HASIL CEK_Development of conceptual framework for cyber fraud investigation

by Imam Riad Hidayati, Ramadhani, Al Amany

Submission date: 23-Apr-2022 11:00AM (UTC+0700)
Submission ID: 1817894435
File name: opment_of_conceptual_framework_for_cyber_fraud_investigation.pdf (645.35K)
Word count: 5974
Character count: 32924

7 (2) July 2021 125-135 ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
Register: *Jurnal Ilmiah Teknologi Sistem Informasi*

Contents lists available at www.journal.unipdu.ac.id

Register

Journal Page is available to www.journal.unipdu.ac.id/index.php/register

Research article

Development of conceptual framework for cyber fraud investigation

Anisa Nur Hidayati [a,*], *Imam Riadi* [b], *Erika Ramadhani* [c], *Sarah Ulfah Al Amany* [d]

[a,c] *Department of Informatics, Universitas Islam Indonesia, Yogyakarta, Indonesia*
[b] *Department of Information Systems, Universitas Ahmad Dahlan, Yogyakarta, Indonesia*
[d] *School of International Trade and Economics, Jiangxi University of Finance and Economics, Nanchang, China*
email: [a,*] 18917106@students.uii.ac.id, [b] imam.riadi@is.uad.ac.id, [c] erika@uii.ac.id, [d] sarahulfah13@gmail.com
* *Correspondence*

ARTICLE INFO

Article history:
Received 25 January 2021
Revised 26 March 2021
Accepted 14 April 2021
Available online 28 April 2021

Keywords:
cybercrime
detection
framework
fraud
Jabareen

Please cite this article in IEEE style as:
A. N. Hidayati, I. Riadi, E. Ramadhani and S. U. Al Amany, "Development of conceptual framework for cyber fraud investigation," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 7, no. 2, pp. 125-135, 2021.

ABSTRACT

The increase in the number of internet users in Indonesia as much as 175.4 million as recorded in the Datareportal.com report and 4.83 billion globally, impact the increase in the number of cyber fraud cases. Data states that 96% of fraud cases are not resolved due to fraud methods carried out online and make it difficult for legal officers to obtain evidence. Previous fraud investigation research mainly focused on fraud detection, so this research focuses on submitting a framework for investigating cyber fraud cases. The cyber fraud case requires a new framework for investigation because in this fraud case, there is digital evidence that is very prone to be damaged, lost, or modified, which makes this case unsolved. This research aims to develop a framework that is expected to help auditors to uncover cases of cyber fraud so that resolved cyber fraud cases can increase. The method used in making this framework uses Jabareen's conceptual framework development method, which consists of 6 stages, namely, Mapping the selected data source, extensive reading and categorizing of the chosen data, Identifying and naming objects, Deconstructing and categorizing the concept, Integrating concept, Synthesis, resynthesis. And make it all sense. The framework for cyber fraud investigation uses 22 digital forensic frameworks and eight frameworks for fraud audit investigations. The results of developing a framework using the Jabareen method resulted in 8 stages, integrating various concepts selected from digital forensics and fraud audits. Evaluation of framework development was carried out by giving limited questionnaires to practitioners and academics, which produced 89% for the feasibility value and needs of the framework and 67% there is no need for changes to the framework being developed.

1. Introduction

The issue of cyber fraud is increasing with reports of the multinational company KPMG engaged in financial audits in 2019. 4 types of fraud have increased in number from year to year, namely Card Not Present, Social Engineering, Scams, and Cyber/Online Fraud in 3 parts of the world Asia Pacific, America, Europe, and the Middle East [1]. Cyber Fraud or can be called online fraud, or computer fraud is the fraud that uses digital devices in their crimes. The guide issued by Microsoft explains the various types of online fraud committed by criminals using the internet, such as phishing scams, rogue security software, fake technical support, fraudulent contest and winning, and financial scams [2]. IC3 published a report which states that the media or tools used for this crime use social media or digital currency [3].

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 125-135

According to Accenture, although various financial institutions and businesses are trying to adopt the latest strategies to make digital payments safer from fraud, criminals are increasingly innovative in stealing sensitive personal data with the help of digital platforms [4].

