IJAIT (International Journal
of Applied Information Technology)

http://journals.telkomuniversity.ac.id/ijait/

Simplification of Workflow-oriented Security Assessment

Edri Yunizal [a, *], Aulia Arif Wardana [b], Abdurrahman Niarman [a]

[a] *Dept. of Information Systems, Mahmud Yunus Batusangkar State Islamic University, Indonesia*
[b] *Szkoła Doktorska Politechniki Wrocławskiej, Wrocław University of Science and Technology, Poland*
edriyunizal@uinmybatusangkar.ac.id, aulia.wardana@pwr.edu.pl, aabniarman@uinmybatusangkar.ac.id

ARTICLE INFO

Received October 23rd, 2023
Revised October 29th, 2023
Accepted January 12th, 2024
Available online February 27th, 2024

Keywords
Information security, risk assessment, asset dependency, workflow-oriented, simplification

ABSTRACT

One of the protection mechanisms for organizations to protect their data is through information security risk assessment. The main obstacle in this area is asset dependency. Previous research developments tended to produce models that were difficult to implement because they were only applied to small assets, in contrast to the complexity of implementation in the field. This form of problem solving is a workflow-oriented security assessment solution that provides security rationale from a holistic perspective. The weakness of complexity in workflow oriented then became the basis of this research. The proposed solution is a simplification by using combined nodes that enable a modular concept. The modular concept is then applied to a reliable model, a data flow diagram. The study output shows the contribution of offerings with assessment solutions that consider dependencies by simplifying asset complexity in workflows in a modular manner with data flow diagrams.

Acknowledgment

Researchers are very grateful for financial support from Mahmud Yunus Batusangkar State Islamic University.

* Corresponding author at:
Dept. of Information Systems, Mahmud Yunus Batusangkar State Islamic University
Jl. Sudirman No. 137 Lima Kaum Batusangkar
Indonesia
E-mail address: edriyunizal@uinmybatusangkar.ac.id

ORCID ID:
- First Author: 0000-0001-8632-5030
- Second Author: 0000-0003-2201-0464
- Third Author: 0000-0003-1660-5170

https://doi.org/10.25124/ijait.v7i02.6797
Paper_reg_number IJAIT000070206 2024

1. Introduction

Organizations rely on data as the foundational element for collecting information in the decision-making process, making it essential to implement data protection measures [1]. To establish effective data protection, organizations perform Information Security Risk Assessments (ISRAs). ISRA is an organizational strategy designed to identify vulnerabilities and threats, followed by the selection of appropriate countermeasures to mitigate potential risks [2]. This, in turn, underscores its vital role in ensuring the resilience of organizations [3], [4].

However, recent research indicates that ISRA still faces several challenges [5]–[7]. One significant obstacle is the prevalence of manual procedures [8], [9], with a primary weakness being the need to consider the interdependencies among assets in the assessment [2], [10], [11]. The failure of one asset within an organization can cascade and impact other assets, leading to broader system failures [11]. For instance, even if a website boasts robust security features, its security can be compromised if it resides on a server with inadequate security measures. In such cases, a comprehensive risk assessment for the website should also account for potential risks stemming from the server. Consequently, an assessment that factors in asset dependencies proves more effective than those that do not [12]. Unfortunately, asset dependency is only addressed by a limited number of ISRAs [13].

ISRA which considers asset dependencies, among others [11]: asset dependencies in business models [13]–[17], asset threat-scenario dependencies [18], [19], hierarchical asset dependencies [20], [21], and dependencies with cyclic considerations [22], [23]. Each of these solutions is difficult to implement, as testing each solution is only on a small set of assets. Meanwhile, in practice, the amount of assets can be very large. It requires a simpler approach.

A highly effective method for addressing complex issues is the incorporation of workflow-oriented security assessment [24]. This strategy combines in-depth data regarding the system and potential threats, facilitating a comprehensive approach to security concerns. Complexity is addressed by limiting assets to only those involved in the system workflow. Then, a combination of quantitative evidence is carried out to evaluate security. Unfortunately, this solution is still hampered by the complexity of the offering, limited assets presented, and the difference of assets in the organization in one workflow. The biggest obstacle is that these solutions do not consider asset dependencies. Risk assessment requires simple solutions to asset complexity and dependency [25]. This research aims to present an ISRA solution that considers simpler asset dependencies, using workflow-oriented security assessment [24] as a basis for development. The development opportunity is to utilize the concept of modular systems [12] and compound nodes [26], [27].

