ISSN: 2230-9926

Available online at http://www.journalijdr.com

IJDR

International Journal of Development Research
Vol. 09, Issue, 08, pp. 28920-28928, August, 2019

REVIEW ARTICLE

OPEN ACCESS

A RECOMMENDED DIGITAL FORENSIC READINESS FRAMEWORK FOR NIGERIAN BANKS

*Adamu Abdullahi Garba and Aliyu Musa Bade

Department of Computer Science, Yobe State University Damaturu, Nigeria

ARTICLE INFO

Article History:
Received 09th May, 2019
Received in revised form
21st June, 2019
Accepted 13th July, 2019
Published online 28th August, 2019

Key Words:

Digital, Forensic,
Framework Banks

ABSTRACT

With the coming of the internet manual method of doing businesses has change dramatically to a computerized way of doing operations, similarly it also possess a threat to information security. Consequently, organizations' that fells to address or take serious security measures are likely to fall under cyber-attacks, therefore vital information will be damage. To minimize such occurrences in both public and private organization there is a need to have digital forensic framework that they will be used in other to protect sensitive information from being compromise. Digital forensic framework (DFR) helps to exploit the use of evidence and also reducing the cost of investigation. Moreover, to prepare an organization for incident respond DFR policies and procedures are important to be implemented. Therefor this paper has proposed a framework that will be used to minimize attacks to sensitive information by cyber attackers, the framework was designed by surveying the existing frameworks available so as to find the suitable components to be used in Nigerian banking sectors and a qualitative approach was used to seek expert view on the proposed framework, the results shows the components are likely to be used in most financial sector in Nigeria as it covers the major components needed for investigations.

Citation: Adamu Abdullahi Garba and Aliyu Musa Bade. 2019. "A recommended digital forensic readiness framework for nigerian banks", *International Journal of Development Research*, 09, (08), 28920-28928.

INTRODUCTION

Businesses have being evolvingextremely in this century, with each progress in information technology field comes a new danger. The growth of threats of fraud and security lead to various challenges for the law enforcement and organization to tackle all over the globe. This incident has led many companies and organization to start spending on security measures that will safeguard their sensitive information from any threats. It includes the development of effective strategies to manage any incoming incidents.These strategy help in exposure of a threat and describe it, recover from it by continuing with the normal trade as promising. Lesser amount of consideration is given to the identification and safeguarding of digital forensic (DF) evidence for possible prosecution (Sommer, 2005). DF is a subdivision in information security incident management. The subdivision offers the base to ensure that each organization should consider the obligation to gather permissible information in order to define the actual main cause of an event and effectively indict criminals (Veiga, 2007).

Most organizations oversee the basic requirement of digital forensic, lack of concrete evidence to verify the authenticity of fraudulent transaction that will link to the invader. Consequently, it has become essential for all functioning organization to prepare for the digital forensic examination so that full investigation can be carried out. Organization must implement DF at their organization unit to ensure that all incidents can be examined fully. Many organization undervalue the highly need for digital forensic evidence (Sommer, 2005). When evidence is vital to verify deceitful transaction, is often not enough linkage the foe to the crime. It is important for each organization to be preparing for DF investigation and guarantee that the whole organizational functioning environment is primed for any investigation. The acknowledged literatures on DF readiness concentrate generally on evidence identification, management, and storing and training requirement (Rowlingson, 2004). DF is the process for an association to exploit its possible in order to use the electronic evidence when necessary, it helps to improve security approach and minimize cost of investigation. This paper aims at proposing the appropriate components of digital forensic readiness for operational unit.

***Corresponding author: Adamu Abdullahi Garba,**
Department of Computer Science, Yobe State University Damaturu, Nigeria

Related Works: The main objective of this segment is to study the related literature in the area of digital forensic. DF is the systematic proposition of the procedures involved in the recapture, safeguarding and investigation of digital evidence, including audio and communication devices. DF is the part of science that emphases on evolving proof of computers in court (Reith, 2002). Digital forensic evidence can also be found in digital documents, emails, digital photographs, software programs, or other digital archives and network metadata, which may be at question in a legal circumstance in other to win a case (Marangos, 2014). In another context some authors have recognized three modules in digital forensic: Preemptive, Active and Reactive. These modules are link to one another (Grobler, 2010). Proactive means preparing the organizations for investigations; Active refer to consideration, the procurement and exploration of live evidence; and Reactive as the real 'post- action' forensic investigation Many academicsdisplays that forensic investigation has two approaches: Dead and Live forensic: Dead forensic is the old-tyle ways of collecting and preserving evidence collected in a computer in offline and creating duplicate of the storage media in a bit-stream (Beebe, 2009). Live forensic is the investigation that is performed with the first few hours of an investigation which provide information used during the suspect interview phase. Live analysis techniques uses software to investigate the time frame which is on the system (Reyes, 2011). While dead analysis do not use software that existed on the system throughout the investigation of the time frame (Richard, 2006).

