Implementation Guidelines for a Harmonised Digital Forensic Investigation Readiness Process Model

Aleksandar Valjarevic
Department of Computer Science,
University of Pretoria
Pretoria, South Africa
alexander@vlatacom.com

Hein S. Venter
Department of Computer Science,
University of Pretoria
Pretoria, South Africa

Abstract— **Digital forensic investigation readiness enables an organisation to prepare itself in order to perform a digital forensic investigation in a more efficient and effective manner. Benefits of achieving a high level of digital forensic investigation readiness include, but are not limited to, higher admissibility of digital evidence in a court of law, better utilisation of resources (including time and financial resources) and higher awareness of forensic investigation readiness.**
The problem that this paper addresses is that there is no harmonised digital forensic investigation readiness process model with appropriate implementation guidelines and, thus, there is a lack of an effective and standardised implementation of digital forensic investigation readiness measures within organisations.
Valjarevic and Venter have, in their previous work, proposed a harmonised digital forensic investigation readiness process model. This paper proposes implementation guidelines for such a harmonised digital forensic investigation process model in order to help practitioners and researchers to successfully implement the proposed model. The authors believe that these guidelines will significantly help to properly and consistently implement digital forensic readiness measures in different organisations in a bid to achieve higher admissibility of digital evidence in a court of law, as well as more efficient and effective digital forensic investigations.

Keywords - information systems security, digital forensics, process, mode, guidelines

I. INTRODUCTION

Digital forensics gained importance rapidly over the past years. The need for a standardized digital forensic investigation process, including digital forensic investigation readiness, is on the rise due to a raised number of security incidents, raised complexity of digital forensic investigations and everyday advancement of information and communication technology. The fact that societies depend heavily on information technology also contributes to the importance of digital forensics. Dealing with digital evidence requires a standardized and formalized process in order for digital evidence to be accepted in a court of law. By the time of writing this paper, there currently exists no international standard formalising the Digital Forensic Investigation Readiness Process (DFIRP). An effort to standardize the process has, however, started within the International Standardization Organisation (ISO), by the authors [1]. Note that ISO/IEC 27043 is considering the DFIRP as an integral part to the Digital Forensic Investigation Process (DFIP) and, ultimately, the DFIRP process should be contained within the DFIP processes, i.e. within one holistic DFIP model. Note that the focus of this paper is only on the implementation of a DFIRP and not on the entire holistic implementation of the DFIP as described in ISO/IEC 27043.

Further there is no standardized and harmonised set of implementation guidelines for implementation of a standardized and comprehensive digital forensic investigation readiness process.

The authors define the problem to be addressed in this paper as follows. Due to the fact that there are various digital forensic investigation readiness process models in use across the globe, there currently exists no harmonised model nor there exist implementation guideline for such a process, which can be used as a standardized set of guidelines for any organisation.

Providing guidelines for such a process should expedite Digital Forensic Investigations (DFIs). This would primarily be achieved through enabling easier, more efficient and effective planning and preparation for a DFI. Such guidelines would also be a good departure point to encourage the training of inexperienced persons in the field of digital forensic investigation readiness.

This section introduces the reader to the subject and states the problem to be addressed. The remainder of the paper is structured as follows. Section II provides background on digital forensic investigation readiness, as same as on legal aspects regarding the digital forensic investigation process. Also, this section explains the basics of the comprehensive harmonised digital forensic investigation model proposed by the Valjarevic and Venter [14, 15], with the focus on digital forensic investigation readiness processes. After that, Section IV presents the implementation guideline for a harmonised digital forensic investigation process model. Section IV concentrates on discussing the proposed guideline and Section VI concludes this paper with indications of future work.

II. BACKGROUND

The subsections to follow provide background on the following topics. First, background on digital forensics investigation readiness is provided in order to introduce the reader to the basics of the subject. After that, we provide

background on the legal aspects regarding the digital forensic investigation readiness processes, in order to show and emphasize the need for a harmonised and standardized process to be followed.

A. On Digital Forensics Investigation Readiness

The authors first wish to provide a definition of digital forensics as established in previous works of Valjarevic and Venter [14, 15]. Digital forensics is defined as the use of scientifically-derived and proven methods towards the identification, collection, transportation, storage, analysis, presentation and distribution and/or return and/or destruction of digital evidence derived from digital sources, while obtaining proper authorization for all actions, properly documenting all actions, interacting with the physical investigation, preserving the evidence and the chain of evidence, for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations [2].

