Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

# Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0

*Khairul Akram Zainol Ariffin*[a,*], *Faris Hanif Ahmad*[b]

[a] *Cyber Security Center, Fakulti Teknologi dan Sains Maklumat, Universiti Kebangsaan Malaysia, Bangi, Selangor, Malaysia*

[b] *Pharmacy Enforcement Division, Petaling Jaya, Selangor, Malaysia*

ARTICLE INFO

*Article history:*
Received 19 March 2020
Revised 3 February 2021
Accepted 15 February 2021
Available online 20 February 2021

*Keywords:*
Industrial revolution 4.0
Cybersecurity
Digital forensic
Maturity model
Readiness
Challenges
CMMI
COBIT

ABSTRACT

The introduction of Industrial Revolution 4.0 (IR 4.0) brings benefits to the industries and our daily life. Innovation such as the Internet of Things, cloud computing, and blockchain is not only confined to the manufacturing industry but covers the whole of human life. Notwithstanding the said innovation, it also gives rise to cybercrimes with these technologies' assistance. The botnet called Mirai is one example of compromising the technology in IR 4.0 to launch large-scale cyberattacks through Internet access. It is therefore crucial for the digital forensic (DF) organization to be ready to handle this kind of incident. This paper aims to provide the indicators for DF organizations' maturity and readiness in the era of IR 4.0. To establish the indicators, a systematic literature review (SLR) is conducted. It involves four phases in the SLR, where the focus is; (1) challenges of DF in IR 4.0, (2) chain of custody and DF readiness, (3) existing maturity model, and (4) benchmarking the maturity element, respectively. It covers the research studies taken from five databases. From the comparison analysis, this study has derived five indicators for the maturity and readiness of DF organization: (1) People and capacity development, (2) Organization, policy and cooperation, (3) Process, (4) Technology and technical, (5) Legislation and regulation. Finally the work outlines the DF practices based on the CMMI ver. 2 practice areas and potential governance and management objectives that can govern the DF organization.



## 1. Introduction

The concept of Industrial Revolution 4.0 (IR 4.0) refers to transforming the manufacturing sector by utilizing technological elements towards increasing production. It is the latest technological revolution the world is experiencing today. It involves the latest technology applications in IR 4.0, such as the Internet of Things (IoT), cloud computing, blockchains, and big data. It is not only confined to the manufacturing industry but covers the whole of human life, such as smart cities, smart transportation, digital economy, health, and more (Lee et al., 2018). Notwithstanding that, IR 4.0 also attracts criminals to apply technology in launching cybercrime activities (Ervural and Ervural, 2018).

Interpol defines cybercrime into two categories, which are cyber-dependent crime and traditional cyber-enabled crime. Cyber dependent crime refers to direct crimes against computers, systems, and information related to it. The examples of them are the hacking of websites to obtain confidential

* Corresponding author.
*E-mail address:* k.akram@ukm.edu.my (K.A.Z. Ariffin).
https://doi.org/10.1016/j.cose.2021.102237

information on individuals or organizations. On the contrary, traditional cybercrime relates to crimes such as theft, gambling, and the sale of counterfeit drugs using the device and the Internet (Ariffin et al., 2015).

From the legal aspects, the definition of evidence in the Malaysian provisions of Section 3 of the Evidence Act 1950 is "all documents submitted for judicial review" (AGC, 2017). These documents can be categorized as "a piece of information or data recorded, stored, processed, retrieved or released by a computer." Meanwhile, the US National Institute of Justice defines digital evidence as any information stored or transmitted in the form of a binary that is admissible in court (DOJ, 2008). Hence, any data and information stored on or through digital devices and networks is potentially digital evidence.

There are challenges in the context of devices related to IR 4.0, especially in retrieving the digital evidence. The IoT, cloud computing and encrypted operating systems require different approaches to extract and retrieve digital evidence. Further, the privacy issue may play a crucial role in protecting the criminal. It can be seen in the case of Microsoft rejecting a warrant from the United States for disclosure of its clients' emails and data in the cloud on the investigation of drug cases (Brier, 2017). Opportunistic criminals always search for vulnerabilities in IR 4.0 technology as it is still in its infancy. The study by Jang-Jaccard and Nepal (2014) reveals that the latest cybercrime trends tend to apply advanced data phishing, remote access attacks such as crypto-jacking, attacking the weaknesses in automation systems, IoT connectivity space, and latest in artificial intelligence (AI) abuse to assist the criminal activities.

Digital forensic (DF) is a forensic science branch that focuses on the recovery and investigation of artifacts derived from digital devices. Digital devices are physical units capable of storing data and information such as computers, laptops, smartphones, smartwatches, pen drives, memory cards, and Global Positioning System (GPS) navigation. At the end of the DF procedure, the investigation results from these digital devices are presented as evidence for the use of court proceedings on civil or criminal offenses. As such, the DF represents one of the critical aspects of law enforcement agencies investigating and bringing criminals to court. To ensure the evidence is accepted and understood by the court, the DF investigation must follow an appropriate and scientific method consisting of; identification, preservation, analysis, and presentation (Interpol, 2019).

Currently, DF is facing the challenges that contribute to the backlog in the investigation. The introduction of IR 4.0 has amplified these challenges in increasing difficulty and complexity to the DF investigation. Thus, this issue creates problems in DF investigation where cases have been dropped from proceeding for the prosecution (Montasari and Hill, 2019). Hence, it requires capability building and a defined measurement to ensure the DF community is always prepared to face future challenges.

Capability building is a process by either individuals or organizations to strengthen and maintain the ability to achieve organizational objectives over time. Organizational assessment that involves the asset and requirement is the primary stage for capability-building, as suggested in the Development Programme by United Nations (UNDP, 2007). One of the capability building components is the Maturity Level assessment, which can improve the process areas by measuring and comparing the capability levels (Ho et al., 2016). However, in the context of the DF maturity level, it is hard to find a study on it even though the DF investigation has been around for a long time. Thus, this scenario highlights the need for a mechanism to measure the level of competence of the DF organization to ensure its capability of handling growing and sophisticated cybercrimes investigation.

The level of maturity depends on the maturity model chosen by the organization. Interpol recently released the Global Guidelines for DF Labs, which states that the laboratory must comprise premises, staff, equipment, management, procedures, and quality assurance (Interpol, 2019). Although it is a good recommendation for the DF community, further study must be conducted to evaluate the indicators and ensure that it supports DF Labs' environment in individual countries.

Further, DF Labs are mostly made up of Enforcement Agencies, which are bound by specific laws and regulations. The selection of appropriate and specific indicators to the organization is highly recommended by the United States Institute of Internal Auditors (IIA). The recommendation states that the maturity model's proper indicators must be adopted and accepted by the organization to guide them toward better improvement and achievability (IIA, 2013). Therefore, this paper aims to identify the indicators for DF organization's maturity and readiness in the era of IR 4.0. In the process, this work will outline all the challenges in DF investigation through the systematic literature review (SLR). The SLR covers the relevant studies from 2011 until 2020 and five databases; IEEE Explore, ScienceDirect, Springer Link, Semantic Scholar, and Emerald Insight. Then, it presents a comparison of the prior maturity levels and indicators from the previous research. Finally, it suggests the crucial indicators to ensure the maturity and readiness of the DF organization.

This paper is divided into ten sections. Section 2 will present the definition and the elements of IR 4.0. It is then followed by Section 3 that highlights cybersecurity as an element of IR 4.0, together with some cybersecurity case studies. Subsequently, the methodology of a systematic literature review (SLR) is described in Section 4. In Section 5, the challenges of DF in the era of IR 4.0 will be outlined. The discussion about the chain of custody and DF readiness is highlighted in Section 6. The basic understanding of the maturity level for the organization is presented in Section 7. The examples of existing maturity models for DF are discussed in Section 8. Section 9 discusses the crucial indicators for DF organizations' maturity and readiness. Finally, Section 10 is the conclusion of the paper.

## 2. Industrial Rrevolution (IR) 4.0

IR 4.0 was first introduced in 2011 by the German government to enhance the industry (Rojko, 2017). Since then, world powers, such as the United States, China, and Russia, have adopted IR 4.0, which impacts the rapid development of technology in computing.

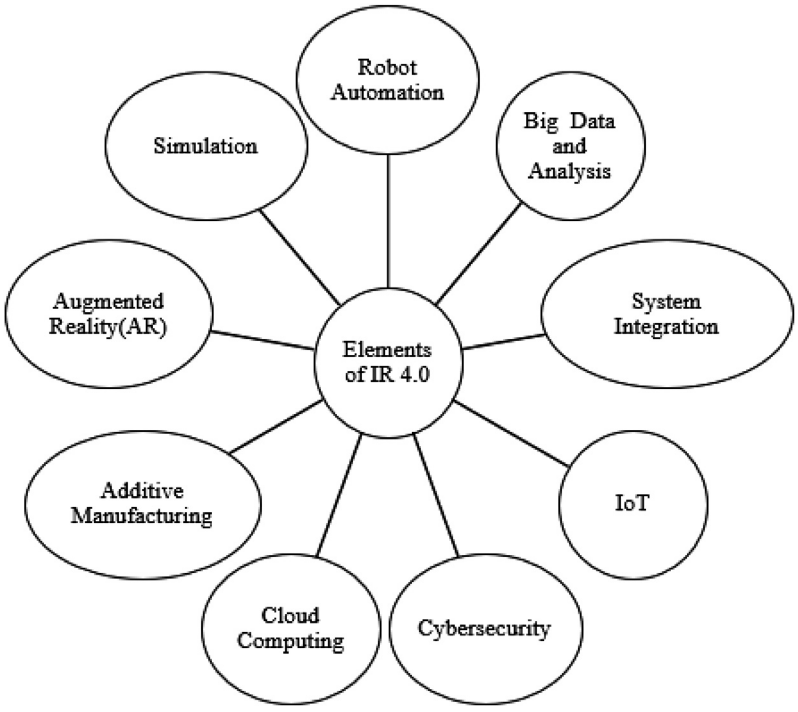


**Fig. 1 – Elements in IR4.0 (adapted from Erboz (2017)).**

(Erboz, 2017) has listed nine elements in IR 4.0, as shown in Fig. 1. By observing these elements, four elements apply to the manufacturing sector, influencing people's daily lives and interaction with one another. These elements are big data, the Internet of Things (IoT), cybersecurity, and cloud computing. It was anticipated by the founder of the World Economic Forum in 2016 that IR 4.0 technology will impact three categories; business, government, and even human beings.

For example, in the healthcare sector, one of the applications of IR 4.0 technology is the design of a security model for e-Health applications called Exalead Cloudview®, as introduced by Suciu et al. (2015). Exalead (2019) incorporates IoT technology, cloud computing, and big data in storing patient health information. However, according to the Health Insurance Portability and Accountability Act (HIPAA), statistics on patient data leakage through hacking and information security incidents reported in the United States keep increasing year by year from 18 cases in 2009 to 365 cases in 2018 (HIPAA, 2019). Thus, it is understood that applying these new technologies is vulnerable to cyber threats such as the intrusion of patient data from hospital databases. As such, the cybersecurity element is vital as the key to the adaptation of new technologies.

## 3. Element of cybersecurity in IR 4.0

The CIA's triad of Confidentiality, Integrity, and Availability are essential components of cybersecurity (Majid and Ariffin, 2019). Any technology used by individuals or organizations must ensure that sensitive information remains confidential, accessible only to the authorized entity and available when the owners wish to access that information. If one of the security components is compromised, the situation is called a cybersecurity incident.

Before introducing of IR 4.0 technology, the 2010 Annual Security Report by Cisco (2010) reported cybersecurity incidents ranging from viruses, worms, social engineering, and cyberattacks. Nevertheless, with the nature of the broader interconnected network in the IR 4.0 operation, it has provided space for a more extensive cyberattack. The sophisticated capabilities of today's network technologies such as IoT and cloud computing have allowed this threat to happen. For example, distributed denial-of-service (DDoS) attacks have a far more significant impact than denial-of-service (DoS) attacks due to the connectivity of digital devices that can reach up to millions or billions of devices (Mahjabin et al., 2017).

In the future, cyberattacks can be hard to predict due to IR 4.0 technology, which is still in development and has not reached the maturity level. Jang-Jaccard and Nepal (2014) show that the trend of cyberattacks is now explicitly geared to newly introduced systems such as social media, cloud computing, and smartphones, which are attacks by malware hidden in the vulnerabilities of the emerging technology system. Therefore, to highlight further in the topic, this paper presents the challenges of cybersecurity and its relationship to DF from the literature on two elements of IR 4.0, namely IoT, cloud computing, and one related technology, blockchain.

### 3.1. *Internet of things (IoT)*

Theoretically, IoT allows for transferring and sharing of data between objects and humans. It involves three relationships in a digital network; between humans and humans, humans with objects and objects with objects. IoT architecture consists of three (3) layers; Perceptions, Networks,

and Applications (Yang et al., 2011). The perception layers act as sensors (such as RFID, barcodes, cameras, and others) to collect data in the environment. The network layer will provide a platform to send collected data to other target devices or objects. The last layer of the application involves the interface between users and IoT devices. One example of a technology application that adapts IoT technology is the smart home, which allows users to access a wide range of things at home using a smartphone (Hsu et al., 2017).

Nevertheless, this extensive network presents both technological and security challenges. As described in the study of Mahmoud et al. (2015), the challenge of IoT security is to ensure that the CIA triad is achieved in IoT technology. It is where the data and information transferred are accessible only to authorized users, at the user's discretion, and unchanged except with the data owner's consent. In addition to that, the process of identifying and verifying interconnected objects must be maintained to ensure a secure connection. However, there are possible threats in the communications layer, such as communication overload and man-in-the-middle attacks, as revealed in the IoT security risk assessment study by Grammatikis et al. (2019). Looking from the DF perspective, this situation may result in the challenge of detecting, verifying the authenticity, and retrieving the required artifacts from IoT-related digital devices.

For example, in October 2016, the United States is startled by a large-scale cyber-attack by a botnet called Mirai. The impact of these Mirai attacks has left Internet users in the eastern United States unable to access popular services such as Twitter, Netflix, Reddit, and CNN (Sinanović and Mrdovic, 2019). Antonakakis et al. (2017), in their study, revealed the ability of Mirai, which has historically recorded 600,000 infections, by exploiting the IoT technology. Mirai works by scanning the Internet to find connected digital devices. Once these IoT digital devices have been compromised, they have become botnets and launch attacks on the network and disable servers for Internet access. The study also suggests that cybercriminals are always trying to discover IoT connectivity's weaknesses, which requires both technical and policy response. It represents an example of the possibility of the closed-circuit television (CCTV) system being manipulated and transformed into a 'weapon' for cyberattacks such as DDoS, as described by Mansfield-Devine (2017). Through this case study, it can be concluded that IoT technology may bring challenges to DF throughout investigation and legislation as it involves many regions.

### 3.2. *Cloud computing*

The National Institute of Standards and Technology (NIST) defines cloud computing as a model that enables users to access sharing computer systems with minimal management and interaction efforts through continuous network communication (Mell and Grance, 2011). Although cloud computing has changed over time, three standard models have become widely established and formalized; Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

The IaaS delivery model represents a virtual IT environment comprising infrastructure resources that can be accessed and managed via user-friendly interfaces and tools. Through IaaS, the IT resources are virtualized and packaged into bundles to simplify the infrastructure's customization (Zhang et al., 2010). On the other hand, the PaaS model is typically applied for general software development. The cloud provider (CSP) hosts pre-packaged products and tools that support the entire delivery lifecycle of custom application development in this model. The user can access these tools over the Internet using either APIs, web portals, or gateway software (O'Shaughnessy and Keane, 2013). The SaaS model is likely to deliver software applications to users over the Internet. Thus, the user can access SaaS through computers or smartphones with an Internet connection. This model provides both free and paid services to the users, depending on their requirement storage or services. One of the popular SaaS applications is Microsoft Office 365 that is used for productivity and email services.

