IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 26, 2021, accepted September 15, 2021, date of publication September 20, 2021,
date of current version September 28, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3114233

K-FFRaaS: A Generic Model for Financial Forensic Readiness as a Service in Korea

SUNG JIN LEE [1,2] AND GI BUM KIM [1]
[1]Department of Forensics, Sungkyunkwan University, Seoul 03063, South Korea
[2]Capital Market Judiciary Enforcement Unit, Financial Supervisory Service, Seoul 07321, South Korea

Corresponding author: Gi Bum Kim (freekgb02@gmail.com)

ABSTRACT While Korean financial companies are currently providing electronic financial services by establishing the high-level information technology and security system in accordance with the Electronic Financial Supervision Regulations (EFSR), they are rarely equipped with digital forensic readiness (DFR) to maximize the capability to collect critical digital evidence (DE). So, there is a limit to identifying the root cause of financial incidents and securing admissible DE. In this paper, we present Financial Forensic Readiness as a Service in Korea (K-FFRaaS), as DFR of financial companies to acquire an admissible DE. Based on ISO/IEC 27043:2015 international standard, K-FFRaaS consists of 3 main processes groups, namely: Planning processes group, Implementation processes group, and Assessment processes group. The purpose of planning processes group is to prepare the organization to be forensically ready before potential incidents happen. The main task of implementation processes group is to carry out the processes defined in the planning processes group. The goal of assessment processes group is to evaluate whether the result of the implementation processes group is consistent with the objective of K-FFRaaS. The contribution of this research is to present that financial companies can adopt the systematic management procedure for identifying causes of incidents, storing potential DE, and presenting scientific evidence to a court of law through K-FFRaaS.

INDEX TERMS Digital forensics, forensic readiness, digital evidence, ISO/IEC 27043:2015, electronic finance.

I. INTRODUCTION

The new technology in the 4th industrial revolution and emergence of COVID-19 lead to the activation of online services, such online transaction and telecommuting, and become the catalysts for the accelerated digitalization of finance. The Financial Services Commission in Korea announced its "Comprehensive Digital Finance Innovation Plan" on 27 July 2020, which will lead to many social changes including the amendments of the Electronic Financial Transactions Act (EFTA). The amendments aimed at furthering an innovative digital financial industry, setting up a user protection system, and fortifying digital finance security. The burden of proving proof of electronic financial incidents previously imposed on users will shift to the financial company by considering the development of information technology (IT) and information asymmetry in a big way [1], [2].

Due to such rapid changes in the financial environment, financial security incidents are becoming more sophisticated and specialized, making it difficult to quickly and accurately analyze the causes of incidents. The development of the financial industry creates various cyber security issues, such as cyber threats, attacks, and data leakage. The cybersecurity attack poses a significant threat to the national economy [3], and causes huge financial losses in particular in the financial industry, thereby risking the existence of a company. Over the past five years, hacking attempts at financial companies in Korea amounted to an average of 67,436 cases per day. It was found that there were 40 incidents that actually resulted in damage to financial companies and consumers, such as website forgery and falsification, and malicious code infection [4]. By type of incidents, DDoS attacks accounted for the most with 23 cases, followed by data break with 7 cases, system forgery and falsification with 5 cases, and malware infections with 2 cases, etc. [5]. Table 1 shows the types of electronic financial incidents that can occur in financial companies [6].

The associate editor coordinating the review of this manuscript and approving it for publication was Xabier Larrucea.

TABLE 1. Types of electronic financial incidents.

Types	Description
DDoS Attack	• Slowing down or shutting down IT services of a financial company through various denial of service attacks
Data Breach	• Information leakage caused by the malicious purpose or negligence of internal employees
System Forgery and Falsification	• Interfering with normal service by forging the computer system
Data and Program Fabrication	• Fabricating, destroying, or concealing data and programs stored in computer systems
Internal Network Hacking	• Causing information leakage and system down by the vulnerability of internal system or related system

In a situation where telecommuting and easing of network separation have been implemented due to COVID-19, many security loopholes in financial companies, such as non-compliance with network segregation policy, were discovered in examinations by the Financial Supervisory Service (FSS) [7].

Currently, financial companies in Korea are focusing on quick recovery in the event of an electronic financial incident. Their approach to mitigate the incident is only concerned with disaster recovery and business continuity to alleviate the impact [8]. So, they cannot implement it in a timely manner despite the need to acquire digital evidence in the initial investigation. Also, financial companies lack the capability to collect digital evidence related to electronic financial incidents and face a want of traces of evidential data [9], because they do not have adequate experts, software/hardware tools, and procedures for digital forensics. Because electronic information related to the analysis of the actual incident cause is not preserved for more than a certain period of time, cases that consume a lot of time and money in finding the root cause are frequently found.

The financial company needs to have a DFR mechanism in place [10] not only to identify the causes of the incidents, but also to strengthen information security system to prove criminal charges. Implementing DFR [11] is "*having an appropriate level of capability in order to be able to preserve, collect, protect and analyze digital evidence so that this evidence can be used effectively, in any legal matters, in security investigations, in disciplinary proceeding, in an employment tribunal, or in a court of law.*" Namely, that will make it possible to prove the crime by presenting admissible scientific evidence in a court of law [12] and secure the precautionary effect to raise awareness about digital crime [13].

To date, there has been minimal research regarding the DFR model across the entire computer system of the financial companies in Korea. Because the financial companies in Korea secure the safety of IT system in accordance with EFTA and EFSR, they should have high-level information security system enhance the security control in terms of cyber-hygiene [14]. So, the adoption of the DFR will be a major driver for information security to have digital forensic evidence ready when needed for investigations [9].

Notably, the main objective of this paper is to present financial forensic readiness as a service (K-FFRaaS) model that can be viewed as the methodology for achieving DFR in Korea. "X as a Service" is mainly used to describe the service of cloud computing. Recently, many studies [15]–[18] have proposed a digital forensic readiness model based on cloud computing service [19]. In the future, the computer system of financial company is also expected to be transferred to the cloud computing environment. Subsequently, we leverage the established concept of K-FFRaaS in order to propose DFR of the financial company in Korea.

In this study, K-FFRaaS model is composed of comprehensive multidimensional processes in which legal, technical, and organizational aspects are combined. Digital forensics (DF) acquires DE in various steps: preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation [20], [21]. However, K-FFRaaS is different from DF which is the one-dimensional sequential procedural method [22]. Specifically, the K-FFRaaS is designed to present the direction to fully construct DFR consisting of 11 processes optimized to the financial company. Based on laws and regulations related to both the electronic financial transactions and DE collection procedure, major considerations and constraints in the implementation of DFR for financial company is reviewed. And the K-FFRaaS in tandem with ISO/IEC 27043: 2015 [23] is presented in this paper. The practical outcome of this study is to suggest a comprehensive set of processes that the financial company itself can utilize to evaluate and improve the K-FFRaaS model.

The remainder of this paper is organized as follows. Section II covers the background underpinning K-FFRaaS to meet its forensic objectives. Section III introduces K-FFRaaS based on ISO/IEC 27043:2015. Section IV deals with digital forensics investigation based on K-FFRaaS model. Finally, the paper closes with a summary of conclusion and with a discussion on possible extensions in Section V.

II. BACKGROUND

A. DIGITAL FORENSICS

Digital Forensics (DF) was initially coined by Palmer [21] as "*the use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of Digital Evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations*" at the DFRWS in 2001 [24]. By following the chain of custody, DF makes use of scientifically proven methods in conducting any type of digital investigation [12], [25]. When law enforcement agency executes the seizure and search warrant, it seizes digital devices such as a PC and makes a bit by bit copy of the seized device in a forensic procedure [26], [27]. DF refers to the process of ① identifying and collecting digital data stored in information storage device such as computers, USBs, and mobile phones, ② selecting and extracting crime-related information, and ③ preserving and submitting it as evidence to the court [28]. Depending on the purpose of DF, it can be divided into 2 cases: ① the case where a law enforcement agency uses it to reveal the truth behind crimes, ② the case where a company utilizes it for the purpose of internal audit to protect corporate assets. DF has mainly been carried out by the law enforcement agency to prove criminal charges. And DF process is traditionally associated with judicial proceedings [29]. DF itself is in general accepted to have arisen from the working practices of the law enforcement agency [30]. On the other hand, recently, the scope of the execution of DF has been expanded. And DF is also used for the investigation of corporate data breach and internal control nowadays [31].

DF can be divided into a reactive DF and a proactive DF [32]–[34]. The reactive DF can be considered as the general DE collection and analysis procedure to carry out DF to determine the root cause after the incident has occurs [35]. Most of the DF investigations are included in the reactive DF. Meanwhile, the proactive DF means to be called upon in response to the occurrence of an incident [36]. Because forensically sound evidence is one that can endure legal scrutiny in a court of law [37], the substantial effort can be in the direction of collecting forensic data [38]. If an organization implements the DFR environment, its capability, such as the saved time, the minimized cost, and the lack of disruption caused to the environment, can be maximized to conduct DF investigations [39], [40].

B. DIGITAL FORENSIC READINESS

DFR is the preparedness of organizations for conducting DF [29]. Since the term 'digital forensic readiness' first appeared in 2001, numerous studies have been conducted that focus on DFR including time, cost, and resource. The 2 objectives of DFR have been defined in [12], [24], [27]: ① To maximize environmental capabilities to collect reliable DE, and ② To minimize forensics cost to respond to incidents. Rowlingson [41] presented 10-step processes for DFR, in order to define business scenarios for DF, identify necessary assets, and meet the requirements and capabilities of the DE collection. Danielsson and Tjostheim [42] proposed the guideline for compliance, requirements, and procedures for PDE collection in consideration of relevant laws and regulations on DE. Taylor *et al.* [43] identified assets and data for DE collection and reviewed whether a DFR policy is properly defined and applied. Barske *et al.* [44] emphasized the necessity to develop and maintain the appropriate workforce and budget for DFR. Glober *et al.* [34] identified the goal of proactive DF and proposed the incorporation of a theoretical digital forensic framework into the management domain of the organization including governance and policy. Elyas *et al.* [45] presented the key factors necessary for an organization to build the DFR and developed a conceptual framework that includes the relationship between each factor. Valjarevic and Venter [46] reflected Tan's [12] idea of maximizing the utility of DF and minimizing the cost of investigation regarding applying DFR to a public key infrastructure (PKI) system.

By definition, DFR has the capability of the system to efficiently gather the available relevant DE to be used in a court of law [43], [47], hence minimizing the investigation cost [48], [49]. And DFR is the integrated management model to identify the cause of the incident and to have digital forensic evidence ready when needed for investigation [9], [50].

Unlike information security, one of the key features of DFR is to secure and preserve admissible DE, as the outcome that is acceptable by law [51]. Information security has the C.I.A. triad as three objectives, such as confidentiality, integrity, and availability [52], [53]. On the other hand, to secure the admissible DE, DF has additional components, such as authenticity, accuracy, control, relevance, and completeness, [54] other than C.I.A. triad. Information security mechanisms is to detect, preserve, and quickly recover from cybersecurity attacks [55]. DFR can be viewed as an extension to information security mechanism because it aims to proactively set an organization's DF capability to extract, collect, maintain, and analyze DE [53], [56]. Similar to DFR, the cause of the incident in information security is identified by collecting and analyzing logs stored in information system through system logging [57], configuration files, and electronic data of the computer system. However, because digital data is vulnerable to forge, falsify, and damage, it is necessary to comply with due processes and appropriate measures when obtaining evidence [28]. Information security does not comply with the chain of custody. So, the digital files could be altered or deleted during the analysis process. Although this may serve as a decisive clue in determining the cause of an incident, it cannot be admissible as evidence in a court of law, due to a lack of admissibility of evidence collected by the financial company [40], [58].

The DE finding mission can be done fast through DFR. In other words, the financial company can swiftly meet the need to support legal action with admissible DE [59]. Because the DF influences across the entire information security of a company [33], the information security should be set up based on DF given a role in enterprise information system operation [60]. There is a need to establish DFR to identify the cause of the incidents, such as internal information leakage and data breach, and to secure DE to prove a crime. And DFR should be implemented by making use of a systematic and proactive methodology to collect and store DE [61].