Now we introduce the definition of digital forensic investigation readiness.

Digital forensic readiness is defined as the ability of an organisation to maximize its potential to use digital evidence whilst minimizing the costs of an investigation [3]. What follows is a brief overview of work related to the digital forensic readiness processes.

Following works, by different digital forensic experts, scientists and practitioners contain represent past work in digital forensic readiness process itself and give some limited guidance in terms of implementation guidelines.

Tan [3] identified factors that affect digital forensic readiness: how logging is done; what is logged; Intrusion Detection Systems (IDSs); digital forensic acquisition; digital evidence handling.

Yasinsac and Manzano [4] propose six categories of policies to facilitate digital forensic readiness: retaining information; planning the response; training; accelerating the investigation; preventing anonymous activities; protecting the evidence.

Wolfe-Wilson and Wolfe [5] emphasize the need for an organisation to have procedures in place in order to preserve digital evidence in the event that a DFI is needed.

Rowlingson [6] defines a number of goals for digital forensic readiness as follows: To gather admissible evidence legally and without interfering with business processes; To gather evidence targeting the potential crimes and disputes that may adversely impact an organisation; To allow an investigation to proceed at a cost in proportion to the incident; To minimize interruption to the business from any investigation; To ensure that evidence makes a positive impact on the outcome of any legal action. Rowlingson also defines key activities in the implementation of digital forensic readiness and this is, in the opinion of the authors, the closest to DFIRP model defined by Valjarevic and Venter [14,15]: Define the business scenarios that require digital evidence; Identify available sources and different types of potential evidence; Determine the evidence collection requirement; Establish a capability for securely gathering legally admissible evidence to meet the requirement; Establish a policy for secure storage and handling of potential evidence; Ensure monitoring is targeted to detect and deter major incidents; Specify circumstances when escalation to a full investigation should be launched; Train staff in incident awareness, so that all those involved understand their role in the digital evidence process and the legal sensitivities of evidence; Document an evidence-based case describing the incident and its impact; Ensure legal review to facilitate action in response to the incident.

Since the first Digital Forensic Research Workshop (DFRWS) in 2001 [7], the need for a standard framework for digital forensics has been acknowledged by the information security society. A framework for digital forensics needs to be flexible enough so that it can support future technologies and different types of incidents. Therefore, it needs to be simple and abstract. On the other hand, if it is too simple and abstract then it is difficult to create tool requirements and test procedures for each phase [8].

There are several works presenting digital forensic models, which include readiness as a phase, but, to the best knowledge of the authors, there is no DFIRP model proposed, except the one by Valjarevic and Venter [14, 15].

Carrier and Spafford [9] proposed a digital investigation process model, which has 17 phases, divided in five groups, one group being readiness phases. The group contains two phases: operation readiness phase and infrastructure readiness phase.

Mandia, Prosise, and Pepe [10] also proposed a digital investigation process model that includes a readiness phase, known as the pre-incident preparation phase.

Beebe and Clark [11] proposed the Hierarchical, Objectives-Based Framework for the Digital Investigations Process, which includes a preparation phase. Beebe and Clark include a preparation phase in their model. This phase encompasses activities to fulfil the aims of digital forensic readiness. The next section provides details on the proposed DFIRP model.

B. Legal Aspects

In this section the authors provide an overview of the legal aspects pertaining to digital forensics and especially the admissibility of digital evidence in a court of law. This overview is not comprehensive but aims to provide the reader with a sense of the need for a harmonised, and ultimately, a standardized digital forensic investigation process. It should be noted that legal requirements may differ extensively in different jurisdictions across the world. For example, in the United Stated of America cases that include the presentation of digital evidence are treated under rule 702 of the Federal Rules of Evidence, which says: "If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a

witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwize." For application of this rule, the Daubert case (Daubert v. Merel, 1993) is the most important. Other countries have similar guidelines regarding the admissibility of digital evidence. In the United Kingdom, for example, examiners usually follow guidelines issued by the Association of Chief Police Officers (ACPO) for the authentication and integrity of evidence [12, 13].

C. *Overview of the digital forensic investigation process classes*

In this sub-section we wish to introduce the digital forenic investigation process and its classes, for better understanding of the process proposed in [14, 15].

