ISSN 1330-3651 (Print), ISSN 1848-6339 (Online)
DOI: 10.17559/TV-20141121105105

INTEGRATED MANAGEMENT MODEL OF THE CORPORATE DIGITAL FORENSIC INVESTIGATION

Gojko Grubor, Milenko Heleta, Nenad Ristić, Ivan Barać

Original scientific paper

Metrics of the key performances indicators (KPIs) should be established into corporate digital forensic (DF) investigation process management to encourage performances effectiveness and efficiency improvement. The KPIs should lead to a quantitative assessment of gains in the DF investigation objectives, such as creating proved digital evidence (DE), reducing costs and DF investigation cycle time, etc. The KPIs metrics should address alignment with DF principles and standard operating procedures (SOP), forensic and legal requirements, digital evidence (DE) quality, stakeholder satisfaction and digital evidence legal admissibility. As a tool for quality improvement of the DF investigation processes, the KPIs metrics should be well defined and understood, and introduced by all stakeholders in the DF investigation process. The authors of this article suggested an integrated model of the corporate DF investigation management process. The model includes key activities, resources, performances objectives, risks and the KPIs metric. It is relevant for the development and management of the effective corporate DF investigation processes.

Keywords: *DF investigation process management; DF process performance; DF KPI metric; DF process management quality; integrated model*

Integrirani model upravljanja korporativnom digitalnom forenzičkom istragom

Izvorni znanstveni članak

Metrici indikatora ključnih performansi (KPI) treba uspostaviti u upravljačkom sustavu procesa korporativne digitalne forenzičke (DF) istrage, kako bi se ohrabrilo poboljšanje efektivnosti i efikasnosti performansi procesa. Oni trebaju omogućiti kvantitativnu procjenu dobiti u ciljevima DF istrage, kao što su izgradnja čvrstih digitalnih dokaza (DE), redukcija troškova i ciklusa DF istrage itd. Metrici KPI trebaju uključiti usklađivanje s DF principima i standardima, standardnim operativnim procedurama (SOP), forenzičkim i legalnim zahtjevima, smanjenjem troškova, kvalitetom DE, zadovoljstvom relevantnih sudionika i pravosudnom prihvatljivosti DE. Kao alat za poboljšanje kvaliteta procesa DF istrage, metrici KPI trebaju biti dobro definirani i shvaćena te da ih svi relevantni sudionici uvode u proces DF istrage. Autori ovog rada sugeriraju jedan integrirani model upravljanja procesom korporacijske DF istrage, koji obuhvaća ključne aktivnosti, resurse, ciljeve performansi, rizike i metrike KPI. Model je relevantan za razvoj i upravljanje efektivnim procesima DF istrage.

Ključne riječi: *integrirani model; kvalitet upravljanja DF procesa; metrici KPI DF procesa; performanse DF procesa; upravljanje procesom DF istrage*