Although each of the cloud models' functions is different, their architectures remain the same as described by Kavis (2014). In most cases, the cloud computing architecture can be arranged into nine layers: Application, Data, Runtime, Middleware, Operating System (OS), Virtualization, Servers, Storage, and Networking. These layers will determine the portion of control between the users and providers on the cloud application (Ahmad et al., 2020). In the traditional on-premises, the users will manage all the layers from application to networking. However, in IaaS, the users' level of control is permitted from the application to the OS layer. In PaaS, the users can manage the application and the data, while in SaaS, there is no management layer except that the user can only access the data (Jadeja and Modi, 2012). Thus, with a minimal level of management and interaction, users have limitations on data visibility and control.

Well-known providers like Amazon E2, Microsoft Azure, and Google Cloud define the risk of cloud computing security as a 'shared responsibility' (Bernhard, 2019). Tianfield (2012) explain that 'shared responsibility' means that the providers protect the design's security. However, users themselves are responsible for protecting the security and privacy of the data they enter. This issue has been discussed by Takabi et al. (2010), Ren et al. (2012) and most recently by Basu et al. (2018), which agree that users, service providers, and policymakers should prioritize data security and privacy to protect the sensitive information from any misuse by provider or external attacks by hackers.

Cloud Hopper is the latest version of the attack in terms of cyberattacks on the cloud service providers. Reuters recently reported that a group of hackers had penetrated the cloud providers (CSPs) such as Hewlett Packet Enterprise, IBM, Ericsson, and Fujitsu (Stubbs et al., 2019). PwC (2017) exposes the modus operandi of hackers who infiltrate access to CSPs, then using cloud infrastructure to jump or hop from one target to another. It allows them to access sensitive information in government and industries related to electronics, health, manufacturing, and finance in several countries. Hackers leverage CSP clients' lack of control and data monitoring to log-in customers' credentials and subsequently access CSP and other customers' infrastructure independently and uncontrollably. Judging from the DF aspect's perspective, in such cases, the investigation team will face challenges in

power to obtain legal permission to access evidence that may be stored on CSP servers abroad (Ariffin et al., 2015).

### 3.3. *Blockchain*

Blockchain technology is a digital ledger (or referred to as a block) that is shared through a peer-to-peer network with a consensus mechanism. By applying cryptographic techniques, users can store and update data in a matching bracket chain without being compromised and modified by a third party. The distinguishing feature of this technology compared to traditional data storage systems is decentralized ownership, where there is no specific authority that owns the data blocks starting from the creation, retention, and addition of the block. It is approved by the community to preserve the value and integrity of the data. Whereas the Proof of Work is a mechanism involving only two-party consent, it eliminates the need for third parties to handle data.

Cryptocurrency is one example of applying the blockchain technology. Despite the advantages of faster transactions, lower costs, and trust in a central bank-like system, it also provides room for crime and misconduct. Matanović (2017) points out that among the challenges and issues of digital currency security such as Bitcoin is an increase in ransomware and the illegal transactions of malicious services on the dark web. In addition to cryptocurrencies, blockchain technology has weaknesses in storing private and sensitive data. It is an issue that relates to public blockchain or blockchain with limited bandwidth and storage capacity, where it leads to penetrating and data leakage.

The WannaCry ransomware is one of the recent global cybersecurity incidents in 2017. The attack targeted the Microsoft Windows operating system through worms that subsequently encrypted data on the machine. Interestingly, attackers demanded a certain amount of money to be paid in Bitcoin if the user wishes to access the data within a specified time frame (Paquet-Clouston et al., 2019). These cunning cybercriminals do not solicit ransom through the traditional banking system but exploit pseudo-anonymity and irreversibility as Bitcoin's features as it is difficult to detect by law enforcement (Conti et al., 2018).

## 4. Methodology for systematic literature review (SLR)

A systematic literature review is used as an approach to conducting a thorough literature. (Fink, 2019) defines this methodology as "A systematic, explicit, comprehensive, and reproducible method for identifying, evaluating, and synthesizing the existing body of completed and recorded work produced by researchers, scholars, and practitioners". A systematic literature review is conducted to address this study's objective, which is to come up with indicators for the maturity and readiness of the DF organization. This systematic literature review is conducted based on Kitchenham (2004) and the formal systematic literature review methodology to the Information Systems research that is by Okoli (2015). The combination of guidelines is done by incorporating the 'Appraise Quality' method proposed by Okoli (2015) into Kitchenham (2004) guideline. Appraise Quality involves explicitly setting out criteria and scoring to judge the literature screened and thus produce a quality review. The steps taken to conduct this review are explained in Fig. 2.

### 4.1. *Outlining systematic literature review*

This study's main objective is to identify the indicators for developing a maturity and readiness model based on DFs' challenges in the 4.0 Industrial Revolution era. These five (5) electronic databases are selected to obtain information about the challenges, maturity and readiness model, and indicators specific for DF;

- Emerald Insight (https://www.emerald.com/insight/)
- IEEE Xplore Digital Library (https://ieeexplore.ieee.org/Xplore/home.jsp)
- ScienceDirect (https://www.sciencedirect.com/)
- Semantic Scholar (https://www.semanticscholar.org/)
- Springer Link (https://link.springer.com/)

Generally, the review includes both abstract and the full articles written in English. Further, the articles exclusively accepted during the review are journals, conference proceedings, and reports. The research strategies are categorized into four (4) phases; 1. Identify the challenges, 2. Present the definition of the chain of custody and elements of DF readiness, 3. Search for DF maturity model, and 4. Identify indicators for DF maturity model related to challenges in IR 4.0. Also, each step of the research strategy has specific selection criteria for reviewing purposes.

In Phase 1, the aim is to observe the research related to DF challenges after the era of IR 4.0 officially started. Therefore, the practical screen applied in this step is the keyword with the Boolean's operator ("digital forensic" OR "computer forensic" OR "cloud forensic" OR "IoT forensic" OR "cryptocurrency forensic") AND "challenges". The filter of years of articles published is set from 2011, when the IR 4.0 is introduced, until 2020.

Phase 2 aims to overview the DF operation from the perspectives of DF readiness and chain of custody. Its purpose is to define the chain of custody and highlight the essential elements in DF readiness. Then, these elements will be used to support the identification of the indicators for the maturity model. The keyword applied for this phase is the "chain of custody" AND "digital forensic readiness".

Next, Phase 3 focuses on searching for the DF maturity model, the keyword with the Boolean's operator "digital forensic" AND "maturity model" is used. The filter of years of articles published is set from 2011 until 2020. During this step, the other inclusion criteria are that the article must propose a DF maturity model from the core maturity model developed for the Information Systems field. Meanwhile, any article that proposes a framework is excluded because it only represents an underlying system's basic structure. A review of the model is a more suitable choice in this study as it is used to idealize the operation, mechanism, and situation within the given framework.

As cybersecurity and DF are interconnected, it is essential to conduct systematic studies of models, indices, and

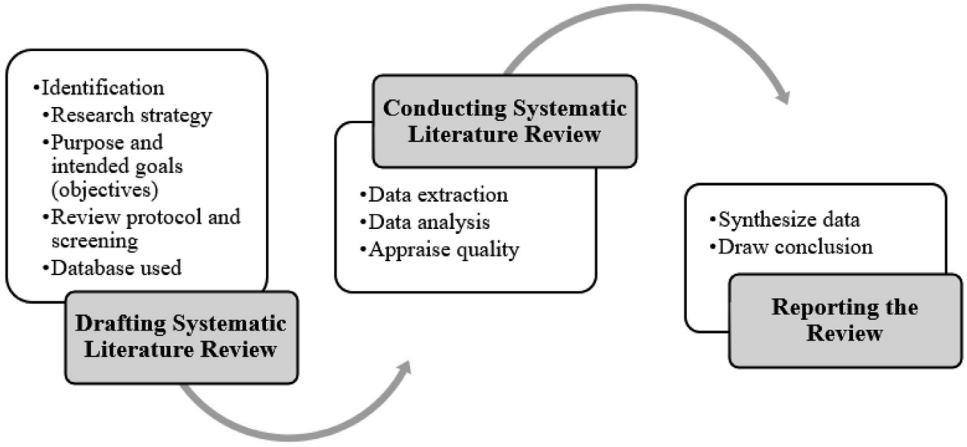


**Fig. 2 – Stages of Systematic Literature Review (adapted from Okoli (2015)).**

maturity levels in both areas. Phase 4 aims to compare and benchmark the maturity elements that have been suggested in the previous studies. Hence, the review selects related research by combining the keywords of the "maturity" AND ("index" OR "model") AND ("digital forensic" OR "cybersecurity") in the literature databases. The filter of years of articles published is set from 2011 until 2020. The inclusion criteria for Phase 4 are articles produced by academicians, government agencies, and research institutes and models that were already tested on organizations. The articles that present indicators based on NIST Cybersecurity Framework for cybersecurity are excluded because those five core functions (Identify, Protect, Detect, Response, and Recover) are generally used to assess cyber risk towards the organization.

### 4.2. *Conducting a systematic literature review*

The reviewing process is performed from August 2019 to August 2020. For Phase 1, a total of 1,835 documents are taken from the databases. These documents include books, research articles, patents, and review papers. From this amount, only review papers and research articles are being selected for the next stage. However, only 1,241 documents passed through to the second stage. In the second stage, the documents' lists are filtered based on the contents in title, keyword, and abstract. Each of these elements must contain the word and description of challenges, issues, and DF readiness for the era of IR 4.0. Further, it must cover both DF and emerging technologies. At the same time, any redundancy on the contents is removed from the lists. Thus, at the end of the second stage, only 99 documents were selected. For these 99 documents, the manuscripts' overall contents are analyzed, captured, and removed redundancy in the lists. Hence, throughout the systematic literature review, only 32 articles are selected as they insightfully answer the research questions. As recommended by Okoli (2015), to perform the quality assessment, researchers appraise selected articles using the same criteria during the screening, prioritize them according to their quality and exclude particular materials deemed not useful to the research questions.

The same approach is applied for Phases 2, 3 and 4. Both phases started with a total of 50, 245 and 663, respectively. Then, through the filtering to remove redundancy and those answering the research questions, the phases end up with 8 (Phase 2), 8 (Phase 3) and 11 (Phase 4) documents, correspondingly. Some additional articles are included in the discussions of Phase 3 and 4 to strengthen the contents.

### 4.3. *Reporting the review*

In order to accurately record and analyze the information obtained, the authors developed a data extraction form with the help of software tools. Each study is adequately recorded and managed using Endnote X9. All articles collected are read carefully and the related data extracted into Microsoft Excel 2019 according to the columns; paper title, authors, date, location of publication, sources, objective, and focus of the paper.

## 5. Challenges in DF in IR 4.0

A systematic review has been conducted to highlight the challenges in DF investigation. Based on this work, it is found that the challenges in the era of IR 4.0 inherit the same issues and problems that have been discussed in the early years of DF. The primary sources of the challenges in DF are the nature of current data, the use of anti-forensic techniques, existing training and skill development, and the practitioner's approaches in handling the investigation. It can be seen that with the advancement in technology, several improvements have been made to the data itself, which affect (1) the mechanisms of storage, (2) format, (3) contents, and (4) the condition of the data. These natures of data will reflect on the issues and challenges in legal procedures (Chen, 2014; Stoyanova et al., 2020), forensic skill set (Buric and Delija, 2015), and tool capabilities (Horsman, 2018). Another finding from the review is that the related IR 4.0 technology challenges inherit the same issue and problem in network forensic (Khan et al., 2016) and smartphone or smart device forensic (MacDermott et al., 2018). It amplifies several of the challenges in these two fields and makes the investigation difficult. Also, based on

the review, it can be concluded that the challenges related to cloud computing are the subset of the challenges in the IoT system. All the sensors and devices in IoT systems will interact with the cloud computing technology (Atlam et al., 2020). The following subsections demonstrate the challenges of DF in era IR 4.0 from the SLR.

### 5.1. *Challenges related to nature of data*

The understanding of the nature of data is crucial for DF investigation. The job of DF practitioners is to translate the digital data into readable information, and if it is related to the case being investigated, they must interpret it as evidence. The first issue with the data is that its volume keeps increasing with technology advancement (Buric and Delija, 2015). The introduction of cloud computing increases the volume of data which if the DF investigation is conducted, it can create a problem in analyzing and examining for evidence (Feng and Zhao, 2017). It is also true for the IoT systems, where it involves billions of interconnected devices (Stoyanova et al., 2020). Hence, it affects the duration of the DF investigation (i.e., it may take months and years). In such cases, it will create a backlog that severely impacts the timeline of criminal investigation and legal process, which may result in the prosecution's discharge in the court.

The distributed nature in the network, cloud computing, and IoT systems contribute to the struggle in locating, seizing, and retrieving the evidence from the system (Baig et al., 2017; Damshenas et al., 2012). Further, depending on the network's size, there is a possibility of not being able to collect the evidence from all sources. For network forensic, data granularity will become the issue as it is not manageable and practical to collect the whole packets in a large network environment. Meanwhile, the evidence in cloud computing is collected from different locations and jurisdictions (Zargari and Benford, 2012). There is a likelihood that the DF practitioners do not know the location of data. This scenario can relate to IoT cases. When the characteristic such as distribution, huge volume, and variety of data coupling together, it will be hard to ensure the investigation is forensically sound and can be solved in a timely fashion. Thus, the existing DF investigation process cannot be deployed in this scenario. Also, several IoT related devices can be difficult to find by the DF practitioner due to their small size (Stoyanova et al., 2020). Considering these two scenarios, it can jeopardize the reconstruction of criminal activities. During the identification and reconstruction, two tasks need to be taken; (1) identify the devices that are relevant to the case, and (2) discard the irrelevant one from the case. These tasks can be complicated and time-consuming, considering the number, size, and distribution of devices. As the data may be located in a different location, it will affect the temporal analysis if there is a difference in time zone information in the collected evidence.

In a DF investigation, data integrity plays a crucial role in ensuring the evidence is admissible to the court (Gold, 2014). Hence, to maintain the evidence's integrity, several approaches must be applied to safeguard the evidence, such as calculating and comparing the hash value, doing documentation to record the activities during the investigation, and maintaining the evidence's chain of custody. However, due to the emerging technology in IR 4.0, the possibility to maintain the integrity of data and evidence becomes a significant issue for DF practitioners. On the other hand, data privacy becomes another subject that may limit the amount of evidence collected during the investigation (Oriwoh et al., 2013). In handling the network forensic, the DF practitioners will depend on data in network devices. Such network devices are built with limited storage and with no persistent storage. Thus, due to the high-speed transmission and massive volume of data passing these devices, there is a possibility for overwriting on the historical data.