The readiness class of processes deals with pre-incident investigation processes aimed at reaching digital forensic investigation readiness within an organisation. Note that the readiness processes are optional to the rest of the digital forensic investigation processes. The main reason why the readiness processes are optional is due to the fact that these are proactive compared to the rest of the investigation processes, which are reactive in nature.

The initialization class of processes deals with the initial commencement of the digital forensic investigation. The processes in this class are concerned with incident detection, first response and planning and preparation of the actual digital forensic investigation.

The acquisitive class of processes deals with the physical scene investigation of a case. Processes in this class are concerned with acquisition of digital evidence and include incident scene documentation, digital evidence identification, collection, transportation and storage of digital evidence.

The investigative class of processes deals with uncovering the digital evidence. It analyses and interprets digital evidence acquired in order to relate these with actual events and entities (i.e. people and computers). Processes in this class are concerned with digital evidence analyses and interpretation, followed by reporting, presentation and investigation closure.

The concurrent class of processes takes place concurrently with all the other processes mentioned above. Concurrent processes are defined as the principles which should be applied throughout the digital forensic investigation process since such concurrent processes are applicable to many other processes within the digital forensic investigation process.

Figure 1 shows the classes of digital forensic investigation processes and an overview of their relations.

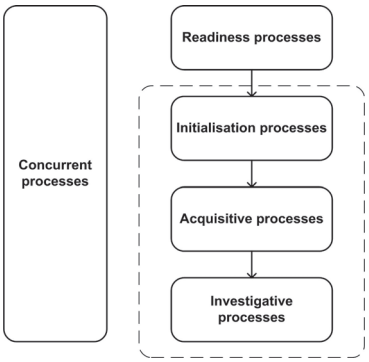

Figure 1: The classes of the comprehensive harmonised digital forensic investigation process model

1) *Overview of the readiness processes*

Figure 2 depicts the readiness processes class (harmonised digital forensic investigation readiness) as described above, refined into process groups as follows. The class of readiness processes consists of three distinctive readiness process groups, being the *planning process group*, the *implementation process group* and the *assessment process group*, as shown on Figure 2.

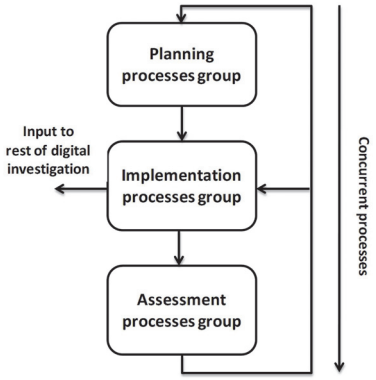

Figure 2: Readiness processes groups

The *planning processes group* includes all readiness processes that are concerned with planning activities, including *scenario definition, identification of possible digital evidence sources, planning pre-incident collection, storage and manipulation of data representing possible digital evidence, planning pre-incident analysis of data representing possible digital evidence, planning incident detection,* and *defining system architecture*, as all depicted in Figure 3 [14].

The *implementation process group* includes the following readiness processes: *implementing system architecture, implementing pre-incident collection, storage and manipulation of data representing possible digital evidence, implementing pre-incident analyses of data representing possible digital evidence* and *implementing incident detection*, as shown in Figure 3. These processes are concerned with the implementation of the results of the *planning processes [14]*.