According to (Adeyemi, 2019), (2019), stated that 97% of organizations in Africa spend less than 10,000 USD in cyber-Security, Nigeria being the highest. Also 64% lack cyber-Security training of their employees, 83% lacks cyber-security management in their organization and lastly, 97% lack skills to comeback cyber-attacks, sadly Nigeria has the highest in all. Nigeria has newly enacted National Cyber Security Strategy which was established on May 2015, this policy and strategy to manage any security threat and coordinate a guild on how to overcome it. According to the office of the national security adviser (ONSA) Nigeria, over N159 billion was lost by Nigeria through online scam and identity theft between 2000 to 2013 with 2.175 websites defaced within the same period, cyber espionage has stolen more than 800 million individual personal information during 2013. Report stated that 25% of the cybercrime in Nigeria are unresolved and that an estimated of 7.5% of world's hacker are Nigerian (Information Security Society of Nigeria, 2015). Economically, the estimated cost of cybercrimes to Nigeria was about 0.08% of their GDP representing about N127 billion (center of strategic and international studies, UK, 2014). Based on the Nigeria n cyber Security report 2016 by Serianu agency, Nigeria has the total number of 97,210,000 internet users and subscribers as of 2016 with the increase of users' cyber threats and attacks also increases, the estimated cost of cybercrime is $550M and with less than 1550 estimated No. of Certified professionals. Also to make this policy and strategy active in 2015, the government passed a new law called The Nigeria n Cyber Crime Act 2015, this act provides a detailed legal regulatory and institutional framework for prohibition, prevention, detection, prosecution and punishment of cybercrimes in Nigeria. E.g. under the section of Identity theft and impersonation. (Sec 22. 1 any person who is engaged in the services of any financial institution, and as a result of his special knowledge commits identity theft of its employer, staff, service providers and consultants with the intent to defraud is guilty of an offence and upon conviction shall be sentenced to 7 years imprisonment or N5, 000,000.00 fine or both). The country also has established the Nigeria n Computer Emergency Response Team (ngCERT), it main activities is to manage the risk of cyber threat in the Nigeria in cyberspace and also coordinate incident response and mitigation strategies to prevent cyber-attacks against the country. The country does not yet use or work with civil societies/ NGO to educate and raise awareness of cyber risk. Nigeria is ranked fifth in the continent, this West African country scored an overall of 0.569 and ranked 46th globally. According to the report, Nigeria's cyber-security programs and initiatives are in "maturing stage", meaning the GCI score is between the 50th and 89th percentage (Richard, 2006).

The table 1 above shows the researcher and also the components they used in their DFR framework. Thirty nine components were found in these existing frameworks from eight different authors. The rows show the components while the columns show the authors that recommended those components.

Concerns to be reflected on

The concern to be considered from Table 1above are:

- Almost all the components are common and can be applied to any digital forensic readiness.
- Most of the frameworks have parallel components like policy and people while only few components are uniquely to some frameworks like incident respond process.
- Also frameworks merge some components to be one like in policy and compliance (Barske, 2010).
- There are no complete frameworks that will suite many organizations.
- Each researcher designs their framework based on their own scopes.

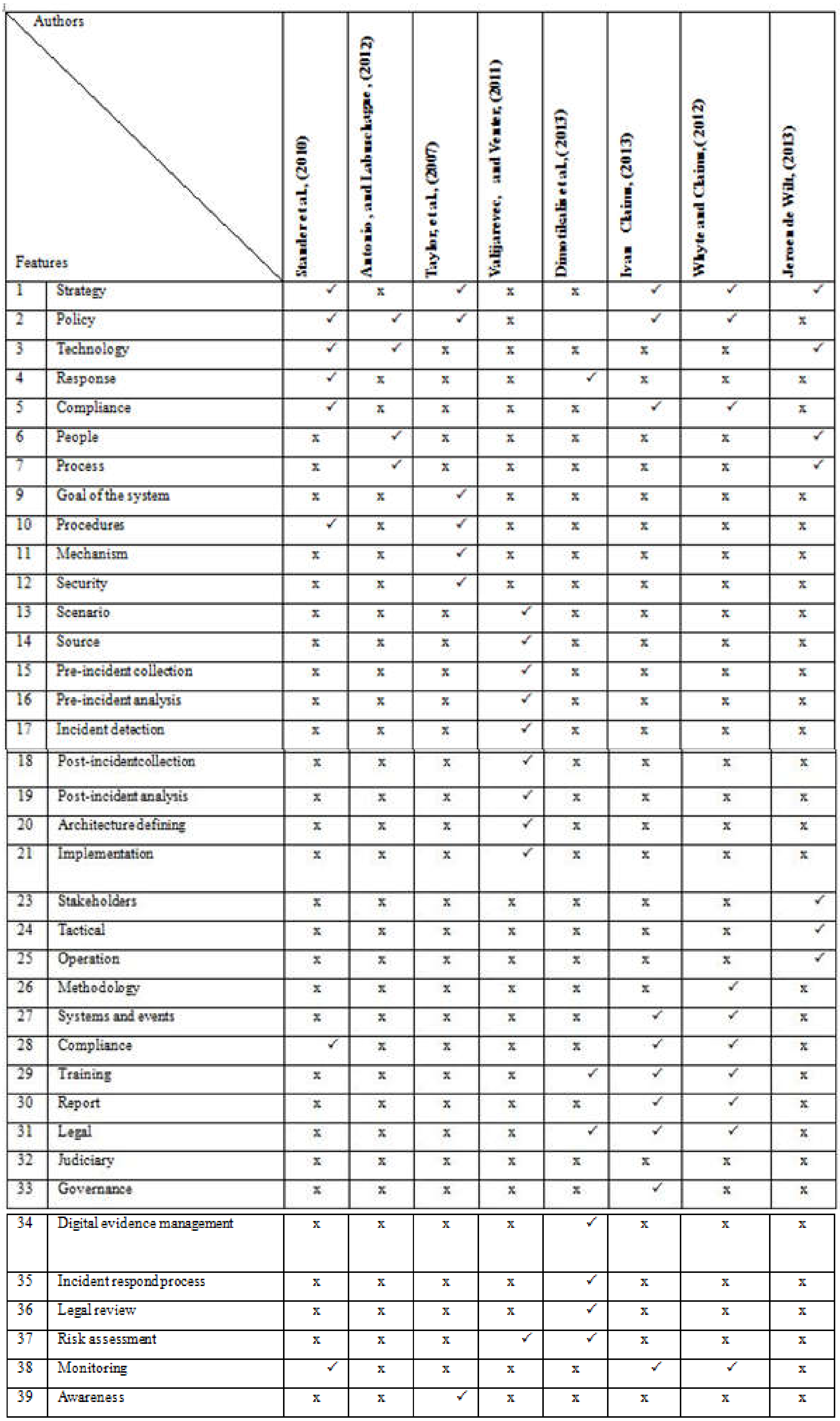
Therefore, a generic DFR is proposed which covers seven components:

- Strategy
- Policy and procedures
- People
- System and event
- Monitor and report
- Forensic preparation.

