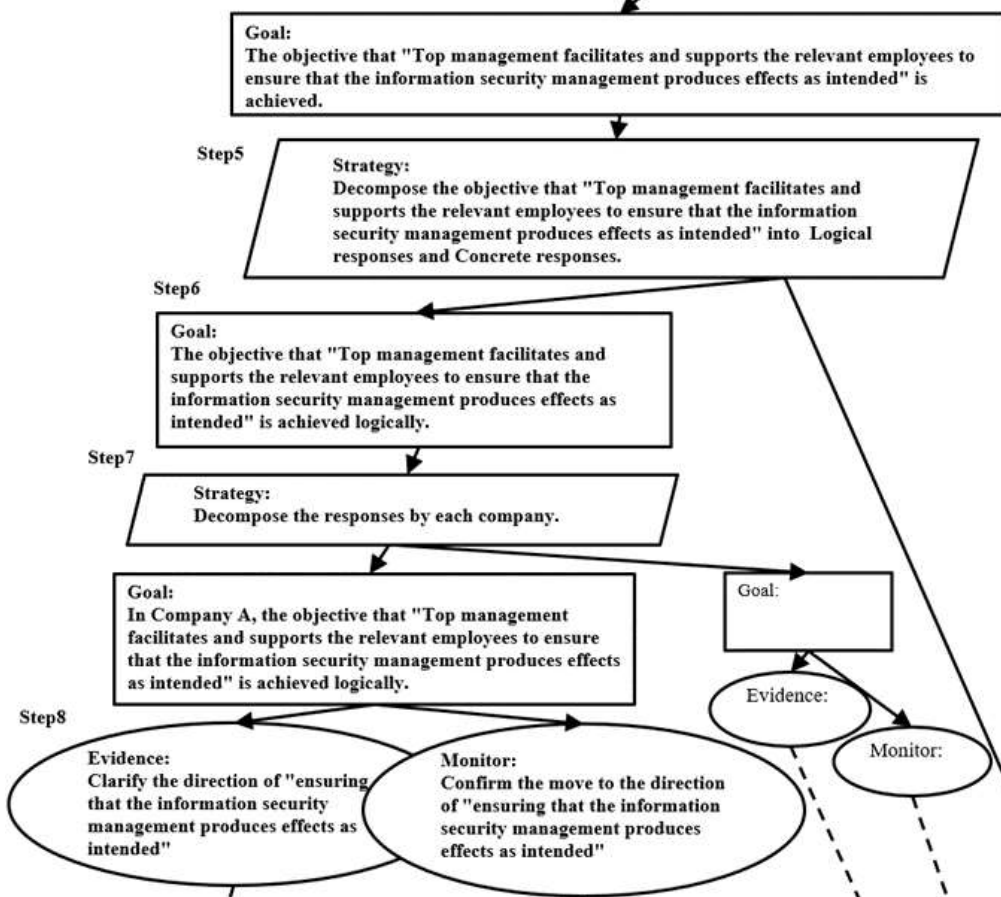


Figure 3: Description steps (2).