In Korea, DFR was first proposed by Baek and Lim [31] for the purpose of responding to personal information incidents in 2012. It is meaningful in that it presented the direction for establishing the procedure of DFR from the perspective of personal information protection. Another study proposed DFR to prevent the leakage of business information [62]. And Kim and Kim [63] suggested the DFR of financial company for infringement incident response. However, the requirements were simply enumerated as clauses and logs according to the related law, and ISO/IEC 27043:2015 was also not considered. From the perspective of DFR, there is a need to present a model to collect admissible DE proactively in conjunction with EFTA. Lately, in the sense that financial company needs to have digital forensic capabilities to fully support the incident investigation, the interest for DFR model has been growing. The DFR is required to ensure that the financial company, such as bank, securities, and insurance, are well prepared operationally and infrastructurally [64].

Most of the financial companies have the information security system to record and manage the operation of computer systems and user action according to EFTA and EFSR. However, there is no way to quickly acquire admissible DE in both criminal and civil cases. If DFR is implemented for the entire information security [65], the financial company can promptly investigate an incident at minimal cost, aiming to the intruders, hacking attack point, the amount of damage caused, and the cause of the incident [66], [67]. And DFR minimizes the reputation damage [68], manages user computer system logs, and make it easy with less hassles to retrieve admissible DE for criminal penalties. Additionally, if DFR is adopted as a major element for overall risk management, the financial company will be able to increase the trust level from financial consumer and investors [69].

C. ISO/IEC 27043:2015

1) DIGITAL INVESTIGATION PROCESS CLASSES

Valjarevic and Venter [70] developed the harmonized Digital Forensic Investigation Readiness Process (DFIRP) model consisting of Planning, Implementation and Assessment, which was added to ISO/IEC 27043 in 2014. ISO/IEC 27043:2015 international standard is the digital investigation concepts covering information technology, security, and incident investigation principles and processes. Kebande and Venter [71] presented the digital readiness model with reference to the ISO/IEC 27043:2015 for the first time. The process for adding event reconstruction was applied to the cloud DFR model based on ISO/IEC 27043:2015. Kebande and Venter [72] designed a detailed DFR model in a cloud environment, and Kebande *et al.* [73] expanded the scope of research to a company equipped with IoT systems, in order to study the DFR model in IoT environment.

The digital investigation process classes specified in the ISO/IEC 27043:2015 [23], as shown in Figure 1, are divided into five classes: Readiness processes class, Initialization processes class, Acquisitive processes class, Investigative processes class, and Concurrent processes class. The readiness processes class is a set of processes to equip the organization with the necessary capabilities to maximize the potential use of DE and cover the pre-incident investigation processes [72], [73]. The initialization processes class deals with uncovering PDE and searching for DE in a legal process. The acquisitive processes class is a set of processes to carry out the investigation of a case where PDE is identified and handled [74]. The investigative processes class consists of processes used in a forensic procedure. Finally, the concurrent processes class is the set of processes that run throughout all 4 processes classes in the digital investigation process [49], [73].

The readiness processes class in ISO/IEC 27043:2015 is specified as DFR. As indicated by the dotted line in Figure 1, the readiness process is optional. In other words, the digital investigation can be performed even if the organization does not obligatorily have the readiness process. However, the efficiency of digital forensic investigation (DFI) can be attained through the implementation of the readiness process. DFIs on the incident, such as civil and criminal cases, can be conducted at a good clip. This can lead to the reduction of the cost for the forensic investigations by utilizing the DFR model.

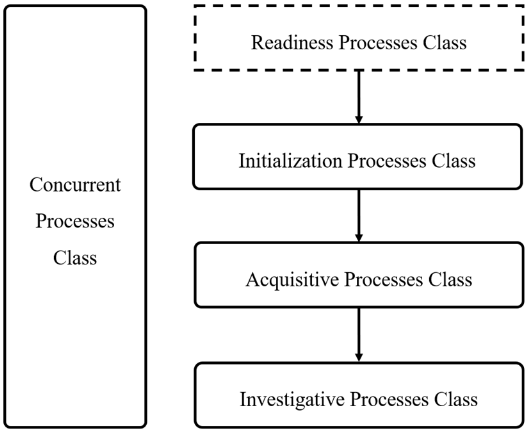

Concurrent Processes Class
Readiness Processes Class
Initialization Processes Class
Acquisitive Processes Class
Investigative Processes Class

FIGURE 1. Digital investigation process classes in ISO/IEC 27043.

2) DFR PROCESSES GROUPS

The DFR processes groups need to be specified in four directions: ① maximize the potential use of DE, ② minimize the cost of DFIs [12], ③ minimize interference with business [41], [75], and ④ strengthen information security posture by continuously improving security system [22]. Given these directions, the ISO/IEC 27043:2015 organizes the readiness processes class of digital investigation process classes into four groups to fully implement DFR. Figure 2 below represents four DFR processes groups which are adopted in this paper for the achievement of K-FFRaaS [76].

Planning processes group is defined as the group to prepare the organization to be forensically ready before potential incidents happen. Getting a forensic preparation plan in place means that it is viable to acquire DE in a timely manner when it is needed [77]. This group includes both legal and business requirements and basic handling tasks required in the event of an incident. Implementation processes group carries out the processes defined in the planning step. In this step, the system structure and policies related to the sources, such as logs, storage, tracking software, and hardware, are

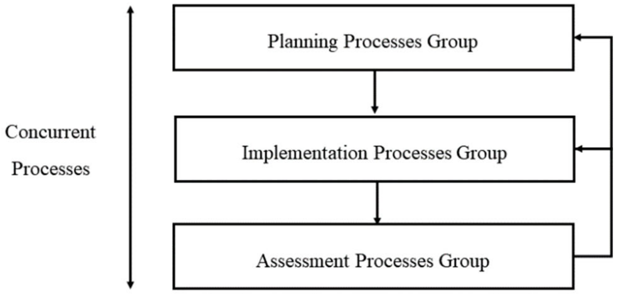


FIGURE 2. DFR processes groups in ISO/IEC 27043:2015.

TABLE 2. K-FFRaaS policy of financial company.

Step		Description
① Advance Preparation		• Identification of legal requirements related to electronic finance and DF (L) • Providing direction to DE collection reflecting the business characteristics (O) • Policy for DE collection and preservation (L) • Securing capabilities, such as technology, experts and budget, for DF (O) • Identification of DF types (L) • Equipping with specialized forensic software and technique (T)
② Main Target Identification		• Definition of the classification criteria for each business and system (O) • Identification of the source of PDE for each business classification (O) • Identification of assets related to PDE (O) • System architecture definition and implementation for DE collection (T)
③ DFR Implementation and Execution	Pre-incident	• Testing and risk assessment for potential losses and threats (T) • Application of the DF policy according to the chain of custody (L) • PDE collection, preservation and documentation (T)
	Post-incident	• DE investigation and analysis (T)
		• Review of incident response legality according to relevant laws (L)
④ Follow-up Control		• Conduct educational training to enhance understanding of DF (O) • Detect major incidents through monitoring (O) • Incident report to FSS or accusation to investigation authority (O) • Evaluation and improvement of digital forensic readiness (L)

implemented to collect DE. Notably, log files are essential in identifying the source of the problem for DFIs because the investigator can use the files as meta-data related to the history of specific actions [78]. Assessment processes group consists of processes that evaluate whether the result of the implementation processes group is consistent with the objective of K-FFRaaS. The result of the assessment can be used to improve the whole K-FFRaaS process. Additionally, whether the collected DE is admissible is an important evaluation criterion. The concurrent processes are not limited to a specific step and includes processes that may apply to other processes groups across K-FFRaaS. The concurrent processes include obtaining authorization, documentation, managing information flow, preserving the chain of custody, preserving DE, and interaction with the physical investigation [79].

III. DFR FOR FINANCIAL COMPANY

A. K-FFRAAS MODEL

This paper presents an approach that can be used to construct DFR model for financial company in Korea. This echoes the recommendations in the ISO/IEC 27043:2015 international standard [23], [80], [81], which underlines the importance of the use of standardized process to implement the readiness processes class [73]. The model provided by ISO/IEC 27043:2015 is too abstract. But, the implementation of DFR in an financial company entail a systematic and complex work, including the incorporation of infrastructural readiness strategies, such as risk assessment, tool deployment, and evaluation metrics [82]. From the perspective of information security based on the ISO/IEC 27043:2015, K-FFRaaS needs to be organized by referring to the main contents of Table 2. A detailed view of K-FFRaaS is shown in Figure 3.

The People-Process-Technology (PPT) indicator has long been recognized as a key for improving organizations [83]. The main indicator of DF is People-Processe-DE (PPD), referring to PPT indicators. Figure 3 diagrammatically describes K-FFRaaS model which is comprised of three processes groups with PPD indicator. First, the establishment of the policy is designed to identify the basic direction to build K-FFRaaS. DF is classified considering the digital devices and digital assets owned by financial company. After determining the scenarios for each work group to acquire DE, methods for collecting, preserving, and documenting PDE are presented. Finally, the level of K-FFRaaS is evaluated so that it can be continuously improved. The concurrent processes including documentation and preserving chain of custody are commonly reflected in the entire processes group to secure the admissibility of DE [79]. Figure 3 presents how total 11 processes of this model are fully connected to each other to construct K-FFRaaS, which are then discussed throughout the remainder of the paper.

B. PLANNING PROCESSES GROUP FOR K-FFRAAS

1) DFR POLICY PLAN

The DFR policy plan includes the legal, technical, organizational factors that should be taken into for K-FFRaaS. DFR can help the company not only to fulfil compliance requirements, but also to provide PDE during DFI [84]. So, This process is included in the planning processes group of the ISO/IEC 27043:2015, and the intrinsic DFR policy optimized to each financial company is reinforced via the feedback from other processes in a continuous and repeating fashion, rather than being a one-off process [85]. Because the policy is interconnected with other processes and is updated for DFR [86], the improvement of this process will also affect other processes [87].

It is essential to present forensically sound evidence, in order to verify the authenticity and reliability of the DE

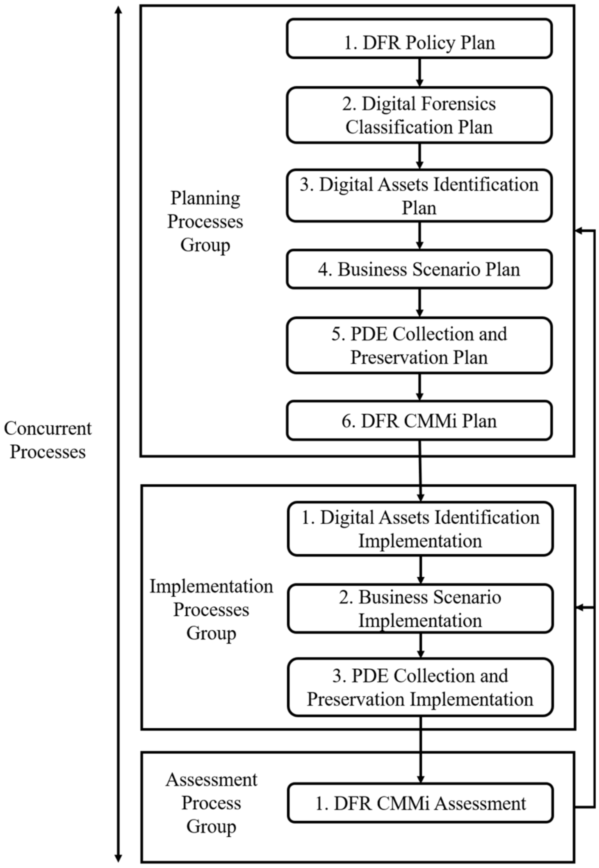

Concurrent Processes
Planning Processes Group
1. DFR Policy Plan
2. Digital Forensics Classification Plan
3. Digital Assets Identification Plan
4. Business Scenario Plan
5. PDE Collection and Preservation Plan
6. DFR CMMi Plan
Implementation Processes Group
1. Digital Assets Identification Implementation
2. Business Scenario Implementation
3. PDE Collection and Preservation Implementation
Assessment Process Group
1. DFR CMMi Assessment

FIGURE 3. **K-FFRaaS Model.**

that is admissible in a court of law [88]. So, the policy should include the legal recommendations and requirements for a digital investigation hence increasing admissibility of PDE during litigation [89]. It is of paramount importance for financial company to secure the admissibility of the acquired PDE via DF. Therefore, the financial company should be put in place the policy and technical guideline for DE collection and preservation to manage the entire computing infrastructure.