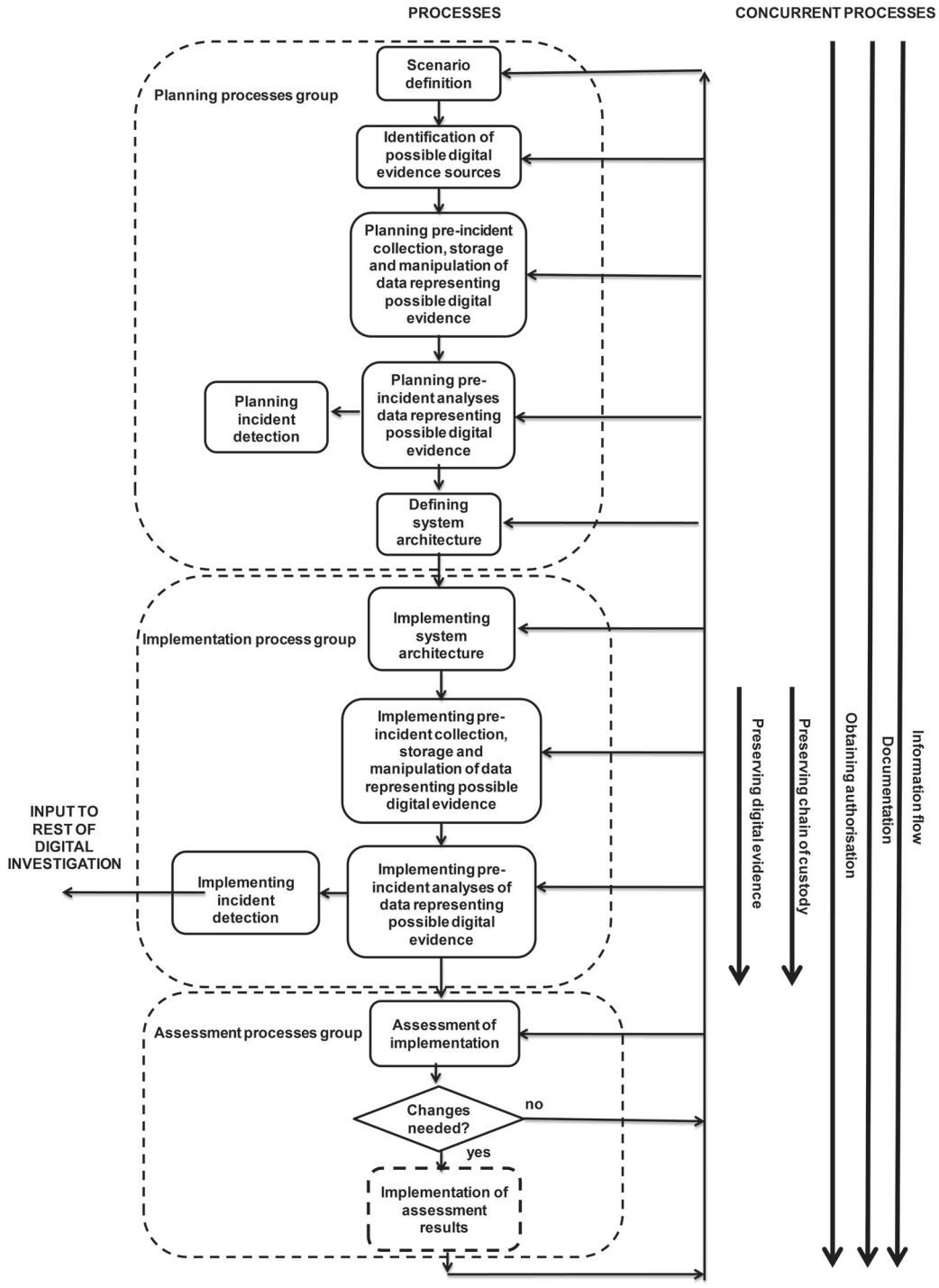

Figure 3: Readiness processes

The *assessment process group* includes two readiness processes, being the *implementation assessment process* and the *application of assessment results process [14]*.

The readiness processes are iterative, which implies that, after the last process, one can return to previous readiness processes, as shown in Figure 3.

III. Implementation Guidelines for a Harmonised Digital Forensic Investigtion Readiness Process Model

This section defines guidelines for the implementation of a comprehensive, harmonised digital forensic investigation readiness process, which forms part of the comprehensive and harmonised digital forensic investigation process model.

The process has been proposed by Valjarevic and Venter in 2012 [14, 15]. These papers propose a harmonised organisation of the processes while introducing a novel

approach in the way some of the processes have been implemented.

Guidelines are proposed based on a literature study and detailed analyses of processes proposed within the harmonised digital forensics investigation readiness process [14, 15]. The aim of the guidelines is to enable persons or entities responsible for digital forensic investigation readiness in their organisation to apply the harmonised digital forensics investigation readiness process, for any type of potential digital forensic investigation, while conforming to the basic principles of digital forensics and digital evidence admisibility.

The following subsections will present the proposed guidelines for each of the sub processes within the harmonised digital forensics investigation readiness process. In each of the specific subsections the authors first provide a summary of the harmonised digital forensics investigation readiness process itself, after which the guidelines for its implementation are provided.

Each of the readiness processes and relevant implementation guidelines are explained in the clauses that follow.

A. Scenario definition

In this process one should examine all scenarios where digital evidence might be required. The output of this process includes the defined scenarios. These might be scenarios of information security incidents, such as unauthorized use of resources. These can also be scenarios of other events that, as a consequence, require a digital forensic investigation, such as investigating the use of a computer to distribute child pornography.