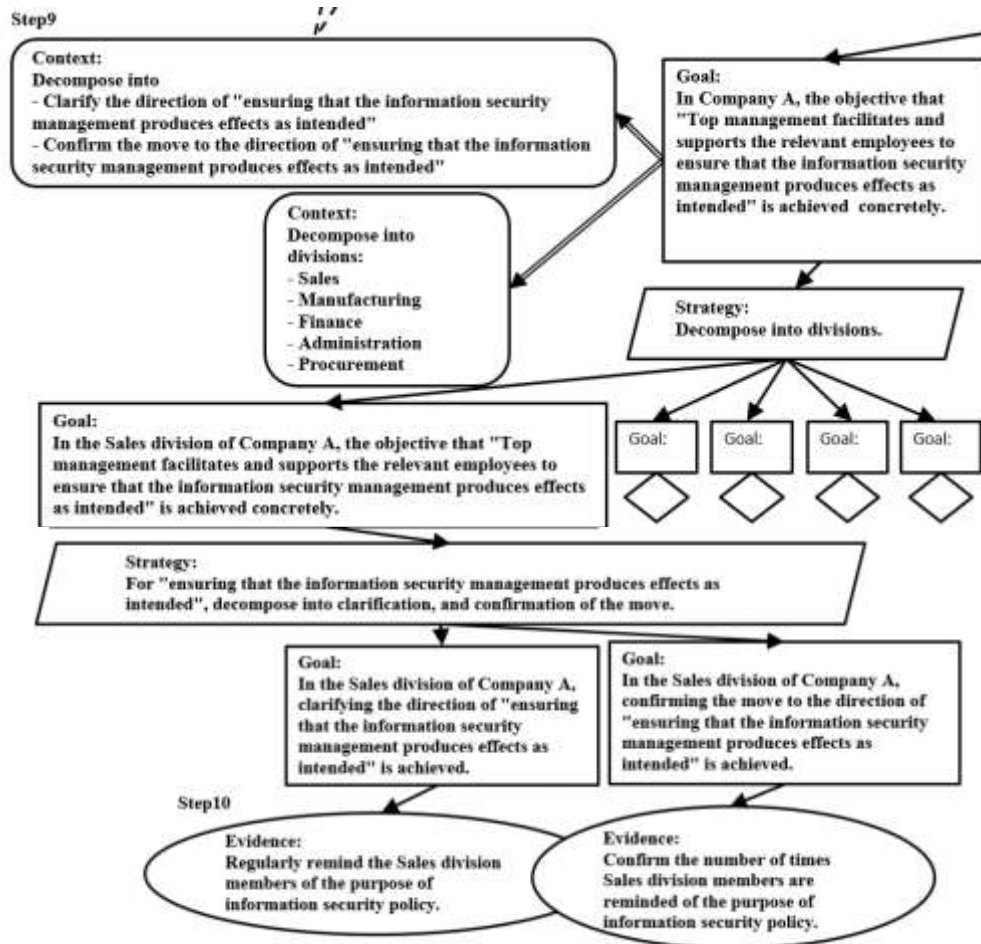


Figure 4: Description steps (3).

Step 4: Set the sub-goals (in prioritized order if any) underneath the Strategy node. In addition, set Evidence nodes if the sub-goals need to be prioritized.

Assume Step 4 to be Step 1, and repeat this process until sub-goal nodes are completely deconstructed.

Step 5: For Strategy node, divide the Goal node on the bottom into Logical responses and Concrete responses.

Step 6: Set Goal nodes respectively for Logical responses and Concrete responses.

B. Description steps for Logical Argument Model

Step 7: Deconstruct for each company the Goal node of Logical responses, and set it as Strategy node.

Step 8: Set Evidence nodes or Monitoring nodes for each company's Goal nodes.

C. Description steps for Concrete Model

Step 9: Set the Evidence nodes or Monitoring nodes as Context nodes since they are prerequisites of the Goal nodes of each company's Concrete responses. In addition, prioritize the prerequisites if necessary, and set them as the Context node. Repeat the process of setting the Goal, Context, and Strategy nodes (See Steps 1–4) as needed until sub-goal nodes are completely explicated.

Step 10: Set Evidence nodes underneath the Goal nodes on the bottom of Concrete Model.

The reasons for setting the Logical Model, the Logical Argument Model, and the Concrete Model are as follows. The description method up to Step 4 shows the range the two companies are able to agree on the unified information security policies. Next, the description method up to Step 8 shows Evidence nodes and Monitoring nodes, which are decomposed for each company so that each company can stipulate its information security policy. The description results up to Step 8 enable to show clearly the range the two companies agreed. The rest of the description methods shows the range of information security policies each company decides. The steps above thereby enables to confirm the range of the information security policies unified by the two companies, and the range decided differently by each company.

4 Evaluation for the Proposed Description Method of Assurance Cases

A. Data Collection Method

Studied companies.

This study applies the proposed assurance case to the Japanese manufacturing industry. The studied companies, a parent company and its subsidiary with a different organizational culture, have completed M&A and are proceeding with their business. An assurance case was created for the information systems of the two companies, which are different depending on the enterprise resources planning.

One of the differences in the organizational culture between the two companies (hereinafter referred to as “Company A” and “Company B”) is the perception of information leakage, which affects information security policy. Company A’s culture prevents information leakage by allowing only an analogue way of outputting to paper. The information does not leak unless the paper is viewed. Company B’s culture prevents information leakage by exchanging digital data only, and recording in a log the routes the information is communicated outside the company. Each company perceives the other’s method of leakage prevention as faulty. Another difference between the two companies is the business model, and programming languages used for the information systems. We therefore consider we can confirm the range of information security policies agreed between two companies, and the range set differently by each company in relation to the business model, and programming languages. The reason is that the feasible means for complying with the information security policies are different depending on the organizational culture, business model, and programming language.