Table 2 shows the reorganized list of K-FFRaaS tasks by referring to systematic literature-based studies [41]–[44], [46], [90]. ① Advance preparation step suggests legal, technical, and organizational guidelines for the establishment of a DFR model. ② main target identification step includes assets and data identification for DE collection. ③ DFR implementation and execution step is divided into pre-incident and post-incident. The pre-incident step includes the collection and preservation of PDE and the post-incident step is for DE investigation and analysis [91]. ④ follow-up control step is for training and monitoring to enhance the capability of K-FFRaaS.

The main point for constructing the K-FFRaaS is divided into the Politic and Technical (T) factor, and the Politic factor consists of two factors: Legal (L) factor as outside the organization environment and Organizational (O) factor within the organization guideline [92]. Consequently, Each description for K-FFRaaS is classified by three factors: Technical (T), Legal (L), and Organizational (O) factors [93], [94].

2) DIGITAL FORENSICS CLASSIFICATION PLAN

This section presents the classification of DF types. Because the financial company provides various electronic financial services and its computer systems are inextricably complicated, the DF taxonomy needs to be established to present all data at an abstraction layer and format that can be effectively used by an investigator to acquire DE in forensically sound environment [95]. Wu *et al.* (2020) [96] attempted to define the classification criteria of digital forensics by adding memory forensics and malware forensics to the modified and extended version of the Netherlands Register of Court Experts (NRGD) taxonomy. However, it is not appropriate to classify the database included in the server group to the simple software forensics group. The malware and memory forensics should be classified as separate categories because two forensics could be applied to the entire computer system across the financial company. Additionally, the computer system of financial company is composed of complex information processing systems, such as the accounting system, information system, external system, and securities system. Therefore, there is a need to suggest the DF taxonomy only considering the unique characteristics of the financial company in conjunction with EFSR.

Figure 4 shows the DF types of financial company in Korea. The web browser included in software forensics [96] is moved to computer forensics and software forensics is changed to database forensics. Because the financial company uses electronic approval system, we newly add electronic approval to DB forensics. An important clue for the crime can be acquired from the in-house messenger between employees. So, the in-house messenger is added to DB forensics. Also, because mobile financial services, such as mobile banking, are provided via mobile applications, mobile forensics is classified as a separate category. The financial company uses the business process reengineering system to store internally produced documents in image file format, such as contracts and consultation details. So, multimedia forensics should also be considered a critical category in the financial sector.

Malware and memory forensics proposed by Wu *et al.* (2020) [96] cannot be completely separated from other types of DF. Malware forensics should be carried out with other types for vulnerability analysis and intrusion response. Because malware and memory forensics affect the entire DF, there is a need to classify them into the separate categories. The financial company can utilize cloud services from cloud computing service providers in accordance with EFSR. When using a cloud service, data in a remote storage need to be managed in the network forensics category. Additionally, EFSR makes it mandatory for the financial company to separate its networks into internal and external networks. So, it is necessary to add network segregation to the network forensics category to collect PDE. By referring to the proposed DF

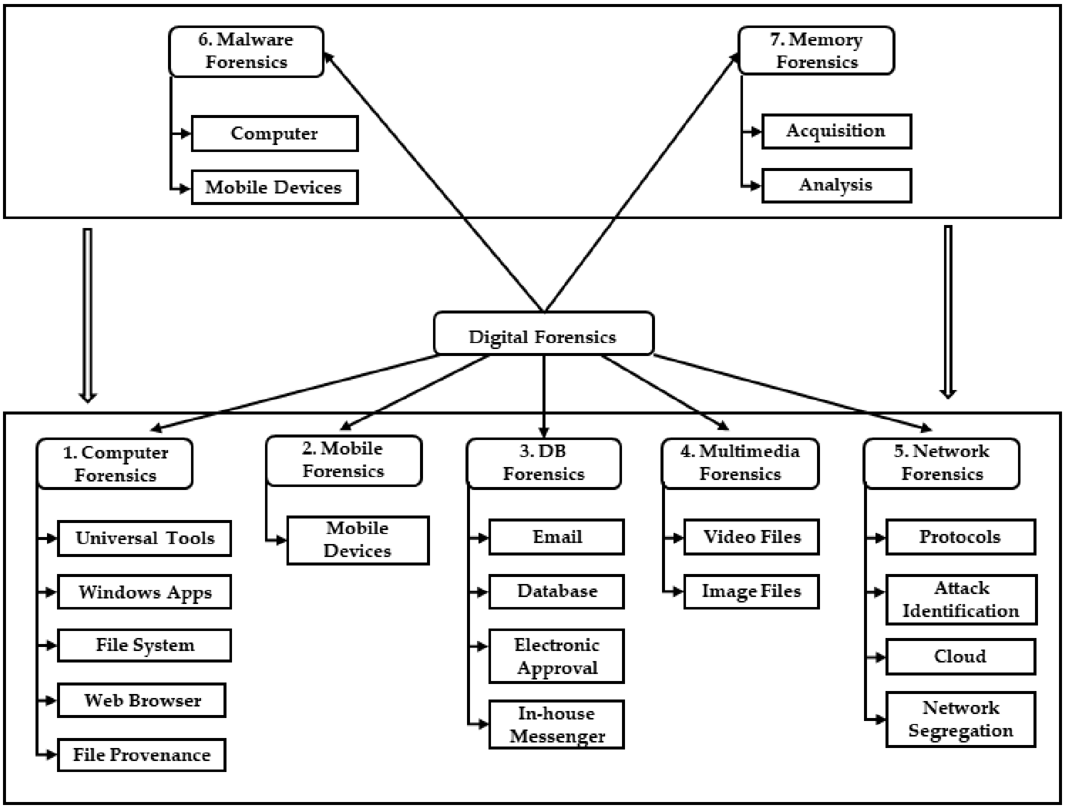


FIGURE 4. DF types of financial company in Korea.

taxonomy and preparing DF experts and tools related to each category, the financial company can keep business continuity on with no data loss and prevent an incidents [97].

3) DIGITAL ASSETS IDENTIFICATION PLAN

In this chapter, the digital assets, such as work manager and work group, are identified. In DFR, due diligence and good corporate governance are key considerations to manage the company's information assets [98]. Therefore, it is necessary to identify major areas of work and assets, the source of DE, to preserve the PDE while maintaining the company's objectives. The ISO/IEC 27043:2015 describes DE as "*information or data, stored or transmitted in binary form, that may be relied on as evidence*" [23]. So, DE can be related to every aspect of the system, ranging from the local device to the server through K-FFRaaS [9].

The financial company has established the policy to manage information systems in accordance with EFSR. By referring to this regulation, the classification by business and system can be deduced and the assets, such as information processing systems, networks, terminals, and servers, can be identified by defining logs, event records, and artifacts from those assets and collecting DE.

The main components of DF are humans, DE, and process [99]. Because DF is very closely related to information security, K-FFRaaS can rely on information security checks. Therefore, the check items for information security of financial company determined by the governor of FSS can be viewed as individual work groups of K-FFRaaS. In this paper, this study introduces 11 work groups of K-FFRaaS, namely: ① Computer room, ② Device, ③ Digital data, ④ Information processing system, ⑤ Anti-hacking measures, ⑥ Malicious code, ⑦ Public web server, ⑧ Internal user password, ⑨ General user password, ⑩ User notices, ⑪ E-financial incident report [100]. These work groups pursue the same purpose of ensuring safe electronic financial transactions. Thus, they can be viewed as an organically fused service-oriented architecture (SOA). But, because K-FFRaaS needs to be approached independently for each work group in the context of information security, it can be viewed as the loose coupling, which means that the behavior of one part barely affects other parts [101].

4) BUSINESS SCENARIO PLAN

Business scenarios in this phase are specified as addressing the possible threats and vulnerabilities and evaluating the potential risk (PR). And the regular tests for risk assessment are conducted with regard to potential threats and vulnerabilities. It is a process of incessantly supplementing K-FFRaaS by checking whether the digital forensic policy is properly applied. Based on information security check items for a total of 11 tasks stipulated in the Detailed Enforcement

Regulations for EFSR [102], business scenarios for K-FFRaaS were created as shown in Table 3. Additionally, in accordance with the relevant provisions of the Regulation, available sources and individual types of PDE can be identified for each business scenario [33] and chief information security officer of the financial company is required to report these information security check items to chief executive officer. K-FFRaaS scenarios need to be looked at based on these check items.

5) PDE COLLECTION AND PRESERVATION PLAN

This stage involves collecting and preserving DE to be admissible in a court of law. Figure 5 shows that the client, such as the work manager and the financial consumer, accesses to 11 work groups to stably use financial services, such as internet or mobile banking, deposit and withdrawal services, by using smartphone and PC [103]. Forensic Logging is safely stored in the form of backup and recovery and is managed systematically by documentation. In case of the incident, keeping Forensic Logging from each work group enables financial companies to use PDE in a timely manner.

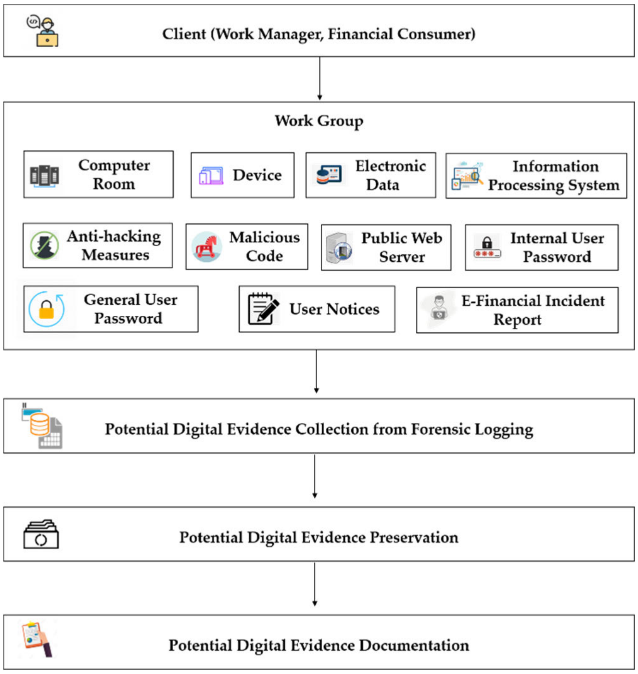

Client (Work Manager, Financial Consumer)
Work Group
Computer Room
Device
Electronic Data
Information Processing System
Anti-hacking Measures
Malicious Code
Public Web Server
Internal User Password
General User Password
User Notices
E-Financial Incident Report
Potential Digital Evidence Collection from Forensic Logging
Potential Digital Evidence Preservation
Potential Digital Evidence Documentation

FIGURE 5. PDE collection and preservation.

Because an information processing system of a financial company is basically composed of a client-server architecture, the characteristics of system logs can be designated as indicators of compromise (IoCs). In other words, IoCs include Hash, IP address, URL, fully qualified domain names (FQDNs), Filename, Email, Mutux, and Registry from the system [104]. For instance, as shown in Figure 6, the probe [105] for individual network process can be generated by adding IoCs to DE from each work group in '4) BUSINESS SCENARIO PLAN'. And these probes for each

TABLE 3. K-FFRaaS business scenario for financial company.