1 Introduction

The difficulties and even impossibilities of measuring the DF investigation process are well described by Dr. Fred Cohen in his reference [1]. According to the accessible references, a few authors have described the corporate DF investigation (CDFI) process. However, an integrated management model including DF resources, objectives, key performances and the key performance indicator (KPI) metrics has not yet been defined, even theoretically. Michael W. Andrew [2] has introduced the concepts of efficiency and accuracy as the central issues in the DF analysis phase. Authors Siti R. Selamat, et al. [3] introduce an original Trace Map Model to facilitate the investigator in tracing and mapping the rate of evidence and offender identification. Mapping the DF investigation framework process, defined with between 3 and 21 phases, with activities and outputs for each phase, in order to optimize the whole DF investigation process, is suggested by Siti R. Selamat et al. [4]. A comprehensive model of the proactive, active and reactive DF investigation, and definition for Comprehensive Digital Evidence with evidentiary weight in a courtroom, has been proposed by authors C. P. Grobler et al. [5]. A model of high-performance computing in reactive, active and proactive DF is defined by authors Soltan Alharbi et al. [6]. Authors Henry Nnoli et al. [7] present a corporate forensic framework and sound forensic practices in large organizations. A detailed, iterative DF process model in the five main phases and the different roles it can perform (in each phase in general), followed by a mathematical algorithm to increase the reliability of DE, and are presented by the authors Marjan Khatir et al. [8]. The authors Richard E. Overill and Jantje A. M. Silomon [9] suggest quantifying methods for evaluation of the extent to which the recovered DE traces support suspicion of the prosecution that a particular computer crime has been committed, as well as the cost-effectiveness of the DF investigative process. George Sibiya et al. [10] propose a guideline for DF procedures in network forensics and a harmonized DF investigation process. An integrated reactive physical and digital investigation process model has been suggested by authors Brian Carrier and E.H. Spafford [11]. The authors of this paper propose an integrated process model of the CDFI management system, including risks, objectives, and recourses, key performances and KPI metrics, which is based on the four-phase reactive DF investigative process model defined by authors David C. Smith and Samuel Petreski [12]. This model, also accepted by the U. S. Department of Justice, is appropriate for the CDFI key performances to be chosen in this research. The CDFI KPI metrics are designed following the suggestions for very complex and uncertain metrics in DF as outlined by Dr. Fred Cohen in his reference [1]. The KPI metrics of the CDFI process proposed in this paper must be considered as a part of a more complex and comprehensive approach to the CDFI metric system. The CDFI process consists of a computer incident management team, including a qualified digital forensic examiner, and is intended to be integrated into an organization's information security management system

(ISMS) and total quality management system (TQM), to form a larger QMS framework in organizations.

2 Accepted model of the DF investigation process

The complexity of the DF investigation process has been analysed by many authors. Just as any process can be decomposed according to purpose, such as implementation, analysis, improvement, etc., the decomposition of the DF investigative process can be into four phases [12], five [2], or more [3]. In this research, the main purpose of the integrated CDFI process model decomposition is to avoid failed investigation and to improve CDFI procedures. Therefore, the four-phase DF investigation process was applied (Fig. 1): (1) identification & preparation, (2) acquisition, (3) analysis, and (4) presentation. In Phase 1 the DF investigative process should be prepared and planned, the forensic request identified and well understood, and all resources and communications provided. All digital devices in a computer incident that may be or may contain potential digital evidence (DE) must be identified and properly documented. In Phase 2, which is the most critical from a DF analysis point of view, sources of the potential DE are collected, packed, transported, and preserved, and their integrity maintained. In the next step of the logical acquisition, the potential DE is imaged or cloned into forensically clean media. In Phase 3 the relevant data for the case are identified, extracted and analysed. According to the forensic request, a proved piece of DE is constructed by corroborative DE traces, retrieved from different locations of the image/clone of digital data sources. In phase 4, the proved piece of DE must be reported and presented to the management of the organization, to law enforcement, or in a courtroom in a clear and understandable way. Obviously, live forensics are not considered in this CDFI model due to management support to the process and free access to the digital data (DD) sources.

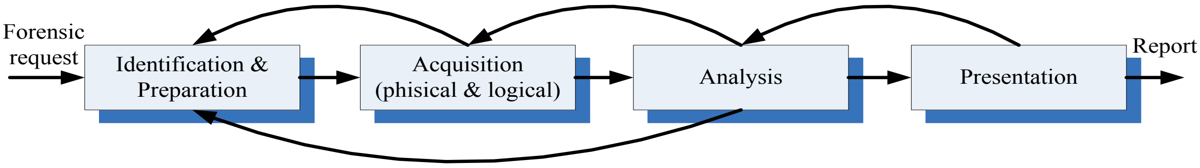
Forensic request
Identification & Preparation
Acquisition (phisical & logical)
Analysis
Presentation
Report