Interview with Experts in Information Security.

This study conducted interviews three experts of information security software to ask them how they evaluate the Understanding, Utility and Effectiveness of the proposed assurance case description method which the studied participants used. We asked three questions as shown in Table 2. The interviewees included three experts. Two experts in information security management were interviewed to learn if the proposed method could actually be utilized in business. The third interviewee was an expert in charge of marketing strategy for information security software. With the information security software being purchased and introduced by each company based on the

information security policy the company established, the software marketing expert understands the differences of information security policies among the purchasing companies. The expert is also aware of how group companies with more than two different information security policies respond when maintaining more than two information security policies.

This study conducted interviews three experts of information security software to ask them how they evaluate the Understanding, Utility and Effectiveness of the proposed assurance case description method which the studied participants used. We asked three questions as shown in Table 2. The interviewees included three experts. Two experts in information security management were interviewed to learn if the proposed method could actually be utilized in business. The third interviewee was an expert in charge of marketing strategy for information security software. With the information security software being purchased and introduced by each company based on the information security policy the company established, the software marketing expert understands the differences of information security policies among the purchasing companies. The expert is also aware of how group companies with more than two different information security policies respond when maintaining more than two information security policies.

Table 2: Evaluation criteria and questions for experts.

Evaluation criteria	Question
Understanding	Have you understood, with the assurance case that was created, the differences of information security policies among the multiple companies?
Utility	Do you think the created assurance case is likely to be used going forward while being revised in accordance with future changes in information security policies?
Effectiveness	Do you think multiple companies can agree to the information security policies with the assurance case that was created?

B. Results of Using the Proposed Assurance Case Description Method

We created the assurance case shown in Fig. 1 using the proposed description method, and then had the experts evaluated. First, we created an assurance case by using ISO 27001 as a framework. We then set as Logical Model the range that the two companies agreed on, and as Logical Argument Model the range that the two companies did not agree on in relation to ISO 27001. Finally, the Concrete Model described the actual countermeasures of each company against information leakage.

C. Evaluation on the Results of Using the Proposed Assurance Case Description Method

This section shows the evaluation results in terms of: (1) Whether the assurance case created clarifies the range of agreement and disagreement between the two companies' information security policies; (2) Whether the assurance case created allows the participants to achieve a final agreement for the entire range. The results of deconstruction until the participants' agreement is achieved is shown in Figure 5.

Figure 5 clarifies the ranges that are agreed (above the bold line) and not agreed (below the bold

line) by the two companies. Stakeholders clarify the range of agreement for the Logical Model through deconstruction using Strategy nodes as far as both companies can agree on unification of the information security standards. In addition, the Goal node agreed by the Evidence node is clarified. Accordingly, when stakeholders agree on all the Goal nodes and Evidence nodes, stakeholders have agreed to the entire range of the two companies' information security policies. Making an assurance case in this way is thus co-creation of value. We are thereby able to confirm the range the two companies agreed to unify, and the range they agreed to set respectively.

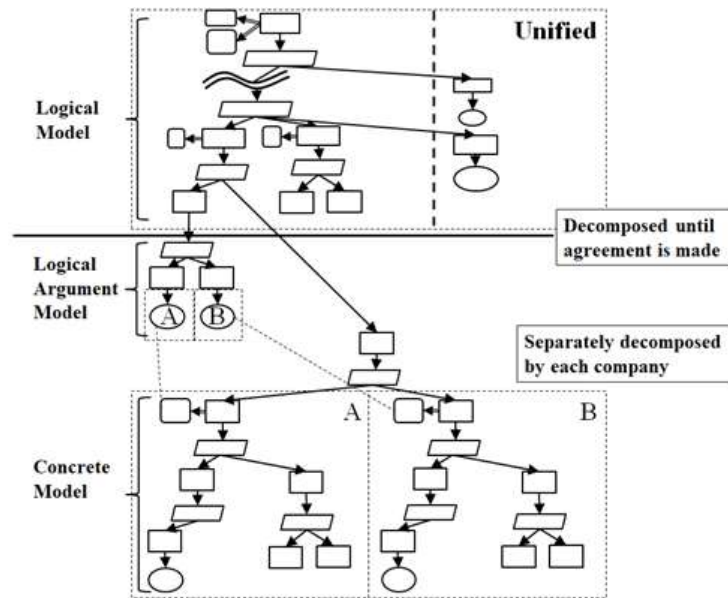


Figure 5: Deconstruction to clarify the ranges that are agreed and not agreed between Company A and B.