Tasks	Requirements based on the Regulation	DE
Computer Room	• Verify that a visitor log is in use to record physical access.	Visitor logs
	• Verify that either video cameras or access control mechanisms are in place to monitor the entry/exit points.	Data from CCTV
Device	• Protect the device from unauthorized modifications.	Device logs
	• Verify authorized use of device to access to information processing system.	Log of user accounts
	• Verify prohibition of taking a critical device outside.	Taking out logs
	• Examine the direct access between internet and important device.	Security system logs
	• Verify that portable or mobile devices are attached to the device with access control in place.	External storage device logs
Electronic Data	• Provide account and password to individual user.	Account lists
	• Control addition, deletion, and modification of user accounts and passwords.	Account usage logs
	• Control call and output of user information	Electronic data logs
	• Prohibit the use of user information during testing and if unavoidable, change, use and delete it immediately after the test ends	Input/output history of electronic data
	• Prohibit the storage of critical information on the device and if	Account management history
	unavoidable, get approval from the director.	
	• Prohibit sharing the device.	Account management history
	• Control the export/import of electronic data or computing device.	Input/output history of electronic data
	• Verify that information processing system is managed with access control immediately after personnel transfer.	Account management history
Information Processing System	• Verify that unauthorized or wireless communication devices are managed with access control in the internal network.	Security system log
Anti-Hacking Measures	• Verify that the security system is operating normally to prevent hacking.	Security system log
	• Verify that the minimum service ports and functions are specified to the security system.	Security policy
	• Remove functions or programs other than the objective in the security system.	Security policy
	• Prohibit remote management of the security system.	Remote management history
	• Verify that urgent and critical corrections of system programs are immediately done.	Patch management history
	• Verify the approval for wireless network.	Wireless security measures history

TABLE 3. ***(Continued.)*** **K-FFRaaS business scenario for financial company.**

Malicious Code	• Check the latest malware search and treatment programs	Anti-virus program logs
	• Verify critical devices are inspected daily for malware infection	Malware inspection history
Public Web Server	• Verify additional authentication methods other than ID and password to user accounts.	Additional authentication history
	• Verify critical information, such as user information, is stored and managed in DMZ.	Device access logs
Internal User Password	• Verify internal users set or operate password.	Security measures history
	• Verify passwords are encrypted.	Security measures history
General User Password	• Verify user passwords in the information processing system or electronic data are encrypted.	Account management history
User Notices	• Verify notice, such as risks of password leakage, is announced.	Notice history
	• Verify notice of user protection policy is announced.	Notice history
	• Verify notice of electronic infringement prevention such as hacking and phishing is announced.	Notice history
E- financial Incident Report	• Verify electronic infringement incident is reported and taken action.	Report history

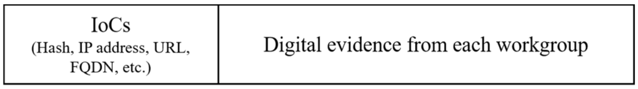

IoCs
(Hash, IP address, URL, FQDN, etc.)
Digital evidence from each workgroup

FIGURE 6. **Probe Structure for Forensic Logging.**

work group can be stored in Forensic Logging which is a centralized storage space.

6) DFR CMMI PLAN

Capability maturity model integration (CMMi) plan is the stage to thoroughly evaluate the level of K-FFRaaS. Currently, there are many researches to evaluate DFR. However, most models are intended for examining the DFR of individual systems, and there is no standardized model to assess the readiness for the entire enterprise [106]. The self-assessment maturity model for financial company, as described by Englbrecht's (2020) [107], is adopted in this research. Because K-FFRaaS is composed of 11 processes at each stage, the level of maturity can be determined by reckoning the capability of each process via the process mining techniques, such as the conformance checking [108].

Each process capability of CMMi can be evaluated into four levels, namely: incomplete, performed, managed, completely defined (see Table 4). Level 0 (incomplete) is when the process is not executed or is temporarily executed. Level 1 (performed) is the phase that there is not a complete set of practices in place; however, it refers to the state in which each process has been performed according to its intended purpose. In Level 2 (managed), there is a full set of processes in place that specifically address improvement in the practice area. Level 3 (completely defined) is the phase that the corporate has the organizational standard to both achieve organizational performance objectives and continually improve the model [109].

TABLE 4. **The capability level of CMMi for K-FFRaaS.**

Level	Description
0 - Incomplete	• Processes to implement the K-FFRaaS are either not running or are running partially.
1 - Performed	• Each process of the K-FFRaaS has performed necessary tasks.
2 - Managed	• The process of the K-FFRaaS is effectively managed, reviewed, and monitored by the business manager based on a separate policy.
3 – Completely Defined	• here are standard guidelines related to the process of configuring K-FFRaaS and is constantly improved and supplemented.

In the maturity stage of CMMi, the level of maturity for K-FFRaaS can be determined by means of evaluating the capability of each process. As shown in Table 5, the level of maturity is composed of five levels according to the CMMi level criteria [110], namely: initial, managed, defined, quantitatively managed, and optimized. The initial level is the

TABLE 5. **The maturity level of CMMi for K-FFRaaS.**

Level	Description
1 - Initial	• An organization that does not have a process for configuring K-FFRaaS. • As it does not have a structured K-FFRaaS configuration process, the organization has no choice but to respond on an ad hoc basis.
2 - Managed	• An organization that has the basic processes that make up K-FFRaaS. • It has a minimally structured process management framework.
3 - Defined	• An organization with documented processes, tools and technologies to manage the processes that make up K-FFRaaS. • It has a standard process at the organizational level and reviews and improves process activities, progress status, and results.
4 - Quantitatively Managed	• An organization where the process constituting K-FFRaaS is quantitatively managed and is continuously improved and supplemented. • Process performance can be predicted quantitatively, the cause can be identified, and corrective action can be taken.
5 - Optimized	• Based on the performance change of K-FFRaaS processes, an organization continuously improves the model for its purpose. • Organizational requirements and legal reviews are ceaselessly reviewed and supplemented by introducing new technologies from a digital forensic perspective.

starting point for processes, which are new and often undocumented for K-FFRaaS; hence, the organization responds in an ad-hoc manner. The managed level is focused on the management of requirements, processes, and services. The defined level is that processes are well-defined and documented in standards [111]. The quantitatively managed level represents that the company is quantitatively managing the processes constituting K-FFRaaS. Finally, the optimized level is that the financial company carries out the process innovation activities by promoting new technology to improve the process capability consistent with its objective.

C. PLANNING PROCESSES GROUP FOR K-FFRAAS

1) DIGITAL ASSETS IDENTIFICATION IMPLEMENTATION

The financial company needs to separate and manage the authority of the work manager. For example, Barings Bank, the UK's oldest commercial bank, went bankrupt due to insider misconduct, such as a failure of internal control of the person in charge [56]. Article 26 of EFSR requires the separation of duties to prevent incidents that may occur due to the manager performing several duties simultaneously: ① Programmer and operator, ② Application programmer and system programmer, ③ System security manager and system programmer, ④ Computer data manager (librarian) and other work manager, ⑤ Work operator and internal auditor, ⑥ Internal personnel and external personnel including electronic financial assistants and maintenance companies, ⑦ Information technology personnel and information protection personnel, ⑧ Requirements of separation of duties concerning internal control. Thus, it is clear for the work managers to be loosely coupled. Subsequently, the work groups and the work managers should operate separately. So, after formalizing a loose coupling, it can be reflected in K-FFRaaS model [101].

The work manager is composed of $\{WM_1, WM_2, \ldots, WM_m\}\,(m \geq 1)$ and the work group is composed of $\{WG_1, WG_2, \ldots, WG_n\}\,(n \geq 1)$. In this study, 11 work groups are identified, namely: Computer room, Device, Electronic data, Information processing system, Anti-hacking measures, Malicious code, Public web server, Internal user password, General user password, User notices, and Electronic financial incident report. So, the range of n is $1 \leq n \leq 11$. If i work manager and j work group have mutual independence, they are loosely coupled and are expressed as follows.

$$Set(WM_i, WG_j) \tag{1}$$

The set has two properties namely WM_i and WG_j which are independent of each other. Also, the properties consisting of the set can be expressed as follows.

$$WM_i \cap WM_j = \emptyset (0 \leq i, j \leq m, i \neq j) \tag{2}$$

$$WG_i \cap WG_j = \emptyset (0 \leq i, j \leq n, i \neq j) \tag{3}$$

The properties show that i and j work managers are independent and not affecting each other. And i and j work groups are also independent. The set consisted of the work manager and the work group is the loose coupling. Even if it is expanded into multiple sets, the independence between the sets will be maintained, resulting in the same coupling condition. This can be expressed as follows.

$$Set\left(WM_{i1}, WG_{j1}\right) \cap\ Set\left(WM_{i2}, WG_{j2}\right) = \emptyset \tag{4}$$

where

$$0 \leq i, j \leq m, i \neq j \tag{5}$$

If the sets are connected by the loose coupling during constructing K-FFRaaS, they don't affect each other. For example, provided that the sets of the computer room (cr) and the information system (is) are independent, they are constructed as the loose coupling and can be described as $Set\,(WM_{cr}, WG_{cr}) \cap\ Set\,(WM_{is}, WG_{is}) = \emptyset$.

The organization that focuses on security could consider DF regardless of the size of the financial company [45]. However, there may be cases according to the size of the financial company that several managers are assigned to one work group in the large-sized banks or that one manager is in charge of all work groups in the small-sized savings bank. When each manager is designated and responsible to handle the individual work group, the separation of duties can be considered appropriate. If not, despite Article 26 of EFSR, FSS can recommend to the financial company to separate the manager's work.

$$S_{kl} = \begin{cases} \emptyset & if\ k = l \\ WM_{k1} \cap WM_{k2} & otherwise\ k \neq l \end{cases} \tag{6}$$

where

$$S_{kl} = Set\left(WM_{k1}, WG_{j1}\right) \cap\ Set\left(WM_{l2}, WG_{j2}\right), 0 \leq j \leq m \tag{7}$$

When $k = l$, independence of the set can be guaranteed and when $k \neq l$, duplicate work managers can be extracted. For example, there would be cases that the information system of small-sized financial company, such as savings bank and asset management company, can be managed by one IT engineer. In this case, it can be considered as weak loose coupling. On the other hand, in the case of large-sized financial company, such as banks, a large number of IT engineers divide and manage each work group. If then, the separation of duties is well regulated by the company itself, and it is considered as a strong loose coupling. If there is the weak loose coupling, FSS may recommend that the duties be separated for the safe management of the computer system.