The remainder of this article follows this structure: Section 2 provides an overview of the research methodology, encompassing the research context, research design, the identification of security models, the utilization of assessment models, and an exploration of how the proposed method can streamline workflow-oriented processes. Moving to Section 3, the article delves into the outcomes of the proposed solution and engages in a comprehensive discussion of its findings, including comparisons with preceding solutions. Lastly, Section 4 serves as the conclusion of this study, encapsulating key findings and presenting recommendations for future research.

2. Research Methodology

2.1. Context of The Study

This research is an identification of the remaining problems of information security risk assessment methods that consider asset dependencies. Based on the previous description, it is concluded that the main problem is complexity, and the feature needed to overcome this problem is modularization. Thus, this research proposes a workflow-oriented development that can provide this feature.

The approach employed is centered around a process of workflow-oriented development, aligning with the context of the research at hand. A significant challenge in modeling asset dependencies lies in acquiring the necessary data for constructing the model [28]. In this regard, the proposed model case study also incorporates data from [24]. The case under examination pertains to the smart grid, a modern power distribution network characterized by extensive monitoring and control capabilities. The system in focus is the Advanced Metering Infrastructure (AMI), comprising multiple smart meters capable of recording household electricity consumption data, energy consumption storage, and the provision of dynamic pricing to influence consumer behavior. The architectural configuration is depicted in Figure 4 within [24]. Data transmitted to and from the meters is aggregated in the Data Concentrator Unit (DCU), which is installed in each household.

2.2. Research Design

Overall, the research design consisted of seven phases. First, a literature study to identify modelling in information security risk assessment. Second, identifying the use of assessment models. Third, analyze the use of assessment models. Fourth, analysis and extraction of basic knowledge from workflow-oriented solutions [24]. Fifth, identify and analyze workflow-oriented development. Sixth, solution development. Finally, presentation of results and discussion of proposed solutions.

2.3. Identification of Modeling in Security Assessment

A model is a simple form of mathematical description built based on existing knowledge and experience combined with data from the past [29]. Security assessments require models because they have the capability to: connect and enable risk discovery; enables integration and visibility; linking risk parameters to process, project and business parameters; and provide significant value to risk management [30]. Risk models make scientific connections, for example linking risks with project goals. Risk-matrix models can also provide goal motivation and set the context for analyzing risks.

There are two forms of modeling in assessment [31]: inductive and deductive. Inductive reasoning is based on individual cases to obtain general conclusions. Deductive reasoning is achieved by finding out what components contributed to failure. An example of deductive modeling is fault tree analysis. There are several model types: physical, analog, and symbolic. A physical model is a physical replica that can be operated, tested and assessed. Analog models are models that share similarities. Finally, the symbolic model is a more abstract model with symbolic representation.

2.4. Utilization of Assessment Models

A system is a collection of sub-systems that work with each other to achieve one goal. A system is a deterministic entity consisting of an interacting collection of discrete elements [31]. In order to map the risks of a system, the model created should be able to show the interactions of each sub-system. One way to show interaction is by mapping it into 3 layers: organizational, logical, and physical [28]. The organizational layer focuses on people and behavior within the organization. Organizational functions are then realized at the Logical layer. And the last layer is the physical layer which shows components that can interact physically.

Information security in an organization is not only determined by one incident, but also requires an organizational perspective, rules, and even infrastructure. So the use of assessment models in information security can be grouped into several types [32], [33]: (1) to build/verify system flow or business processes; (2) information security assessment based on organizational models; and (3) defining and adding security requirements to the organizational model.

2.5. Workflow-oriented Security Assessment

Workflow-oriented security assessment [24] is a security assessment method that aims to overcome complexity. Complexity can be reduced by ensuring that the assets that are taken into account are those that are involved in the workflow. The assessment framework is based on abstract descriptions of actors and interactions in the system. The description then becomes the basis for defining aspects of the system that must be considered based on activities and services. The solution offers automatic workflow preparation, manual preparation presents a scale that is not very good and can be responded to differently by each stakeholder. This approach offers a flexible solution for modeling cyber, physical, and human interactions but is also formal enough to enable automation and increase scalability [24].

The central concept within the workflow model outlined in reference [24] can be encapsulated as follows.

1. It is imperative to conduct security assessments throughout the design, implementation, and operational phases of a system's lifecycle.
2. Different system components necessitate various forms of security-related information or evidence.
3. The utilization of tools becomes essential to amalgamate this evidence into a comprehensive security evaluation of the system.