A report from the Federal Trade Commission or FTC in America states that in 2019 the most reported crime cases were the highest reported fraud crimes. The type of fraud most reported was the imposter scam which caused losses of up to 152 million USD, followed by Identity Theft and crimes. Others [5]. In 2020 since the Covid-19 pandemic, the FTC received many complaints about fraud which caused a loss of 44.56 million USD in the first half of 2020. In the news published in the UK, it was stated that more than 96% of fraud cases were not resolved even though they were reported. On the side of the authorities. The main cause of difficulty in disclosing fraud cases is that most of the perpetrators are anonymous, or most crimes occur online. Even The Office for National Statistics (ONS) states that 63% of fraud cases occur online where there is no contact between the perpetrator and the victim [6]. In a survey report conducted by ACFE in 2016, as many as 77% of cases of losses due to fraud in Indonesia were dominated by corruption cases, with the second position being a misuse of state and company assets/assets at 19% while the last place in the form of 4% was occupied by fraudulent financial statements [7].

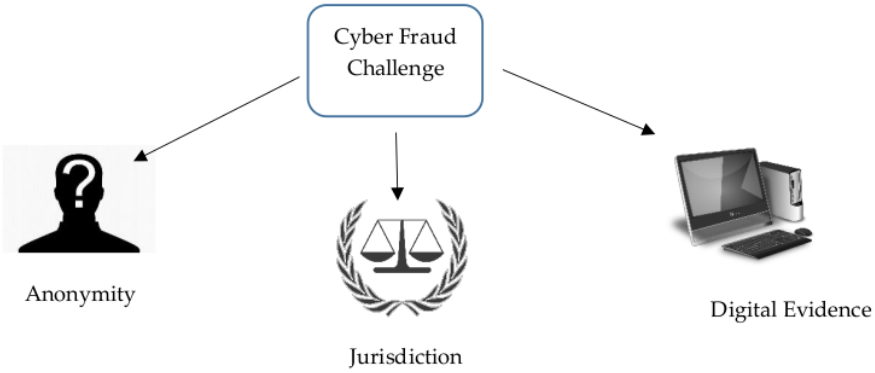

Fig. 1. Cyber fraud challenge [8]

Three things support the increase in cyber fraud cases as illustrated in Fig. 1, namely the first is the anonymity factor where criminals can commit crimes anonymously where when the agency realizes that when they become victims of fraud, it is too late for the authorities to identify who is responsible in charge of this case. Although anonymity is a form of freedom of speech, this also does not guarantee that users will not abuse this right [9]. Jurisdiction is the following-reason why there are more and more cyber fraud crimes. This is because crimes committed in cyberspace will make it difficult for legal officers to choose the jurisdiction where the legal process will be processed. This character is also called borderless, and one of the things that make law enforcement about constraints is the lack of jurisdictional cooperation between countries such as countries in Southeast Asia, South America, and Africa [10]. The last reason is the difficulty in finding evidence that law enforcers must seek [8].

The use of digital devices in cases of fraud requires a particular stage to investigate because the evidence, in this case, is a digital document/information whose characteristics are very different from physical evidence. Digital evidence has several factors, namely very easy to erase and modify, sensitive to time, cross-jurisdiction, and hidden [11]. Digital evidence has a wider range, contains sensitive personal data, can be carried easily, and requires more sophisticated training and tools for data acquisition than handling physical evidence [12] so that these characteristics require experts because if those who handle this case are less trained personnel, it can cause damage to evidence [13] and the cyber fraud case is not resolved.

Efforts that can help solve cyber fraud cases are using an investigative framework that supports the characteristics of digital evidence, where case resolution still uses conventional methods. In contrast, previous research on fraud still focuses on fraud detection methods and has not discussed investigating cyber fraud cases. This study aims to develop a cyber fraud investigation framework due to the high number of unresolved fraud cases due to the use of digital devices in this crime and the challenges of

http://doi.org/10.26594/register.v7i2.2263

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 125-135

investigating cyber fraud as described in Fig. 1. The development of a cyber fraud investigation framework can help investigators and audits to resolve cases so that the percentage of cyber fraud cases resolution is getting higher. The framework development method in this study uses the conceptual framework development method from Jabareen, which supports the development of a cross-disciplinary framework, namely digital forensics and audit fraud. This paper will be divided into 5 parts: introduction, state of the art, research methods, results and discussion, and conclusions. The introduction contains the reality of many cyber fraud cases that have not been resolved due to the existence of a component of digital evidence that requires special handling. Previous research discussed several previous studies regarding digital forensic investigations and fraud investigations where there was no joint research framework for handling fraud cases using digital devices. The research method contains the stages of the methods used in the development of a cyber fraud framework, namely using Jabareen's conceptual framework development method and instruments for framework evaluation. Results and discussion contain the process of developing the framework and how the results of the framework evaluation using a questionnaire. The conclusion discusses the results of the framework development and evaluation, and expectations for further research.