2) BUSINESS SCENARIO IMPLEMENTATION

The risk assessment methodology [112] complies the results of the threat, vulnerability, and impact rating to arrive at a numeric value. The PRs of the business scenarios specified for each work group can be calculated from future threats and vulnerabilities. the PR for each work group [113] can be

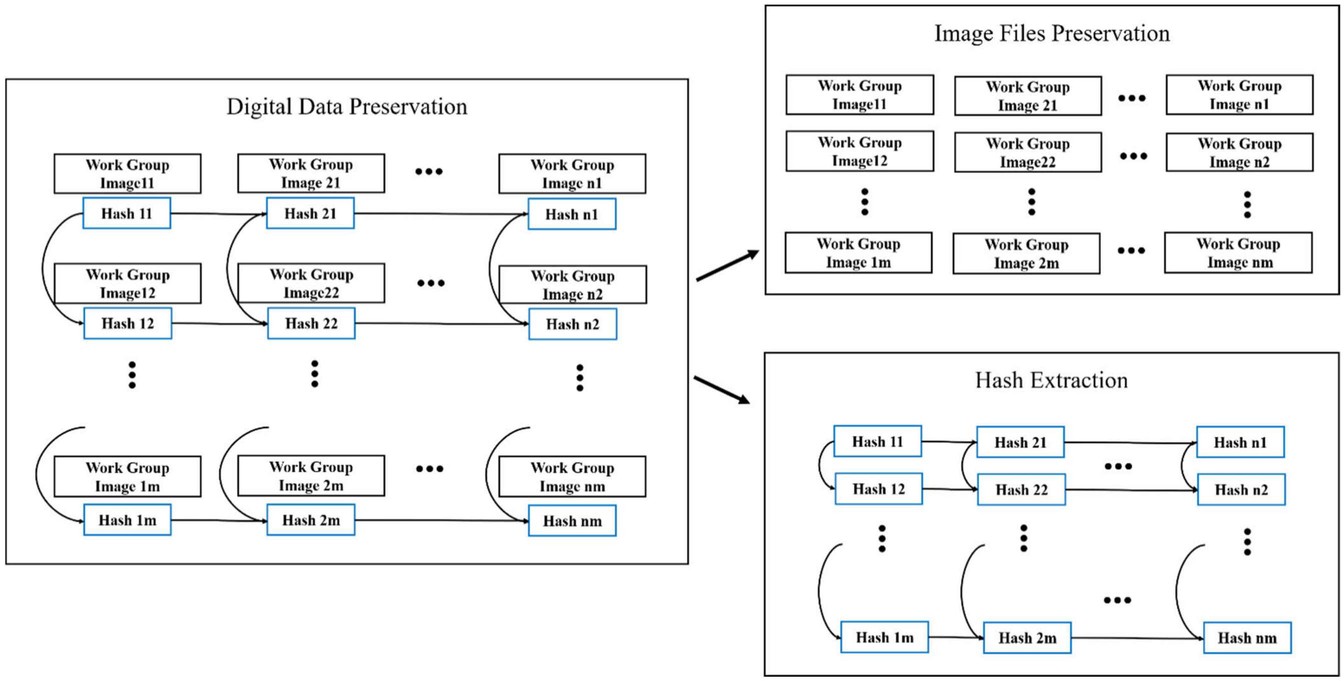


FIGURE 7. Digital Data Preservation.

calculated by predicting threats and vulnerabilities for each scenario within one work group.

$$PR = Threat\ (T) \times Vulnerability\ (V) \times Impact(I) \tag{8}$$

In this formula, Threat and Vulnerability rating can be expressed as RPNNA namely Ready, Partially ready, Not ready, and Not Applicable. The corresponding value is R = 1, P = 0.5, N = 0, and NA. NA does not need to be counted and is excluded from final aggregation [87]. Impact Rating represents the degree of influence within the work group and has a value of 1 when only one scenario is included in one work group. If the work group has two or more scenarios, the value of Impact Rating, $\sum_{i=1}^{n} ImpactRating_i = 1$, is reflected in each scenario. For example, if two scenarios have the same influence in one work group, both scenarios would have an Impact Rating of 0.5.

The PR of each business scenario enables financial companies to identify the PR of each work group. Furthermore, it is possible to expand to the PR of the financial company from 11 PRs of all work groups.

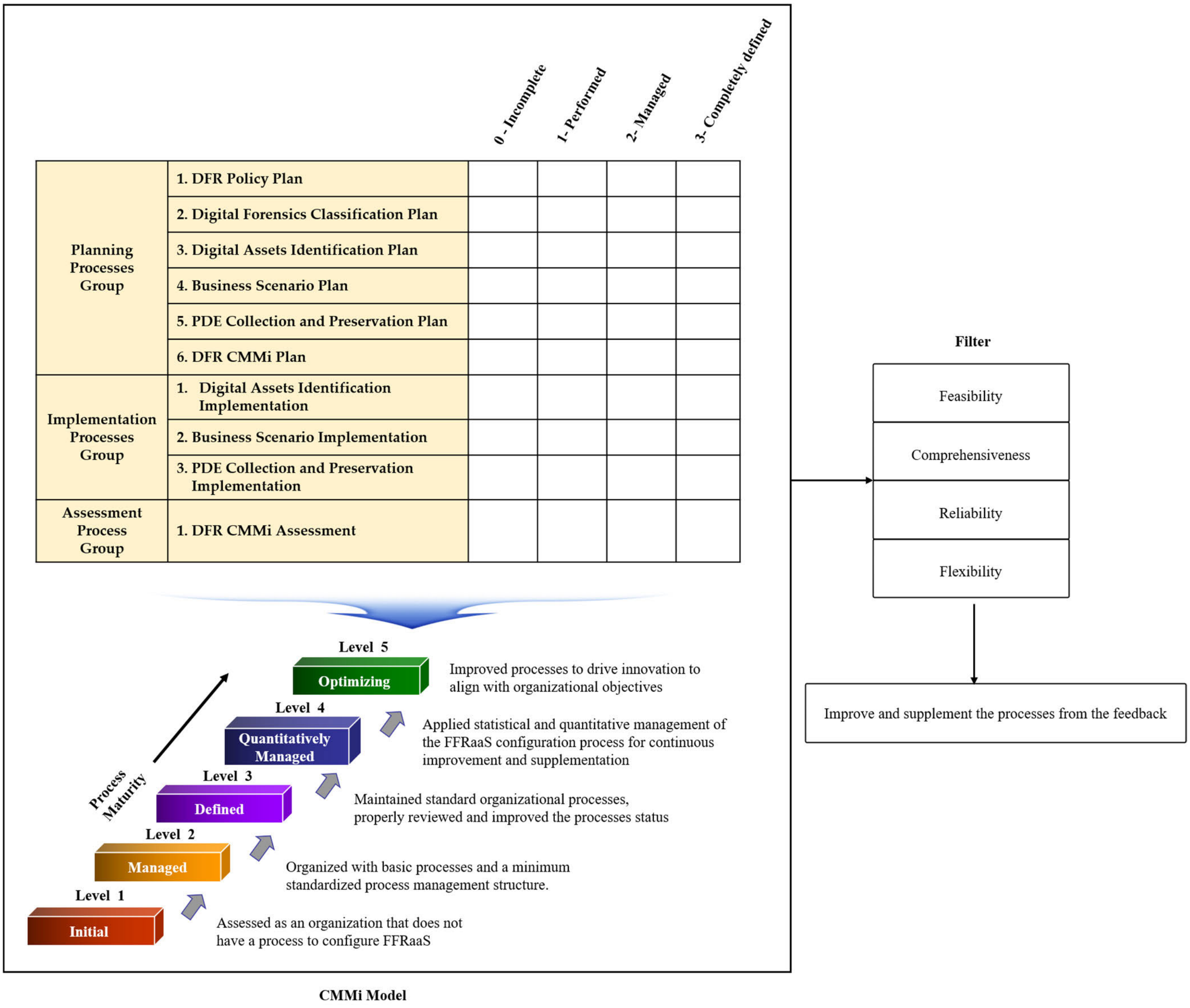
$$PR\ of\ Organization = \sum_{g=1}^{11} \Big(\sum_{s=1}^{n} PR_s\Big)_g \tag{9}$$

The financial company can calculate PR referring to the business scenario items specified in Table 3 regardless of its size. So, the PR for each financial company is evaluated and each financial sector, such as banks, securities, and insurance, can be compared with its peers. The 11 PRs of the work groups can be taken into account as the PR of the financial company. Because the nature of risk quantified by the probability can be identified using the Bayesian Network [90], the financial company will be able to respond to the threats and vulnerabilities by finding expugnable parts. Additionally, the risk level of each work group allows the financial company to evaluate the K-FFRaaS of the entire organization. Threats and vulnerabilities of each financial company can be measured by using their business scenarios. Hence, regular training and testing will be required to assess risks to prepare for potential losses and threats. And then the financial company will be able to come up with improvement and supplementary measures.

3) PDE COLLECTION AND PRESERVATION IMPLEMENTATION

One of the main considerations of proactive forensics is where to store the data for a centralized repository that can be easily accessed by digital forensic investigators [114]. Additionally, business continuity and incident response plans can be established in the case of the occurrence of electronic financial incidents [115], and according to these plans, major financial data will regularly be backed up to a location that won't be impacted by disaster. The managers for the 11 work groups can record and handle the stored data classified in Table 3. The financial data that need to be stored for preservation period [6] according to EFSR are included in Forensic logging and managed as PDE. And it can be used as evidence in the future.

This stage entails the pre-processing to safely transfer and save data, such as electronic financial transaction records and computer system log records, to the storage in accordance



		0 - Incomplete	1- Performed	2- Managed	3- Completely defined
Planning Processes Group	1. DFR Policy Plan				
	2. Digital Forensics Classification Plan				
	3. Digital Assets Identification Plan				
	4. Business Scenario Plan				
	5. PDE Collection and Preservation Plan				
	6. DFR CMMi Plan				
Implementation Processes Group	1. Digital Assets Identification Implementation				
	2. Business Scenario Implementation				
	3. PDE Collection and Preservation Implementation				
Assessment Process Group	1. DFR CMMi Assessment				

Level 5 Optimizing: Improved processes to drive innovation to align with organizational objectives

Level 4 Quantitatively Managed: Applied statistical and quantitative management of the FFRaaS configuration process for continuous improvement and supplementation

Level 3 Defined: Maintained standard organizational processes, properly reviewed and improved the processes status

Level 2 Managed: Organized with basic processes and a minimum standardized process management structure.

Level 1 Initial: Assessed as an organization that does not have a process to configure FFRaaS

Filter: Feasibility, Comprehensiveness, Reliability, Flexibility

Improve and supplement the processes from the feedback

FIGURE 8. Feedback process via DFR CMMi.

with relevant laws and regulations [116]. DE should satisfy rigorous requirements in such a way that it can be presented as digital evidence to be admissible in a court of law [88]. Currently, when the financial company backs up the data and keeps it separately, it is stored in the form of raw data without any measures to preserve data integrity. Thus, the basic requirements of evidence, such as identity and integrity, are not guaranteed. Therefore, in the data preservation stage, we proposed the method for converting raw data to the logical image files and preserving them to be more efficient for data recovery [117]. The backup files cannot be tampered because hash signatures are attached to the file [118], thereby ensuring the integrity and identity of PDE.

Figure 7 shows a conceptual image of how to manage backup files for each work group image with the hash value. The contents of creating image files are illustrated when m backups occur for n work groups. Because files for each work group are backed up at each retention time point, the backup files can be converted into image file and be preserved for use in the future. After imaging the files for each unit task, the hash value can be extracted and be managed in separate databases [9], [119] so that it can be used promptly, when and if needed. Additionally, because the backup files exist standalone, there is a possibility of tampering with evidence. So, this study presents that the file hash values at the previous and current time steps can be configured in the form of chain link. For example, Hash 12 is calculated by including the value of Hash 11, and Hash 13 by the value of Hash 12. When backing up files by point in time, a hash value at the time of backup is generated referring to the hash value of

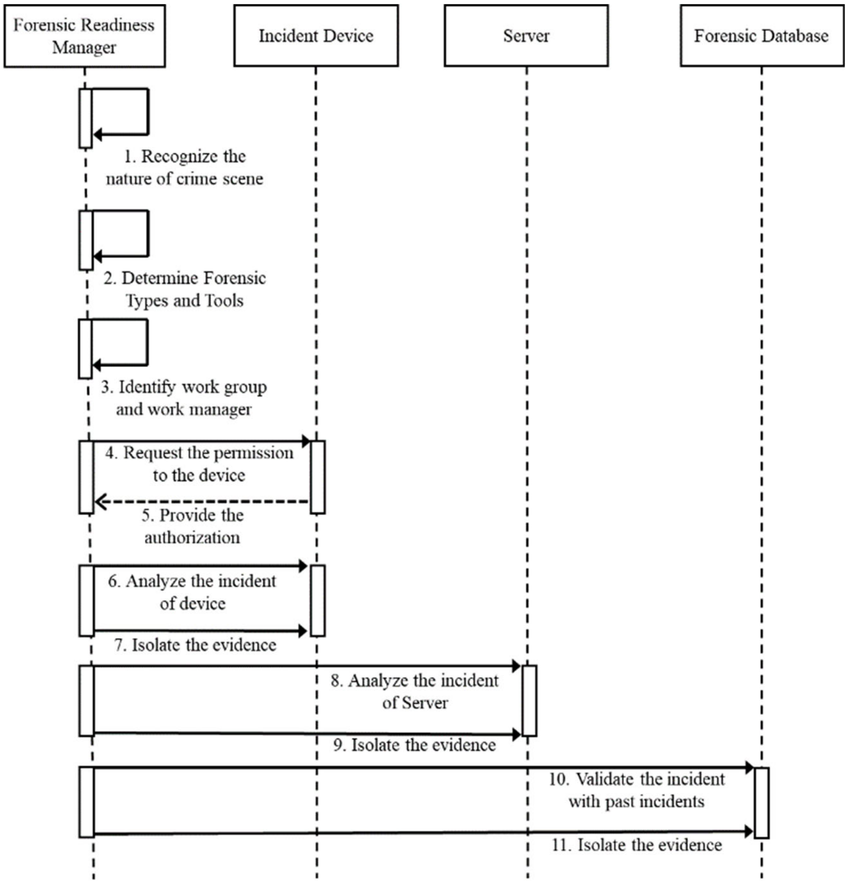

Forensic Readiness Manager
Incident Device
Server
Forensic Database
1. Recognize the nature of crime scene
2. Determine Forensic Types and Tools
3. Identify work group and work manager
4. Request the permission to the device
5. Provide the authorization
6. Analyze the incident of device
7. Isolate the evidence
8. Analyze the incident of Server
9. Isolate the evidence
10. Validate the incident with past incidents
11. Isolate the evidence

FIGURE 9. Procedural flow for K-FFRaaS.

the previous time. Accordingly, it is possible to record and manage the hash value for the entire backup data, thereby further enhancing the integrity of the digital data. Henceforth, for the security of the database, the hash value stored in the database will need to be encrypted and be managed such that only authorized users are allowed to access it [120].