The following implementation guidelines have been identified for this process. It is recommended that a proper risk assessment is performed during this process for each identified scenario, respectively. A risk assessment would enable one to better identify all possible threats, vulnerabilities and related scenarios that would expose particular information assets. Based on the assessed risk from certain threats, vulnerabilities or scenarios, one can, in later processes, better decide on the required measures to achieve investigation readiness within an organisation. This will enable an organisation to take into account the risk level, costs, and benefits of possible measures in a bid to reduce the identified risk.

B. Identification of possible digital evidence sources

In this process one should identify all possible sources of digital evidence within an organisation. The output of this process is the defined possible sources of digital evidence.

The following implementation guidelines have been identified for this process. It is recommended that an organisation makes a complete list of their information resources, including, but not limited to: hardware (computers, servers, smart phones, phones, ip phones, cellular phones, fax machines, network equipment, storage systems, tape libraries, memory mediums etc.), software (operating systems, applications, database management software, drivers, add-ons etc.), data (electronic data in all its forms and formats) and users of specified hardware, software and data. Obtaining the said lists is often also an outcome of a risk assessment as indicated in the previous process. After this, possible sources of digital evidence within these identified information resources should be analysed. This analysis should be performed based on identified possible scenarios when digital evidence might be required. One should map all information resources and all possible risks identified in order to define all possible digital evidence sources.

Some of the identified possible sources might not be available as identified during the *scenario definition* process. For example, if access logs are not introduced within the system, it means that access logs will not be available as a source of data in the case of a digital forensic investigation. In that case, measures should be explored to make the identified source available.

All activities should be documented as specified during the *documentation* process, which is a parallel process as shown in Figure 1.

C. Planning pre-incident collection, storage and manipulation of data representing possible digital evidence

In this process one should define activities for pre-incident collection, storage and manipulation of data representing possible digital evidence. The output of this process includes the defined activities for pre-incident collection, storage and manipulation of data representing possible digital evidence.

The following implementation guidelines have been identified for this process. One should determine which of identified possible digital evidence artifacts should be collected. Collection, storage and maniputaltion (processing) techniques as well as technology to be used for these activities should be defined, including techniques and technology for eventual destruction of digital evidence. Note that the collection period of potential digital evidence is to be determined by a risk assessment. Also note that the collection, storage and manipulation of data have to conform to digital forensic investigation principles in order for digital evidence to be admissible in a court of law. Lastly, note that the retention period of data is to be determined based on three factors: by conducting a risk assessment; previous experience regarding incident detection, data quantities, network capacity and all other matters that could influence cost or efficiency of this process; laws within the particular jurisdiction.

During this process, one should also make a list of all needed resources in order to perform needed actions, including human resources and technology resources. A list of human resources needed should include the investigator's level of education, knowledge and skills. A list of technology resources needed should include the needed hardware and software, with special attention to specialized hardware and software devices for

collection, storage and manipulation of potential digital evidence.

All activities should be documented as specified during the *documentation* process, which is a parallel process as shown in Figure 1.

D. Planning pre-incident analysis of data representing possible digital evidence

In this process one should define procedures for pre-incident analysis of data representing possible digital evidence. The input to this process includes the scenarios as defined in the scenario definition process as well as the output from the pre-incident collection process. The input must also include the aims for the readiness processes. The output of this process includes the defined activities for pre-incident analysis of the data that represent possible digital evidence. The aim of this analysis is to detect an incident. Therefore, activities defined in this process must include exact information on how the incident is detected and what behaviour constitutes an incident. As the output of this process is delivered in the form of detected incidents, this links to the input of the incident detection process of the digital forensic investigation processes as listed in Figure 3.

The following implementation guidelines have been identified for this process. As the task of data analysis and incident detection is often outside the scope of the functionalities of targeted information systems, it is recommended that this process defines an interface between the readiness processes and a monitoring system, which would analyse data in order to detect incidents. The monitoring system can be any system that is specialised for this purpose. For example, it can be any or more of the following systems: intrusion detection and prevention systems, change-tracking systems, logging systems, etc.

Furthermore, a decision should be made on a solution that will be chosen for a monitoring system, as defined above. In addition, an interface and the data format for data exchange over such an interface should be strictly defined. Special attention should be given to the automation of the interface. As activities of this process are often outside the scope of the functionalities of the target information system, and are performed within an external system, it is of high importance that the appropriate interfaces are defined in detail.