2. Related Work

Previous research on fraud in fraud detection methods using Artificial Intelligence and Machine Learning [14] so that fraud detection can be done faster than conventional methods. The collaboration of computer forensics in forensic accounting applications is considered to help the fraud detection process more quickly [15] due to the increasingly complex types of fraud using digital tools. Other studies mention the need for more specific laws regarding computer-related fraud and restitutive steps to prevent internet-based fraud crimes in Indonesia [16].

In other research, the development of a digital forensic framework is increasingly diverse based on the development of digital devices such as the preparation of a framework for investigating the Smart Home Environment [17], A proposed framework for eGovernment in African countries, namely Uganda [18], a framework for IoT investigations [19], Making of an acquisition model IoT devices [20], the development of mobile device investigation frameworks such as Android [21] and the IaaS Cloud Computing platform [22]. Methods in developing an investigative framework or model from previous research can be categorized into several methods, as shown in Table 1.

Table 1. Framework development methods

No	Research	Development Methods
1	A Forensic Investigation Framework for Smart Home Environment	Based on the challenges on the device
2	A Proposed Digital Forensic Investigation Framework for an eGovernment Structure for Uganda	Modify the previous framework or model
3	IoT Forensic A digital investigation framework for IoT systems	Based on the challenges on the device
4	An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I: A Theoretical Framework	Using the theoretical framework method for its development
5	Proposed Workable Process Flow with Analysis Framework for Android Forensics in Cyber-Crime Investigation	Framework development is based on existing models and is tailored to the needs of the device
6	Proposed Network Forensic Framework for Analyzing IaaS Cloud Computing Environment	The development framework is based on an existing model and adapted to the needs of the environment

Table 1 is identified in the development of a framework that can be done by looking at the challenges that exist on the issue or developing it based on an existing investigative model or a combination of both. This study uses the same concept in developing an investigative framework, namely, looking at the challenges in cyber fraud cases and existing digital forensic investigation models.

3. Method

This research will develop a conceptual framework for cyber fraud investigation, where the conceptual framework is a model compiled by researchers to explain the relationships that exist in variables in research or it can be an adaptation of an existing model which is then adapted according to the objectives of the study [23]. The conceptual framework is different from the theoretical framework, where the conceptual framework is more specifically focused on the object under investigation. Making a

http://doi.org/10.26594/register.v7i2.2263

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 125-135

conceptual framework will be made according to research needs. Researchers who better understand what is needed in making the framework so that in this study will use the conceptual framework development method based on research by Jabareen [24]. The main reason for choosing to use Jabareen's development method is because the conceptual framework accommodates the creation of a cross-disciplinary framework as this research is multidisciplinary [25], namely in the field of Fraud Audit and Digital Forensics. Meanwhile, some other investigative framework development methods have not yet accommodated cross-disciplinary frameworks. In making this framework, there are 8 phases as mentioned by Jabareen as depicted in Fig. 2.

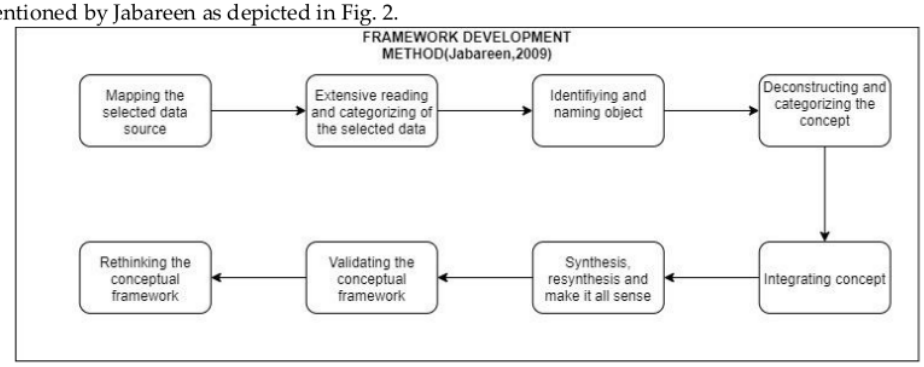

Fig. 2. Framework development methods

In this study, the development of the framework will be modified into only 6 stages, as shown in Fig. 3. The stages of Validating the Conceptual Framework and Rethinking the Conceptual Framework are stages that are expected to be further investigated by other researchers/academics because at the Validating the Conceptual stage. The framework will be better when presented at a conference to gets feedback from the participants as a form of framework improvement in the future [26].