Finally, regarding ISO/IEC 27043:2015, the documentation of PDE is normally not included in the DFR model. The investigative processes class includes the documentation for the submission of DE by DF jobs. But it is necessary for the investigator to facilitate the documentation to promptly collect the evidence and indicate the direction of investigation. In this study, we add the documentation to this process for systematic management of collecting and preserving PDE. This paper thus attempts to examine what needs to be added to the documentation.

First, the scope of DFI should be described in terms of each work group. Although data are regularly backed up at locations which is isolated from the main business center in the case of a disaster, PDE for unexpected cases needs to be recorded and managed in the context of an investigation other than DE for regular occurrence. Furthermore, the reliability and expertise are required, in addition to identity and integrity, for ensuring the admissibility of DE to prove the allegation. Therefore, it is necessary to document and manage various tools, technologies, and methodologies for digital data analysis depending on the type of work group. Additionally, because the operator expertise is also the important factor, it should be possible to prove that the qualified expert capable of performing DF continuously manages DF. One of the main contents included in documentation is the priority of preserved data according to importance. After distinguishing the relevant and irrelevant PDE [18] from Forensic logging, there is a need to systematically manage major considerations that DF experts would consider first in the event of an incident by referring to each characteristic of the work groups and designating the relevant PDE [81].

D. ASSESSMENT PROCESS GROUP FOR K-FFRAAS

1) DFR CMMI ASSESSMENT

Figure 8 presents the model to assess the maturity level by using the CMMi of K-FFRaaS. After calculating the capabilities for 10 processes and reflecting them to the maturity level of the K-FFRaaS, the maturity level for the company can be derived. The level of K-FFRaaS of each company can be evaluated, managed, and improved.

After evaluating the result of CMMi, a feedback can be given to the processes that needs to be supplemented. Because the feedback should be in line with the direction pursued by K-FFRaaS, it can be checked via the filter before being passed on to the corresponding process. The filter consists of four factors: Feasibility, Comprehensiveness, Reliability, and Flexibility [121]. Feasibility is that the feedback should be provided as a requirement to minimize the cost for K-FFRaaS. In other words, the feedback that requires excessive costs to improve K-FFRaaS should be excluded. Comprehensiveness is that the feedback should be considered as the relevant operations of K-FFRaaS without collecting the irrelevance. Reliability needs to check whether the feedback is for the purpose of providing forensically sound evidence. Finally, unlike other forensic sciences, DF subject matter keep evolving, as do the techniques [122]. Flexibility should be provided in a way that it can reflect the growing new technologies. As long as all four of these requirements are met, the feedback is passed through the filter and moved to the process in need of improvement.

IV. DIGITAL FORENSICS INVESTIGATION

This section will briefly explain how it can be deployed by the financial company. The forensic readiness manager should conduct the forensic investigation to uncover what happened or the root cause of the problem when the electronic financial incident [49], such as data corruption, leakage, alteration, and other attacks, occurs. Figure 9 shows the sequential diagram for K-FFRaaS model. After the incident, the forensic readiness manager first recognizes the nature of crime scene and determines the type of digital forensic and related tools according to Digital Forensics Classification. After identifying the work group and the work manager of the computer system via Digital Assets Identification, the forensic readiness manager requests the permission to access the data and acquires the authorization of the device. Then, the forensic readiness manager investigates both digital devices and servers according to due process, to acquire admissible DE from PDE Collection and Preservation. If the data cannot be checked at the time of the alleged crime on the currently running server, DE could be acquired by restoring the backup data [123].

V. CONCLUSION AND FUTURE WORK

After the amendments of EFTA by Financial Services Commission in Korea, the burden of proving electronic financial incident will be transferred to the financial company. And hence there is a need for financial company to be equipped with the DFR to identify the root cause of incident and to acquire DE to be admissible in a court of law. The main goal of this paper is to develop K-FFRaaS as DFR model for the financial company.

This study lays the foundation for future work on K-FFRaaS. In summary, the K-FFRaaS is proposed by referring to readiness processes class of ISO/IEC 27043:2015. First, we suggested the policy and procedure of K-FFRaaS as DFR for financial company in Korea. Based on the information security check items of the financial company, 11 work groups as main targets are identified. And digital forensics classification criteria is set up in consideration of the computer systems of the financial company. We acquire a list of digital files that can be used as evidence in a court of law by designating business scenarios for 11 work groups and present the integrity management plan for collecting and preserving PDE. Finally, by introducing the CMMi model, the way to evaluate and manage the level of K-FFRaaS is proposed. A concrete suggestion of K-FFRaaS is provided and reflected with the support of ISO/IEC 27043:2015.

K-FFRaaS enables the financial company to maximize the capability to efficiently collect DE to be admissible in the court and minimize the investigation cost. Because the financial company promptly conduct the investigation to proactively collect the admissible DE through K-FFRaaS, K-FFRaaS mitigates the damage of reputation and make it easy with less hassles to retrieve available DE.

What remains to be determined by future research is the experiment that deal with the real-world implementation. The financial company needs to implement countermeasures to preserve and protect personal information and financial transaction information. Because the information can be used as PDE in the future, the evidence preservation measures unique to financial company need to be suggested by referring to the Sedona Conference's Commentary. Additionally, the above-mentioned Forensic Logging can be used only for the analysis of one case while the method of creating the context between several cases over time is not offered. So, case management system will be useful for the holistic documentation and management of the cases [124]. And this paper did not specifically deal with concurrent process. It is to be hoped that a plan to systematically manage the entire DFR model can be suggested as a blueprint for the detailed design of K-FFRaaS model by developing a DFR model management system [125] and adding it to the concurrent process in the future.

Because the protection measures specified in EFSR are equally applied to the financial company, it is necessary to propose a detailed K-FFRaaS to be standardized and managed. Even if the security of the financial company can be considered stronger than that of non-financial company in accordance with EFSR, the financial company needs to be equipped with K-FFRaaS to minimize potential disputes over no-fault liability proof. Thus, it is necessary to legislate a plan to establish a mandatory DFR [126] to related laws and regulations to tighten security controls.

REFERENCES

[1] *Comprehensive Digital Finance Innovation Plan in the 4th Industrial Revolution Era*, Financial Services Commission, Seoul, South Korea, Jul. 2020.

[2] (Mar. 18, 2021). *Recent Developments in Korea's Fintech Industry. Chambers and Partners*. [Online]. Available: https://practiceguides.chambers.com/practice-guides/fintech-2021/south-korea/trends-and-developments

[3] R. A. McFeely, "Cyber security: Preparing for and responding to the enduring threat," Federal Bureau of Investigation (FBI), Washington, DC, USA, Tech. Rep., 2013.

[4] D. H. Kim and D. W. Joa, *Financial Companies 'Targeted by DDoS'*, Korea Economic Daily, Seoul, South Korea, 2021.

[5] M. Y. Park, "Is your finance safe? E-banking without a safe zone," in *Boan News*. Security World, 2020.

[6] *Guideline for Incident Response Readiness in Financial Businesses*, Financial Security Institute, Seoul, South Korea, 2016.

[7] J. K. Kang, "After loosening regulations due to COVID-19.. Financial security loopholes revealed," in *Digital Today*. 2021.

[8] M. Reggiani. (2016). *A Brief Introduction to Forensic Readiness*. INFOSEC. [Online]. Available: https://resources.infosecinstitute.com/topic/a-brief-introduction-to-forensic-readiness/

[9] S. M. Makura, H. S. Venter, R. A. Ikuesan, V. R. Kebande, and N. M. Karie, "Proactive forensics: Keystroke logging from the cloud as potential digital evidence for forensic readiness purposes," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Feb. 2020, p. 200.

[10] J. Hermans, H. W. Tinholt, and J. D. Wit, "Achieving digital forensic readiness," in *Point of View Forensic Readiness*. Amstelveen, Netherlands: KPMG, 2015.

[11] *Digital Continuity to Support Forensic Readiness*, Richmond, U.K.: National Archives, 2011.

[12] J. Tan, *Forensic Readiness*. Cambridge, MA, USA: @ Stake, 2001, pp. 2–23.

[13] S. P. Lee, "Some proposals for improvement of digital forensics," *Sogang Law Rev.*, vol. 10, no. 2, pp. 139–178, 2008.

[14] R. Parlour, S. Bouyon, and S. Krause, "Cybersecurity in finance getting the policy mix right," Eur. Credit Res. Inst., Rep. CEPS-ECRI Task Force, Jun. 2018.

[15] S. Zawoad, A. K. Dutta, and R. Hasan, "SecLaaS: Secure logging-as-a-service for cloud forensics," presented at the ASIA CCS 8th ACM SIGSAC Symp. Inf., Comput. Commun. Secur., 2013.

[16] S. Nanda and R. A. Hansen, "Forensics as a service: Three-tier architecture for cloud based forensic analysis," in *Proc. 15th Int. Symp. Parallel Distrib. Comput. (ISPDC)*, Jul. 2016, pp. 178–183.

[17] B. K. Raju, B. Moharil, and G. Geethakumari, "FaaSeC: Enabling forensics-as-a-Service for cloud computing systems," presented at the 9th IEEE/ACM Int. Conf. Utility Cloud Comput., 2016.

[18] V. R. Kebande and H. S. Venter, "CFRaaS: Architectural design of a cloud forensic readiness as-a-service model using NMB solution as a forensic agent," *Afr. J. Sci., Technol., Innov. Develop.*, vol. 11, no. 6, p. 749, 2019.

[19] M. Chernyshev, S. Zeadally, and Z. Baig, "Healthcare data breaches: Implications for digital forensic readiness," *J. Med. Syst.*, vol. 43, no. 1, p. 7, Jan. 2019.

[20] S. Y. Lee, "The admissibility of digital evidence–the status of identity and integrity in assessing the admissibility of digital evidence and the interpretation of article 313 of the amended criminal procedure act," *Justice*, vol. 161, pp. 164–199, Apr. 2017. [Online]. Available: http://www.riss.kr/link?id=A103308765

[21] G. Palmer, "A road map for digital forensic research," presented at the Digit. Forensic Res. Conf., 2001.

[22] J. Sachowski and J. Sachowski, *Implementing Digital Forensic Readiness: From Reactive to Proactive Process*. Boca Raton, FL, USA: CRC Press, 2019.