The same issue can occur due to software and hardware errors, malfunction of the system, and malware attack (Khan et al., 2016). As the evidence data must be collected from multiple remote devices, it can significantly complicate maintaining a proper chain of custody during the investigation. A similar case can be found in the investigation of cloud computing and IoT system. Together with the distributed nature, the data in cloud computing involves multiple ownerships and tenancies. A single cloud node contains many instances from other users. Taking the example from mobile cloud computing, the study in Khan et al. (2014) pinpoints that legitimate users and criminals can offload their data on the same cloud server. One user can run a legitimate service from the cloud, where at the same time, the cloud is being used to launch the malware attack. Hence, while acquiring the evidence, two considerations must be made during the investigation on the cloud. Firstly, the DF practitioners must ensure that the evidence is not co-mingled with other users' data. Next, the other user's data must not be accessed to preserve its privacy.

The lacking of CSP transparency with international regulation in the Service Level Agreement (SLA) plays a significant role in making the investigation difficult (Alqahtany et al., 2015). Some information on cloud computing is hidden from the user's point of view; (1) location of the user's data, and (2) movement or replication of user's data. Besides, the capabilities to track and audit the history on file access and data are not fully provided by the CSP. Currently, the CSPs have full control over the user's data, where they can tamper and modify such data. The issue in integrity and trustworthiness of the evidence becomes tough if the CSP works together with the malicious user. If such a case happens, the CSP can remove the traces of any criminal activities regarding the suspects or providing incomplete evidence for the investigation. In the case involving cryptocurrency forensic, the study in Irwin and Turner (2018) emphasizes that the suspect can conduct the transactions to empty the crypto wallets when DF practitioners walk away from the crime scene. It is because crypto wallets can be accessed from several devices, making the seizing and maintaining evidence integrity inadequate.

In a DF investigation, the knowledge and understanding of the data in the devices and tools are critical for DF practitioners. Such knowledge is necessary to ensure that the DF practitioners are able to collect the correct, related, and essential data to the case being investigated. The data may reside in the devices (i.e. hard disk, server, IoT devices), transmit through the network, and execute by the system. In all these phases, the data can be presented by its types, format, content, condition, and accessibility. Type and format define whether the data is in structured or unstructured form. The content of the

data represents the information that the system holds. It can be temporal, process, application, network, or other information. The condition and accessibility of data will determine its availability and the required mechanisms to obtain the data. Thus, it relates to the data's level volatility, proprietary or standard form, and method to access the data.

In the network environment, there is no standardization of data. By comparing with the filesystem, this data does not become visible as file and metadata but instead range from raw to logs of network devices (Fahdi et al., 2015). Thus, this complexity may affect the analysis phase. The DF practitioner may require preparation and be ready with various tools and methods to handle this issue. Nevertheless, the data representing evidence from cloud computing is generally volatile, short-lived, and stored on a device that DF practitioners do not have any control (Hraiz, 2017). When the user loads and runs the application on IaaS, it will leave some traces of evidence on the client-side. It can be in temporary Internet files or registry entries. However, once the user terminates the application from a virtual environment, this data will be deleted.

In most cases, the CSP only provides persistent storage to store all user's data through an additional package with extra cost. As for SaaS and PaaS, the models have limited API or predefined interface, which can be used by the DF practitioners to collect the data from the system (Damshenas et al., 2012). Hence, it blocks the ability to obtain the system status and log files from the cloud computing system. The log data can play a crucial role in the investigation as it may contain information such as IP address, browser type, HTTP requests, and content requests. Also, it is not possible to perform physical acquisition on the SaaS and PaaS. The task is now given to the CSP to support performing evidence collection from the cloud environment. This scenario may create a severe issue in evidence integrity and trust in CSP. It may contribute to the people factor challenges where the CSPs do not hire certified professional DF practitioners to handle the incident forensically.

The challenges in the IoT system may become much more than cloud computing. It is due to the variety of technologies and devices that are included in the IoT system. The range of IoT systems covers technologies and devices such as unmanned aerial vehicles (UAVs), smart devices, smart grid, smart building, embedded digital devices, and more (Baig et al., 2017). Starting from the network environment, the visibility and recognition of IoT devices to be included in the investigation are complex and complicated. In the traditional computer and network-based, it is clearly defined as the boundary lines to perform the investigation; in terms of the number of devices and people involved. However, with IoT, the networks can transfer between the layers, such that from Body Area Network (BAN) to Wide Area Network (WAN) as the users move in their daily life (Oriwoh et al., 2013). The IoT devices can be related to having limited memory space, which depends on the usage; the data could be easily overwritten, resulting in losing evidence. This scenario will affect the way of collection and acquisition for DF investigation. Besides, the study in Zareen et al. (2013) outlines that the standard DF procedures and tools may fail in acquiring and processing the data for SCADA investigation due to; (1) proprietary in the protocol, (2) high volume of data and devices, (3) type of devices (e.g., too old with no technical solution), (4) focus of logging (i.e., not security and forensic centric) and (5) privacy issue.

The introduction of smart devices in IoT has created a new way for the user to interact with the application. On every smart device, the user can install, manage, and run a variety of applications. It may involve open source and proprietary OS, which limits the method that can be implemented to communicate or locate evidence. A smart device such as a wearable can operate independently or through a secondary device. It creates additional challenges to DF practitioners as some questions need to be answered; (1) is the data being stored locally or in the cloud? and (2) is the data being encrypted? Such operations from the smart device represent the anti-forensic mechanisms for the criminals to hide their activities. Further, to acquire and analyze the data, the DF practitioners require a special tool. This will depend on the tools' capability to decode and reconstruct the application data (Zawoad and Hasan, 2015).

Taking the example of an autonomous vehicle, the study in Torre et al. (2020) highlights criminals or terrorists' potential to exploit vulnerabilities in this technology to accommodate their activities. From the DF perspective, this technology has introduced new data complexity in the investigation. For the investigation's success, the DF practitioners need to rely on the vehicle's residual data. Hence, if the vehicle's technology is not facilitated with the build-in forensic collection mechanism, the data's availability as evidence will be impossible (Le-Khac et al., 2020).

Bouafif et al. (2018) outlines the challenges for DF practitioners when dealing with drones (UAV). Due to the versatility of an embedded digital container in UAV drones, implementing a single forensic tool to extract evidence is impossible. Although there is a USB connection on the drone, it does not allow direct access to the physical address. The DF practitioners need to rely on protocols such as Telnet, SSH, Bluetooth, or Wi-Fi to establish the interconnection. Further, as several data storage is access protected, it only allows live acquisition for the drone. With no standardization in software, hardware, and firmware between the drone vendors, it therefore requires the knowledge and understanding of structures on such data. However, the manual and documentation on this information are still limited.

Additionally, alarms have been raised concerning the difficulties identifying UAV owner, who has committed a crime (Horsman, 2016). As the UAV is supplied with low power, there is a possibility that the device loses power and crash. If the owner flees from the scene, the UAV will become abandoned and the DF practitioner may have to identify its owner during investigation.

Cryptocurrency is a technology from Internet-based to store value. It is used to store a monetary value with the same purpose as physical currency but with no physical representation. It is created, stored, and use for the electronic and online transaction. The forensic challenge is due to its ability to transfer monetary value instantaneously, borderless, and anonymity (Irwin and Dawson, 2019). In this scenario, the user does not hold a currency unit, but the system approves the transaction by giving authority over the account. Simultaneously, no personally identifiable information (PII) is included in the blockchain records during conducting transactions. By

creating a P2P transaction, no information of the users is included, and it allows the transactions to have a high level of anonymity, compared with the traditional financial platform. Hence, it creates the issue of identifying the cryptocurrency user and transaction. The process may become tedious and time-consuming as the DF practitioners need to track the transaction carefully online, observing the specific public keys and pair transaction across datasets to identify the individual. Only from there, the DF practitioner can draw the scene of the criminal activity that is related to cryptocurrency (Yousaf et al., 2019).

### 5.2. *Challenges in anti-forensic*

The study in Horsman (2017) expresses the relevancy of DF in the current ages. By referring to the case study in the UK where 60% of the cases are not possible to proceed for prosecution, it highlights the challenges on the anti-forensic tool that create problems for the DF investigation. The use of encryption and data obfuscation to protect privacy by criminals play a massive role in protecting their activities from detection and analysis. For example, utilizing the encryption in the traffic through an SSL VPN connection gives the criminals an advantage. Through this method, the only information that the practitioners may obtain is the port and address. However, the data stream will not be available.

The work in Zareen et al. (2013) describes that with the availability of resources (i.e., materials and tools) on cybersecurity and DF, it helps give awareness to criminals, resulting in anti-forensic mechanisms to hide their tracks. The availability of the facilities such as the Deep Web and anonymous market to offer unlawful tools and services contributes to the investigation's challenges. Through the services, the criminals can implement several mechanisms to protect themselves while performing the attack: zombie machine, remote proxy server and encryption.

When handling the data in network forensics, the DF practitioner will mostly investigate the IP addresses and destination. The attackers can deploy different methods to hide the original IP address from both the investigator and the network security devices. It may include IP spoofing to create a forged IP address to hide the sender or impersonate another person.

From cloud computing's perspective, it can either represent an anti-forensic agent or a victim. Due to its ability to provide the users with high computing power and resources, it can decode any encrypted files, perform malicious activity such as stealing information, wiping, and as a botnet to disturb and damage other systems (Chen, 2014). Simultaneously, the opportunity is given to criminals to conduct and cover their malicious activity by applying the anonymizing tools and storage in cloud computing. As a result of sharing minimal information during registration for cloud computing and applying IP anonymity, the DF practitioner cannot identify the criminal in the cloud environment.

In most cases, the launch of malicious attacks is conducted through a Tor browser, which gives a significant barrier to identify, detect, analyze, and prosecute these activities (Irwin and Dawson, 2019). The IP address can sometimes not represent a real identity for the individual responsible for the illicit transaction (i.e., through cryptocurrency), launch botnet, communication, or any action. The user can connect to the Internet in several approaches; from open wireless networks, open space (e.g., library and cafe), Tor exit relay, or virtual private network (VPN). Through any of these approaches, it does not display information related to the exact person that is responsible for the illicit activity and communication.

The use of encryption is not only being applied in the network. It has been implemented in the devices. With the emerging technology, smartphones have increasingly utilized encryption, which becomes a drawback for digital evidence acquisition. The same can be stated for the Operating System and filesystem, which enhance the security measure on the system (Fahdi et al., 2015). Nevertheless, the malware in the standalone system is no longer utilizing the hard disk as storage. Instead, the malware resides in the volatile resources and launch any malicious activity from there. By doing so, it executes the codes without the knowledge of the user. With these tools and techniques, DF practitioners' ability to locate relevant evidence will become even more challenging.

### 5.3. *Challenges in tools reliability and capabilities*

The tool errors and limitations can be considered one of the DF investigation challenges. As the DF practitioners aim to produce substantial evidence, they face a difficult task to ensure the tool effectively use and maintain its accuracy. The tool's limitation can lead to user error in DF investigation. User error is defined as the misuse of the tools due to a failure to detect the tool's limitation. Such error comes from the use of push-button tools and the operation of the tool by the untrained individual (Horsman, 2018). Besides, the practitioner may rely on free and open-source tools to investigate due to financial constraints. Such a tool may be developed by individuals who may not be professional or without documented testing for validation. Thus, accepting the manufacturer's word about the tool without validating the result may be an issue in DF and jeopardize the overall investigation. The statement is supported by SWGDE (SWGDE, 2015), where it highlights DF as a complex field that relies on the embedded algorithms in the automated tools, in which the errors can potentially lead to incorrect findings. If the process of interpreting the evidence is incorrect and inaccurate, it may lead to flawed data being presented for the practitioner to evaluate, which can then compromise the investigation.

By considering the network environment, cloud computing, IoT, and cryptocurrency, it can be seen that the existing tools are not able to give 100% support to the DF practitioners in making the investigation easier. The current forensic tools for the network environment only focus on capturing and recording the traffics from communication. With the high-speed transmission and the massive volume of data, it will be time-consuming, hard to process and visualize the data due to the absence of intelligence tools (Buric and Delija, 2015). It is the same for the forensics tool on Cloud and IoT forensics. The currently available tools possess various limitations and cannot cope with such technologies' distributed and elastic characteristics. It is due to the working assumption that DF practitioners have physical access to the computing resources. However, such an assumption does not work with the current technologies in IR 4.0. Thus, using these tools may lose access

to crucial evidence such as network logs, process logs, and storage snapshots. In the case of cryptocurrency, the forensic tool's focus is on retrieving the information from the smartphone. The current forensic tools are able to extract the details from the devices that hold the crypto wallets (i.e., IMEI, IP address, MAC address, brand, and model). However, it could not extract the information on the crypto wallet itself.

### 5.4. *Challenges with people factor*

In the context of challenges with the people factor, it is related to the DF practitioner's ability to conduct an investigation successfully. It will reflect on the skill of the DF practitioner. Simultaneously, the potential criminal's ability must be monitored to ensure the DF community is always prepared for any new wave of cybercrime. It has been a debate in Horsman (2017) that highlights the changing demographic and the availability of scientific computing knowledge may create a new cybercrime wave. Thus, with the advancement in education and technology, it can result in such progression being responsible for creating a smarter cybercriminal. Although it is still a hypothetical statement as no published content pinpoints the definitive link between these progressions and digital crime, the DF practitioner needs to consider this statement as the preparation for the challenge.

In terms of practitioner's technical skill sets, there is still lacking in the availability of training to educate the practitioners on cloud forensic, IoT and cryptocurrency procedures (Tziakouris, 2018). The existing materials for forensic training are not updated and addressing the current issues. Simultaneously, the policies and standard of operation for each emerging technology are not 100% implemented by the forensic community. Apart from the DF practitioner, the jury and lawyer will also be involved in the prosecution of crimes related to IR 4.0. However, currently, most of these individuals have only a basic understanding of this emerging technology. It will be challenging to enlighten them on the technicalities behind the complex architecture of such technologies.

Apart from the technical issue, the quality of investigation is also crucial for DF practitioners. Therefore, it is critical to make sure the investigation is free from any bias. The study in Sunde and Dror (2019) discussed the cognitive bias from perception and interpretation that may affect the investigation. It pinpoints seven (7) bias factors that can impact the decision in the investigation; (1) cognitive architecture and the brain, (2) training and motivation, (3) organizational factors, (4) base rate expectations, (5) irrelevant case information, (6) reference materials and (7) case evidence. These factors are derived from the DF practitioner's experience, interaction with another party, and knowledge. For example, DF's current education system and training only focus on computer science, physics (e.g., electronics), and mathematical theory domains. It does not consider the formal knowledge of bias and its relevant countermeasures.

## 6. Chain of custody and DF readiness

As DF's objective is to reveal the event that happened, digital evidence plays a crucial role. Digital evidence is defined as data that can be applied to support or reject the digital event hypothesis. In terms of criminal investigations, it can be referred to as data or information that holds a crucial link between the cause of crime and the victim. However, as discussed in the previous section, digital evidence is fragile and either stored or transmitted by the devices. Hence, understanding the chain of custody and DF readiness is essential in establishing the ability to obtain digital evidence from the investigation related to IR 4.0.

DF readiness refers to the organization's capability to utilize digital data as evidence in the investigation. The revision of the aspect of processes, implementation of technology, and employment of people must be conducted. The study in Collie (2018) highlights two objectives for the readiness; (1) maximizing the ability to collect credible digital evidence and (2) minimizing the cost of forensic in the investigation. However, most previous studies in DF readiness only focus on the non-digital-forensic organization (Englbrecht et al., 2019). Such a statement is workable in traditional DF, but it does not help handle cybercrime investigations in IR 4.0. Whereas in IR 4.0, both organizations have to collaborate to ensure the investigation can be performed in proactive measures instead of reactive.