This methodology achieves a comprehensive perspective by employing workflows as the underlying framework to collect diverse information from the system undergoing assessment. This information encompasses specific details about the information system, empirical data derived from its components, and potential attack scenarios. Drawing from these distinct information sources, the framework constructs a computable argument graph, capturing significant interactions among various system elements and potential threats. Subsequently, the solution quantitatively assesses system attributes, such as Confidentiality, Integrity, and Availability (CIA), through the application of a Graph [24].

The research presents a case example involving 3 processes with 2 actors. Cases are part of a workflow, not the workflow as a whole. Case then automates a model with 60 nodes with 82 edges [24]. Case studies show that solutions do not yet meet the need to address complexity. This research still needs to be developed into a more readable form. This solution still uses aggregation with Boolean equations, of course this research also does not consider asset dependencies in its calculations. So, even though it is quite promising, there are several weaknesses in the workflow-oriented security assessment: complex and not considering asset dependencies.

2.6. Simplification of Workflow-oriented (SLOW)

Based on the introduction, several identifications can be produced to improve the development of workflow-oriented security assessments. Identification of needs includes, among other things, the model must: (1) be simple; (2) map the assets involved completely; and (3) supports asset dependencies. This research utilizes the concept of modular compound nodes [12], [26]-[27] to overcome complexity. The model is created with three levels, where the simulation results from the lowest level are used as input at the higher level. This model is still conceptual and is well worth developing.

This research uses an assessment stage in a structured form starting from the highest level to the lowest. The first stage is building a workflow from the system provided at the design stage. Then, after a system description has been obtained (such as network topology, user rights, etc.), this detailed form allows translating the workflow into a Data Flow Diagram. Simplification is achieved by applying compound nodes using Data Flow Diagrams (DFD). The basis for using DFD is: (1) DFD for risk analysis [34]; (2) extended development for threat modeling [35]; and (3) DFD for dependencies [36].

Since the attacker only needs one attempt to succeed, qualitative subjectivity is detrimental. Threat modeling involves understanding a complex system and identifying all possible threats whether or not they can be exploited. Identifying threats will help build realistic security requirements. Security requirements are then analyzed based on criticality and likelihood, and a decision is made whether the threat is mitigated or left alone. Identifying threats and selecting appropriate countermeasures reduces an attacker's ability to abuse the system.

The research uses a top-down approach where the process begins with a description of the workflow (can be in UML or BPMN form). The workflow description is then combined with a system description such as network topology or asset-specific configuration. These two documents are the basis for forming the DFD. The next step is adding details of the attack process, which involves the attack strategy and possible vulnerabilities that will be exploited in the DFD. The final step is testing the model with available evidence to produce quantitative assessment results.

The model consists of three basic components: input, process, and output. The input model requires a workflow description, system description, attacker model, and evidence. Meanwhile, the model process consists of creating DFD level 0, DFD next level, DFD with attacker, Entity fault tree, and calculation. Finally, the output consists of DFD, DFD with attacker, and quantitative results, see Figure 1.

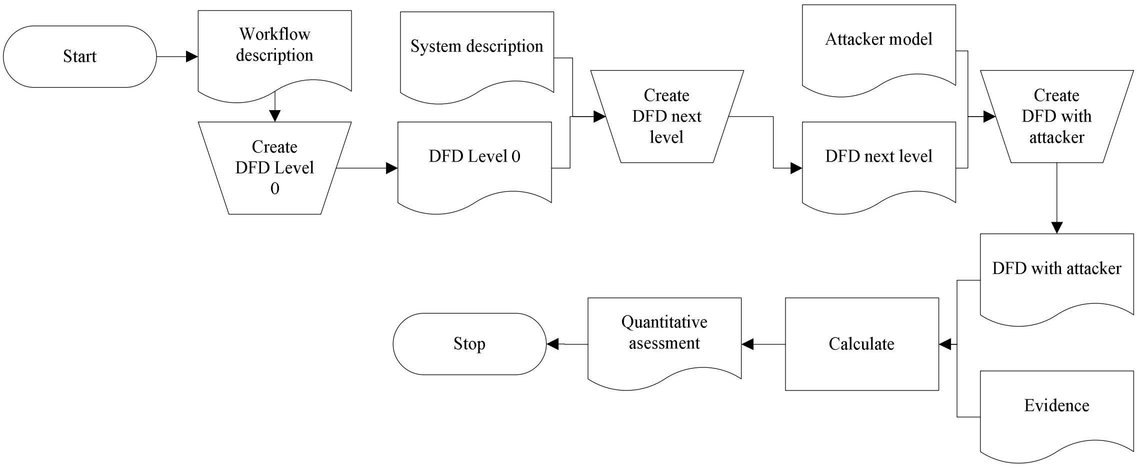


Figure 1 SLOW for Security Assessment

A simpler form allows the process identification process to be simpler. The identification and assessment pattern uses a hierarchical method as done by [21]. Identification is carried out from the highest process DFD to the lowest. Then, evidence is entered at the lowest level of the DFD so that the final value calculation is produced at the highest level of the DFD.