- From the above Table 1.2 it shows that the proposed framework almost cover every aspect of the existing frameworks, the last row shows the components available in the framework with a sign.
- The proposed framework has a big difference with the existing frameworks. The author believes the framework will highly going to be effective and efficient in the organization as their digital forensic readiness.

Suggeted digital forensic components activities: There is presently no holistic based digital forensic readiness framework. Therefore, no application of holistic based forensic readiness framework to the best of the author's knowledge.

Table 1.1. The Common Components from the Existing Frameworks



Authors Features		Stander et al., (2010)	Antonio , and Labuschagne , (2012)	Taylor, et al., (2007)	Valijarevec, and Venter, (2011)	Dimotikalis et al.,(2013)	Ivan Chima, (2013)	Whyte and Chima,(2012)	Jeroen de Wilt, (2013)
1	Strategy	✓	x	✓	x	x	✓	✓	✓
2	Policy	✓	✓	✓	x		✓	✓	x
3	Technology	✓	✓	x	x	x	x	x	✓
4	Response	✓	x	x	x	✓	x	x	x
5	Compliance	✓	x	x	x	x	✓	✓	x
6	People	x	✓	x	x	x	x	x	✓
7	Process	x	✓	x	x	x	x	x	✓
9	Goal of the system	x	x	✓	x	x	x	x	x
10	Procedures	✓	x	✓	x	x	x	x	x
11	Mechanism	x	x	✓	x	x	x	x	x
12	Security	x	x	✓	x	x	x	x	x
13	Scenario	x	x	x	✓	x	x	x	x
14	Source	x	x	x	✓	x	x	x	x
15	Pre-incident collection	x	x	x	✓	x	x	x	x
16	Pre-incident analysis	x	x	x	✓	x	x	x	x
17	Incident detection	x	x	x	✓	x	x	x	x
18	Post-incidentcollection	x	x	x	✓	x	x	x	x
19	Post-incident analysis	x	x	x	✓	x	x	x	x
20	Architecture defining	x	x	x	✓	x	x	x	x
21	Implementation	x	x	x	✓	x	x	x	x
23	Stakeholders	x	x	x	x	x	x	x	✓
24	Tactical	x	x	x	x	x	x	x	✓
25	Operation	x	x	x	x	x	x	x	✓
26	Methodology	x	x	x	x	x	x	✓	x
27	Systems and events	x	x	x	x	x	✓	✓	x
28	Compliance	✓	x	x	x	x	✓	✓	x
29	Training	x	x	x	x	✓	✓	✓	x
30	Report	x	x	x	x	x	✓	✓	x
31	Legal	x	x	x	x	✓	✓	✓	x
32	Judiciary	x	x	x	x	x	x	x	x
33	Governance	x	x	x	x	x	✓	x	x
34	Digital evidence management	x	x	x	x	✓	x	x	x
35	Incident respond process	x	x	x	x	✓	x	x	x
36	Legal review	x	x	x	x	✓	x	x	x
37	Risk assessment	x	x	x	✓	✓	x	x	x
38	Monitoring	✓	x	x	x	x	✓	✓	x
39	Awareness	x	x	✓	x	x	x	x	x

Table 2. Comparison between Components from the Existing Frameworks and the proposed framework Components

	Authors Features	Stander *et al.* (2010)	Antonio and Labuschagne (2012)	Taylor, *et al.*(2007)	Valijarevec and Venter (2011)	Dimotikalis *et al.* (2013)	Ivan Claims (2013)	Whyte and Claims (2012)	Jeroen de Wilt (2013)	Proposed components
1	Strategy	✓	x	✓	x	x	✓	✓	✓	✓
2	Policy	✓	✓	✓	x	✓	✓	✓	✓	x
3	Technology	✓	✓	x	x	x	x	x	✓	✓
4	Response	✓	x	x	x	✓	x	x	x	x
5	Compliance	✓	x	x	x	x	✓	✓	x	x
6	People	x	✓	x	x	x	x	x	✓	✓
7	Process	x	✓	x	x	x	x	x	✓	✓
9	Goal of the system	x	x	✓	x	x	x	x	x	x
10	Procedures	✓	x	✓	x	x	x	x	✓	x
11	Mechanism	x	x	✓	x	x	x	x	x	x
12	Security	x	x	✓	x	x	x	x	x	x
13	Scenario	x	x	x	✓	x	x	x	x	x
14	Source	x	x	x	✓	x	x	x	x	x
15	Pre-incident collection	x	x	x	✓	x	x	x	x	x
16	Pre-incident analysis	x	x	x	✓	x	x	x	x	x
17	Incident detection	x	x	x	✓	x	x	x	x	x
18	Post-incident collection	x	x	x	✓	x	x	x	x	x
19	Post-incident analysis	x	x	x	✓	x	x	x	x	x
20	Architecture defining	x	x	x	✓	x	x	x	x	x
21	Implementation	x	x	x	✓	x	x	x	x	x
23	Stakeholders	x	x	x	x	x	x	x	x	✓
24	Tactical	x	x	x	x	x	x	x	x	✓
25	Operation	x	x	x	x	x	x	x	x	✓
26	Methodology	x	x	x	x	x	x	✓	x	x
27	Systems and events	x	x	x	x	x	✓	✓	✓	x
28	Compliance	✓	x	x	x	x	✓	✓	x	x
29	Training	x	x	x	x	✓	✓	✓	✓	x
30	Report	x	x	x	x	x	✓	✓	✓	x
31	Legal	x	x	x	x	✓	✓	✓	✓	x
32	Judiciary	x	x	x	x	x	x	x	✓	x
33	Governance	x	x	x	x	x	✓	x	x	x
34	Digital evidence management	x	x	x	x	✓	x	x	x	x
35	Incident respond process	x	x	x	x	✓	x	x	x	x
36	Legal review	x	x	x	x	✓	x	x	✓	x
37	Risk assessment	x	x	x	✓	✓	x	x	✓	x
38	Monitoring	✓	x	x	x	x	✓	✓	✓	x
39	Awareness	x	x	✓	x	x	x	x	✓	x