D. Interview with Experts in Information Security about Evaluation for the Description of the Assurance Case

We employed interviews to ask three experts in information security about the Understanding, Utility and Effectiveness of the proposed assurance case description method for agreement of information security policy. As a result, the interviews suggested that the proposed method was effective in terms of the Understanding, Utility and Effectiveness.

First, the experts in information security management commented as follows. The method was effective in terms of Understanding since the assurance case made the structure (relationship) of information security policies visible, which was previously invisible. The method was also effective in terms of Utility. Using an assurance case makes the changes visible and recordable though the users previously found the structure invisible and did not know where to record the changes. The method was successful in terms of Effectiveness. Assurance cases allow the stakeholders to achieve an agreement by clarifying the differences. In an assurance case, they can also agree on what they cannot agree to regarding the information security policies.

Next, the expert who is in charge of marketing strategy for information security software commented as follows. The method was effective in terms of Understanding because the assurance

case has a simple look and allowed him to understand, by looking at items as necessary, the responses required in information security policies. The method was also effective in terms of Utility. Assurance cases are simple and easy to understand and practical because the creation is relatively easy to start, and the software for creating Dependability Case (D-Case) provides Microsoft PowerPoint format as well. The method was successful in terms of Effectiveness. With assurance cases visualizing the structure, useless communication costs are unlikely to incur even if more companies are included in creating an assurance case.

Communication with a diagram helps the users avoid errors, which are easy to occur when communicating in different languages. The users can have a discussion while considering the possibility to expand the range above the agreeable level (the bold line in Figure 5). It could be linked to the motivation to unify the information security policies among companies.

However, the interviewers raised two issues. First, the person who handles with the created assurance case needs to understand the entire picture in order to consider the relevance to the changes. The person thus needs to have a sufficient understanding about information security policies and the related areas. Future research needs to visualize the range where the change in information security policy/policies may have an effect within the policy/policies. Second, the expected results are possibly unavailable when the creator of the assurance case has insufficient understanding. The creator would need to use a third party or a template. In addition, the evaluation for the effectiveness of the proposed method in this study is limited to these companies' case, therefore, future research needs to increase the number of applications to verify the Effectiveness of the proposed method. Future research needs to confirm whether other users can describe an assurance case using the proposed description method. Future research also needs analysis of process data for creating an assurance case in order to evaluate both usability and optimality for the proposed assurance case description method.

E. The quantitative evaluation results from horizontal viewpoints and vertical viewpoints separately.

This study shows the results of the viewpoints aligned in the horizontal direction and the viewpoints aligned in the vertical direction for the assurance case created by the proposed assurance case description method (Figure 1). We derived the results in Table 3 by using quantitative evaluation method [16]. The numeric values of each strategy node shown in Figure 6 corresponds to "s" in Table 3.

We showed the consideration using the results of analysis of Table 3. We showed the required abilities ($V = 130$, $H = 69$) to understand the proposed description method by quantitative of the description results. For example, it will be possible to educate considering the depth of the hierarchy based on the result of $V = 130$ by using the above result. Additionally, it will be possible to educate considering the number of viewpoints in the horizontal direction using the result of $H = 69$. The above reason of the viewpoints aligned in the vertical direction is that the layer to consider indicates in which order the layers should be considered and how many layers need to consider by using the result of Table 3. The above reason for the viewpoints aligned in the horizontal direction is that it is possible to quantitatively grasp items that need to consider in each layer. This study showed that it is difficult to qualitatively understand the contents described in assurance cases using the evaluation method.