Initial development was carried out by assembling an assessment tool for creating a DFD. Development is carried out in Python 3.7 using Spyder 3.3.6 IDE. The database uses MySQL 5.0.51b-community-nt-log on Windows 8 64 bit with a Core™ i7-4702MQ processor and 16GB memory. The prototype requires four entities: project, DFD, process and entity (Figure 2). The project entity is used to accommodate project analysis information carried out with the project_id and project_name attributes while DFD entity is used to store a list of DFDs involved in each project. The process entity stores the processes required for each DFD. Finally, the entity is used to store the entity and the value of the goal of each entity involved in the process.

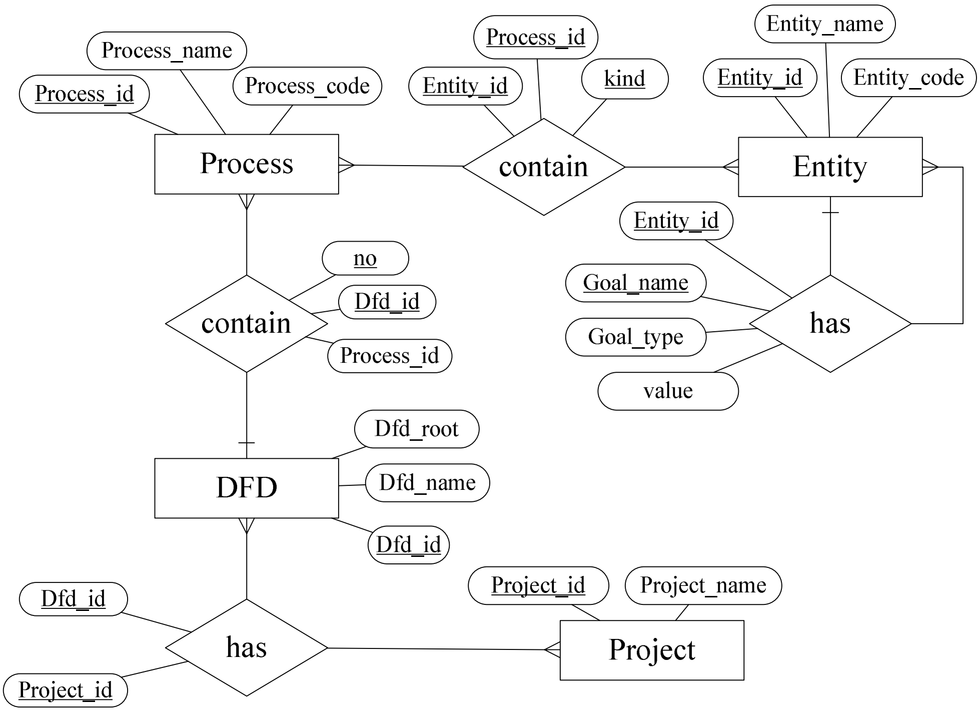


Figure 2 SLOW Entity Relationship Diagram

3. Result and Discussion

3.1. Result

As stated previously, this research is a workflow-oriented development. Therefore, no data collection was carried out. However, using previous research data as a comparison. In this case, SLOW is used to execute smart grid data [24]. The data produces evidence with fault trees as in Figure 3.