The author is commending a framework which comprises of eight components as basic components in DFR and is described in details in this section. These components were chosen by the author based on the analysis conducted using table 1 above and also the scope of this research. As mention earlier, these components make a basic holistic based digital forensic readiness framework. Other researchers can adopt and enhance based on their own scope. The activities of each component will be discussed in details in the following section:

Strategy: This component ensures that the organization has a DFR strategy aligned to the organization needs. There must be a tactical order from executive to instrument and maintain DFR (Grobler, 2010). Successful implementation of this component will allow the alignment of business risk unit incident- monitoring unit (Imtiaz, 2006). To form an organization strategy, adequate resources and support must be ensured and the following activities should be performed:

- A DFR strategy aligned to the organization
- Finding what lawmaking and procedures enacts on the organization to preserve records
- Detecting which situations cloud possibly requires digital evidence
- Ascertaining the evidence source and diverse forms of digital evidence within the organization
- Confirm adequate cash to the setup of digital forensic readiness program.

Policy and Procedure: Organization need some form of policy and procedure within the workplace to guide the staffs' regarding their activities. These policy and procedure can only be successful when top management didn't simply ignore the policies. Failure to comply with policy and procedure will result to bad result to the organization (Grobler, 2006). Proper policy and procedure can provide the organization with authority to conduct investigations and collect evidence that are admissible in court (Von Solms, 2006). The following policy should be implemented in the organization:

- Policies and procedures about the acceptance of evidence system within the organization
- Policies that stated all systems and resources within are sole property if the organization and activities will be monitored
- preserved and the duration of storing the evidence
- Policies that indicate when will internal investigation will begin

A) **People:** An organization must have forensic processes to implement the DFR completely at their workplace. People are the spine of all investigation. People are so important because they contribute toward the presentation and detection of security incident (Pangalos, 2010). The below activities should be performed:

- Identifying the individuals and procedures that will have to be followed in reacting to attack.
- Identifying another providers and enter into a service planning, which will confirm that they can respond anytime there are needed
- Selecting Forensic response Team in the organization

B) Forensic Preparation: This component ensures that Digital forensic staff training strategy is well developed; also DFR awareness campaigns are design so that all the organisation staffs' are aware of the forensic strategy and polices. Also its helps to reduce disturbance to the business from any exploration (Mouhtaropoulos, 2011). Activities to be performed include:

- Awareness campaigns
- Regular workshops and awareness program to update the forensic team on current issues and challenges in cyber-attack world.
- Training strategy
- Certifications and accreditation programs

C) System and Events: This component is to detect all the source system (hardware, software, technologies, people, policies and procedures) that contains possible information, which may be incorporated in DFR strategy. Some rare examples of system and tools that might contain possible evidence are; logs, firewall, network devices, surveillance devices and computer (Valjarevic, 2011).

D) Therefore, organization must have necessary resources to gather evidence in a forensically sound manner. Activities to be performed include:

- A list of System and infrastructure requirement (proactive and reactive tools)
- The identification and classification of source system
- Record all system activities and logs (computers and other connected device to the network)
- Identify storage for potential evidence and network requirement.

E) Monitor and Report: This component ensures that organisation digital forensic incident reports arecompilingwith the requirements and have an incident escalation policy. Also it can be used to monitor sources that house potential evidence to detect threat. Activities to be performed include:

- Identify correct Tools to monitor incident
- Incident escalation policy
- Report generation
- Audit report

F) Risk Assessment: Risk assessment is very important to be considering in any organisation. Risk assessment should be performed combined with the preparation of the rest of the forensic readiness policy which will cover the security issues. All processes and designs defined when applying DFR have to go through legitimate review during evaluation phase in order to ensure acceptability of potential evidence in court [18]. Activities to be performed include:

- Threats identification
- Threat categorization:
- Exposure assessment:
- Conduct the risk mitigation strategy
- Risk classification

Methodology and proposed framework Result

The proposed framework was validated using qualitative approach to determine whether the selected components meet organizational needs, as the framework was meant for expert working in the banking sector. Many banks have being requested to participate but only zenith bank was able to give full support, therefore the paper focuses on the results obtain from zenith bank and the results cannot generalize as not all bank participated.

Expert Details

The proposed framework was validated by Zenith bank experts to ensure that the framework is suitable banking sector as the bank is one of the best and widely accepted bank in Nigeria. Four experts and one major stakeholders were among the experts that filled the questionnaires, all given questionnaires were returned and answered. Table 1.3 shows the experts' information and their respective duties in the organization. The objectives of evaluating the proposed framework components include:

- To confirm that the components and their activities are suitable for banking sector
- The arrangement of the components and activities are in accordance with the forensic investigation preference
- To finally acquire experts feedback, recommendation toward the proposed framework.