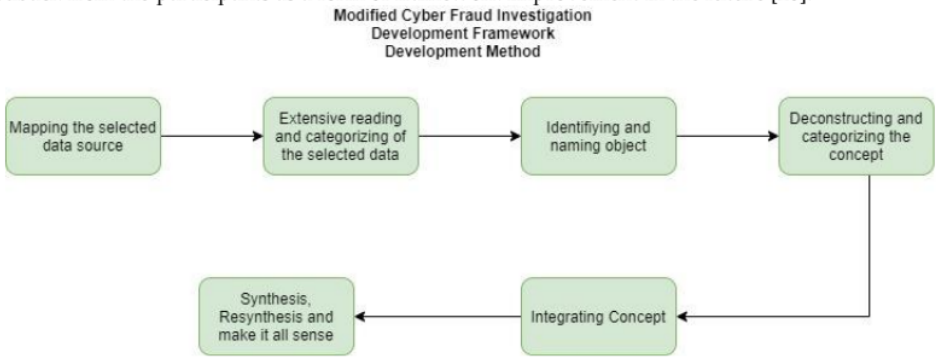

Fig. 3. Modification of framework development methods

The evaluation of the development of this framework uses the Delphi survey method, where this method is a survey conducted on an expert. This method can also be used to gather opinions about identifying constraints on the problem to be studied [27]. There are two types of Delphi method applications, namely for forecasting and problem identification, and for testing the concept/framework development [28]. This study uses the second type of Delphi method instrument for testing framework development because the purpose of this study is to develop a framework.

The questionnaire regarding the development of the framework will use a research instrument developed by Bacon [29] with a slight change consisting of 5 questions with three answer indicators, as shown in Table 2. Changes were made to this questionnaire because one point was not suitable for use in the framework being developed.

The questionnaire as shown in Table 2 will then be submitted to digital forensic practitioners and fraud auditor practitioners and academics who will then analyze the results of the questionnaire. The results of this questionnaire can be used as an evaluation framework development and become material for improvement in further research. The selection of respondents was limited to evaluating framework development because the evaluation stage was carried out as an effort to validate the framework.

http://doi.org/10.26594/register.v7i2.2263

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 125-135

Table 2. Delphi method questionnaire table

No	Question (Cluster I: Needs and Feasibility of Framework Development)	Answer		
		Yes	No	Maybe
1	Is the framework being developed needed in the field?			
2	Is the framework being developed suitable for use in the field?			
3	Are the concepts/stages presented suitable in the field of Cyber Fraud?			
No	**Questions (Cluster II: Changes needed to the framework being developed)**	**Answer**		
		Yes	**Minor Change**	**Major Change**
4	Is the provision of concepts/stages in the framework acceptable (yes), or what changes are needed?			
5	Are the differences in concepts/stages acceptable (yes), or are changes needed?			

4. Results and Discussion

This section will discuss the stages of developing a cyber fraud framework using the Jabareen method, which has been modified and adapted to this research which consists of six phases, namely Mapping the selected data source, extensive reading and categorizing of the chosen data, Identifying and naming objects, Deconstructing. and classifying the concept, Integrating concept, Synthesis, resynthesis and make it all sense. The implementation of each of the above stages will be described in the discussion below.

4.1. Mapping selected data

The first stage is mapping selected data. The data to be taken here is data from books and research journals. Data were taken from two disciplines, namely Fraud Audit and Digital Forensics, especially regarding the framework and stages in the investigation process. To search for data using the help of Google's search engine to help map data, where journals are taken from ScienceDirect, Emerald, ResearchGate, SagePublishing. Data were collected using the keyword "digital forensic framework, audit fraud, framework development". Search results obtained 128 data with 53 data regarding Digital Forensics, 31 data regarding Forensic Audit and 44 other data regarding framework development methods.

4.2. Extensive reading and categorizing of the selected data

The second stage is extensive reading and categorizing of the selected data. At this stage, the material is deepened on various data in the first stage, which is then categorized according to the existing scientific disciplines. At this stage, the data will be classified according to current fields of science, namely, Fraud Audit, Digital Forensics, and additional stages of making a framework. Of the 53 data regarding digital forensics, 22 were selected regarding the digital forensic framework, and from 31 data on fraud audits, 8 were selected regarding fraud investigations. The selection of this data is based on the closest suitability to the purpose of this study, namely for the development of a framework and examples of the previously developed digital forensic investigation and fraud audit framework.

4.3. Identifying and naming concept

In the third stage, namely identifying and naming concepts, the previously extracted data will be broken down into concepts related to the field of study to be studied. Between several data will allow the same concept, and later it will be seen the similarity of concepts from some existing data. The data that will be broken down into concepts is data obtained from the digital forensic framework and the stages of the fraud audit investigation. The concepts that have been obtained in this process can be seen in Table 3 and Table 4.