For this planning process it is also imperative to make a list of all needed resources in order to perform all needed actions, including human resources and technology resources.

All activities should be documented as specified during the *documentation* process, which is a parallel process as shown in Figure 1.

E. Planning incident detection

In this process one should define actions to be performed when an incident is detected. The output of this process includes defined actions to be performed once an incident is detected, in particular information to be passed on to the rest of digital forensic investigation process. Information should also include pre-known system inputs, results from all of the readiness class processes as well as data gathered and generated during the *implementation process group* processes.

The following implementation guidelines have been identified for this process. While defining what constitutes an incident is a task of previous process, in this process one should define all information to be collected about an incident and one should also define specific actions to be performed when an incident is detected. Information to be collected might include details on:

- hardware,
- software,
- data
- users affected by the incident,
- description of the threat,
- description of the vulnerability used,
- description of exposure,
- information available about origin, technique and technology used to cause an incident.

Furthermore, actions to be performed once an incident is detected depend on the particular system used for incident detection, policies of the organisation and the jurisdiction. Actions can range from neutralising threats using anti-virus software, shutting-down a network connection, or notifying an internal or external department, which will then act on the incident.

At this point one should plan for possible needed interactions with the physical investigations at the crime scene (event scene). Also, there should be a clear procedure on which persons and which institutions should be notified during the occurrence of a specific incident.

Once again, one should make a list of all needed resources in order to perform the needed actions, including human resources and technology resources.

All activities should be documented as specified during the *documentation* process, which is a parallel process as shown in Figure 1.

F. Defining system architecture

In this process one should define information system architecture for the organisation, while taking into account the output results of all previous readiness processes. Input to this process is the results from all previous readiness processes. The input must also include the aims for the readiness processes. The output of this process is the defined system architecture for the organisation. The aim is to customize system architecture to accommodate the accomplishment of the aims of the readiness processes.

The following implementation guidelines have been identified for this process. One should consider including all changes that might contribute to achieving a higher level of digital

forensic investigation readiness. Examples of this would include measures and solutions for collecting, storing and analyzing possible digital evidence, introducing new sources of possible digital evidence and introducing solutions to improve the organisation's overall level of information security. One should repeat risk analysis at this point, to weigh possible benefits of changes to system architecture and compare these to needed economical investment to achieve these changes. The repeat of a risk analysis is needed as there are going to be changes to the resources and therefore changes in possible vulnerabilities, threats and exposures. It should be noted that the level of risk analysis required here should not be as exhaustive as the original risk analysis, since many of the issues would have been dealt with during the initial risk analysis.

One must make sure that proposed changes do not interfere with functionalities of the target information system and that they do not change or improve current level of information systems security.

Proposed changes must detail changes in:

- logical system layout,
- physical system layout,
- system network layout,
- hardware,
- software,
- firmware,
- operating procedures,
- functionalities,
- data formats,
- data flows.

During this process one should also make a list of all needed resources in order to perform needed actions, including resources to undertake changes to current system architecture.

All activities should be documented as specified during the *documentation* process, which is a parallel process as shown in Figure 1.

G. Implementing system architecture

In this process one should implement the system architecture as defined in the *defining system architecture* process. The output of this process is the implemented system architecture. Examples of *implementing system architecture* include the installation of new software, hardware and/or policies which will permit the remainder of the readiness processes to be instantiated across the information system and the organisation.

The following implementation guidelines have been identified for this process. One should make sure that all implementations are first tested in a test environment, prior to impelemnting any solution into a production environment information system. All testing results should be documented. All information system users should be timely informed on changes and any impact on the use of the system. At this point one should also make sure that actions to be taken are in line with existing organisational policies and jurisdiction. Also, one should make sure that all needed autorizations are in place.

All activities should be documented as specified during the *documentation* process, which is a parallel process as shown in Figure 1.

Implementing pre-incident collection, storage and manipulation of data representing possible digital evidence

In this process one should implement pre-incident collection, storage and manipulation of data representing possible digital evidence, as defined in the *planning pre-incident collection, storage and manipulation of data representing possible digital evidence* process. The output of this process is the implemented pre-incident collection, storage and manipulation of data representing possible digital evidence.

Examples of *pre-incident collection, storage and manipulation of data representing possible digital evidence* include the implementation of logging software and hardware, with time stamping and digital signature mechanisms in place, or the implementation of customized software to collect the data of importance (i.e. system usage data).