Table 3. Experts Description

Expert	Description
Expert A	Forensic and investigation leader
Expert B	Lab expert
Expert C	Forensic team member
Expert D	Chief information security officer
Expert E	Stakeholder

Components Arrangement Validation

Based on the questionnaires given all the selected components of the DFRC were agreed by the expert as essential. These components will assist the organization in preparing for any incident that might occur during business operations. Also the arrangements from Strategy to Monitor and report were agreed without correction, which make each component interlink with the next one. Table 1.3explains the results of the validated components of the proposed framework.

Table 4. Components Validation Acceptance

Expert	Expert	Expert	Expert	Expert	Expert
Component	A	B	C	D	E
Strategy	✓	✓	✓	✓	✓
Policy and procedure	✓	✓	✓	✓	✓
Legal requirements	✓	✓	✓	✓	✓
People	✓	✓	✓	✓	✓
Forensic preparation	✓		✓	✓	✓
System and event	✓	✓	✓	✓	✓
Risk assessment	✓	✓	✓	✓	✓
Monitor and report	✓	✓	✓	✓	✓

Table1.4 aboveshows that all the experts have agreed on the chosen components by the author, its shows that each component is important in this framework as the experts have no objection to any of it. From this the author is confident that the components have met the security requirements of the banking sector.

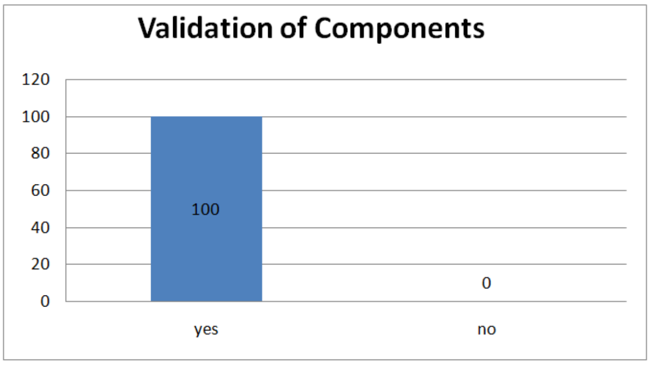
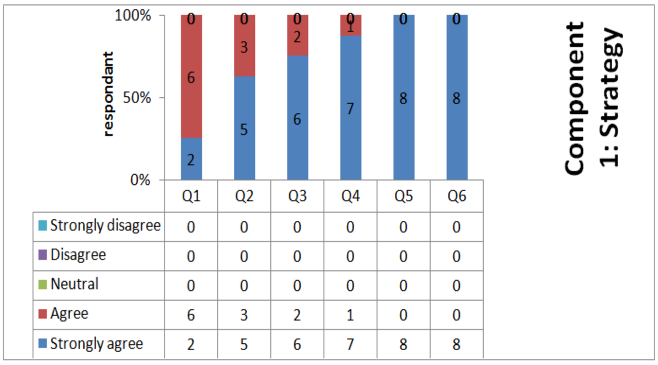


Figure 1. Components Validation Result

Figure shows that all selected components in the proposed framework were accepted by the experts that fill the questionnaires. The figure shows 100% of acceptance level while 0% of no acceptance level.

Component 1: Strategy

This component helps the organization to plan a strategy that will be used in implementing digital forensic readiness. Objectives must be identified by the organization to ensure the DRF has enough of resources and support for the organization. It also helps in identifying policies that ensure digital forensic readiness, and the validity of evidence preservation practice.



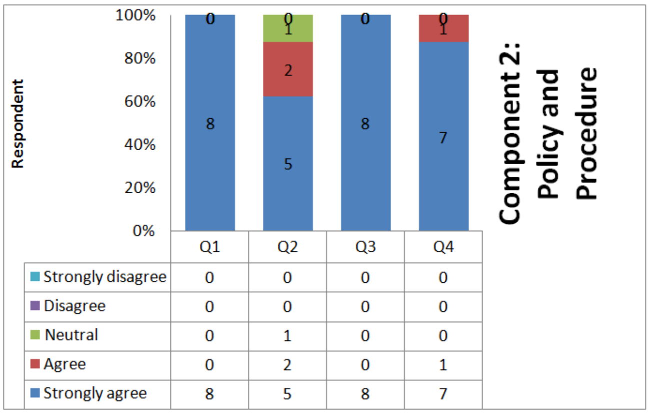
	Q1	Q2	Q3	Q4	Q5	Q6
🟦 Strongly disagree	0	0	0	0	0	0
🟪 Disagree	0	0	0	0	0	0
🟩 Neutral	0	0	0	0	0	0
🟥 Agree	6	3	2	1	0	0
🟦 Strongly agree	2	5	6	7	8	8

Figure 2. Experts Results on Strategy

Therefore, 85%, of respondents agreed tothis component and its activities, therefore, the component was considered and retained.

Component 2: Policy and Procedure

This component ensures to implement policy and procedure within the workplace to guide the staffs' regarding their activities. These policy and procedure can only be successful when top management didn't simply ignore the policies. It does also provide the organization with authority to conduct investigations and collect evidence. Figure 1.3: the feedback from the experts. Consequently, 90% of respondents consider this component important, therefore, the component and the activities was considered and retained.

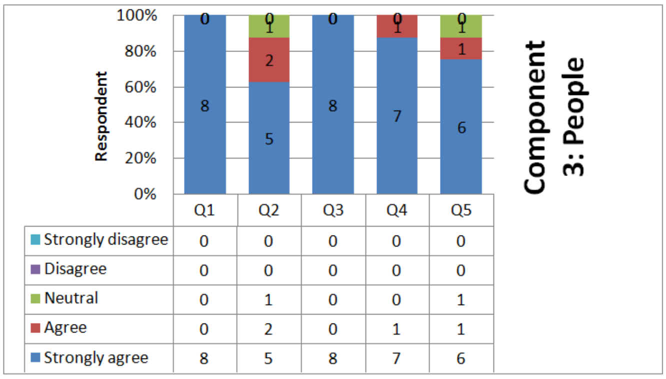


	Q1	Q2	Q3	Q4
🟦 Strongly disagree	0	0	0	0
🟪 Disagree	0	0	0	0
🟩 Neutral	0	1	0	0
🟥 Agree	0	2	0	1
🟦 Strongly agree	8	5	8	7

Figure 3. Experts Results on Policy and Procedure

Component 3: People

An organization must have forensic processes to implement the DFR completely at their workplace. People are the backbone of all investigation. This component identifies the suitable personnel to carry out all forensic activities in the organization. Figure 1.4: shows the experts feedbacks on this component.