The digital forensics concept is obtained from 22 digital forensic investigation frameworks where if the concept between frameworks has the same name, only one concept will be taken. From these 22 frameworks, 55 concepts are obtained from the digital forensic investigation process stages as shown in Table 3.

The concept identification of the Fraud Audit uses 8 fraud investigations that have been obtained in the previous process which are then broken down and got 20 concepts from the fraud audit which

http://doi.org/10.26594/register.v7i2.2263

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 125-135

are shown in Table 4 where several concepts have the same meaning even though given the names mentioned in Table 4 are the stages of the case investigation process fraud.

Table 3. Concepts of digital forensics

No	Concept Name	No	Concept Name
1	Recognize	29	Internet
2	Identify	30	Case-Specific
3	Individualise	31	Interaction
4	Reconstruct	32	Preparation
5	Acquire	33	Image Processing
6	Authenticate	34	Output
7	Analyze	35	Detection
8	Collect	36	Capturing
9	Examine	37	Extraction
10	Report	38	Proactive
11	Preservation	39	IoT Forensic
12	Classification	40	Reactive
13	Readiness	41	Searching
14	Deployment	42	Understanding
15	Traceback	43	Checking Security Level
16	Dynamite	44	Incident
17	Review	45	Incident Response
18	Initialization	46	Digital Forensic Investigation
19	Investigative	47	Documentation
20	Presentation	48	Evidence
21	Decision	49	Organization
22	Incident Detection	50	Egov Forensic
23	First Response	51	Concurrent
24	Storage	52	Front End
25	Planning	53	Middle Layer
26	Triage	54	Back End
27	User Usage Profile	55	Incident Closure
28	Chronology Timeline		

Table 5. Categorization of concepts according to discipline

Concept	Disciplines	Nature of Concept
Detection	Fraud Audit	Ontological
Planning		Ontological
Collection		Ontological
Investigation		Ontological
Report		Ontological
Readiness	Digital Forensics	Epistemological
Identification		Ontological
Collection		Ontological
Analyze		Ontological
Report		Ontological
Concurrent		Methodological
Incident Closure		Ontological
Incident Response		Ontological

4.4. Deconstructing and categorizing the concept

In the fourth stage, namely deconstructing and categorizing the concept, the existing concept will be deconstructed. Because many concepts have the same purpose, a re-deconstruction of the concept will be carried out and then categorized according to the current roles. Table 5 shows the deconstruction of the same idea into one concept only to reduce the concept redundancy. And each concept will be given a role, where the Ontological role is a function where a concept already exists, the next is the Epistemological role which is how the concept should exist, and the last one is the Methodological role, which is how the concept can work properly.

The method used to simplify the concept in Table 5 is by looking at the meaning of each concept mentioned in Table 3 and Table 4. If the concept is different, the name has the same meaning or the same scope, then the concept is put together.

http://doi.org/10.26594/register.v7i2.2263

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 125-135

4.5. Integrating concept

The fifth stage is the integrating concept, wherein this process the integration of the concept between digital forensics and audit fraud has been carried out, which in the previous step simplified the concepts between disciplines that have almost the same meaning or in the same scope. To integrate the concept, it is done by eliminating the same concept both in language or sense and choosing one of the two concepts that are the same into one concept that is suitable for the two fields.

Table 6 shows how the integration of the two concepts is the same, where the concepts on the same line are identical concepts either in meaning or language so that they are reduced to one concept. This process is similar to the concept deconstruction stage, except that the integration process is carried out in two different disciplines, namely digital forensics and fraud auditing. This integration process is an important point in developing a conceptual framework from Jabareen that facilitates the integration of the two disciplines.

Table 6. Concept intergration

Digital Forensics	Fraud Audit	Concept Integration
Readiness	Detection	Readiness
Identification	Planning	Planning
Collection	Collection	Collection
Analyze	Investigation	Analysis
Report	Report	Report
Concurrent		Concurrent
Incident Closure		Incident Closure
Incident Response		Incident Response