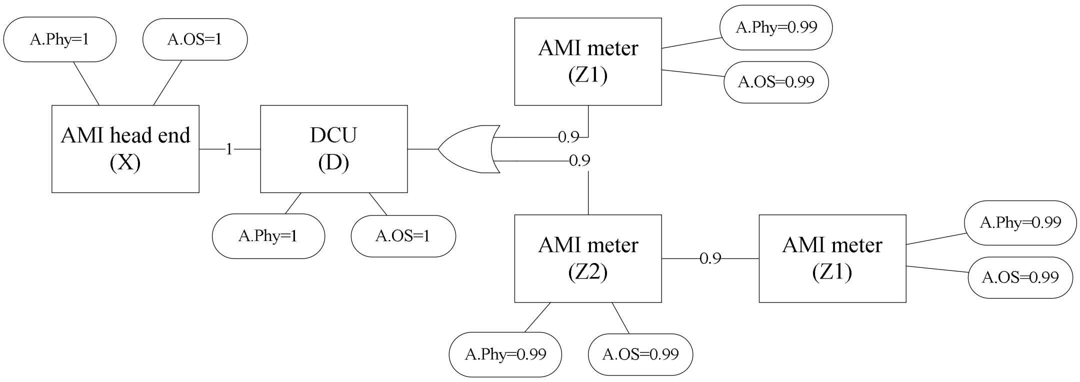


Figure 3 Entity Fault Tree

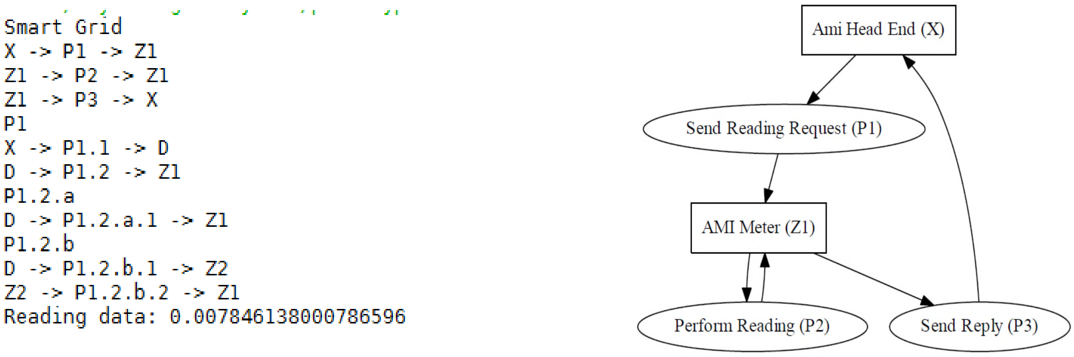
Figure 4 part (A) shows how the SLOW prototype performs readings involving 24 nodes and 16 edges from available evidence. All data can be read in 0.078 seconds. Next, the researcher visualized the DFD with Graphfiz 2.38, presenting DFD level 0 as in Figure 4 part (B).

Equation 1 where P (A) is prior probability of A, whereas P (A|B) is posterior probability of A given B. Its applies for two variables A and B which are mutually independent [37], Equation 1 then supports Equation 2, so it can be used as Equation 3.

$$P(A|B) = P(A) \qquad \text{Equation 1}$$

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{P(A|B)P(B)}{P(A)} = \frac{P(A)P(B)}{P(A)} = P(B) \qquad \text{Equation 2}$$

$$P(A \cap B) = P(A|B).P(B) = P(A).P(B) \qquad \text{Equation 3}$$



```
Smart Grid
X -> P1 -> Z1
Z1 -> P2 -> Z1
Z1 -> P3 -> X
P1
X -> P1.1 -> D
D -> P1.2 -> Z1
P1.2.a
D -> P1.2.a.1 -> Z1
P1.2.b
D -> P1.2.b.1 -> Z2
Z2 -> P1.2.b.2 -> Z1
Reading data: 0.007846138000786596
```

(A) (B)

Figure 4 Console Result and DFD Level 0 Visualization

Based on Equation 3 and Figure 3, we get Equation 4, so that the value obtained is 0.9801, when sliced with Link Z1 and Z2 0.9 to make 0.88209. Because in the

DCU there are two independent events, in accordance with the addition rule for two arbitrary events [38], see Equation 5, the value obtained is 1.66017277-0.686339029=0.973833741.

$$P(Z1) = P(A.Phy) \cap P(A.OS) \quad \text{Equation 4}$$

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) \quad \text{Equation 5}$$

Comparison results with a workflow-oriented, attacker-free workflow-oriented provided in [24], where there are 5 workflow stages. Here it can be seen that the value of the DCU is involved twice, in the second and fourth processes, in the DCU processing it also actually involves Z1 (3rd process), but it is still taken into account. This results in a low value for the overall workflow even without any attacks at all ($1 \cap 0.97 \cap 0.9801 \cap 0.97 \cap 1 = 0.92217609$). The difference with the value of the bid solution also shows the influence of the dependencies of the assets involved.

3.2. Discussion

Utilizing SLOW includes four stages: workflow description, system description, attacker model, and DFD formation. First, in the workflow description, [24] limits the case to the workflow on the AMI component, here the company's AMI Head end initiates on-demand reading on the AMI Meter at the consumer's location. On-demand reading begins with sending a reading request from the AMI head end. After the reading request is received by the AMI meter, the AMI meter then takes a reading and produces a reading result. Reading results are then sent back to the AMI head end.