The following implementation guidelines have been identified for this process. One should make sure that all implementations are first tested in a test environment, prior to impelemnting any solution into a production environment information system. All testing results should be documented. As stated for the previous process, at this point one should make sure that actions to be taken are in line with existing organisational policies and jurisdiction and that all needed autorizations are in place.

All activities should be documented as specified during the *documentation* process, which is a parallel process as shown in Figure 1.

H. Implementing pre-incident analysis of data representing possible digital evidence

In this process one should implement pre-incident analyses of data representing possible digital evidence, as defined in the *planning pre-incident analyses of data representing possible digital evidence* process. The output of this process is the implemented pre-incident analyses of data representing possible digital evidence. Examples of *pre-incident analyses of data representing possible digital evidence* include the implementation of change-tracking software, intrusion detection/prevention software and/or anti-virus software.

The following implementation guidelines have been identified for this process. One should make sure that all implementations are first tested in a test environment, prior to impelemnting any solution into a production environment information system. All testing results should be documented. As this process entails implementation of an external system to the target information system, one must make sure that interface introduced between these two will not influence

functionalities of the target information system. Further interface activities should be closely monitored in order to detect any deviations from desired functionality and performance of the target information system.
All activities should be documented as specified during the *documentation* process, which is a parallel process as shown in Figure 1.

I. Implementing incident detection

In this process one should implement the actions defined in the *planning incident detection* process. The implementation of incident detection depends also on and receives input from the *implementing pre-incident analyses of data representing possible digital evidence* process, as detection occurs based on the analyses performed. During the *implementing incident detection* process, detection of an incident occurs according to the rules defined during *planning incident detection* process. Also, during the *implementing incident detection* process, one should decide on which data about the incident should be passed on to the rest of digital forensic investigation process. Examples of incident detection can be if change tracking software detects changes in a certain archived log or if an intrusion is detected via intrusion detection system. Requirements for an event to be declared an incident requiring digital forensic investigation would depend on policies of organisation and can not be prescribed by this paper. This process represents an interface to the rest of the digital forensic investigation process. This process is an overlap between readiness processes and an investigation itself. The reason for overlap is that the digital forensic investigation can not start until there is an incident detected.

The following implementation guidelines have been identified for this process. One should make sure that all implementations are first tested in a test environment, prior to impelemnting any solution into production environemnt information system. All testing results should be documented. As this process entails implementation of an interface to the rest of digital forensic investigation processes, one must make that the interface is tested and functional. Note that interface does not necesserelly have to be electronic interface. It can also be a manual interface, i.e. notifying external entity via telephone or in writing. Further interface activities should be closely monitored in order to detect any deviations from desired functionality and performance. Also, where communication with external entities, being organizations, persons or systems is needed as part of this process, one should timely establish communication lines and identify and contact responsible persons within these external entities.

All activities should be documented as specified during the *documentation* process, which is a parallel process as shown in Figure 1.

J. Assessment of implementation

In the *assessment of implementation* process, one performs an assessment of the results of the *implementation process group* and compares these to the aims for achieving digital forensic investigation readiness. The output of this process is the results of the assessment of implementing digital forensic investigation readiness for an information system.

The following implementation guidelines have been identified for this process. One should analyse how successful each of the processes is in fullfilling aims of digital forensic readiness. Also, holistic view should be taken to analyse interdependencies between the processes and whether these are optimal and produce best resutls. It is recommended that, at this process, a legal revision is carried out for all procedures, measures and architectures defined previously. The revision should show, amongst other, whether there is conformity with the legal environment and digital forensics principals of the particular jurisdiction, in order to ensure admissibility of possible evidence in court.

All activities should be documented as specified during the *documentation* process, which is a parallel process as shown in Figure 1.

K. Implementation of assessment results

This process is concerned with the implementation of the conclusions from previous process. Note that this process is optional, as it is possible that no changes are needed, based on the *assessment of implementation* process. During this process one should decide on recommendations for changes in one or more of the previous processes. The main decision here is whether to go back to one of the planning processes in the *planning processes group* of the *readiness class* of processes or to go back to one of the processes in the *implementation process group,* depending on the conclusions of the *assessment of implementation p*rocess.