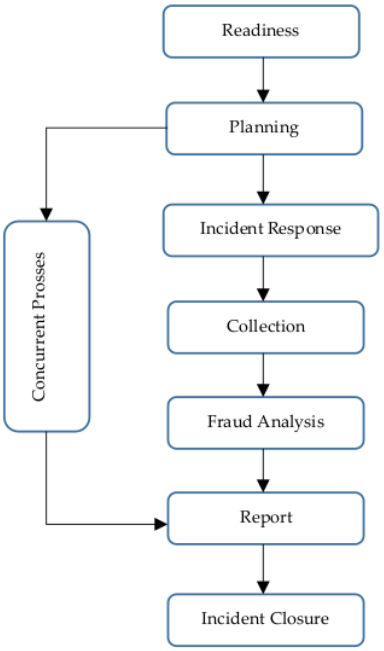

Fig. 4. Cyber fraud framework

4.6. Synthesis, resynthesis and make it all sense

The last stage, namely synthesis, resynthesis and make it all sense, is the stage of preparing a cyber fraud framework to make more sense based on the integration of the concepts mentioned in Table 6. From Table 6 the same concepts are put together and added with other concepts that have not been covered such as Concurrent, Incident Closure, and Incident Response. From this concept, a Cyber Fraud Framework is compiled which is the result of collaboration on key matters in the Forensic Digital Investigation and Fraud Audit. The results of the Cyber Fraud Framework can be seen in Fig. 4, which

http://doi.org/10.26594/register.v7i2.2263

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 125-135

consists of eight stages with one active process used to ensure that the digital evidence obtained is suitable to prove a case of cyber fraud.

The first stage of the cyber fraud framework begins with Readiness, where one of the factors hampering the fraud investment process is the lack of readiness of the institution in the event of a fraud case. The second stage, namely Planning, is the process of planning and identifying fraud cases, where the role of the chief investigator is indispensable at this stage. Incident Response is an important step in cyber fraud because there is digital evidence that is volatile and requires a faster process before the evidence is lost. The collection stage is the core of the importance of digital forensics because the evidence in the cyber fraud case is related to digital proof.

The Fraud Analysis stage is the investigation stage carried out by the Fraud Auditor to find fraud cases based on digital evidence collected. The Reporting stage is carried out after the analysis is complete and is reported to the competent authorities, both the institution and the legal apparatus. There is an active process between the Planning and Reporting processes, namely Concurrent Processes, where there are irregularities between the methods above. The process can be carried out again from the beginning. The last stage is Incident Closure was. In this process, fraud cases are closed both within the relevant institution and in the realm of law.

4.7. Evaluation of framework development

The evaluation of developing a framework for cyber fraud investigation was assisted by 2 practitioners (Ministry of Finance and from PUSFID UII) and an academician from the Islamic University of Indonesia, a former auditor at a financial institution. This limited selection of respondents is indeed an initial evaluation of the development of this framework, and the sample of respondents is represented by experts in the field of digital forensics, forensic auditing, and academics who are involved in the audit field who have also worked at Big 4 Public Accounting Firms. The results of the three questionnaires obtained can be seen in Table 7 as answers from both practitioners and one academic.

Table 7. Questionnaire results from practitioners and academics

No	Question	Practitioner 1	Practitioner 2	Academics
1	Is the framework being developed needed in the field?	Yes	Yes	Yes
2	Is the framework being developed suitable for use in the field?	Yes	Maybe	Yes
3	Are the concepts/stages presented suitable in the field of Cyber Fraud?	Yes	Yes	Yes
4	Is the provision of concepts/stages in the framework acceptable as is (yes); or what changes are needed?	Yes	Minor Changes	Yes
5	Are the differences in concepts/stages in the field acceptable (yes); or are changes needed?	Yes	Minor Changes	Yes

Table 8. Percentage of survey results from 2 practitioners and 1 academician

No	Question	Cluster	Percentage of Results (For Yes Answers)	Average Result
1	Is the framework being developed needed in the field?	Need and Feasibility of Cyber Fraud Investigation	100%	89%
2	Is the framework being developed suitable for use in the field?	Framework	67%	
3	Are the concepts/stages presented suitable in the field of Cyber Fraud?		100%	
4	Is the provision of concepts/stages in the framework acceptable (yes), or what changes are needed?	Changes needed to the framework being developed	67%	67%
5	Are the differences in concepts/stages acceptable (yes), or are changes needed?		67%	

From Table 7 above, for the needs of developing a cyber fraud investigation framework in the field, the three respondents stated that all stated that this framework was needed to be developed, but for the feasibility of the framework, it was necessary to conduct another evaluation which was the opinion of one practitioner. The conceptual presentation in the developed framework was stated to be suitable by the three respondents. The two respondents said that the concept change in this framework was unnecessary. However, one respondent stated that it still needed more evaluation to adapt it to the growing trend of digital technology.