The usefulness of data as digital evidence relies on four components; (1) it has evidentiary weight in the court, (2) it is sufficient and relevant to the event, (3) it determines the root cause and (4) link the criminal to the event (Ho, 2015). The evidentiary weight of digital evidence is presented by the degrees of trustworthiness, sufficiency, relevance, and validity. The level of trustworthiness of digital evidence depends on the accuracy, completeness, and the way it is collected and handled. Thus, it is pointing towards the aspect of reliability, authenticity, and integrity. In terms of sufficient, it reflects on the amount of data or information, whether it is enough to be allowed for analysis. Simultaneously, the relevancy of the evidence demonstrates its value in proving or disproving the event being investigated. The validity of the evidence and its acceptance to the court of law depends on the legal, digital investigation regulations and digital evidence (Granja and Rafael, 2017). Similar to the previous discussion on the challenges, the validity depends on the country's admissibility requirement in the region. Thus, it may require consideration on jurisdiction and legal basis for the criminal event related to IR 4.0. However, the most crucial action can be applied to ensure the evidence's validity by collecting it in a forensically sound manner. It is to ensure the quality and credibility of the evidence in the court.

The term chain of custody is related to the digital investigation and digital evidence. It represents the process of maintaining and documenting the chronological history of evidence during the investigation (Giova and Politecnica, 2011). It is crucial for the credibility of evidence as it tracks the event that happens to the evidence. Therefore, the evidence management must ensure that there is no compromise on the chain of custody. The activities to maintain the chain of custody may include (Dimpe and Kogeda, 2018):

- Specific source from where the evidence is acquired
- Identify and document the person involved in handling the evidence

**Table 1 – Role and responsibility for the DF practitioner.**

| Role | Responsibility |
|---|---|
| First Responder | Responsible at the initial state of investigation to secure the incident, make primary identification, and secure the digital evidence while following a proper and forensically sound procedure |
| DF Specialist | Responsible for identifying and collecting digital evidence. The forensic principle must be strictly followed for both live and offline forensic |
| DF Analyst | Responsible for analyzing digital evidence from different sources and producing a report on the result |
| Lead Investigator | Responsible for organizing and coordinating the investigation activities. Also, involved in interpreting the finding from the report |
| Data Retention Specialist | Ensure the evidence management is kept in a proper and forensically sound manner, according to the policy and requirement |

- Protect the evidence by storing it in a safe place with limited accessibility
- Record all the processes involved in retrieving the evidence and information
- Ensure the result from the processes is reproducible

Apart from the chain of custody, the DF organization needs to comply with the well-defined DF investigation standard. Three standards can be referred to as ISO/IEC 27037, ISO/IEC 17025, and NIST SP 800-86 (Dilijonaite et al., 2017). Both ISO/IEC 27037 and NIST SP 800-86 focus on the general requirement for investigation processes, with NIST SP 800-86 outlining more detailed guidelines. The ISO/ IEC 27037 also highlighted the governance principle of DF with sufficiency, reliability, and relevance. On the other hand, ISO/IEC17025 outlines forensic laboratory requirements, including methodology, equipment handling, and quality assurance.

Another crucial aspect of DF readiness is the people. For a successful investigation, it is essential to define the person's roles and responsibilities in charge. Further, gathering the team with proper skill sets and competencies is vital to ensure the investigation processes run successfully. This scenario must be applied for both DF organization and non-DF organization as a part of proactive action. As suggested by Dilijonaite et al. (2017), both parties must be equipped with five roles or persons in charge, such as First Responders, DF Specialists, DF Analysts, Lead Investigators, and Data Retention Specialists. The responsibilities of these roles are given in Table 1.

The cyclical process, such as Aware, Alert, and Always-on (AAA) in the study of Collie (2018), can help the first responder proactively in handling the investigation. As the IR 4.0 involves complexity in the DF investigation, the concept known as the RACI matrix by Gobler and Dlamini (2010) can be included to clarify the practitioner's accountability and responsibility in the investigation process.

The study in Almarzooqi and Jones (2016) and Grobler (2011) highlights the importance of policy as it helps govern the process, people, and technology. As such, the DF organization must adopt policies across the other indicators to ensure the evidence's admissibility.

## 7. Maturity level for organization

The rapid development of technology affects not only human life but also the organization. Complexity, instability, and unforeseen factors lead to innovation in an organization that is sustainable to remain relevant to the changing environment (Attafar et al., 2013). Based on these three factors, evolutionary processes are fundamental to the maturity level of an organization. In general, the maturity level concept refers to evolution and development that involve organizational indicators, namely people, process, technology, ability, and willingness to adapt to the quality improvement practices.

Prodan et al. (2015) define people as the most valuable asset for organizations because, with the right skills and knowledge, efficient performance can be achieved and improved with other elements. The process is defined by the American Quality Association (AQS) as a set of work activities related to specific procedures for converting inputs into output. In contrast, technology is defined as equipment and techniques that include systems, designs, hardware, or software for communication and make the work process more efficient.

Attafar et al. (2013) emphasize the dimensions of individual maturity, procedure, and organizational agility to support the concept of organizational maturity level. It argues that organizational maturity cannot be achieved with only one-dimensional development. Individual maturity is fundamental to organizational growth as it involves the knowledge that forms through continuous training. On the other hand, the maturity of the procedure is necessary to well-balanced the working structure. Organizational agility refers to the rate of problem-solving that occurs within the organization. Although the study is implemented in the manufacturing industry, it is essential to highlight that the same dimensions can improve other sectors. It is because every organization must have at least these dimensions or indicators; people, process, and technology. It is supported by Zakaria and Yusof (2001), which states the organization's transition depends mainly on the strategic plan implementation, cooperation of the people, and adaption of the right technology as the tools.

Assessing organizational maturity is the first step that organizations need to improve with the changing environment. Maturity assessments can be used to measure an organization's current maturity level or baseline. At the same time, management can then identify strengths, areas of improvement and act on priorities to achieve higher maturity levels (Proenca and Borbinha, 2016). There are various methods for assessing the organization's maturity level, whether it is self-assessment through questionnaires, surveys, or standardized methods. The standards that can be used for reference are ISO / IEC TR 15504-7: 2008 Information technology - Process assessment - Part 7 - Assessment of organizational

**Table 2 – Comparison between maturity model in-field variation.**

| Field | Model | Description | Level |
|---|---|---|---|
| Project Management | Project Management Maturity Model | Evaluating the effectiveness of project management, starting from the implementation stage until a project is completed (Crawford, 2014) | 5 |
| Software Engineering | CMM | Measuring organizational effectiveness in software development (Crawford, 2014) | 5 |
| Business Process | Business Process Maturity Model | Measuring and improving business process efficiency (Lee et al., 2007) | 5 |
| IT | OITM | Measuring non-IT users' ability to use IT in their organization (Ragowsky et al., 2012) | 6 |

maturity issued by the International Standards Organization (ISO, 2008).

The maturity levels of an organization depend on the model chosen by the organization. Each model has a different number of levels that suit the purpose of the organization. For example, the Capability Maturity Model (CMM) contains five maturity levels, while Organizational Information Technology Maturity (OITM) has six levels (Paulk et al., 1993; Ragowsky et al., 2012). Other factors contributing to selecting specific models are variations in the organization's field, such as project management, software engineering, business process, and information technology. A comparison of the variation of the field, as mentioned above, is listed in Table 2.

In other aspects of designing the maturity assessment model, the study in Mettler (2011) highlights the need to define the application field's scope. When considering the DF field, it applies the technology and information to handle and retrieve the digital evidence. Thus, through the definition by Bourgeois and Bougeios (2014), the field of DF can be categorized as Information System because it combines people, processes, and technology to create, collect, and disseminate the relevant information in the organizational environment.

The study by Proenca and Borbinha (2016) outlines the twenty-two-maturity model for the field of Information System. The comparison result highlights that only four models define the maturity level, namely ISO/ IEC 15504 Model, Software Engineering Institute Capability Model Integration (CMMI), Information Technology Capability Model Framework, and COBIT Maturity Model. Thus, it shows a contradiction with the suggestion by Bourgeois and Bougeios (2009) that the model must have a predefined maturity level. It is noted that only nine models are evaluated, with proposed improvements after assessing maturity level. The rest of the models focus on general practice and do not specifically address the issue and problem after the maturity assessment. However, it is crucial to note the importance of the proposed improvement as it helps in practicality and reduces the organization's time for continuous and comprehensive improvement.

Documentation Process Maturity Model (DPMM) is proposed by Visconti and Cook (1998), to evaluate the documentation process and identify the practices for improving software development. This model's assessment is through a questionnaire that contains questions about the practicalities, indicators, and challenges in the documentation process. However, the attribute has not been named due to the model's focuses is the documentation system. Further, the assessment result is generally formed because it gives an advantage in terms of short-time consumption and less cost. Thus, to obtain detailed and specific improvement, the organization needs to allocate additional cost to refine the global assessment report. The model does not define every level of maturity but only includes grades from 1 to 4.

The Capability Maturity Model Integration (CMMI) is introduced in 2002 to enhance the Capability Maturity Model (CMM). Since CMM was developed in 1991, this model had been widely applied in various disciplines, such as system engineering, software acquisition, and labour management. However, the usage of CMM in other disciplines poses problems that impede the organization's ability to focus on practical and integrated improvement activities. In this regard, the CMMI has been developed to include a set of model integration. This set of models can identify various disciplines, integrate the training and support evaluation to solve the prior problem in CMM (Mahmood, 2016). The CMMI consists of 5 maturity levels, and the description of each level is listed in Table 3.

In addition to the definition of maturity level, CMMI names the attribute as Process Area. This attribute has four primary categories, namely, Process Management, Project Management, Engineering and Support. Subsequently, each category is divided into two (2) goals: Generic Goals and Specific Goals.These attributes and categories' advantage is to provide a precise and comprehensive evaluation output for each proposed improvement. A new version of CMMI (CMMI ver. 2) is introduced in 2019. This version has redefined the model's requirements into category areas, capability areas and practice areas (ISACA, 2019). The category areas, namely "doing, managing, enabling and improving". It further defines the capability areas within the organization's activities as listed in Table 4. The new definition of the category area gives a better understanding of how the organization's capability and maturity can be measured. In the preceding version, the focus is only on monitoring the individual process area and measuring its performance over time. However, this model gives a new dimension to translate the organization's progress to achieve maturity with a new definition. In the "doing" area, the aim is for the organization to deliver quality solutions, while in "managing", it ensures the operation runs accordingly. The "enabling" acts as the element to guide and support the activities of both "doing" and "managing" areas. In addition, this area can deliver suggestion to the "improving" area through analyzing practices within it. The "improving" area, on the

**Table 3 – Definition of Maturity Level for CMMI.**

| Maturity Level | Description |
|---|---|
| 1-Initial | There is a presence of the process, but it is unexpected with a weak control and reactive |
| 2-Managed | There is a project specified process but in reactive form |
| 3-Defined | There is existing of organizational process and in a proactive form |
| 4-Quantitatively Managed | The process is wholly measured and controlled |
| 5-Optimizing | The process always focus on improvement |

**Table 4 – Definition for category area in CMMI ver. 2.**

| Category Area | Description |
|---|---|
| Doing | It includes the capability areas to deliver quality services or products |
| Managing | It includes the capability areas to plan and manage the process and workforce |
| Enabling | It includes the capability areas to analyze, decision making, maintain the integrity of work and communicate with the stakeholders |
| Improving | It includes the capability areas to improve organizational performance |

**Table 5 – Definition for Maturity Level for COBIT 5.**

| Maturity Level | Description |
|---|---|
| 0-Non-existent | No process used at all |
| 1-Initia/Ad hoc | There is a process but not standardized |
| 2-Repeatable but Intuitive | The procedure in the process is followed but depending on the individual's knowledge |
| 3-Defined Process | The procedure in the process follows the standard, but it is not sophisticated enough |
| 4-Managed and Measurable | Compliance with the requirements of the procedure is measured, and significant errors are detected |
| 5-Optimized | There are process improvements to achieve best practices, and the differences are continually being reduced |

other hand, is responsible towards the improvement and sustainability for the organization performance. The model has twelve capability areas which cover; (1) quality, (2) development of product, (3) deliverable of service, (4) supplier, (5) work plan, (6) business resilience, (7) workforce management, (8) implementation on support, (9) safety management, (10) security management, (11) sustainability and persistence, and (12) performance improvement. In terms of the practices, it outlines 25 activities. However, some of the practices refer to the context of supplier management and product integration. Thus, only 22 of them are identified as relevant to the DF organization and can be modified to suit the DF environment. These practices are as follow;(1) Implementation Infrastructure, (2) Causal Analysis and Resolution, (3) Decision Analysis and Resolution, (4) Organizational Training, (5) Continuity, (6) Risk and Opportunity Management, (7) Peer Reviews, (8) Managing Performance and Management, (9) Process Quality Assurance, (10) Configuration Management, (11) Monitor and Control, (12) Planning, (13) Estimating, (14) Governance, (15) Process Management, (16) Verification and Validation, (17) Technical Solution, (18) Process Asset Development, (19) Requirement Development and Management, (20) Incident Resolution and Prevention, (21) Strategic Service Management and (22) Service Delivery Management.

In 2007, the Institute of Information Technology Governance introduced the Control Objectives for Information and Technology (COBIT 5) model to IT Administration organizations. Its framework is developed by using CMMI as a reference. One of the differences between COBIT 5 and CMMI is that it proposes six maturity levels, as outlined in Table 5. This model covers several areas such as policy, leadership, organizational structure, and processes to ensure that the field of IT enterprise is continually evolving with the organizational strategies and objectives (ISACA, 2017). For the COBIT 5 model, there are six (6) Enablers involved, such as (i) Consciousness and Communication, (ii) Policies, Plans and Procedures, (iii) Hardware and Automation, (iv) Skills and Expertise, (v) Accountability and Goals, and (vi) Measurements. Thus, with the specifically named attribute, the suggestion for improvements can be made more comprehensively and precisely.

The latest improvement of the COBIT model has been developed by the Information Systems Audit and Control Association (ISACA) in 2019. The critical difference in this new COBIT model is that it focuses on governance and management of IT enterprise, which allows this model to be widely used in organizations that embrace IT in their operations (Steuperaert, 2019). It categorizes the principle into two areas, such as Governance Systems Principles and Governance Framework Principles. The Governance Systems Principles comprise six items highlighting the governance system's core requirements. Whereas the Governance Framework Principles provide the items for developing the governance system for the enterprise. (Svata, 2019) concludes that the newest version of COBIT 2019 has been improved in four areas as stated in Table 6.

In COBIT 2019, there are some changes in terms of the definition compared to COBIT 5. The enablers in COBIT 5 remain the same but have been renamed as components

**Table 6 – Area(s) of Improvement in COBIT 2019.**

| Area(s) | Description |
|---|---|
| Flexibility and openness | The open design (definition and use of design factors) allowed IT enterprises to tailor according to their business focus without significantly impacting the proposed core model's structure and content. |
| Currency and relevance | The COBIT 2019 adopts the latest references (i.e., latest IT standards and compliance regulations), making it more relevant for IT enterprises to adapt. |
| Prescriptive application | According to the business model, the imposition of COBIT 2019 can be regarded as prescriptive due to its customization ability. The customization can be implemented by referring to the design factors. |
| Performance management of IT | The introduction of a performance management model in the new COBIT 2019 showed better configuration with its base model (CMMI). |

of the Governance Systems, while the IT Related Goals are renamed as Alignment Goals. The Core Model in COBIT 2019 is an upgraded version of the COBIT 5 Process Reference Model with three additional objectives (ISACA, 2019c).