Second, the system description. The workflow description is indeed simple, but the implementation is different. In order to get a clear picture, you must be guided by the system description such as the network topology in Figure 5. The process of sending reading requests (call M1) from the AMI head end (call X) not directly to the AMI Meter (call Z1), but via DCU (Y). The reading request received by Y is then sent to Z1 in 2 ways: direct link and indirect path via another AMI meter (called Z2). After the reading request is received by Z1, Z1 performs the reading and produces a reading result (called M2). M2 is then sent back according to how it was received, whether directly to Y or via Z2.

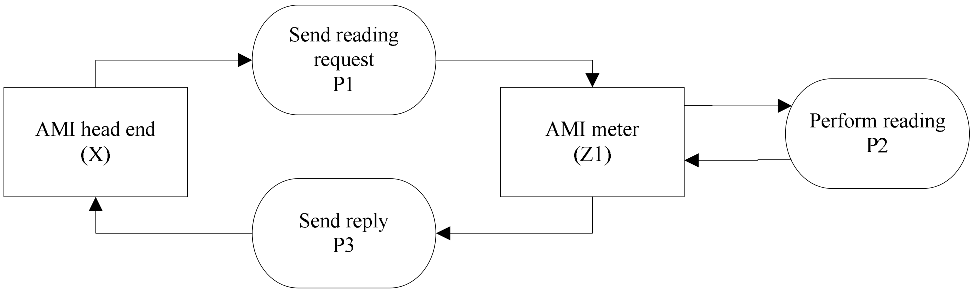


Figure 5 Smart Meter On-Demand Reading Workflow [24] Modified using DFD Level 0

Third, the attacker model, the stage of providing possible attacks that will appear in the workflow being prepared for local exploit. Possible threats/vulnerabilities can be done by breaking down the process into entities and the relationships between the entities involved. There are several forms of process depending on the entity relationship. [24] give an example that an attacker can enter a company location and use a local exploit or remote exploit of the operating system of X. This action will affect the confidentiality and availability of X. The attacker can also physically damage X which affects the availability of X.

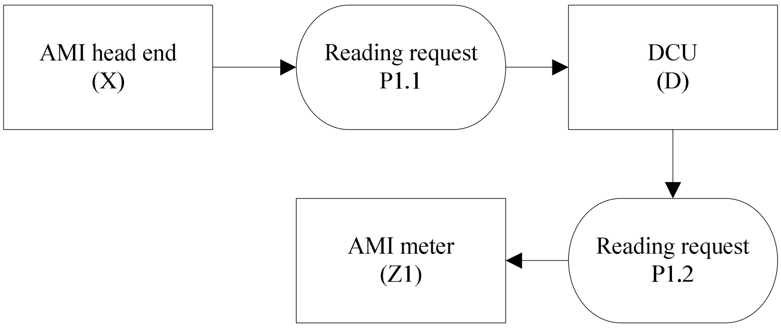


Figure 6 DFD Level 1: P1 Process Details

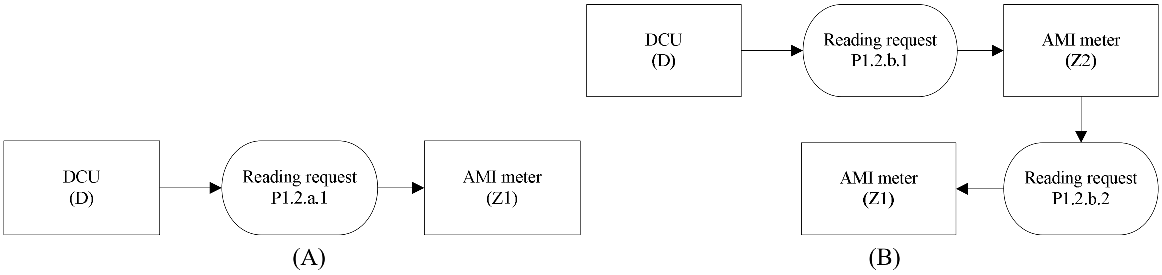


Figure 7 DFD Level 2: Process Details

Finally, the formation of DFD level 0 and DFD next level. First, DFD level 0. Based on the description of the workflow, DFD level 0 is then created (see Figure 5). There are two entities involved in the processes involved. Based on the workflow description and system description, the DFD creation process is carried out. DFD consists of several levels, DFD level 1 (Figure 6) is used to map the workflow description and then detailing it using Figure 7 with part A for P1.2.a and part B for P1.2.b.