http://doi.org/10.26594/register.v7i2.2263

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 125-135

Fig. 5. Percentage of cyber fraud investigation framework needs

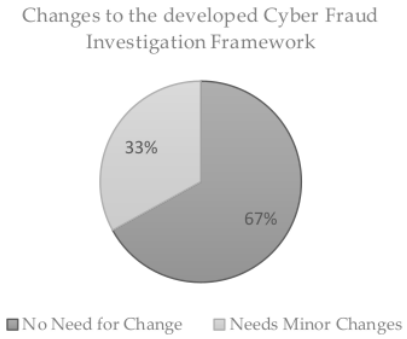

Fig. 6. Percentage change in cyber fraud investigation framework developed

Table 8 describes the percentage of questionnaire results given based on clusters. There are two clusters in this questionnaire, namely Cluster I concerning the level of need and feasibility of developing a cyber fraud investigation framework and Cluster II concerning the level of change in the cyber fraud investigation framework that has been created. The questionnaire results in cluster 1 show the numbers 100%, 67%, and 100% for Yes answers, while in cluster II, the numbers show 67% for both questions for Yes answers.

The calculations from the previous questionnaire are processed into a percentage as shown in Table 8 on the average value, which is then visualized in Fig. 5 and Fig. 6. Fig. 5 illustrates that in cluster I, 89% of results were obtained, which indicated that the framework for investigating cyber fraud was indeed necessary and feasible to use, and 11% that the framework that is developed is essential but not feasible. Fig. 6 regarding cluster II concludes that there is no need for changes to the cyber fraud framework created by 67%, while 33% stated that they need minor changes so that this framework can be used in the field. The slight difference in question is that the framework needs to be adjusted to current technological developments.

5. Conclusion

Cyber Fraud Framework development is based on the conceptual framework development method from Jabareen, which uses 6 phases, namely mapping the selected data source, extensive reading and categorizing of the chosen data, identifying and naming objects, deconstructing and classifying the concept, integrating concept, synthesis, resynthesis and make it all sense produces 8 stages of an investigation, namely: Forensic Readiness, Investigation Planning, Incident Response, Collection, Fraud Analysis, Report, Incident Closure, and Concurrent Process. Evaluation of the development of a cyber fraud investigation framework from the results of questionnaires to two practitioners and one academician, in general, stated that the development of a cyber fraud investigation framework is indeed needed and needed in the field, but to find out whether the developed framework is feasible or not requires a broader evaluation such as conducting surveys of auditing institutions and adjusting to

http://doi.org/10.26594/register.v7i2.2263

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 125-135

trends in the technology used in cyber fraud cases, such as the use of social media. The framework developed is considered sufficient to be used, but some evaluation is needed by the growing trend of digital technology. Testing on a larger scale is expected to become a topic for further research with improvements needed to make the framework even better and be used as a reference for auditors to resolve cyber fraud cases.

Author Contributions

Anisa Nur Hidayati: Conceptualization, methodology, and writing - original draft. Imam Riadi: Supervision and writing - review & editing. Erika Ramadhani: Validation and writing - review & editing. Sarah Ulfa: Validation and visualization.

Declaration of Competing Interest

We declare that we have no conflict of interest.

References

[1] N. Faulkner, I. Pollari, M. Dougall and B. Watson, "Global Banking Fraud Survey 2019," KPMG, 25 June 2019. [Online]. Available: https://home.kpmg/au/en/home/insights/2019/05/the-multi-faceted-threat-of-fraud-are-banks-up-to-the-challenge-fs.html. [Accessed 15 April 2021].

[2] Microsoft, "Online Fraud: Your Guide to Prevention, Detection, and Recovery," 2012.

[3] F. B. o. Investigation, "2019 Internet Crime Report," Internet Crime Complaint Center, 2019.

[4] accenture, "Unmask digital fraud. Today," accenture, 2018.

[5] J. Carter, "Consumer Sentinel Network," *Policing: An International Journal*, vol. 31, no. 4, 2008.

[6] M. Elkin, "Crime in England and Wales: year ending March 2019," Office for National Statistics, 2019.

[7] H. Murdock, "Association of Certified Fraud Examiners (ACFE)," in *Auditor Essentials*, Auerbach Publications, 2018.

[8] N. Fletcher, "Challenges for regulating financial fraud in cyberspace," *Journal of Financial Crime*, vol. 14, no. 2, pp. 190-207, 2007.

[9] N. I. Nawang, "Combating anonymous offenders in the cyberspace: An overview of the legal approach in Malaysia," in *2017 2nd International Conference on Anti-Cyber Crimes (ICACC)*, Abha, Saudi Arabia, 2017.

[10] B. Hayes, J. Jeandesboz, F. Ragazzi, S. Simon and V. Mitsilegas, "The law enforcement challenges of cybercrime: are we really playing catch-up?," Study for the LIBE Committee, 2015.

[11] N. F. S. T. Center, "A Simplified Guide To Digital Evidence," 2014.