Further, COBIT 2019 introduces two new concepts: focus area and design factor (ISACA, 2019a). The focus area represents the governance domain addressed by the governance and management objectives and their components. In the early phase of COBIT 2019, only a few focus area guidance is available, such as small and medium enterprises, security, information security, and DevOps. However, as COBIT 2019 represents an open-ended framework, the number of focus areas is unlimited, and DF may also be included. Design factors are the elements that can be applied to influence the design of an organization's governance system. There are 11 design factors, and they are broadly divided into three categories; (1) contextual, (2) strategic, and (3) tactical.

The design factors' application will impact the management objective priority or selection, focus area, and the components' variations. Initially, COBIT 2019 has 40 governance and management objectives; thus, the design factors can influence each objective's importance. Some design factors (e.g., risk, landscape threats, and development method) are different according to specific focus areas, resulting in variation in governance and management objectives. Nevertheless, the design factor can specify the required components based on their importance to achieving the governance and management objectives. ISACA (2019a) provide a guideline to design a tailored governance system for the organization.

COBIT's goals cascade represents the flow of transforming the stakeholder's needs into an actionable strategy in the organization. There are slight but fundamental changes between COBIT 5 and COBIT 2019. In COBIT 5, the goal cascade starts with the stakeholder drivers influencing the stakeholder needs, focusing on the value creation elements in governance objectives (e.g., benefits realization, risk optimization, and resource optimization). Subsequently, the stakeholder needs cascade to enterprise goals. However, in COBIT 2019, it simplifies the flow by taking both the stakeholder drivers and needs to cascade to the enterprise goals simultaneously.

Further, the enterprise goal is one of the critical design factors for a governance system in COBIT 2019. Thus, through the prioritization of enterprise goals, it supports the prioritization of management objectives. The enterprise goal is translated into priorities for the alignment goals that finally cascade to governance and management objectives. In COBIT 5, the enterprise goals are translated into IT-related goals, reaching the enabler goals. Both enterprise and alignment goals in COBIT 2019 have been reduced, updated, and clarified to avoid confusion during implementing the goals cascade (ISACA, 2019c). In terms of performance management, COBIT 5 uses Process Assessment Model (PAM) to determine the process's level capability. It is aligned with the ISO/IEC 15504 model (ISACA, 2017). However, COBIT 2019 uses COBIT Performance Model, which aligns with CMMI ver. 2, with the following concepts (ISACA, 2019c):

- Process activities are associated with the capability levels.
- Governance and management components have the capability levels for future guidance.
- The maturity levels are related to the focus area, which will be achieved if all required capability levels are achieved.

With the above-said concepts, COBIT 2019 is able to give a comprehensive overview of the organization's capability and maturity. The maturity level for the focus area in COBIT 2019 is given in Table 7.

With five (5) models selected, a comparison between them has been conducted to observe the practices of their usage for maturity level. The critical aspects of the comparison are the number of maturity levels, the definition, background of model developer, practicality, continuous assessment, and advanced improvement. Table 8 summarizes the comparison between these models.

Based on the comparative analysis of the five models, the CMMI and COBIT models have advantages over the DPMM as follows; (1) Each maturity level provides a definition that enables organizations to label their achievement level (2) Both have attributes that can facilitate organizations to identify benchmarks within their organization, thus, to focus on improvement (3) Both have proposed the improvements to be more specific on the attributes identified as immature and (4) Both encourage for continuous assessment and further improvement despite reaching the highest maturity level.

## 8. Model adaptation for DF organization

The maturity models have been developed in various fields due to the field's specialization factors, although some may be included in the same domain and relevant to each other. For example, the cybersecurity maturity model may not be fully utilized by the DF field even though these two areas are IT related.

**Table 7 – Definition for Maturity Level for COBIT 2019.**

| Maturity Level | Description |
|---|---|
| 0-Incomplete | Work may or may not be completed towards achieving the purpose of governance and management objectives in the focus area |
| 1-Initial | Work is completed, but the full goal and intent of the focus area not yet achieved |
| 2-Managed | Planning and performance measurement takes place, although not yet in a standardized way |
| 3-Defined | Enterprise standards provide guidance across the enterprise |
| 4-Quantitative | The enterprise is data-driven, with quantitative performance improvement |
| 5-Optimizing | The enterprise is focused on continuous improvement |

**Table 8 – Comparison between DPMM, CMMI 1.3, CMMI ver. 2, COBIT 5 and COBIT 2019.**

| Key Aspects | DPMM | CMMI (1.3) | CMMI (2.0) | COBIT 5 | COBIT 2019 |
|---|---|---|---|---|---|
| Number of Maturity Level | 4 | 5 | 6 | 6 | 6 |
| Definition of Maturity Level | - | Yes | Yes | Yes | Yes |
| Background of Model Developer | Academic | Academic | Industry | Industry | Industry |
| Practicality | General | Specific | Specific | Specific | Specific |
| Continuous Assessment | Not mentioned | Yes | Yes | Yes | Yes |
| Advanced Improvement | Not mentioned | Yes | Yes | Yes | Yes |

The US Department of Energy released the Cybersecurity Capability Maturity Model (C2M2) in 2014 to assess its department's cybersecurity (Miron and Muita, 2014). A year later, by referring to the core of the C2M2 model, Curtis et al. (2015) developed the Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services). It is for the use of IT services in the United States to evaluate security programs for cyberattacks. Although in the same field, the justification of this proposed model is based on the fact that IT services have different functions and frameworks than the Department of Energy in terms of the services, assets, and environment.

In the year 2019, the latest version of C2M2 has been introduced (DOE, 2019). It is organized into ten domains, which contain a group of cybersecurity practices. The ten domains are; (1) risk management; (2) asset, change, and configuration management, (3) situational awareness, (4) information sharing and communication, (5) supply chain and external dependencies management, (6) event and incident response and continuity of operations, (7) cybersecurity program management, (8) identity and access management, (9) threat and vulnerability management, and (10) workforce management. The model defines four maturity indicator levels (i.e., MIL0 to MIL3) with two particular objectives; approach and management. The approach objective focuses on thoroughness and completeness of activities in the domain, while the management refers to the extent to which the activities fix in the organization's operations. The model's key indicators are strategy, policy, improvement, quality (e.g., documentation), financial, technology, people, and process.

Another maturity model for cybersecurity is the Cybersecurity Maturity Model Certification (CMMC) by DoD (OUSD, 2020). It has five maturity levels and focuses on two types of maturity, such as the processes and best practices. Those processes and best practices are measured against the capability to protect sensitive information from a range of threats. It covers 17 domains that originated from Federal Information Processing Standards (FIPS) and NIST SP 800-171 and includes Asset Management, Recovery, and Situational Awareness. In this model, Level 3 can be considered maturity has been reached since it presents the capability to protect controlled unclassified information. Whereas, the Level 4-5 focus on the capability to reduce the risk of Advanced Persistent Threats.

Based on the examples of the above situations, it is to be expected that the DF organization needs to adapt the maturity model according to the DF work environment and norms. It is because the DF organization requires expertise, skills, processes, technology (hardware and software) to operate efficiently. Further, the DF organization is bound by different and specific laws. As a comparison, the scope of cybersecurity is more broader and more general than the scope of DF. Cybersecurity may involve three phases of the incident; pre, during, and post-incident, whereas DF will focus only on the post-incident and after the criminal activities have already been committed.

Subsequently, both C2M2 and DF readiness emphasized that the policy can be treated as a crucial indicator. For DF organization, its capabilities to perform can be divided into two views; (1) the ability to perform investigation and (2) the DF organization's ability as a whole. The second view is directed towards the management and development perspectives. Hence, it requires the policy to govern the available resources in DF organization to perform effectively and efficiently. It is supported by the work in Grobler (2011) and Almarzooqi and Jones (2016), which both introduce the framework for DF capabilities, namely Digital Forensic Management Framework (DFMF) and Digital Forensic Organization Core Capability (DFOCC), respectively. The work in Almarzooqi and Jones (2016) expresses the relationship of the indicators in the equations and defines the policy as the multiplier in which the other indicators cannot exist without it. Further, both DFMF and DFOCC can act as the baseline to obtain the indicators of maturity model as the works in-

clude elements from the perspectives of people, process and technology.

*A. Cloud Forensic Maturity Model (CF-MM)*

Ruan and Carthy (2012) has developed a specific maturity model of DF for the cloud computing environment. This model applies the CMM basic model as a reference. The uniqueness of this model is the integration of Cloud Forensic Investigative Architecture (CFIA) and Cloud Forensic Capability Matrix for the maturity assessment. Hence, it enables the DF agencies to measure their ability to perform the cloud forensic but follow the rules of investigation as recommended by the CFIA only. The CFIA consists of four investigation methods: Pre-Investigation, Forensic Process, Support Process, and Investigation Interface.

This model is useful for measuring agencies' ability to handle and perform cloud forensic for suitability and practicality. However, it is not practical for other IR 4.0 technologies such as IoT and blockchain or cryptocurrency. Therefore, the enforcement agencies need to select another model to measure the maturity of other IR 4.0 related technologies as they require different DF investigation processes when compared to cloud computing.

*B. Digital Investigation - Capability Maturity Model (DI-CMM)*

Kerrigan (2013) has adopted the CMMI model to measure DF process maturity based on three benchmarks: people, process, and technology. By ignoring the general and specific objectives of the DF process, this model focus on identifying key features based on the Extended Model of Cybercrime Investigation (EMCI) by Ciardhuain (2004). The work supports the EMCI as the best process model that represents all the phases and activities involved in the DF investigation process. The EMCI model has eleven (11) DF investigative processes ranging from authorization to the presentation of the digital evidence.

However, similar to CF-MM, this model is only suitable with specific DF organization that implements the EMCI process. Whereas, with different kinds of processes, it may need to be modified to ensure it is compatible with them. In the context of IR 4.0, this model does not explicitly recommend a mechanism to measure the latest DF investigation process, such as towards cloud computing, IoT, and blockchain (cryptocurrency). Nevertheless, the model has only been tested on the DF investigation in Ireland. Hence, it requires further case study to ensure it can be applied to other regions as it may involve another type of law and regulation.

*C. Digital Forensic - Comprehensive Capability Maturity Model (DF-C2M2)*

Hanaei and Rashid (2014) has presented the first model dedicated to measuring the level of maturity of the DF organization according to the standard. This model adopts the basic Open-Source Security Testing Methodology Manual 2 (OSSTMM 2) model that has the same requirements as the ISO / IEC 17025 standard. Three (3) fundamental indicators of the organization, namely people, process, and equipment, are included as benchmarks based on existing DF frameworks.

The model considers selecting specific categories according to four types of DF organizations; enforcement agencies, non-law enforcement agencies, judiciary bodies, and unit functions. As for the DF services, DF-C2M2 further details up to the seven types, including Computer Forensics, Mobile Device Forensics, Audio Forensics, Video Forensics, Network Forensics, Cyber Crime Analysis, and Digital Evidence Handling Support. However, the latest DF services or processes, namely IR 4.0 technologies such as cloud computing, IoT, and blockchain (cryptography), are not available for measurement.

*D. Digital Forensic Capability Maturity Model Integration (DFCMMI)*

Profitt (2019) has introduced a model for capability maturity based on CMMI for the DF organization. The model has five levels of maturity and is based on the calculated scoring. However, the study does not mention any indicator for the model. It can be assumed that it focuses on the DF investigation process as it compares several DF framework and models. The newer forensic area is highlighted but not specifically, as the study include process model for obtaining the network-based artifacts.

*E. Digital Forensic Readiness - Capability Maturity Model (DFR-CMM)*

Most recently, Englbrecht et al. (2019) have introduced a model that can measure DF maturity level and subsequently determine DF organizations' availability. DF's availability is defined as a step towards changing the DF investigation perspective from passive to proactive. This proactive perspective is seen as identifying the space and capabilities of the DF organization to move forward in the face of the changes and challenges. Therefore, this model's advantage is that it can measure maturity levels and assess DF readiness aspects. These aspects of readiness are categorized into two (2) aspects, namely infrastructure and organization.

The model is adapted from the combination of CMMI and COBIT 5. It has been improved by incorporating seven features of the enabler; Principles and Policies, Processes, Organizational Structure, Information, Conduct, Skills and Competencies, and Infrastructure. However, it is not mentioned whether the enforcement agencies can apply the possibility of this DFR-CMM. Also, the study states that the DF process should be kept up-to-date with current technological developments as it is focused on availability.

By comparing all the above models for DF, it shows three models adapt the CMMI as the core model. As mentioned earlier, this model has the advantage of its suitability for the start-up organization and focus on improvement. Thus, it is proof that the CMMI can be considered an appropriate model for the information systems and DF. Another finding is that law enforcement agencies can use three proposed models as the models include the legal aspects. Simultaneously, only CF-MM focuses explicitly on the technology in IR 4.0, while the DFR-CMM states the importance of keeping up-to-date with the current technology.

Additionally, DFR-CMM applies the COBIT 5 PAM model, in which the process goals will be the outcome to measure the maturity level. For the DFR-CMM to work based on ISO/IEC 33000, a few modifications to the process outcomes must be implemented as suggested in ISACA (2019b). Under the ISO/IEC 33000 evaluation, the following must be performed on DFR-CMM:

- The process outcomes must be linked to process practices on a one-to-one basis.
- Base practices are equal to the COBIT 2019 process practices for each governance objective.

- The work products are equal to the information of the governance or management objectives in ISACA (2019b).

## 9. DF maturity level indicators

The People-Process-Technology (PPT) indicator has long been recognized as the key to improving an organization. Historically, the concept of strategic change in an organization commenced with Leavitt's Diamond, introduced by Harold Leavitt in 1965. The model contains four organizational components, namely people, structure, tasks, and technology. Meanwhile, the Information Technology Infrastructure Library (ITIL) framework is the first to introduce this People-Process-Technology concept for services management organizations in the IT field.

In the DF field, the PPT indicator can be recognized as crucial for its success. In the operational scenario, the DF organization must be equipped with the latest hardware or software (Technology) to accelerate the DF processes (Process), while the practitioner should have the analytical skills and expertise (People) to ensure the efficient investigation. Thus, for improvement, each element must be improved simultaneously to achieve the organization's aims and objectives.

The PPT indicator has been evolved throughout the time for the application in organizations with various fields. In software engineering, Buttles-Valdez et al. (2008) included the Organizational Culture as a part of the PPT indicator. In 2009, Pearson (2009) argued that information and technology are two different elements for IT-related organizations. Hence, it suggested to include information as a new indicator for the PPT. Prodan et al. (2015) had developed a model for improving the services field by adding three indicators; customer focus, innovation, and management function. Through all these examples, it can be shown that the PPT indicator remains the crucial, relevant, and necessary factor for the improvement of the organization, although the new element is introduced over the time.