[23] *International Standard, Information Technology–Security Techniques–Incident Investigation Principles and Processes*, Standard ISO/IEC 27043, 2015.

[24] V. R. Kebande and H. S. Venter, "On digital forensic readiness in the cloud using a distributed agent-based solution: Issues and challenges," *Austral. J. Forensic Sci.*, vol. 50, no. 2, pp. 209–238, Mar. 2018.

[25] US-CERT. *Computer Forensics*. Accessed: Sep. 20, 2021. [Online]. Available: https://us-cert.cisa.gov/sites/default/files/publications/forensics.pdf

[26] E. Casey, *Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet*. Burlington, MA, USA: Academic, 2011.

[27] I. R. Adeyemi, S. A. Razak, and N. A. N. Azhan, "A review of current research in network forensic analysis," *Int. J. Digit. Crime Forensics*, vol. 5, no. 1, pp. 1–26, Jan. 2013.

[28] M. S. Noh and M. H. Baek, *Digital Forensics*. Seoul, South Korea: Gosigye, 2018.

[29] M. Elyas, S. B. Maynard, A. Ahmad, and A. Lonie, "Towards a systemic framework for digital forensic readiness," *J. Comput. Inf. Syst.*, vol. 54, no. 3, pp. 97–105, 2014.

[30] A. Culley, "Computer forensics: Past, present and future," *Inf. Secur. Tech. Rep.*, vol. 8, no. 2, pp. 32–36, 2003.

[31] S. J. Baek and J. I. Lim, "A study on the forensic readiness as an effective measure for personal information protection," *Internet Inf. Secur.*, vol. 3, no. 2, pp. 34–64, 2012.

[32] A. Soltan, W.-J. Jens, and T. Issa, "The proactive and reactive digital forensics investigation process: A systematic literature review," *Int. J. Secur. Appl.*, vol. 5, no. 4, pp. 59–72, 2011.

[33] G. Pangalos, C. Ilioudis, and I. Pagkalos, "The importance of corporate forensic readiness in the information security framework," in *Proc. 19th IEEE Int. Workshops Enabling Technol., Infrastruct. Collaborative Enterprises*, 2010, pp. 12–16.

[34] C. P. Grobler, C. P. Louwrens, and S. H. von Solms, "A framework to guide the implementation of proactive digital forensics in organisations," in *Proc. Int. Conf. Availability, Rel. Secur.*, Feb. 2010, p. 677.

[35] P. Stephenson, "Conducting incident post mortems," *Comput. Fraud Secur.*, vol. 2003, no. 4, pp. 16–19, Apr. 2003.

[36] P. G. Bradford, M. Brown, J. Perdue, and B. Self, "Towards proactive computer-system forensics," in *Proc. Int. Conf. Inf. Technol.: Coding Comput.*, vol. 2, 2004, pp. 648–652.

[37] L. Pasquale, D. Alrajeh, C. Peersman, T. Tun, B. Nuseibeh, and A. Rashid, "Towards forensic-ready software systems," in *Proc. 40th Int. Conf. Softw. Eng.: New Ideas Emerg. Results*, May 2018, pp. 9–12.

[38] B. Endicott-Popovsky, N. Kuntze, and C. Rudolph, "Forensic readiness: Emerging discipline for creating reliable and secure digital evidence," *J. Harbin Inst. Technol. (New Series)*, vol. 22, no. 1, pp. 99–106, 2015.

[39] F. Mouton and H. S. Venter, "A prototype for achieving digital forensic readiness on wireless sensor networks," in *Proc. IEEE Africon*, Sep. 2011, pp. 1–6.

[40] T. Grobler and B. Louwrens, "Digital forensic readiness as a component of information security best practice," in *IFIP Advances in Information and Communication Technology*, vol. 232. 2007, pp. 13–24.

[41] R. Rowlingson, "A ten step process for forensic readiness," *Int. J. Digit. Evidence*, vol. 2, no. 3, pp. 1–28, 2004.

[42] J. Danielsson and I. Tjostheim, "The need for a structured approach to digital forensic readiness," in *Proc. IADIS Int. Conf. e-Commerce*, Lisbon, Portugal, 2004, pp. 417–421.

[43] C. Taylor, B. Endicott-Popovsky, and D. A. Frincke, "Specifying digital forensics: A forensics policy approach," *Digit. Invest.*, vol. 4, pp. 101–104, Sep. 2007.

[44] D. Barske, A. Stander, and J. Jordaan, "A digital forensic readiness framework for South African SME's," in *Proc. Inf. Secur. South Afr.*, Aug. 2010, pp. 1–6.

[45] M. Elyas, A. Ahmad, S. B. Maynard, and A. Lonie, "Digital forensic readiness: Expert perspectives on a theoretical framework," *Comput. Secur.*, vol. 52, pp. 70–89, Jul. 2015.

[46] A. Valjarevic and H. S. Venter, "Towards a digital forensic readiness framework for public key infrastructure systems," in *Proc. Inf. Secur. South Afr.*, Aug. 2011, pp. 1–10.

[47] C. Lankshear and M. Knobel, *Digital Literacies: Concepts, Policies and Practices*. New York, NY, USA: Peter Lang, 2008.

[48] D. Masvosvere and H. Venter, "A conceptual model for digital forensic readiness in e-supply chains," in *Proc. Eur. Conf. e-Learning*, 2015, pp. 413–422.

[49] S. Makura, H. S. Venter, V. R. Kebande, N. M. Karie, R. A. Ikuesan, and S. Alawadi, "Digital forensic readiness in operational cloud leveraging ISO/IEC 27043 guidelines on security monitoring," *Secur. Privacy*, vols. 4, no. 3, p. e149, May/Jun. 2021, doi: 10.1002/spy2.149.

[50] G. Mohay, "Technical challenges and directions for digital forensics," in *Proc. 1st Int. Workshop Systematic Approaches Digit. Forensic Eng. (SADFE)*, 2005, pp. 155–161.

[51] M. Köhn, J. H. P. Eloff, and M. Olivier, "UML modelling of digital forensic process models (DFPMs)," in *Proc. ISSA*, 2018, pp. 1–13.

[52] A. F. A. Rahman, R. Ahmad, and M. Z. Mohamad, "Developing forensic readiness secure network architecture for wireless body area network (WBAN)," *Int. J. Secur. Its Appl.*, vol. 8, no. 5, pp. 403–420, Sep. 2014.

[53] D. Frincke, "Adding the fourth 'R': A systems approach to solving the hacker's arms race," in *Proc. 39th Hawaii Int. Conf. Syst. Sci. (HICSS)*, Kauai, HI, USA, Jan. 2006.

[54] G. S. Dardick, "Cyber forensics assurance," in *Proc. Austral. Digit. Forensics Conf.*, Farmville, VA, USA: Longwood Univ., 2010.

[55] E. Bajramovic, K. Waed, Y. Gao, and M. Parekh, "Shared responsibility for forensic readiness-related security controls: Prerequisite for critical infrastructure maintenance and supplier relationships," in *Proc. IEEE 17th Int. Conf. Smart Technol. (EUROCON)*, Jul. 2017, pp. 364–369.

[56] A. Mouhtaropoulos, P. Dimotikalis, and C.-T. Li, "Applying a digital forensic readiness framework: Three case studies," in *Proc. IEEE Int. Conf. Technol. Homeland Secur. (HST)*, Nov. 2013, pp. 217–223.

[57] S. Kwon, J. Jeong, and T. Shon, "Digital forensic readiness for financial network," in *Proc. Int. Conf. Platform Technol. Service (PlatCon)*, Jan. 2019, pp. 1–4.

[58] Y. N. Shin and D. K. Lim, "Model and implementation of forensic readiness for privacy protection on cloud service," *Information*, vol. 17, no. 12B, p. 6419, 2014.

[59] L. Duranti and B. Endicott-Popovsky, "Digital records forensics: A new science and academic program for forensic readiness," *J. Digit. Forensics, Secur. Law*, vol. 5, no. 2, pp. 45–62, 2010.

[60] B. Endicott-Popovsky, D. A. Frincke, and C. A. Taylor, "A theoretical framework for organizational network forensic readiness," *J. Comput.*, vol. 2, no. 3, p. 1, May 2007.

[61] A. Agarwal, M. Gupta, S. Gupta, and S. C. Gupta, "Systematic digital forensic investigation model," *Int. J. Comput. Sci. Secur. (IJCSS)*, vol. 5, no. 1, pp. 118–131, 2011.

[62] K. H. Moon, "A design of digital forensic readiness for the protection of trade secret," M.S. thesis, Dept. Forensic, Sungkyunkwan Univ., Seoul, South Korea, 2020.

[63] D. E. Kim and Y. H. Kim, "A study on the readiness of financial company infringement incidents," e-Finance and Financial Security, Financial Secur. Inst., Yongin, Gyeonggi, Tech. Rep., 2017.

[64] B. D. Carrier and E. Spafford, "Getting physical with the digital investigation process," *Int. J. Digit. Evidence*, vol. 2, no. 2, pp. 1–20, 2003.

[65] G. Pangalos, V. Katos, G. Pangalos, and V. Katos, "Information assurance and forensic readiness," in *Proc. Int. Conf. e-Democracy*, 2010, pp. 181–188.

[66] H. Jaehyeok, Y. Yoon, G. Hur, J. Lee, J. Choi, S. Hong, and S. Lee, "Secure file transfer method and forensic readiness by converting file format in network segmentation environment," *J. Korea Inst. Inf. Secur. Cryptol.*, vol. 29, no. 4, pp. 859–866, 2019. [Online]. Available: http://www.riss.kr/link?id=A106342070

[67] A. Johnston and J. Reust, "Network intrusion investigation–Preparation and challenges," *Digit. Invest.*, vol. 3, no. 3, pp. 118–126, 2006.

[68] K. Tam and K. Jones, "Forensic readiness within the maritime sector," in *Proc. Int. Conf. Cyber Situational Awareness, Data Analytics Assessment (Cyber SA)*, Jun. 2019, pp. 1–4.

[69] G. Gojko, B. Ivan, N. Simeunovic, and R. Nenad, "Achieving business excellence by optimizing corporate forensic readiness," *Amfiteatru Econ.*, vol. 19, no. 44, pp. 197–214, 2017.

[70] A. Valjarevic and H. S. Venter, "Implementation guidelines for a harmonised digital forensic investigation readiness process model," in *Proc. Inf. Secur. South Afr.*, Aug. 2013, pp. 1–9.

[71] V. R. Kebande and H. S. Venter, "Adding event reconstruction to a cloud forensic readiness model," in *Proc. Inf. Secur. South Afr. (ISSA)*, Aug. 2015, pp. 1–9.

[72] V. R. Kebande and H. S. Venter, "Novel digital forensic readiness technique in the cloud environment," *Austral. J. Forensic Sci.*, vol. 50, no. 5, pp. 552–591, Sep. 2018.

[73] V. R. Kebande, P. P. Mudau, R. A. Ikuesan, H. S. Venter, and K.-K. R. Choo, "Holistic digital forensic readiness framework for IoT-enabled organizations," *Forensic Sci. Int., Rep.*, vol. 2, Dec. 2020, Art. no. 100117.

[74] D. Y. Kao, "Exploring the cybercrime investigation framework of ATM Heist from ISO/IEC 27043: 2015," presented at the Int. Conf. Adv. Commun. Technol., ICACT, 2017.

[75] C. Grobler and B. Louwrens, "High-level integrated vie of digital forensics," in *Proc. ISSA*, 2009.

[76] D. J. E. Masvosvere and H. S. Venter, "Using a standard approach to the design of next generation e-supply chain digital forensic readiness systems," *SAIEE Afr. Res. J.*, vol. 107, no. 2, pp. 104–120, Jun. 2016.

[77] N. H. Nik Zulkipli and G. B. Wills, "An exploratory study on readiness framework in IoT forensics," *Proc. Comput. Sci.*, vol. 179, pp. 966–973, Jan. 2021.

[78] P. M. Trenwith and H. S. Venter, "Digital forensic readiness in the cloud," in *Proc. Inf. Secur. South Afr.*, Aug. 2013, pp. 1–5.