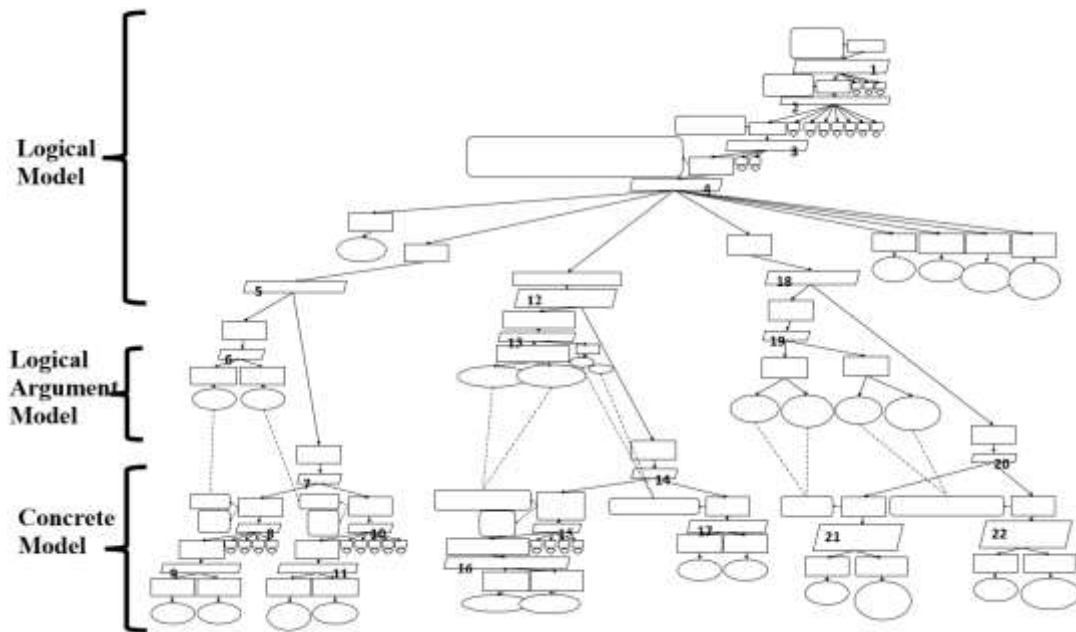


Figure 6: A correspondence to each strategy node number.

Table 3 Results of $V(s)$ and $H(s)$.

s	V	H
1	1	4
2	2	8
3	3	3
4	4	8
5	5	2
6	6	2
7	6	2
8	7	5
9	8	2
10	7	6
11	8	2
12	5	2
13	6	2
14	6	2
15	7	5
16	8	2
17	7	2
18	5	2
19	6	2
20	7	2
21	8	2
22	8	2
Total	130	69

Additionally, the results in Table 3 can be used to compare the proposed description method with other description methods. It is necessary to set the criteria to make a relative comparison between

the proposed description method and other description methods as future research topics. If we can set the above criteria, it is possible to grasp the numerical values that can structuralize systems from multiple viewpoints for each description method. These results help companies clarify the difficulties in applying ISO 27001. Therefore, when we create a new description method, it is possible to understand the difficulties of the description method.

Future research topics are as follows:

- The degree of difficulty setting of the assurance case description method is not clear. The above is useful to recognize an easy order when learning.
- Since the degree of difficulty of conventional description methods has not been grasped, we need to understand the difficulty among description methods by comparing description methods.

5 Conclusions

This study proposed, based on the framework of ISO 27001, an assurance case description method for agreeing to information security policies through co-creation of value between a parent company and its subsidiary or subsidiaries merged or acquired. As a result, we confirmed that the proposed method enabled the participants to create an assurance case. This study shows that: 1) The range of agreement and disagreement based on the two companies' information security policies were clarified; 2) the two companies finally achieved an agreement for the entire range using the assurance case created. We also present the quantitatively evaluated results from Goal Structuring Notation (GSN) users' ability to structuralize systems with multiple viewpoints by using GSN. This evaluates the proposed description method. Additionally, our interviews to experts suggested that the proposed method was effective in terms of the Understanding, Utility and Effectiveness. Principal issues and areas of future research include:

- Visualizing the range where the change in information security policy/policies may affect the policy/policies.
- Checking by a third party or a template which help the creator of an assurance case.
- Increasing the number of applications to verify the Effectiveness of the proposed method.
- Evaluating quantitatively for the range of agreement and disagreement based on the two companies' information security policies using the quantitative evaluation method [19] for assurance case description results.
- The degree of difficulty setting of the assurance case description method is not clear.
- we need to understand the degree of difficulty among description methods by comparing description methods.

Acknowledgement

Nobuyuki Kobayashi, the first author of this research, is supported research activities by Andgate Inc. (<https://www.andgate.co.jp/>).