Based on the analysis of the five DF maturity models from the previous section, it is found that all of them use the PPT indicator. In addition to that, each of the models further refines the indicator of PPT depending on the focal point of its maturity model. Nevertheless, the models include some additional elements to suit their model. For example, Ruan and Carthy (2012) delves deep into the indicator of process, namely cloud computing investigative processes, and added legal elements as the study's scope involved enforcement agencies. This step is followed by Kerrigan (2013), where it introduces the process indicator into eleven processes to predict the DF process's maturity.

Furthermore, Hanaei and Rashid (2014) added organizational elements in the DF-C2M2 maturity model. On the other hand, Englbrecht et al. (2019) added four additional enablers in addition to PPT as it claims them as a concept that allows for the guideline's development related to future challenges. By doing so, the study is able to focus on the scope of DF Readiness.

In this regard, it can be concluded that the People-Process-Technology indicator remains relevant and should be used by the DF field and may even be improved by other indicators. The reason behind it is because this indicator is essential for the continuous improvement strategy in the focus area required by this study. Additionally, other cybersecurity indicators can be included in developing the maturity model for the DF organization.

Through the selection, this study discovers eleven (11) studies that are recommended and necessary in the field of cybersecurity and DF. Seventeen indicators have been compared, as shown in Table 9.

From Table 9, seven (7) models are categorized in the DF field. Five of these models have been discussed previously, namely models from Kerrigan (2013), Hanaei and Rashid (2014), Almarzooqi and Jones (2016), Grobler (2011) and Englbrecht et al. (2019). Amann and James (2015) defines and identifies the key indicators required by the DF laboratory to remain robust and resilient in conducting investigations. Meanwhile (Park et al., 2015) introduced a model and index that includes organizations, humanities, technology, facilities, and processes to assess DF organizations' capabilities.

In the field of cybersecurity, TGCSCC (2016) has developed a state-of-the-art Cybersecurity Capability Model that focuses on evaluating critical indicators as a benchmark for a country's ability to increase its capacity in cybersecurity. ASPI (2017), on the other hand, measures the maturity of countries in the Asia Pacific from open-source studies. The Global Cyber Security Index was developed by ITU (2018) to measure the country's commitment to cybersecurity and enhance its awareness. Meanwhile, Rikk (2018) has released the National Cyber Security Index, which assesses the country's readiness to prevent cyber threats and manage cyber incidents.

Based on Table 9, it can be concluded that most of the recent studies indicate technology as the most crucial parameters in the field of cybersecurity and DF. The hardware tools and technology are a prerequisite for the DF organization, as emphasized by Park et al. (2015). Besides, Kerrigan (2013) and Hanaei and Rashid (2014) agreed that the availability of specialized hardware and technology is necessary to measure the organization's maturity in carrying out DF activities. Rikk (2018) notes that the use of technology should contribute to an organization's maturity. The hardware and technology must, therefore, be in line with current technological developments as required by TGCSCC (2016), whereas ITU (2018) and Englbrecht et al. (2019) incorporate the technical indicator along with the technology because the adaptation of the technology without the technical expertise will cause the organization to remain weak and will not show a proper maturity. For example, DF organizations equipped with state-of-the-art hardware and software (technology) will not effectively conduct digital evidence-based investigations if analysts do not have the expertise and skills to use them (technical).

In consideration of the technical and tools, the attention should be focused on the data's nature. As the data volume becomes massive, the DF organization needs to consider the mechanism to control and manage it. Current tools with the evidence-finding specification are not suitable for massive data. Thus, the solution such as artificial intelligence, big data analytic, data mining, and data reduction must be the features to be added in the technology and technical indicator. Together with the increase in equipment's power, these features could be implemented to handle the complex issue and

**Table 9 – Comparison of the suggested parameter in previous studies.**

| Previous Study | People | Process | Technology & Technical | Collaboration | Capacity Development | Policy Framework | Standard | Development | Organization | Facility Operation | Law & Regulation | Culture & Ethics | Management | Monetary | Military Application | Digital Economy | Information |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Englbrecht et al. (2019) | 1 | 1 | 1 | | 1 | 1 | | | 1 | | | 1 | | | | | 1 |
| Rikk (2018) | | | 1 | 1 | | 1 | | | 1 | | 1 | | | | | | |
| ITU (2018) | | | 1 | 1 | 1 | | | | 1 | | 1 | | | | | | |
| ASPI (2017) | | | | 1 | | | | | | | | | 1 | 1 | 1 | 1 | |
| TGCSCC (2016) | | | 1 | | 1 | 1 | | | 1 | | 1 | 1 | | | | | |
| Park et al. (2015) | 1 | 1 | 1 | | | | | | 1 | 1 | | | | | | | |
| Amann and James (2015) | 1 | | | 1 | 1 | 1 | 1 | 1 | | | 1 | | | | | | |
| Hanaei and Rashid (2014) | 1 | 1 | 1 | | | | | | | | | | | | | | |
| Kerrigan (2013) | 1 | 1 | 1 | | | | | | | | 1 | | | | | | |
| Almarzooqi and Jones (2016) | 1 | 1 | 1 | | | 1 | | | | | | | | | | | |
| Grobler (2011) | 1 | 1 | 1 | | | 1 | | | | | | | | | | | |

address the issue associated with capacity and speed. If the cases require data collection from multiple remote servers, blockchain technology can be introduced to protect the evidence's volatile nature. Besides that, the issue in the quality of using the tool must be solved. The DF practitioner must not apply the tool to any investigation without a proper validation process. It ensures that the tools (Technology) function correctly, which produce valid outputs, and they are reproducible with other DF tools. It is good to highlight that the validation process is crucial for DF operations as it represents one of the requirements in ISO 17025.

The people indicator is one of the elements that need to be considered. The process of selecting staff with basic skill eligibility is one of the most critical elements to be considered (Park et al., 2015). Amann and James (2015) set the criteria necessary to demonstrate people's maturity, namely the latest knowledge, expertise in a particular field, and adequate training and courses. Subsequently, as suggested by Kerrigan (2013) and Hanaei and Rashid (2014), DF staffs have to improve themselves with the development of expertise, capability, and efficiency in adapting to new knowledge. This suggestion can be considered as the best approach to ensure that the DF practitioners are on par with the ordinary people in society in terms of scientific knowledge. The DF practitioner must be aware of the current techniques and methods that are useful for increasing the investigation's efficiency and preparing against any anti-forensic mechanism. In addition to training, Englbrecht et al. (2019) proposes assessment by including the aspects of awareness and understanding in the field of DF. It is due to the justification that the number of training does not indicate the actual competency level except with tests and assessments. The DF organization may introduce a formal knowledge of bias as part of its qualification and professional certification. This is crucial to ensure the DF practitioner conducts a fair observation and analysis during the investigation.

Moreover, Rikk (2018) suggests that organizations must establish a robust organizational structure specific to their scope. Incidentally, ITU (2018) states that organizations should coordinate institutional policies with strategies for continuous development to achieve the desired maturity level. Specialization is essential for an organization's functioning that usually consists of management and operational teams (TGCSCC, 2016). Although there is a division of responsibilities, Englbrecht et al. (2019) emphasized that there must be a centralized system on the organizational structure to coordinate each section's tasks to achieve organizational objectives.

Another indicator that should be included in the measurement of the maturity level is the process. Hanaei and Rashid (2014) states that organizations with labs must follow the process as prescribed by the international ISO 17025 standards. Although it does not specify that DF organizations should follow ISO 17025 standards, it emphasizes the importance of focusing on the criteria at each stage of the DF process. Nevertheless, all these studies point out that process documentation is one of the measurements for organizational maturity. On the other hand, for DF organizations belonging to the Non-Enforcement Agency, it is proposed to design their business process with automation to enhance the DF organization's efficiency.

**Table 10 – Description of Indicators for Proposed Maturity Model of DF Organization.**

| Indicator | Description |
|---|---|
| 1-People and Capacity Development | DF comprises management or policymakers who manage and support operations such as first responders, analysts, enforcement officers, and investigators. All members at the organizational level must undergo capacity development to enhance their skills and expertise in DF. |
| 2-Organization, Policy and Cooperation | The DF organization provides guidance to practitioners on their role in ensuring the DF operation and investigation is accurate, forensically sound and compliant with the standard. The policy will govern the people, process, technology, and organization. Additionally, organizations should work with external partners as a means of sharing skills and expertise. |
| 3-Process | DF investigation process needs to be recognized and capable of producing the required analytical reports. The existence of the latest investigative processes related to the IR 4.0 technology is taken into consideration for the measurement of DF's maturity and readiness for the IR 4.0 challenges. |
| 4-Technology and Technical | Existing advanced hardware and software for investigation are critical elements determining an organization's ability to conduct analysis and produce accurate reports accepted by the court. According to the latest technology, advancement and improvement in hardware and software indicate the maturity and readiness of the DF organization. |
| 5-Legislation and Regulation | Law enforcement agencies that conduct DF investigations are bound by legislation and regulations. Assessments should be made to ensure the effectiveness of the current legislation and regulations in force or require improvement. |

The University of Oxford's cybersecurity maturity model states that people, process, and technology indicators are inadequate to combat cybercrime. It highlights the cybercrime trends such as intellectual property theft, data protection issues, and child pornography as international issues and proposes a holistic approach to the legal framework (TGCSCC, 2016). It is agreed by ITU (2018), which clarifies that laws and regulations are the underlying response mechanism to contain and penalize cybercriminals. Therefore, it suggests that organizations should be provided with relevant and sufficient legislation to conduct cybercrime investigations. The legal parameter has been suggested by Kerrigan (2013) as it highlights that compliance with relevant laws and regulations is vital to DF organizations. Amann and James (2015), on the other hand, places a high degree of maturity on DF organizations when it comes to formulating a legal strategy for resolving transnational or external jurisdictions issue. As the emerging technologies in IR 4.0 create a barrier for the DF investigation to function efficiently, a consideration on suggesting any relevant substantive law to these technologies is welcomed. Besides, a few points in law and regulation that involve the application of emerging technologies should be clear to all DF community as a way to improve the investigation. Thus, it includes the regulation on the evidence and the role of the service provider.

Based on the comparison of the above models, this study concludes that the five parameters discussed above, namely, technology and techniques, people, organization, process and legal, are the main benchmarks for measuring the level of maturity of the DF organization. However, it does not reject other parameters' recommendations as they can be integrated with the five significant parameters.

For cooperation and policy, this study combines them with the organization parameter. Amann and James (2015) highlight that DF organizations should work in partnership with the academic and private sectors, while the policy is an essential guide. Based on these two (2) justifications, we have combined these three parameters and named them Organizational, Policy and Cooperation.

The capacity development is considered as a part of the merit for the maturity index. ITU (2018) explains that this parameter is essential for producing qualified professionals for the organization. Since it is related to the human parameter, both parameters are incorporated together in the People and Capacity Development.

From the discussion and incorporation between the indicators, the leading indicators to measure the maturity of the DF organization have been identified as; (1) People and Capacity Development, (2) Organization, Policy and Cooperation, (3) Process, (4) Technology and Technical and (5) Legislation and Regulation. The description of these indicators is outlined in Table 10.

The indicators in Table 10 can be adapted together with the practice areas from CMMI ver. 2 practice areas to create the practices. Subsequently, the concept in COBIT 2019 can be applied to outline the possible governance and management objectives for guiding the DF organization in the IR 4.0 era. The list of these practice areas can be linked together with the indicators to describe the activities that contribute to the capability and maturity of DF organization. Table 11 outlines the relationship between the indicators with the CMMI ver. 2 practice areas, while Table 12 presents the DF activities according to those practice areas.

Based on Tables 11 and 12, the DF organization's operation can complement the CMMI ver. 2 practice areas. The People and Capacity Development contains two practice areas such as "doing" and "managing". While the Organization, Policy and Cooperation indicator outlines the highest number of CMMI ver. 2 practices. These practices focus on the governance, decision making, monitoring and improvement of the DF organization. In the Process indicator, three essential practices are involved; (1) delivering the quality processes (i.e., during the investigation), (2) support the processes through proper documentation and (3) improve the existing processes (i.e., through process management and process asset development practices). The Technology and Technical indicator focus on delivering the quality solution and improving the existing technology to assist in DF operation. Legislation and Regulation

**Table 11 – Relationship between DF indicators with CMMI ver. 2 practices area.**

| Indicator | CMMI ver. 2 Practice Area |
|---|---|
| 1-People and Capacity Development | Organizational Training (M), Risk and Opportunity Management (M) and Peer Review (D) |
| 2-Organization, Policy and Cooperation | Causal Analysis and Resolution (E), Decision Analysis and Resolution (E), Continuity (M), Estimating (M), Planning (M), Managing performance and management (I), Incident resolution and prevention (M), Monitor and Control (M), Governance (I) and Requirement Development and Management (D) |
| 3-Process | Process Quality Assurance (D), Configuration Management (E), Process Management (I) and Process Asset Development (I) |
| 4-Technology and Technical | Implementation Infrastructure (I) and Technical Solution (D) |
| 5-Legislation and Regulation | Verification and Validation (D), Service Delivery Management (D) and Strategic Service Management (D) |

**Table 12 – Description of DF organization activities according to CMMI ver.2 Practice Areas.**

| CMMI ver. 2 Practice Area | Description for DF organization activities |
|---|---|
| Implementation Infrastructure | Provide the technology need and framework to ensure the DF process and investigation can be performed smoothly and in forensically sound manner |
| Causal Analysis and Resolution | Identifies the cause of outcomes from the problem in DF operation and take action to prevent recurrence of negative outcomes or ensure recurrence of positive outcome |
| Decision Analysis and Resolution | Helps in making decision by evaluating the DF operation and investigation |
| Organizational Training | Provides the strategy and capability for appropriate professional training to support the DF operation, meet the current needs, and deliver the training across the organization |
| Continuity | Plans and validates the critical set of resources to ensure DF operations and investigation can be continued |
| Risk and Opportunity Management | Identify the threats and opportunities in DF operation and investigation |
| Process Quality Assurance | Ensure the well-defined DF process is followed and the quality is maintained |
| Configuration Management | Ensure the integrity of the process and investigation through proper documentation, control and audits |
| Monitor and Control | Provides appropriate corrective actions to DF operation and investigation, if there is an issues or challenges |
| Estimating | Forecast the required resources and costs to deliver a forensically sound operation and investigation |
| Governance | Provide guidance to DF practitioner on their role to ensure the DF operation and investigation perform in forensically sound manner |
| Process Management | Manage and implement the continuous improvement of the DF processes and infrastructures to meet the current needs in DF operation and investigation |
| Verification and Validation | Ensure the DF operation and investigation meets the requirement for evidence admissibility to the court of law |
| Technical Solution | Obtain the appropriate technology solution to ensure it meets the requirement for DF operation and investigation |
| Peer Review | Identify and address the issues in DF operation and investigation with peers, colleagues and subject matter expert to get the solution |
| Planning | Determine the necessary resources to accomplish the DF operation and investigation, within the costs |
| Managing performance and management | Managing performance through analysis to achieve the DF organization's objective |
| Process asset development | Develop and keep update on the DF process in order to response to the need in the DF operation and investigation |
| Requirement Development and Management | To enable and keep update the common understanding between the DF's needs and the expectation of DF solution in investigation |
| Incident resolution and prevention | Identify the actual and potential challenges that can impact the deliverable of the DF operation and investigation |
| Service delivery management | Deliver the DF service such as investigation to the expectations of the court of law and in high quality result |
| Strategic service management | Develop and keep the portfolio of DF processes for investigation so that it is relevant and compatible with current situation and Df organizational need |

aims to ensure the DF operation and investigation can be adequately delivered in high quality and forensically sound manner (i.e., "doing" category area in CMMI ver. 2).