[12] S. E. Goodison, R. C. Davis and B. A. Jackson, "Digital evidence and the US criminal justice system," RAND Corporation, Santa Monica, Calif, 2015.

[13] E. F. G. Ajayi, "Challenges to enforcement of cyber-crimes laws and policy," *Journal of Internet and Information Systems*, vol. 6, no. 1, pp. 1-12, 2016.

[14] N. F. Ryman-Tubb, P. Krause and W. Garn, "How Artificial Intelligence and machine learning research impacts payment card fraud detection: A survey and industry benchmark," *Engineering Applications of Artificial Intelligence*, vol. 76, pp. 130-157, 2018.

[15] B. Cusack and T. 'Ahokovi, "Improving Forensic Software Tool Performance in Detecting Fraud for Financial Statements," in *The Proceedings of 14th Australian Digital Forensics Conference*, Perth, Australia, 2016.

[16] A. M. L. Kian, "Tindakan Pidana Credit/Debit Card Fraud dan Penerapan Sanksi Pidananya dalam Hukum Pidana Indonesia," *Hasanuddin Law Review*, vol. 1, no. 1, 2015.

[17] A. Goudbeek, K.-K. R. Choo and N.-A. Le-Khac, "A Forensic Investigation Framework for Smart Home Environment," in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, New York, NY, USA, 2018.

http://doi.org/10.26594/register.v7i2.2263

ISSN 2502-3357 (online) | ISSN 2503-0477 (print)
7 (2) July 2021 125-135

[18] I. Kigwana, V. R. Kebande and H. S. Venter, "A proposed digital forensic investigation framework for an eGovernment structure for Uganda," in *2017 IST-Africa Week Conference (IST-Africa)*, Windhoek, Namibia, 2017.

[19] S. Sathwara, N. Dutta and E. Pricop, "IoT Forensic A digital investigation framework for IoT systems," in *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Iasi, Romania, 2018.

[20] M. Harbawi and A. Varol, "An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework," in *2017 5th International Symposium on Digital Forensic and Security (ISDFS)*, Tirgu Mures, Romania, 2017.

[21] N. L. Htun and M. M. S. Thwin, "Proposed Workable Process Flow with Analysis Framework for Android Forensics in Cyber-Crime Investigation," *The International Journal Of Engineering And Science (IJES)*, vol. 6, no. 1, pp. 82-92, 2017.

[22] S. Ahmad, N. L. Saad, Z. Zulkifli and S. H. Nasaruddin, "Proposed network forensic framework for analyzing IaaS cloud computing environment," in *2015 International Symposium on Mathematical Sciences and Computing Research (iSMSC)*, Ipoh, Malaysia, 2015.

[23] D. Adom, E. K. Hussein and J. A. Agyem, "Theoreticaland Conceptual Framework: Mandatory Ingredients of a Quality Research," *International Journal of Scientific Research*, vol. 7, no. 1, 2018.

[24] Y. Jabareen, "Building a Conceptual Framework: Philosophy, Definitions, and Procedure," *International Journal of Qualitative Methods*, vol. 8, no. 4, pp. 49-62, 2009.

[25] E. Eizenberg and Y. Jabareen, "Social Sustainability: A New Conceptual Framework," *Sustainability*, vol. 9, no. 68, 2017.

[26] A. Haddadi, A. Johansen and B. Andersen, "A Conceptual Framework to Enhance Value Creation in Construction Projects," *Procedia Computer Science*, vol. 100, pp. 565-573, 2016.

[27] M. Abduh, R. D. Wirahadikusumah and Y. Messah, "Framework Development Methodology for Sustainable Procurement of Construction Works in Indonesia," in *MATEC Web of Conferences*, 2018.

[28] C. Okoli and S. D. Pawlowski, "The Delphi method as a research tool: an example, design considerations and applications," *Information & Management*, vol. 42, no. 1, pp. 15-29, 2004.

[29] C. J. Bacon and B. Fitzgerald, "A Systemic Framework for the Field of Information Systems," *The DATA BASE for Advances in Information Systems*, vol. 32, no. 2, 2001.

 http://doi.org/10.26594/register.v7i2.2263

HASIL CEK_Development of conceptual framework for cyber fraud investigation

ORIGINALITY REPORT

7%	0%	7%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

MATCH ALL SOURCES (ONLY SELECTED SOURCE PRINTED)

5%

★ Dewa Gede Hendra Divayana, P. Wayan Arta Suyasa. "Simulation of TOPSIS calculation in Discrepancy-Tat Twam Asi evaluation model", Register: Jurnal Ilmiah Teknologi Sistem Informasi, 2021

Publication

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		