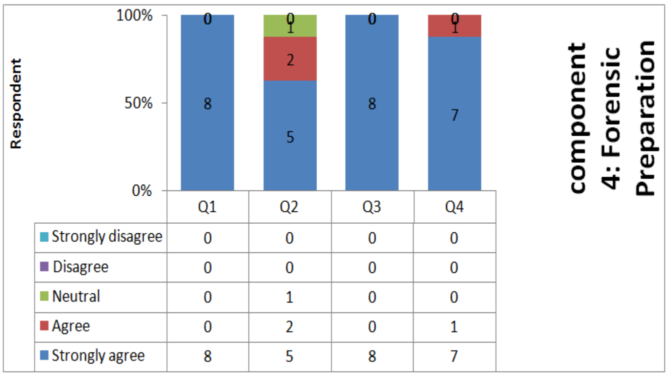
	Q1	Q2	Q3	Q4	Q5
🟦 Strongly disagree	0	0	0	0	0
🟪 Disagree	0	0	0	0	0
🟩 Neutral	0	1	0	0	1
🟥 Agree	0	2	0	1	1
🟦 Strongly agree	8	5	8	7	6

Figure 4. Experts Results on People

Therefore, based on the percentage of respondents (85%), this component and the activities was considered and retained.

Component 4: Forensic Preparation

This component ensures that Digital forensic staff training strategy is well developed; also DFR awareness campaigns are design so that all the organization staffs' are aware of the forensic strategies and polices. Figure 1.5: elucidates the feedback of experts on this component.



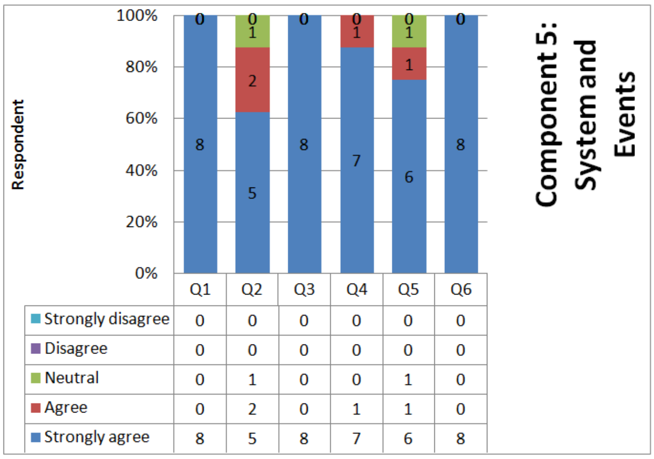
	Q1	Q2	Q3	Q4
🟦 Strongly disagree	0	0	0	0
🟪 Disagree	0	0	0	0
🟩 Neutral	0	1	0	0
🟥 Agree	0	2	0	1
🟦 Strongly agree	8	5	8	7

Figure 5. Experts Results on Forensic Preparation

Therefore, based on the percentage of respondents (more than 95%), this component and the activities was considered and retained.

Component 5: System and Events

This component helps to identify all the source system (hardware, software, technologies, people, policies and procedures) that might contain possible information, which may be incorporated in DFR strategy. Some rare examples of system and tools that might contain possible evidence are; logs, firewall, network devices, surveillance devices and computer. Figure 1.6: illustrates the feedbacks from the experts regarding the component.



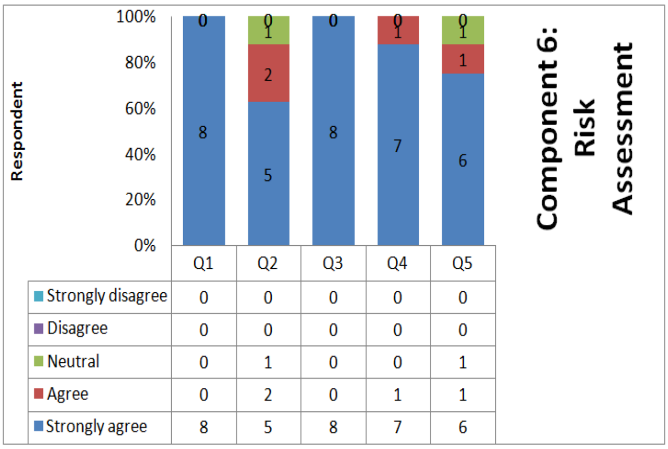
	Q1	Q2	Q3	Q4	Q5	Q6
Strongly disagree	0	0	0	0	0	0
Disagree	0	0	0	0	0	0
Neutral	0	1	0	0	1	0
Agree	0	2	0	1	1	0
Strongly agree	8	5	8	7	6	8

Figure 6. Experts Results on System and Events

Therefore, based on the percentage (more than 95%) of respondents, Only 2 respondent feel is neutral to have this component. this component and the activities was considered and retained.

Component 6: Risk Assessment

This component ensures a systematic method of dealing with risk by expecting possible incident losses, scheming and implementing measures that minimize the occurrence of data loss in the organization. It also identifies all the business situations that will need digital evidence; define the weaknesses and threats during risk assessment. Figure 1.7: illustrates experts' feedbacks on this component.