The contents of practice areas in CMMI ver. 2 are then modified accordingly to represent the DF domain practices. The proposed CMMI ver. 2 practices for the DF domain are listed in Appendix A. Further, to ensure compliance with governance and management objectives, the proposed CMMI ver. 2 practices are compared with the information on COBIT 2019 practices in ISACA (2019b). The purpose of the comparison is to highlight the interrelation between the proposed CMMI ver. 2 practices with COBIT 2019 and identify the

**Table 13 – Relationship between CMMI ver. 2 practices for DF organization with COBIT 2019 practices.**

| Proposed CMMI ver. 2 Practices | COBIT 2019 Governance and Management Objectives (Related Practices) |
|---|---|
| Organizational Training | APO07, DSS04 (for.04) |
| Risk and Opportunity Management | EDM01, EDM03, AP008, APO12, BAI08, DSS03 |
| Peer Reviews | APO01, APO07, BAI08 |
| Causal Analysis and Resolution | EDM03, MEA03, APO08, APO12, BAI08, DSS03, MEA01 |
| Decision Analysis and Resolution | MEA01, MEA02, APO02, BAI04 |
| Continuity | EDM04, DSS04 |
| Estimating | EDM04, APO02 |
| Planning | EDM04, BAI04, BAI05, MEA01 |
| Managing Performance and Management | APO01, APO14, BAI01, BAI08, MEA01 |
| Incident Resolution and Prevention | APO08, APO12, DSS03 |
| Monitor and Control | APO12, BAI04, DSS03, MEA01 |
| Governance | EDM01, APO01, APO02, BAI01, BAI08 |
| Requirement Development and Management | EDM01, APO02, APO08, BAI04, MEA02 |
| Process Quality Assurance | APO11, MEA02, MEA03 |
| Configuration Management | APO14, DSS01, DSS06, MEA02, MEAO4 |
| Process Management | EDM04, APO11, BAI08 |
| Process Asset Development | BAI03, MEA01, APO11, MEA03, MEA04 |
| Implementation Infrastructure | APO01, DSS01, BAI09, MEA03, MEA04 |
| Technical Solution | BAI02, BAI03, DSS01 |
| Verification and Validation | DSS01, DSS06, MEA02, MEA03 |
| Service Delivery Management | APO14, DSS06, MEA02, MEA03, MEA04 |
| Strategic Service Management | APO02, APO05 |

possible governance and management objectives for the DF organization. Table 13 highlights the governance and management objectives for the proposed CMMI ver. 2 practices. Thus, from Table 13, the list of COBIT 2019 governance and management objectives for governing DF organization are as follows; EDM01 Ensured Governance Framework Setting and Maintenance, EDM03 Ensured Risk Optimization, EDM04 Ensured Resource Optimization, APO01 Managed I&T Management Framework, APO02 Managed Strategy, APO07 Managed Human Resources, APO08 Managed Relationships, APO12 Managed Risk, APO11 Managed Quality, APO14 Managed Data, BAI01 Managed Programs, BAI02 Managed Requirement Definition, BAI03 Managed Solutions Identification and Build, BAI04 Managed Availability and Capability, BAI05 Managed Organizational Change, BAI08 Managed Knowledge, BAI09 Managed Assets, DSS01 Managed Operations, DSS03 Managed Problems, DSS04 Managed Continuity, DSS06 Managed Business Process Controls, MEA01Managed Performance, and Conformance Monitoring, MEA02 Managed System of Internal Control, MEA03 Managed Compliance with External Requirements and MEA04 Managed Assurance.

Based on the mapping between proposed CMMI ver. 2 practices against the COBIT 2019 governance and management objective's practices, the priority for the objectives can be divided into three categories:

- Strong (5-6): EDM01, APO02, BAI08, MEA01, MEA02 and MEA03
- Medium (3-4): APO07, APO08, APO11, APO12, BAI04, DSS01, DSS03 and MEA04
- Low (1-2): EDM03, EDM04, APO01, APO05, APO14, BAI01, BAI02, BAI03, BAI05, BAI09, DSS04 and DSS06

## 10. Conclusion

This paper highlights the concept and impact of the IR 4.0 implementation, where the development of the technology poses challenges to both cybersecurity and DF. Due to these challenges, it gives the sign and signal to the DF organizations to implement changes to remain relevant in accordance with technological advancement. Initially, it will require a mechanism to measure the maturity and readiness of the DF organization in handling the cases related to IR 4.0. Hence, this paper outlines five indicators for consideration to develop the DF organization's maturity model related to IR 4.0. These indicators are derived from the previous studies on the cybersecurity and DF maturity model. The work also suggests the potential practices based on the CMMI ver. 2 practice area. By comparing them with information from ISACA (2019b), it is able to list out 28 suggested governance and management objectives (as shown in Table 13) that can be used to guide the DF organization concerning IR 4.0. For future work, it is proposed to develop the DF organization's governance system based on the COBIT 2019 design factors and integrate it with the above indicators. This model is proposed to be implemented in measuring the maturity and readiness of the DF organization, especially in Malaysia, and to envisage the transformation of the digital investigation landscape according to IR 4.0 technology. The current study's limitation is that it neither covers an extended exposure to digital technologies nor addresses digital technologies' evolution. In terms of the technology, the study only presents a suggestion on the importance of including some IR 4.0 solutions to assist in the DF investigation, especially when dealing with increasing power, massive data, and complexity. As the paper is based on the previous studies' review, it limits the scope based on the keywords and requirements given in the methodology.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## CRediT authorship contribution statement

**Khairul Akram Zainol Ariffin:** Conceptualization, Writing - original draft, Writing - review & editing, Funding acquisition, Supervision. **Faris Hanif Ahmad:** Data curation, Writing - original draft, Validation, Methodology.

## Acknowledgement

The authors would like to thank the Ministry of Education on the support given through grant FRGS/1/2018/ICT04/UKM/02/3. Additionally, we would like to express our appreciation to Universiti Kebangsaan Malaysia and Faculty of Information Science and Technology on their support under grant GUP-2019-062.

## Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.cose.2021.102237.

## REFERENCES

AGC, 2017. Laws of Malaysia Evidence Act 1950.

Ahmad NH, Hamid SSA, Shahidan NSS, Ariffin KAZ. Cloud forensic analysis on pCloud: from volatile memory perspectives, vol 332; 2020. p. 3–15. doi:101007/978-3-030-60036-5_1.

Almarzooqi A, Jones A. A framework for assessing the core capabilities of a digital forensic organization. In: Peterson G, Shenoi S, editors. In: Advances in Digital Forensics XII, IFIP AICT 484; 2016. p. 47–65. doi:10.1007/978-3-319-46279-0_3.

Alqahtany S, Clarke N, Furnell S, Reich C. Cloud forensics: a review of challenges, solutions and open problems. In: 2015 International Conference on Cloud Computing (ICCC); 2015. p. 1–9. doi:10.1109/CLOUDCOMP.2015.7149635.

Amann P, James JI. Designing robustness and resilience in digital investigation laboratories. Digit. Invest. 2015;12:S111–20. doi:10.1016/j.diin.2015.01.015.

Antonakakis M, April T, Bailey M, Bernhard M, Bursztein E, Cochran J, Durumeric Z, Halderman JA, Invernizzi L, Kallitsis M, Kumar D, Lever C, Ma Z, Mason J, Menschar D, Seaman C, Sullivan N, Thomas K, Zhou Y. Understanding the mirai botnet. In: 26th USENIX Security Symposium; 2017. p. 1093–110.

Ariffin KAZ, Mahmood AK, Jaafar J, Shamsuddin S. Tracking file's metadata from computer memory analysis. In: 2015 IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing; 2015. p. 975–80. doi:10.1109/CIT/IUCC/DASC/PICOM.2015.147.

ASPI. Cyber Maturity in the Asia-Pacific Region 2017. The Australian Strategic Policy Institute; 2017.

Atlam HF, Hemdan EE-D, Alenezi A, Alassafi MO, Wills G. Internet of things forensics: a review. Internet Things 2020:100220.. doi:10.1016/j.iot.2020.100220.

Attafar A, Barzoki AS, Radmehr R. Determine the level of maturity of organization and organizational agility in industrial companies (case of study: Fakour industrial company). Int. J. Acad. Res.Bus. Social Sci. 2013;3(2):240–57.

Baig ZA, Szewckk P, Valli C, Rabadia P, Hannay P, Chernyshev M, Johnstone, Kerai P, Ibrahim A, Sansurooah K, Sted N, Peacock M. Future challenges for smart cities: cyber-security and digital forensics. Digit. Invest. 2017;22:2–13. doi:10.1016/j.diin.2017.06.015.

Basu S, Bardhan A, Gupta K, Saha P, Pal M, Bose M, Basu K, Chaudhury S, Sarkar P. Cloud computing security challenges & solutions-a survey. In: 2018 IEEE 8th Annual Computing and Communication Workshop and Conference (CCWC); 2018. p. 347–56. doi:10.1109/CCWC.2018.8301700.

Bernhard, T., 2019(accessed October 28, 2019). Understanding the Shared Responsibility Model for Cloud Security. https://cloudcheckr.com/cloud-security/shared-responsibility-model/.

Bouafif H, Kamoun F, Iqbal F, Marrington A. Drone forensics: challenges and new insights, 109; 2018. p. 1–6. doi:10.1109/NTMS.2018.8328747.

Bourgeois, D., Bougeios, D. T., 2009. A Design Science Research Perspective on Maturity Models in Information Systems.

Bourgeois, D., Bougeios, D. T., 2014(Accessed October 30, 2019). Chapter 1: What Is an Information System? In Information Systems for Business and Beyond. https://bus206.pressbooks.com/chapter/chapter-1/#footnote-5-3.

Brier Jr TF. Defining the limits of governmental access to personal data stored in the cloud: an analysis and critique of microsoft Ireland. J. Inf. Policy 2017;7:327–71. doi:10.5325/jinfopoli.7.2017.0327.

Buric J, Delija D. Challenges in network forensics. In: 2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO); 2015. p. 1382–6. doi:10.1109/MIPRO.2015.7160490.

Buttles-Valdez P, Svolou A, Valdez F. A holistic approach to process improvement using the people CMM and the CMMI-DEV: technology, process, people, & culture, the holistic quadripartite. SEPG 2008 Conference, Software Engineering Institute, 2008.

Chen H-Y. Cloud crime to traditional digital forensic legal and technical challenges and countermeasures. In: 2014 IEEE Workshop on Advanced Research and Technology in Industry Applications (WARTIA); 2014. p. 990–4. doi:10.1109/WARTIA.2014.6976441.

Ciardhuain SO. An extended model of cybercrime investigations. Int. J. Digit. Evid. 2004;3(1):1–22.

Cisco, 2010. Cisco 2010 Annual Security Report.

Collie J. A strategic model for forensic readiness. Athens J. Sci. 2018;5(2):161–82. doi:10.30958/ajs.5-2-4.

Conti M, Gangwal A, Ruj S. On the economic significance of ransomware campaigns: a bitcoin transactions perspective. Comput. Secur. 2018;79:162–89. doi:10.1016/j.cose2018.08.008.

Crawford JK. Project Management Maturity Model Providing a Proven Path to Project Management Excellence. Auerbach Publications; 2014.

Curtis P, Mehravari N, Stevens J. Cybersecurity Capability Maturity Model for Information Technology Services (C2M2 for IT Services), Version 1.0; 2015.

Damshenas M, Dehghantanha A, Mahmoud R, Shamsuddin S. Forensics investigation challenges in cloud computing environments. In: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec); 2012. p. 190–4. doi:10.1109/CyberSec.2012.6246092.