References

- [1] H. Alves, C. Fernandes, M. Raposo, “Value co-creation: Concept and contexts of application and study”, *Journal of Business Research*, Volume 69, Issue 5, 2016, pp. 1626-1633.
- [2] E. Mitleton-Kelly, “Coevolutionary integration: The co-creation of a new organizational form following a merger and acquisition”, *EMERGENCE: COMPLEXITY & ORGANIZATION*, Issue Vol. 8, No. 2, 2006, pp. 36-47.
- [3] ISO 27001-2013, *Information technology – Security techniques – Information management systems – Requirements*, 2013.
- [4] ISO 15026-2-2011, *Systems and Software engineering Part2: Assurance case*, 2011.
- [5] T. Kelly, “Arguing Safety – A Systematic Approach to Managing Safety Case”, Ph.D. Thesis, University of York., 1998.
- [6] C. Menon , R. Hawkins, J. McDermid, “Defence Standard 00-56 Issue 4, Towards Evidence-Based Safety Standards”, *Proceedings of the Seventeenth Safety-Critical Systems Symposium*, 2009, pp. 223-243.
- [7] GSN Community., “GSN COMMUNITY STANDARD VERSION 1”, Origin Consulting (York), 2011.
- [8] Y. Matsuno, H. Takamura, Y. Ishikawa, “A Dependability Case Editor with Pattern Library”, *IEEE 12th International Symposium on High Assurance Systems Engineering*, 2010, pp. 170-171.
- [9] H. Ying, “Generic security templates for information system security arguments: mapping security arguments within healthcare systems”, Ph.D. thesis, School of Computing Science University of Glasgow. 2014.
- [10] K. Kaneko, S. Yamamoto, H. Tanaka, “CC-Case as an Integrated Method of Security Analysis and Assurance over Life-cycle Process”, *International Journal of Cyber-Security and Digital Forensics (IJCSDF) 3(1): The Society of Digital Information and Wireless Communications*, 2014, pp. 49-62.
- [11] N. Kobayashi, A. Nakamoto, M. Kawase, F. Sussan, M. Ioki, S. Shirasaka, “Four-Layered Assurance Case Description Method Using D-Case”, *International Journal of Japan Association for Management Systems*, Vol. 10 No.1, 2018, pp. 87-93.
- [12] N. Kobayashi, A. Nakamoto, M. Kawase, F. Sussan, S. Shirasaka, “What Model(s) of Assurance Cases Will Increase the Feasibility of Accomplishing Both Vision and Strategy?”, *Review of Integrative Business and Economics Research*, Vol. 7, No.2, 2018, pp. 1-17.
- [13] N. Kobayashi, A. Nakamoto, M. Kawase, F. Sussan, M. Ioki, S. Shirasaka, “Managing a monolithic system or a System-of-Systems? An assurance case approach to reach intra-organizational consensus”, *proceedings 2018 7th International Congress on Advanced*

- Applied Informatics (IIAI-AAI 2018), 2018, pp. 688-693.
- [14] N. Kobayashi, A. Nakamoto, S. Shirasaka, “Proposal of an Assurance Case Description Method Considering External Environment of Systems: Application to Operation of an Ice-Skating Rink”, *Review of Integrative Business and Economics Research*, Vol. 8(3), 2018, pp. 87-95.
- [15] N. Kobayashi, A. Nakamoto and S. Shirasaka: “What is it to structuralize with multiple viewpoints by using Goal Structuring Notation (GSN)?”, *International Journal of Japan Association for Management Systems*, Vol. 10 No.1, 2018, pp. 125-130.
- [16] N. Kobayashi, A. Nakamoto and S. Shirasaka: “A Quantitative Evaluation Method for Evaluating the GSN Users’ Ability to Structuralize Systems with Multiple Viewpoints”, *International Journal of Japan Association for Management Systems*, Vol. 10 No.1, 2018, pp. 145-150.
- [17] N. Kobayashi, K. Tanaka, N. Yoshioka, A. Nakamoto, S. Shirasaka: Challenges of Assurance Case Description Method in Japan, *International Journal of Japan Association for Management Systems*, Vol.9, No.1, 2017, pp. 43-49.
- [18] S. Yamamoto, Y. Matsuno, “A Consideration on Developing Dependability Case”, *IE-ICE Technical Report; KBSE2012-22*, Vol.112, No.165, 2012, pp. 61-66.
- [19] N. Kobayashi, A. Nakamoto, M. Kawase, S. Shirasaka: Comparison of Two Quantitative Evaluation Methods for Assurance Cases, *International Journal of Japan Association for Management Systems*, Vol. 8 No.1, 2016, pp. 27-34.