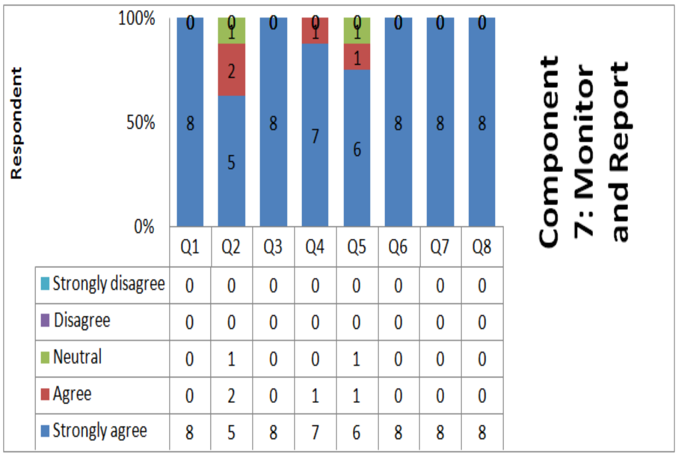
	Q1	Q2	Q3	Q4	Q5
Strongly disagree	0	0	0	0	0
Disagree	0	0	0	0	0
Neutral	0	1	0	0	1
Agree	0	2	0	1	1
Strongly agree	8	5	8	7	6

Figure 7. Results on Risk Assessment

Hence, based on the percentage of respondents (87%), this component and the activities was considered and retained

Component 7: Monitor and Report

This component ensures that organization digital forensic incident report which compiles with requirements and has an incident escalation policy. Also it can be used to monitor sources that house potential evidence to detect threat. Figure 1.8: explains the experts' feedbacks on the component.



	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8
Strongly disagree	0	0	0	0	0	0	0	0
Disagree	0	0	0	0	0	0	0	0
Neutral	0	1	0	0	1	0	0	0
Agree	0	2	0	1	1	0	0	0
Strongly agree	8	5	8	7	6	8	8	8

Figure 8. Results on Monitor and Report

Henceforth, based on the percentage (90%) of respondents, this component and the activities was retained

Expert reviews and comments

After experts' have validated the proposed framework, there are some comments and future recommendations were proposed to be included in the framework.

Based on the chosen framework components all experts agreed on it and stated were essential, therefore the author didn't change any components. Some experts recommend some important activities to be included in some components. Table 1.5: shows what experts have recommend to be added into the proposed framework.

Table 15. Experts Recommendation

No	Expert	Activity recommended
1	Forensic team member	Protect evidence
2	First responder	Specify certification required
3	Lab expert	Restrict knowledge of attack to authorized personnel
4	Forensic and investigation leader s	Review report monthly The last component most always be active and working as required.
5	Project examiner	Change C4 to Training and include double arrow between C2 and C3

Table 1.5: describes the suggested activities in some components by the experts. These activities were added into the final framework for banks in Nigeria.

Figure 1.9: shows the finalized Digital Forensic Readiness Framework Components for banks in Nigeria.