[79] A. Valjarevic and H. S. Venter, "Introduction of concurrent processes into the digital forensic investigation process," *Austral. J. Forensic Sci.*, vol. 48, no. 3, pp. 339–357, May 2016.

[80] V. R. Kebande, N. M. Karie, K. R. Choo, and S. Alawadi, "Digital forensic readiness intelligence crime repository," *Secur. Privacy*, vol. 4, no. 3, pp. 1–11, May 2021.

[81] N. M. Karie, V. R. Kebande, H. S. Venter, and K.-K.-R. Choo, "On the importance of standardising the process of generating digital forensic reports," *Forensic Sci. Int., Rep.*, vol. 1, Nov. 2019, Art. no. 100008.

[82] C. Alexakos, C. Katsini, K. Votis, A. Lalas, D. Tzovaras, and D. Serpanos, "Enabling digital forensics readiness for internet of vehicles," *Transp. Res. Proc.*, vol. 52, pp. 339–346, Apr. 2021.

[83] K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," *Comput. Secur.*, vol. 105, Jun. 2021, Art. no. 102237.

[84] CYFOR. *Specialists in Organisational Forensic Readiness Planning and Implementation*. Accessed: Jun. 29, 2021. [Online]. Available: https://cyfor.co.uk/corporate-forensic-investigations/forensic-readiness-planning/

[85] N. Serketzis, V. Katos, C. Ilioudis, D. Baltatzis, and G. J. Pangalos, "A socio-technical perspective on threat intelligence informed digital forensic readiness," *Int. J. Syst. Soc.*, vol. 4, no. 2, pp. 57–68, Jul. 2017.

[86] S. Yong-Nyuo, "Implementation privacy reference architecture for forensic readiness," *Int. J. Fuzzy Logic Intell. Syst.*, vol. 12, no. 1, pp. 53–58, 2012.

[87] F. Gunawan and S. Yazid, "Improving digital forensic readiness in DevOps context: Lessons learned from XYZ company," in *Proc. Int. Seminar Appl. for Technol. Inf. Commun. (iSemantic)*, Sep. 2020, pp. 459–463.

[88] R. McKemmish, "When is digital evidence forensically sound?" in *Proc. IFIP Int. Conf. Digit. Forensics*, 2008, p. 3–15.

[89] A. Valjarevic and H. S. Venter, "Harmonised digital forensic investigation process model," in *Proc. Inf. Secur. South Afr.*, Aug. 2012, pp. 1–10.

[90] A. Mouhtaropoulos, M. Grobler, and C.-T. Li, "Digital forensic readiness: An insight into governmental and academic initiatives," in *Proc. Eur. Intell. Secur. Informat. Conf.*, Sep. 2011, pp. 191–196.

[91] B. K. S. P. K. Raju and G. Geethakumari, "An advanced forensic readiness model for the cloud environment," in *Proc. Int. Conf. Comput., Commun. Autom. (ICCCA)*, Apr. 2016, pp. 765–771.

[92] S. Park, Y. Kim, G. Park, O. Na, and H. Chang, "Research on digital forensic readiness design in a cloud computing-based smart work environment," *Sustainability*, vol. 10, no. 4, p. 1203, Apr. 2018.

[93] A. Alenezi, R. K. Hussein, R. J. Walters, and G. B. Wills, "A framework for cloud forensic readiness in organizations," in *Proc. 5th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*, Apr. 2017, pp. 199–204.

[94] A. Alenezi, H. F. Atlam, and G. B. Wills, "Experts reviews of a cloud forensic readiness framework for organizations," *J. Cloud Comput.*, vol. 8, no. 1, pp. 1–14, Dec. 2019.

[95] B. Carrier, "Defining digital forensic examination and analysis tools," presented at the Digit. Forensic Res. Conf., 2002.

[96] T. Wu, F. Breitinger, and S. O'Shaughnessy, "Digital forensic tools: Recent advances and enhancing the status quo," *Forensic Sci. Int., Digit. Investigation*, vol. 34, Sep. 2020, Art. no. 300999.

[97] A. Pooe and L. Labuschagne, "A conceptual model for digital forensic readiness," in *Proc. Inf. Secur. South Afr.*, Aug. 2012, pp. 1–8.

[98] A. Kyaw, B. Cusack, and R. Lutui, "Digital forensic readiness in wireless medical systems," in *Proc. 29th Int. Telecommun. Netw. Appl. Conf. (ITNAC)*, Nov. 2019, pp. 1–6.

[99] M. I. Ali and S. Kaur, "Next-generation digital forensic readiness BYOD framework," *Secur. Commun. Netw.*, vol. 2021, pp. 1–19, Mar. 2021.

[100] *Explanation of Electronic Finance Supervision Regulations*, Financial Supervisory Service, Seoul, South Korea, 2017.

[101] G. Chunye, L. Jie, Z. Qiang, C. Haitao, and G. Zhenghu, "The characteristics of cloud computing," in *Proc. 39th Int. Conf. Parallel Process. Workshops (ICPPW)*, Sep. 2010, pp. 275–279.

[102] *Detailed Regulations on Supervision of Electronic Finance*, Financial Supervisory Service, Seoul, South Korea, 2019.

[103] G. Sibiya, T. Fogwill, H. S. Venter, and S. Ngobeni, "Digital forensic readiness in a cloud environment," in *Proc. Africon*, Sep. 2013, pp. 1–5.

[104] N. Serketzis, V. Katos, C. Ilioudis, D. Baltatzis, and G. J. Pangalos, "Actionable threat intelligence for digital forensics readiness," *Inf. Comput. Secur.*, vol. 27, no. 2, pp. 273–291, Jun. 2019.

[105] F. R. Van Staden and H. S. Venter, "Adding digital forensic readiness to electronic communication using a security monitoring tool," in *Proc. Inf. Secur. South Afr.*, Aug. 2011, pp. 1–5.

[106] M. P. Makutsoane and A. Leonard, "A conceptual framework to determine the digital forensic readiness of a cloud service provider," in *Proc. Conf.: Portland Int. Center Manage. Eng. Technol.; Infrastruct. Service Integr.*, Jul. 2014, pp. 3313–3321.

[107] L. Englbrecht, G. Pernul, and S. Meier, "Towards a capability maturity model for digital forensic readiness," *Wireless Netw.*, vol. 26, no. 7, pp. 4895–4907, 2020.

[108] L. Daubner, M. MacAk, B. Buhnova, and T. Pitner, "Verification of forensic readiness in software development: A roadmap," presented at the ACM Symp. Appl. Comput., 2020.

[109] S. K. White. *What is CMMI? A Model for Optimizing Development Processes*. CIO FROM IDG. Accessed: Jun. 26, 2021. [Online]. Available: https://www.cio.com/article/2437864/process-improvement-capability-maturity-model-integration-cmmi-definition-and-solutions.html

[110] M. B. Chrissis, *CMMI: Guidelines for Process Integration and Product Improvement*. Upper Saddle River, NJ, USA: Addison-Wesley, 2007.

[111] S. K. White. *CMMI Maturity Levels: A Guide to Optimizing Development Processes*. CIO FROM IDG. Accessed: Jun. 25, 2021. [Online]. Available: https://www.cio.com/article/3304245/cmmi-maturity-levels-a-guide-to-optimizing-development-processes.html

[112] *FEMA 452 Risk Assessment: A How-to Guide to Mitigate Potential Terrorist Attacks Against Buildings*, Federal Emergency Management Agency, Washington, DC, USA, 2005.

[113] C. Liu, C.-K. Tan, Y.-S. Fang, and T.-S. Lok, "The security risk assessment methodology," *Proc. Eng.*, vol. 43, pp. 600–609, Jan. 2012.

[114] J.-L. Kruger and H. Venter, "Requirements for IoT forensics," in *Proc. Conf. Next Gener. Comput. Appl. (NextComp)*, Sep. 2019, pp. 1–7.

[115] A. Mouhtaropoulos, C.-T. Li, and M. Grobler, "Digital forensic readiness: Are we there yet," *J. Int. Commercial Law Technol.*, vol. 9, no. 3, pp. 173–179, 2014.

[116] V. R. Kebande, N. M. Karie, and H. S. Venter, "A generic digital forensic readiness model for BYOD using honeypot technology," in *Proc. IST-Africa Week Conf.*, May 2016, pp. 1–12.

[117] G. Grispos, T. Storer, and W. B. Glisson, "A comparison of forensic evidence recovery techniques for a Windows mobile smart phone," *Digit. Invest.*, vol. 8, no. 1, pp. 23–36, Jul. 2011.

[118] A. Singh, A. R. Ikuesan, H. S. Venter, A. Singh, A. R. Ikuesan, and H. S. Venter, "Digital forensic readiness framework for ransomware investigation," in *Proc. Int. Conf. Digit. Forensics Cyber Crime*, 2019, pp. 91–105.

[119] I. Kigwana and H. S. Venter, "A digital forensic readiness architecture for online examinations," *South Afr. Comput. J.*, vol. 30, no. 1, pp. 1–39, Jul. 2018.

[120] M. Mohlala, A. R. Ikuesan, and H. S. Venter, "User attribution based on keystroke dynamics in digital forensic readiness process," in *Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS)*, Nov. 2017, pp. 124–129.

[121] R. Nordvik, Y.-C. Liao, and H. Langweg, "AccountabilityFS: A file system monitor for forensic readiness," in *Proc. IEEE Joint Intell. Secur. Informat. Conf.*, Sep. 2014, pp. 308–311.

[122] A. Reyes, *Cyber Crime Investigations: Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors*. Rockland, MA, USA: Syngress, 2007.

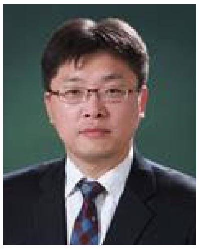
[123] P. Sharma, D. Arora, and T. Sakthivel, "Mobile cloud forensic readiness process model for cloud-based mobile applications," *Int. J. Digit. Crime Forensics*, vol. 12, no. 3, p. 58, 2020.

[124] S. Kurowski and S. Frings, "Computational documentation of IT incidents as support for forensic operations," in *Proc. 6th Int. Conf. IT Secur. Incident Manage. IT Forensics*, May 2011, pp. 37–47.

[125] K. Reddy and H. S. Venter, "The architecture of a digital forensic readiness management system," *Comput. Secur.*, vol. 32, pp. 73–89, Feb. 2013.

[126] S. Park, N. Akatyev, Y. Jang, J. Hwang, D. Kim, W. Yu, H. Shin, C. Han, and J. Kim, "A comparative study on data protection legislations and government standards to implement digital forensic readiness as mandatory requirement," *Digit. Invest.*, vol. 24, pp. S93–S100, Mar. 2018, doi: 10.1016/j.diin.2018.01.012.

SUNG JIN LEE received the B.Sc. degree in computer engineering from Dankook University, South Korea, in 2004, the M.Sc. degree in computer engineering from Seoul National University, South Korea, in 2006, the L.L.M. degree in law from Yonsei University, South Korea, in 2015, and the M.B.A. degree from Kelley School of Business, Indiana University, USA, in 2018. He is currently pursuing the Ph.D. degree with the Department of Forensics, Sungkyunkwan University. Since 2011, he has been working as a Senior Examiner and a Digital Forensic Investigator with the Capital Market Judiciary Enforcement Unit, Financial Supervisory Service. His research interests include digital forensics, cyber investigation, machine learning, IT audit, and financial crime.



GI BUM KIM received the B.A. degree from Korean National Police University, and the M.S. and Ph.D. degrees from Korea University. He has also worked as a Police Officer for a period of 23 years and had an Honorary Retirement as a Senior Superintendent, in 2020. He worked as a Professor with the Department of Police Science and as the Director of the International Cybercrime Research Center, Korean National Police University. He is currently an Associate Professor with the Department of Forensics, Sungkyunkwan University, South Korea. His research interests include investigation of cybercrime, digital forensics, cybersecurity policy, and international development cooperation.