The following implementation guidelines have been identified for this process. This process entails only the decision on going back to one of the previous processes. A decision is to be made according to the previous process conclusions, while taking into account the aims of the process, available time, financial and human resources. Furthermore, one can, at this point, perform a risk analysis in terms of what are the risk levels if one does or does not go back to a specific previous process.

All activities should be documented as specified during the *documentation* process, which is a parallel process as shown in Figure 1.

The following subsection discusses the proposed implementation guidelines.

IV. DISCUSSION

Our proposed implementation guidelines for harmonised digital forensic investigation readiness process model [14, 15] represent a valuable contribution to the field of digital forensics, and in particulat digital forensic readiness. It can be

used as a holistic guide for implementation of processes within digital forensic readiness process.

The guidelines given cover each of the processes within comprehensive harmonised digital forensic investigation process model. The guidelines represent addition to the proposed model and improvement upon it.

Use of the proposed guideline could bring multiple benefits for digital forensic practitioners and academics. Possible benefits include:

- Higher admissibility of digital evidence in a court of law, due to the fact that a standardized process was used;
- Human error and omissions during the digital forensic investigation readiness process would be minimized once such a harmonised process was introduced;
- The proposed implementation guidelines would enhance the efficiency and effectiveness of digital forensic investigations, trough achieveing higer level of digital forensic readiness within organisations;
- Reaching standardization in the field of digital forensic investigation process models.

V. CONCLUSION

Let us revisit the problem statement. "There currently exists no harmonised digital forensic investigation readiness process model nor there exist implementation guidelines for such a process, which can be used as a standardized set of guidelines for any organisation."

The authors strongly believe that the proposed guidelines are a further step towards harmonization of existing digital forensic process models and application of such a harmonised model, in the area of digital forensic investigation readiness.

The proposed guidelines should be used by scientists and practitioners in the field in their attempt to adopt harmonised and standardized digital forensic investigation process readiness model.

Claims made in this paper are to be verified through an appropriate prototype as future work. The prototype will include mechanisms for the verification and validation of the proposed guidelines presented.

REFERENCES

[1] ISO/IEC 27043 (2012), "Information technology — Security techniques — Investigation principles and processes", unpublished draft international standard

[2] Valjarevic and Venter (2012), "Harmonised Digital Forensic Investigation Process Model", Proceedings of Information Security South Africa 2012 Conference

[3] Tan, J. (2001);"Forensic readiness"; Technical. Cambridge USA: @stake, Inc.

[4] Yasinsac, A. and Manzano, Y. (2001); "Policies to Enhance Computer and Network Forensics"; Proceedings of the 2001 IEEE Workshop on Information Assurance and Security.

[5] Wolfe-Wilson, J. and Wolfe, H.B. (2003); "Management strategies for implementing forensic security measures"; Information Security Technical Report Volume 8, Issue 2.

[6] R Rowlingson (2004); "A Ten Step Process for Forensic Readiness"; International Journal of Digital Evidence.

[7] Gary Palmer (2001); "A Road Map for Digital Forensic Research"; Technical Report DTR-T001-01, DFIRWS, November 2001; Report From the First Digital Forensic Research Workshop (DFIRWS).

[8] Carrier B. and Spafford E. (2005); "An Event-Based Digital Forensic Investigation Framework"; Digital Investigation 2(2) 2005.

[9] Carrier B. and Spafford E. (2003); "Getting Physical with the Digital Investigation Process"; International Journal of Digital Evidence Vol. 2, 2.

[10] Mandia, Kevin, Prosise, Chris, and Pepe (2003); "Incident Response & Computer Forensics"; (Second Ed.) McGraw-Hill/Osborne, Emeryville.

[11] Nicole Lang Beebe, Jan Gayness Clark (2005);"A Hierarchical, Objectives-Based Framework for the Digital Investigations Process"; Digital Investigation 2(2) 2005.

[12] Pollitt (2001), "Report on digital evidence", 13th Interpol Forensic Science Symposium, Lyon, France, 2001

[13] ACPO, "ACPO Good Practice Guide for Computer-Based Evidence", http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence_v4_web.pdf, last accessed 18.02.2013, 2008

[14] Valjarevic and Venter (2013), "A Comprehensive and Harmonised Digital Forensic Investigation Process", Unpublished journal paper

[15] Valjarevic and Venter (2013), "Towards a Harmonised Digital Forensic Investigation Readiness Process", Proceedings of Ninth Annual IFIP WG 11.9 International Conference on Digital Forensics