4. Conclusions and Future Work

Organizations' needs to secure data should be resolved with ISRA. Unfortunately, ISRA is still hampered by asset dependencies. The range of solutions offered for asset dependencies is still hampered by complexity. Conditions that present solutions that are not readily applicable to the real number of assets in the field. This research proposes the development of workflow-oriented security assessment with SLOW. Workflow-oriented does not yet support asset dependencies, and also still has problems with the complexity of assets in the workflow. Development was carried out by utilizing the modular compound node concept, utilizing a model that is also very familiar in system development: DFD. The trial results of the proposed method were able to show development both in terms of complexity and calculation results that considered dependencies.

The form of the offered solution can already show the advantages of workflow oriented. It needs development by utilizing direct data in the form of case studies on an organization. Development should be able to utilize organizational information systems to help form data-driven solutions.

Bibliography

[1] R. Stair and G. Reynolds, *Principles of information systems*. Cengage Learning, 2020.

[2] A. Shameli-Sendi, R. Aghababaei-Barzegar, and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)," *Comput. Secur.*, vol. 57, pp. 14–30, 2016, doi: 10.1016/j.cose.2015.11.001.

[3] D. Landoll, *The security risk assessment handbook: A complete guide for performing security risk assessments*. CRC Press, 2011.

[4] T. R. Peltier, *Information security fundamentals*. CRC press, 2013.

[5] S. Andersson, "Problems in information classification: insights from practice," *Inf. Comput. Secur.*, vol. ahead-of-print, no. ahead-of-print, Jan. 2023, doi: 10.1108/ICS-10-2022-0163.

[6] A. TamjidYamcholo and A. Toloie Eshlaghy, "Subjectivity reduction of qualitative approach in information security risk analysis," *J. Syst. Manag.*, vol. 8, no. 1, pp. 145–166, 2022.

[7] L. A. Alexei, "Design & development of a cyber security conceptual framework for higher education institutions in the Republic of Moldova," *Sci. Pract. Cyber Secur. J. SPCSJ*, no. 1, pp. 35–52, 2022.

[8] M. Sterbak, P. Segec, and J. Jurc, "Automation of risk management processes," in *2021 19th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, IEEE, 2021, pp. 381–386.

[9] E. Yunizal, K. Surendro, and J. Santoso, "Asset identification in information security risk assessment using process mining," *Int. J. Adv. Sci. Eng. Inf. Technoloy*, vol. 12, no. 4, 2022.

[10] I. Kotenko, E. Doynikova, A. Fedorchenko, and V. Desnitsky, "Automation of asset inventory for cyber security: investigation of event correlation-based technique," *Electronics*, vol. 11, no. 15, p. 2368, 2022.

[11] E. Yunizal, J. Santoso, and K. Surendro, "Simple and multi risk assessment framework for information security using process flow diagram," *Sainstek J. Sains Dan Teknol.*, vol. 15, no. 1, pp. 20–35, 2023.

[12] Y. Y. Haimes, "Risk modeling of interdependent complex systems of systems: Theory and practice," *Risk Anal.*, vol. 38, no. 1, pp. 84–98, 2018, doi: 10.1111/risa.12804.

[13] T. Alpcan and N. Bambos, "Modeling dependencies in security risk management," in *Post-Proceedings of the 4th International Conference on Risks and Security of Internet and Systems, CRiSIS 2009*, 2009, pp. 113–116. doi: 10.1109/CRISIS.2009.5411969.

[14] K. Khanmohammadi and S. H. Houmb, "Business process-based information security risk assessment," in *2010 Fourth international conference on network and system security*, IEEE, 2010, pp. 199–206. doi: 10.1109/NSS.2010.37.

[15] I. Loloei, H. R. Shahriari, and A. Sadeghi, "A model for asset valuation in security risk analysis regarding assets dependencies," in *ICEE 2012 - 20th Iranian Conference on Electrical Engineering*, IEEE, 2012, pp. 763–768. doi: 10.1109/IranianCEE.2012.6292456.

[16] S. Schmidt and S. Albayrak, "A quantitative framework for dependency-aware organizational IT Risk Management," in *2010 10th International Conference on Intelligent Systems Design and Applications*, IEEE, 2010, pp. 1207–1212. doi: 10.1109/ISDA.2010.5687022.

[17] B. Suh and I. Han, "The IS risk analysis based on a business model," *Inf. Manage.*, vol. 41, no. 2, pp. 149–158, 2003, doi: 10.1016/S0378-7206(03)00044-2.

[18] B. Rahmad, S. H. Supangkat, J. Sembiring, and K. Surendro, "Threat scenario dependency-based model of information security risk analysis," *IJCSNS*, vol. 10, no. 8, p. 93, 2010.