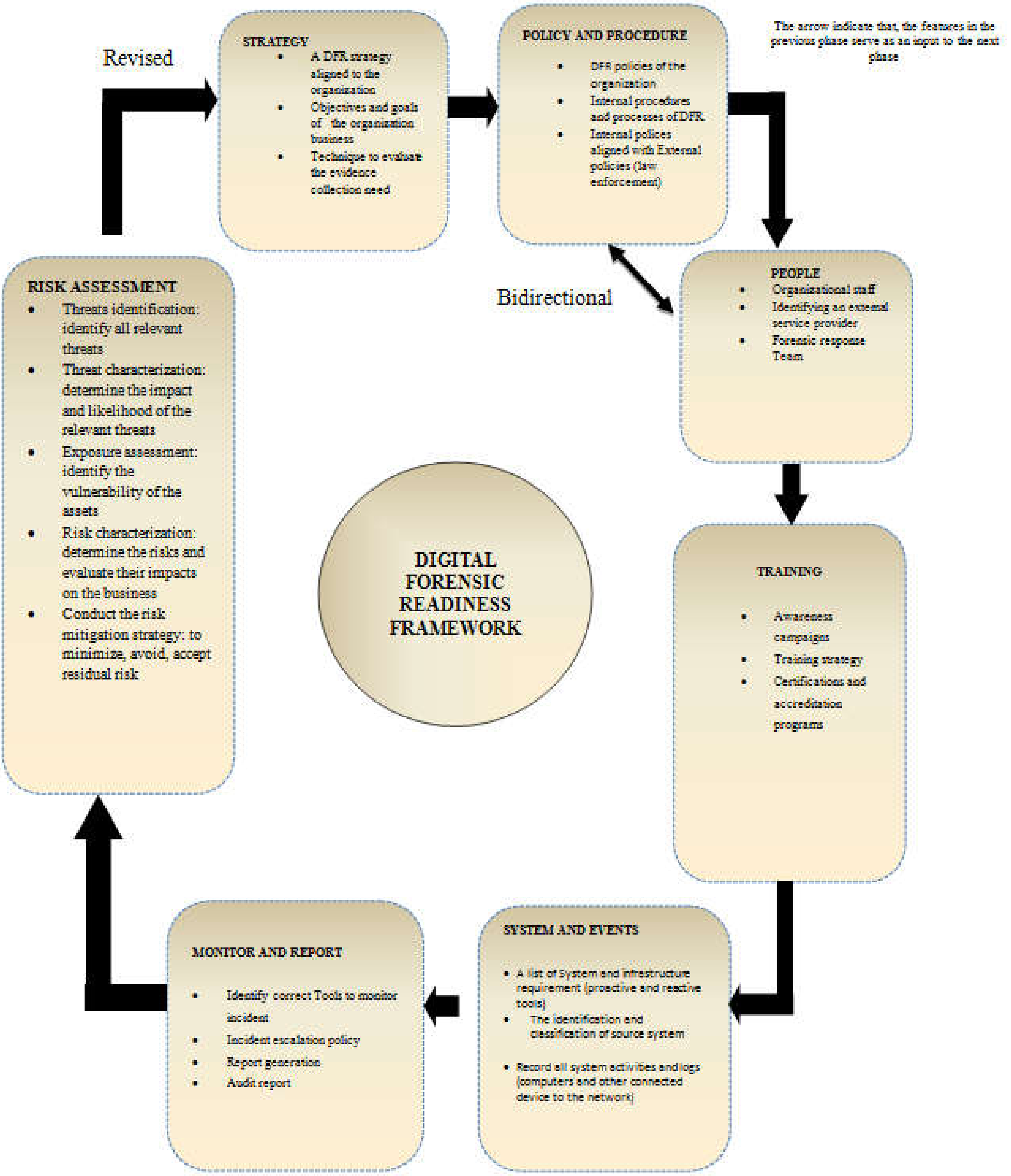

Revised
STRATEGY
A DFR strategy aligned to the organization
Objectives and goals of the organization business
Technique to evaluate the evidence collection need
POLICY AND PROCEDURE
DFR policies of the organization
Internal procedures and processes of DFR
Internal polices aligned with External policies (law enforcement)
The arrow indicate that, the features in the previous phase serve as an input to the next phase
Bidirectional
PEOPLE
Organizational staff
Identifying an external service provider
Forensic response Team
RISK ASSESSMENT
Threats identification: identify all relevant threats
Threat characterization: determine the impact and likelihood of the relevant threats
Exposure assessment: identify the vulnerability of the assets
Risk characterization: determine the risks and evaluate their impacts on the business
Conduct the risk mitigation strategy: to minimize, avoid, accept residual risk
DIGITAL FORENSIC READINESS FRAMEWORK
TRAINING
Awareness campaigns
Training strategy
Certifications and accreditation programs
MONITOR AND REPORT
Identify correct Tools to monitor incident
Incident escalation policy
Report generation
Audit report
SYSTEM AND EVENTS
A list of System and infrastructure requirement (proactive and reactive tools)
The identification and classification of source system
Record all system activities and logs (computers and other connected device to the network)

Figure 9. Digital Forensic ReadinessComponents

Conclusion

In conclusion, the author proposed digital forensic readiness components for Banks in Nigeria, but validation was done using one zenith bank as case study as the results shows all seven components were selected with more than 85% confidence. Feedback were used to finalize the final framework as one expert suggested one component name to be change to training from initial name: forensic preparation and also double arrow should be included in component 2 and 3 to shows investigations can be reverseThis framework will serve as guidance to other researchers to explore more in this area. This framework is can be adopted for wide range of organizations dealing will electronic information as an asset, so that it will help to minimize the impact of attacks to the organizations and avoid any unwanted situation that may occur in the organization.

REFERENCES

Adeyemi A, 2019. Nigeria: Financial Losses to Cybercrimes on Steady Rise to N198b, retrieved on 5/4/2019, https://allafrica.com/stories/201806070110.html

Barske, D., A. Stander, and J. Jordaan. 2010. A Digital Forensic Readiness framework for South African SME's. in Information Security for South Africa (ISSA). IEEE.

Beebe, N. 2009. Digital forensic research: The good, the bad and the unaddressed, in Advances in digital forensics Springer. p. 17-36.

Global Cybersecurity Index, 2017. Global Cyber Ranking, retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf

Grobler, C. and B. Louwrens. 2006. Digital forensics: a multi-dimensional discipline. in Proceedings of the ISSA 2006 from Insight to Foresight Conference. Pretoria: University of Pretoria.

Grobler, C., C. Louwrens, and S.H. von Solms. 2010. A framework to guide the implementation of proactive digital forensics in organisations. in Availability, Reliability, and Security, 2010. ARES'10 International Conference on. IEEE.

Grobler, M. and I. Dlamini. 2010. Managing digital evidence-the governance of digital forensics. *Journal of Contemporary Management,* p. 1-21.

Imtiaz, F. 2006. Enterprise Computer Forensics: A defensive and offensive strategy to fight computer crime.

Marangos, N., P. Rizomiliotis, and L. Mitrou. 2014. Time synchronization: pivotal element in cloud forensics. Security and Communication Networks,

Mouhtaropoulos, A., M. Grobler, and C.-T. Li. 2011. Digital forensic readiness: an insight into governmental and academic initiatives. in Intelligence and Security Informatics Conference (EISIC), IEEE.

Pangalos, G. and V. Katos. 2010. Information Assurance and Forensic Readiness, in Next Generation Society. Technological and Legal Issues, Springer. p. 181-188.

Reith, M., C. Carr, and G. Gunsch, 2002. An examination of digital forensic models. *International Journal of Digital Evidence,* 1(3): p. 1-12.

Reyes, A. 2011. Cyber crime investigations: Bridging the gaps between security professionals, law enforcement, and prosecutors.

Richard III, G.G. and V. Roussev. 2006. Next-generation digital forensics. *Communications of the ACM*,49(2): p. 76-80.

Rowlingson, R. 2004. A ten step process for forensic Readiness. *International Journal of Digital Evidence*, 2(3): p. 1-28.

Sommer, P. 2005. Directors and corporate advisors' guide to digital investigations and evidence.

Valjarevic, A. and H.S. Venter. 2011. Towards a digital forensic readiness framework for public key infrastructure systems. in Information Security South Africa (ISSA)

Veiga, A.D. and J.H. Eloff. 2007. An information security governance framework. *Information Systems Management,* 24(4): p. 361-372.

Von Solms, S. 2006. A control framework for digital forensics, in Advances in Digital Forensics II. Springer. p. 343-355.

****