Dilijonaite A, Flaglien A, Sunde IM, Hamm JP, Sandvik JP,

Bjelland PC, Franke K, Axelsson S. Digital Forensic Readiness. Wiley; 2017.
Dimpe PM, Kogeda OP. Generic digital forensic requirements. In: 2018 Open Innovations Conference (OI); 2018. p. 240–5. doi:10.1109/OI.2018.8535924.
DOE, 2019(accessed August 8, 2020). Cybersecurity Capability Maturity Model (C2M2) Version 2.0. https://www.energy.gov/.
DOJ, 2008. Electronic Crime Scene Investigation: A Guide for First Responders, Second Edition.
Englbrecht L, Meiser S, Pernul G. Towards a capability maturity model for digital forensic readiness. Wirel. Netw. 2019. doi:10.1007/s11276-018-01920-5.
Erboz G. How to define industry 4.0: Main pillars of industry 4.0. In: International Scientific Conference Managerial Trends in the Development of Enterprises in Globalization; 2017. p. 761–7.
Ervural BC, Ervural B. Overview of cyber security in the industry 4.0 era. In: Industry 4.0: Managing The Digital Transformation, Springer Series in Advanced Manufacturing; 2018. p. 267–84. doi:10.1007/978-3-319-57870-5_16.
Exalead, 2019(accessed October 2, 2019). Exalead Cloudview. https://www.3ds.com/products-services/exalead/products/exalead-cloudview/.
Fahdi MA, Clarke NL, Furnell SM. Challenges to digital forensics: a survey of researchers practitioners attitudes and opinions. In: 2013 Information Security for South Africa; 2015. p. 1–8. doi:10.1109/ISSA.2013.6641058.
Feng X, Zhao Y. Digital forensics challenges to big data in the cloud. In: 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); 2017. p. 858–62. doi:10.1109/iThings-GreenCom-CPSCom-SmartData.2017.132.
Fink A. Conducting Research Literature Reviews: From the Internet to Paper. Sage Publications; 2019.
Giova G, Politecnica E. Improving chain of custody in forensic investigation of electronic digital systems. Improving Chain Custody Forensic Invest. Electron. Digit. Syst. 2011;11(1):1–9.
Gobler M, Dlamini I. Managing digital evidence - the governance of digital forensic. J. Contemp. Manage. 2010:1–21.
Gold S. Challenges ahead on digital forensics and audit trails. Netw. Secur. 2014;2014(6):12–17. doi:10.1016/S1353-4858(14)70060-1.
Grammatikis PIR, Sarigiannidis PG, Moscholios ID. Securing the internet of things: challenges, threats and solutions. Internet Things 2019;5:41–70. doi:10.1016/j.iot.2018.11.003.
Granja FM, Rafael GDR. The preservation of digital evidence and its admissibility in the court. Int. J. Electron. Secur.Digit. Forensics 2017;9(1). doi:10.1504/IJESDF.2017.10002624.
Grobler CP. A digital forensic management framework. Department of Informatics, Faculty of Science, University of Johannesburg, Auckland Park; 2011. Ph.D. Thesis.
Hanaei EHA, Rashid A. DF-C2M2: a capability maturity model for digital forensics organisations. In: 2014 IEEE Security and Privacy Workshops; 2014. p. 57–60. doi:10.1109/SPW.2014.17.
HIPAA, 2019(accessed January 7, 2020). Healthcare Data Breach Statistics. https://www.hipaajournal.com/healthcare-data-breach-statistics/.
Ho D, Kumar A, Shiwakoti N. Maturity model for supply chain collaboration: CMMI approach. In: 2016 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM); 2016. p. 845–9. doi:10.1109/IEEM.2016.7797996.
Ho HL. In: Metaphysics Research Lab. The legal Concept of Evidence. Stanford University; 2015.
Horsman G. Unmanned aerial vehicles: a preliminary analysis of forensic challenges. Digit. Invest. 2016;16:1–11. doi:10.1016/j.diin.2015.11.002.
Horsman G. Can we continue to effectively police digital crime. Sci. Justice 2017;57(6):448–54. doi:10.1016/j.scijus.2017.06.001.
Horsman G. I couldn't find it your honour, it mustn't be there! - tool errors, tool limitations and user error in digital forensics. Sci. Justice 2018;58(6):433–40. doi:10.1016/j.scijus.2018.04.001.
Hraiz S. Challenges of digital forensic investigation in cloud computing. In: 2017 8th International Conference on Information Technology (ICIT); 2017. p. 568–71. doi:10.1109/ICITECH.2017.8080060.
Hsu Y-L, Chou P-H, Chang H-C, Lin S-L, Yang S-C, Su H-Y, Chang C-C, Cheng Y-S, Kuo Y-C. Design and implementation of a smart home system using multisensor data fusion technology. Sensors (Basel) 2017;17(7):1631. doi:10.3390/s17071631.
IIA, 2013. Selecting, Using, and Creating Maturity Model: A Tool For Asssurance and Consulting Engagements.
Interpol, 2019. INTERPOL Global Guidelines For Digital Forensics Laboratories.
Interpol, 2019(accessed September 13, 2019). Cybercrime.
Irwin ASM, Dawson C. Following the cyber money trail: global challenges when investigating ransomware attacks and how regulation can help. J. Money Laundering Control 2019;22(1):110–31. doi:10.1108/JMLC-08-2017-0041.
Irwin ASM, Turner AB. Illicit bitcoin transactions: challenges in getting to the who, what, when and where. J. Money Laundering Control 2018;21(3):297–313. doi:10.1108/JMLC-07-2017-0031.
ISACA, 2017. Getting Started with data Governance using COBIT 5.
ISACA, 2019a. COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution.
ISACA, 2019b. COBIT 2019 Framework Governance and Management Objectives.
ISACA, 2019c. COBIT 2019 Framework Introduction and Methodology.
ISACA, 2019(accessed August 8, 2020). CMMI V2.0.
ISO, 2008. Information Technology - Process Assessment - Part 7: Assessment of Organizational Maturity.
ITU, 2018. Global Cybersecurity Index (GCI) 2018.
Jadeja Y, Modi K. Cloud computing - concepts, architecture and challenges. In: 2012 International Conference on Computing, Electronics and Electrical Technologies (ICCEET); 2012. p. 877–80. doi:10.1109/ICCEET.2012.6203873.
Jang-Jaccard J, Nepal S. A survey of emerging threats in cybersecurity. J. Comput. Syst. Sci. 2014;80(5):973–93. doi:10.1016/j.jcss.2014.02.005.
Kavis MJ. Architecting the Cloud: Design Decisions for Cloud Computing Service Models (SaaS, PaaS, and IaaS). John Wiley & Sons; 2014.
Kerrigan M. A capability maturity model for digital investigations. Digit. Invest. 2013;10(1):19–33. doi:10.1016/j.diin.2013.02.005.
Khan S, Ahmad E, Shiraz M, Gani A, Wahab AWA, Bagiwa MA. Forensic challenges in mobile cloud computing. In: 2014 International Conference on Computer, Communications, and Control Technology (I4CT); 2014. p. 343–7. doi:10.1109/I4CT.2014.6914202.
Khan S, Gani A, Wahab AWA, Shiraz M, Ahmad I. Network forensics: review, taxonomy and open challenges. J. Netw. Comput. Appl. 2016;66:214–35. doi:10.1016/j.jnca.2016.03.005.
Kitchenham B. Procedure for Performing Systematic Reviews. Keele, University, Keele, 33; 2004.
Le-Khac N-A, Jacobs D, Nijhoff J, Bartens K, Choo K-KR. Smart vehicle forensics: challenges and case study. Future Gener. Comput. Syst. 2020;109:500–10. doi:10.1016/j.future.2018.05.081.
Lee J, Lee D, Kang S. An overview of business process maturity model (BPMM). In: Advances in Web and Network Technologies, and Information Management; 2007. p. 384–95. doi:10.1007/978-3-540-72909-9_42.

Lee M, Joseph J, Pkya A, Won D, Kodama F, Schiuma G, Park H, Jeon J, Park K, Jung K, Yan M-R, Lee S, Zhao X. How to respond to fourth industrial revolution, or the second information technology revolution? Dynamic new combinations between technology, market, and society through open innovation. J. Open Innov. 2018;4(3):1–24. doi:10.3390/joitmc4030021.

MacDermott A, Baker T, Shi Q. Iot forensics: challenges for the ioa era. In: 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS); 2018. p. 1–5. doi:10.1109/NTMS.2018.8328748.

Mahjabin T, Xiao Y, Sun G, Jiang W. A survey of distributed-of-service attack, prevention and mitigation techniques. Int. J. Distrib. Sens.Netw. 2017;13(12):1–33. doi:10.1177/1550147717741463.

Mahmood S. Capability maturity model integration CMMI. 3rd International Multidisciplinary Research Conference, 2016.

Mahmoud R, Yousuf T, Aloul F, Zualkernan I. Internet of things (IoT) security: current status, challenges and prospective measures. In: 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST); 2015. p. 336–41. doi:10.1109/ICITST.2015.7412116.

Majid MA, Ariffin KAZ. Success factors for cyber security operation centre (SOC) establishment. 1st International Conference on Informatics, Engineering, Science and Technology, INCITEST 2019, 2019.

Mansfield-Devine S. Weaponising the internet of things. Netw. Secur. 2017;10:13–19. doi:10.1016/S1353-4858(17)30104-6.

Matanović A. Blockchain/cryptocurrencies and cybersecurity, threats and opportunities. In: 9th International Conference on Business Information Security (BISEC-2017); 2017. p. 11–15.

Mell, P., Grance, T., 2011. SP 800-145 The NIST Definition of Cloud Computing.

Mettler T. Maturity assessment models: a design science research approach. Int. J. Soc. Syst. Sci.(IJSSS) 2011;3:81–98. doi:10.1504/IJSSS.2011.038934.

Miron W, Muita K. Cybersecurity capability maturity models for providers of critical infrastructure. Technol. Innov. Manage. Rev. 2014;4(10):33–9. doi:10.22215/timreview/837.

Montasari R, Hill R. Next-generation digital forensics: challenges and future paradigms. In: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3); 2019. p. 205–12. doi:10.1109/ICGS3.2019.8688020.

Okoli C. A guide to conducting a standalone literature review. Commun. Assoc. Inf.Syst. 2015;37:880–910. doi:10.17705/1CAIS.03743.

Oriwoh E, Jazani D, Epiphaniou G, Sant P. Internet of things forensics: challenges and approaches. In: 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing; 2013. p. 608–15. doi:10.4108/icst.collaboratecom.2013.254159.

O'Shaughnessy S, Keane A. Impact of cloud computing on digital forensic investigations, vol 410; 2013. p. 291–303. doi:101007/978-3-642-41148-9_20.

OUSD, 2020(accessed August 8, 2020). Cybersecurity Maturity Model Certification (CMMC). https://www.acq.osd.mil/cmmc/draft.html.

Paquet-Clouston M, Haslhofer B, Dupont B. Ransomware payments in bitcoin ecosystem. J. Cybersecur. 2019;5(1). doi:10.1093/cybsec/tyz003.

Park Hil, seong Yoon J, jin Lee S. A study on development of digital forensic capability evaluation indices. J. Korea Inst. Inf.Secur. Cryptol. 2015;25(5):1153–66. doi:10.13089/JKIISC.2015.25.5.1153.

Paulk MC, Curtis B, Chrissis MB, Weber CV. Capability maturity model, version 1.1. IEEE Softw. 1993;10(4):18–27. doi:10.1109/52.219617.

Pearson, J., 2009(Accessed October 30, 2019). People-Process-Technology-the Eternal Triangle. https://deconstructingitsm.wordpress.com/2009/.

Prodan M, Prodan A, Purcarea AA. Three new dimensions to people, process, technology improvement model. Adv. Intell. Syst. Comput. 2015;353:481–90. doi:10.1007/978-3-319-16486-1_47.

Proenca D, Borbinha J. Maturity models for information systems - a state of the art. Procedia Comput. Sci. 2016;100:1042–9. doi:10.1016/j.procs.2016.09.279.

Profitt T. A framework for assessing the core capabilities of a digital forensic organization. Int. J. Forensic Comput. Sci. 2019;14(1):25–33. doi:10.5769/J201901003.

PwC, 2017. Operation Cloud Hopper.

Ragowsky A, Licker PS, Gefen D. Organizational IT maturity (OITM): a measure of organizational readiness and effectiveness to obtain value from its information technology. Inf. Syst. Manage. 2012;29:148–60. doi:10.1080/10580530.2012.662104.

Ren K, Wang C, Wang Q. Security challenges for the public cloud. IEEE Internet Comput. 2012;16(1):69–73. doi:10.1109/MIC.2012.14.

Rikk, R., 2018. National Cyber Security Index 2018, e-Governance Academy.

Rojko A. Industry 4.0 concept: background and overview. Int. J. Interact. Mob.Technol. (iJIM) 2017;11(5):77–90.

Ruan K, Carthy J. Cloud forensic maturity model, vol. 114; 2012. p. 22–41. 978-3-642-39891-9_2

Sinanović H, Mrdovic S. Analysis of Mirai malicious software. In: 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM); 2019. p. 1–5. doi:10.23919/SOFTCOM.2017.8115504.

Steuperaert D. Cobit 2019: a significant update. EDP Audit Control Secur. Newsl. 2019;59:14–18. doi:10.1080/07366981.2019.1578474.

Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the internet of things (IoT) forensics: challenges, approaches, and open issues. IEEE Commun. Surv. Tutor. 2020;22(2):1191–221. doi:10.1109/COMST.2019.2962586.

Stubbs, J., Menn, J., Bing, C., 2019(accessed October 28, 2019). Inside the West's Failed Fight against China's 'Cloud Hopper' Hackers. https://www.reuters.com/investigates/special-report/china-cyber-cloudhopper/.

Suciu G, Suciu V, Martian A, Craciunescu R, Vulpe A, Marcu I, Halunga S, Fratu O. Big data, internet of things and cloud convergence-an architecture for secure e-health applications. J. Med. Syst. 2015;39:141. doi:10.1007/s10916-015-0327-y.

Sunde N, Dror IE. Cognitive and human factors in digital forensics: problems, challenges, and the way forward. Digit. Invest. 2019;29:101–8. doi:10.1016/j.diin.2019.03.011.

Svata V. Cobit 2019: should we care. In: 2019 9th International Conference on Advanced Computer Information Technologies (ACIT); 2019. p. 329–32. doi:10.1109/ACITT.2019.8779995.

SWGDE, 2015. SWGDE Establishing Confidence in Digital Forensic Result by Error Mitigation Analysis.

Takabi H, Joshi JBD, Ahn G-J. Security and privacy challenges in cloud computing environments. IEEE Secur. Privacy 2010;8(6):24–31. doi:10.1109/MSP.2010.186.

TGCSCC, 2016. Cybersecurity Capacity Maturity Model for Nations (CMM), University of Oxford.

Tianfield H. Security issues in cloud computing. In: 2012 IEEE International Conference on Systems, Man, and Cybernetics (SMC); 2012. p. 1082–9. doi:10.1109/ICSMC.2012.6377874.

Torre GDL, Rad P, Choo K-KR. Driverless vehicle security: challenges and future research opportunities. Future Gener. Comput. Syst. 2020;108:1092–111. doi:10.1016/j.future.2017.12.041.

Tziakouris G. Cryptocurrencies - a forensic challenge or opportunity for law enforcement? An interpol perspective. IEEE Secur. Privacy 2018;16(4):92–4. doi:10.1109/MSP.2018.3111243.

UNDP, 2007. Supporting Capacity Development: The UNDP Approach.
Visconti M, Cook CR. Evolution of a maturity model-critical evaluation and lessons learned. Softw. Qual. J. 1998;7(3–4):223–37. doi:10.1023/A:1008979221881.
Yang Z, Yue Y, Yang Y, Peng Y, Wnag X, Liu W. Study and application on the architecture and key technologies for IoT. In: 2011 International Conference on Multimedia Technology; 2011. p. 747–51. doi:10.1109/ICMT.2011.6002149.
Yousaf H, Kappos G, Meiklejohn S. Tracing transactions across cryptocurrency ledgers. In: 28th USENIX Security Symposium; 2019. p. 837–50. arXiv preprint arXiv:1810.12786v2.
Zakaria N, Yusof SA. The role of human and organizational culture in the context of technological change. In: IEMC'01 Proceedings. Change Management and the New Industrial Revolution. IEMC-2001; 2001. p. 83–7. doi:10.1109/IEMC.2001.960485.
Zareen MS, Waqar A, Aslam B. Digital forensics: latest challenges and response. In: 2013 2nd National Conference on Information Assurance (NCIA); 2013. p. 21–9. doi:10.1109/NCIA.2013.6725320.
Zargari S, Benford D. Cloud forensics: concepts, issues, and challenges. In: 2012 Third International Conference on Emerging Intelligent Data and Web Technologies; 2012. p. 236–43. doi:10.1109/EIDWT.2012.44.
Zawoad S, Hasan R. Towards a systematic analysis of challenges and issues in secure mobile cloud forensics. In: 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering; 2015. p. 237–8. doi:10.1109/MobileCloud.2015.32.
Zhang Q, Cheng L, Boutaba R. Cloud computing: state-of-the-art and research challenges. J. Internet Serv. Appl. 2010;1(1):7–18. doi:10.1007/s13174-010-0007-6.

**Khairul Akram** earned his Bachelor and Master degrees with First Class Honours in System Engineering with Computer Engineering from University of Warwick, United Kingdom in 2008 and 2009 respectively. He later joined Universiti Teknologi PETRONAS (UTP) in 2010 to pursue his journey towards academic research and teaching courses to earn his PhD in Information System. During his time in UTP, a number of journal articles and conference papers have been produced and published internationally. Then, he was appointed as Researcher in Digital Forensic Department, CyberSecurity Malaysia and had been entrusted with the research on embedded system and live forensic. Currently, he a member of Technology and Information Science Faculty of National University of Malaysia to pursue his passion in research towards cyber security, digital forensics, algorithms, and embedded system. He is GCFA certified and member for both IEEE and IET.

**Faris Hanif** earned his Bachelor of Pharmacy (Honours) from International Islamic University Malaysia in 2011. After finished one-year compulsory Provisionally Registered Pharmacists, he worked as a procurement pharmacist in Queen Elizabeth Hospital, Sabah. He later joined Enforcement Pharmacy Terengganu Branch in 2013, where he conducts enforcement activities to ensure safe pharmaceuticals and cosmetics that are available in the conventional and also online market. Although he is a pharmacist by profession, he proves himself adapted to a change in new knowledge and demands. During his enforcement years, he obtained an Executive Diploma in Enforcement Law from Judicial & Training Institute, Selangor, and is a certified Digital First Responder by the Pharmaceutical Services Division, Ministry of Health. For meeting the demand in his field, which is the digital transformation of healthcare, he is currently completing his Master in Cybersecurity in the Faculty of Information Science & Technology, The National University of Malaysia, to pursue his passion for Cybersecurity and especially Digital Forensics.