[19] B. Rahmad, S. H. Supangkat, J. Sembiring, and K. Surendro, "Modeling asset dependency for security risk analysis using threat-scenario dependency," *Int. J. Comput. Sci. Inf. Secur.*, vol. 10, no. 4, p. 103, 2012.

[20] J. Breier, "Asset valuation method for dependent entities," *J. Internet Serv. Inf. Secur.*, vol. 4, no. 3, 2014.

[21] Ü. Tatar and B. Karabacak, "An hierarchical asset valuation method for information security risk analysis," in *International Conference on Information Society (i-Society 2012)*, IEEE, 2012, pp. 286–291. [Online]. Available: https://fuse.franklin.edu/facstaff-pub

[22] S. Muller, C. Harpes, Y. Le Traon, S. Gombault, J.-M. Bonnin, and P. Hoffmann, "Dynamic risk analyses and dependency-aware root cause model for critical infrastructures," in *International Conference on Critical Information Infrastructures Security*, Springer, 2016, pp. 163–175.

[23] S. Muller, C. Harpes, Y. Le Traon, S. Gombault, and J.-M. Bonnin, "Efficiently computing the likelihoods of cyclically interdependent risk scenarios," *Comput. Secur.*, vol. 64, pp. 59–68, 2017, doi: 10.1016/j.cose.2016.09.008.

[24] B. Chen *et al.*, “Go with the flow: Toward workflow-oriented security assessment,” in *Proceedings of the 2013 New Security Paradigms Workshop*, 2013, pp. 65–76.

[25] E. Yunizal, K. Surendro, and J. Santoso, “A Method of Simplifying the Asset Dependency Cycle in Security Risk Analysis,” in *The 5th International Conference on Information Technology and Digital Applications (ICITDA 2020)*, Yogyakarta: IOP Publishing Ltd, Nov. 2020. doi: 10.1088/1757-899x/1077/1/012002.

[26] A. M. Omer and A. Schill, “Automatic management of cyclic dependency among web services,” in *2011 14th IEEE International Conference on Computational Science and Engineering*, IEEE, 2011, pp. 44–51.

[27] K. Surendro and C. Martini, “Hierarchical i* modeling in requirement engineering,” *Telkomnika*, vol. 14, no. 2, p. 784, 2016, doi: 10.12928/telkomnika.v14i3.3333.

[28] K. Andersson, *Mapping out dependencies in network components in critical infrastructure*. 2018.

[29] S. A. Klugman, H. H. Panjer, and G. E. Willmot, *Loss models: from data to decisions*, vol. 715. John Wiley & Sons, 2012.

[30] C. R. Pandian, *Applied software risk management: A guide for software project managers*. Auerbach Publications, 2006.

[31] W. E. Vesely, F. F. Goldberg, N. H. Roberts, and D. F. Haasl, “Fault tree handbook,” Nuclear Regulatory Commission Washington DC, NUREG-0492, 1981.

[32] P. Johnson, R. Lagerström, and M. Ekstedt, “A meta language for threat modeling and attack simulations,” in *Proceedings of the 13th International Conference on Availability, Reliability and Security*, ACM, 2018, p. 38.

[33] S. Taubenberger and J. Jürjens, “IT security risk Analysis based on business process models enhanced with security requirements.,” in *MODSEC@ MoDELS*, 2008.

[34] L. Sion, K. Yskout, D. Van Landuyt, and W. Joosen, “Solution-aware data flow diagrams for security threat modeling,” in *Proceedings of the 33rd Annual ACM Symposium on Applied Computing*, 2018, pp. 1425–1432. doi: 10.1145/3167132.3167285.

[35] B. J. Berger, K. Sohr, and R. Koschke, “Automatically extracting threats from extended data flow diagrams,” in *International Symposium on Engineering Secure Software and Systems*, Springer, 2016, pp. 56–71.

[36] N. Olayan, V. Patu, Y. Matsuno, and S. Yamamoto, “A dependability assurance method based on Data Flow Diagram (DFD),” in *2013 European Modelling Symposium*, IEEE, 2013, pp. 113–118. doi: 10.1109/EMS.2013.20.

[37] T. D. Nielsen and F. V. Jensen, *Bayesian networks and decision graphs*. Springer Science & Business Media, 2009.

[38] R. E. Walpole and R. H. Myers, *Ilmu Peluang dan Statistika untuk Insinyur dan Ilmuwan.* Instirut Teknologi Bandung, 1995.