Figure 1 CDFI investigation process model using four phases

From the legal point of view, all DD are essentially circumvent evidence due to the nature of digital data, and as such could be unacceptable by a legal system. In fact, direct evidence in a digital environment can only be an immediate confession of an attacker caught by police during the attack itself, which is almost impossible and extremely rare at best. To be admissible in a courtroom, the nature of circumvent DD and the importance of the acquisition phase for DE construction must be carefully considered in accordance with DF science. Otherwise, admissibility of DE at trial does not depend so much on the acquisition but on the legality of the seizure, legality of the search, and relevance of the DD for the case. The DE, coming from many types of digital devices, can be easily modified and damaged, since it [3]: (1) is dispersed through the computer's traces; (2) is barely readable to humans; (3) gives a partial view of an incident/crime; (4) comprises abstractions of certain events; (5) is volatile and easily altered; and (6) must be retrieved from different sources and created by corroborative digital traces.

Collecting, maintaining and protecting the chain of custody of DE through a structured process and documented standard operating procedures (SOPs) in order to be admitted by law enforcement for further processing is crucial for the first incident responders in the CDFI process. In the acquisition phase of the CDFI process there are two aspects: (1) physical acquisition or collection of the DE sources, and (2) logical acquisition of the potential DE, retrieving them from a forensic image/clone in the post-mortem model applied in this model. In big data and cloud computing environments, the diversity of devices and locations generates a huge volume of DE that is not easily identified and traced [3]. In the acquisition and analysis phases of the CDFI process, forensic tools must be scientifically proved, legally accepted and performed by qualified DF experts responsible for the integrity of the DE. The DE must be easily tracked and preserved. In the presentation phase of the CDFI process, the main activities are documenting and explaining the DE in a clear and understandable way. As any forensic case could end up in the courtroom, consistency in terms of DE identification and traceability is very important and the most challenging feature of the CDFI process.

2.1 Quality of the DF investigation process performance

The quality of any process performance mainly depends on the KPIs metrics that must be defined completed and broadly accepted. Measuring the KPIs, as the key activities essential for the development and management of the effective DF investigation process, is proposed in this article. In order to develop quality of the DF investigation process, an objectively measurable KPI metric system must be defined. Except specification of DF case hypothesis and KPIs definitions, some thresholds of the KPIs metrics must be defined, too. These can be levels of: support by law; qualitative criteria; effectiveness and efficiency; industry standards application; statistical analysis; metric attainability; forensic examiner expertise, and the KPIs metric acceptance in the DF community, etc.

Quality of the DF investigation process KPIs metrics enables compliance with existing forensics standards. In these metrics, Yes/No measure must be used due to many uncertainties, such as: establishing DF process and KPIs criteria; measuring process performances effectiveness and efficiency; analysing the DF investigation reports, arbitrary assessing achieved threshold level, etc.

2.2 Iterative process of the DF KPI metric system development and implementation

The DF KPI metric system, focused on the specific forensic needs, can help significantly in developing DF investigation process maturity. It requires a quantitative measuring the DF KPI through the iterative activities and reality checks of the capabilities to capture and report DE. Before any KPIs metrics are implemented, the processes to define, develop and educate the stakeholders must be performed. However, any pre-defined DF KPI metrics could be ineffective due to uniqueness of each forensic case. Except measuring key performance of the DF investigative process the DF KPI metric includes knowledge and skill of the forensic examiner and other stakeholders. However, an initial set of the DF KPI metrics must be developed by digital forensic examiners and forensic community. The other stakeholders, including justice system, must be involved later on, and aligned the metric results with the DF investigation objectives. Therefore, once selected and agreed, the quantitative DF KPI metrics must be incorporated into the DF investigative management standards, principles and procedures. However, many of the DF KPI metrics are uncertain and some of them cannot be defined easily or even at all [1]. Therefore, very often there are no metrics associated with the DF KPIs, especially in changeable e-business and cybercrime environment. The DF objectives sometimes could be unrealistic (too high or too low) and the associated DF KPIs metrics' objectives must be changed. However, there is nothing wrong in that, if it is supported by the sound DE admitted by judge.

3 Establishing integrated model of the DF process performances objectives and the KPIs metrics

The main objective of the DF investigation process is to reconstruct event of the computer incident/crime and prove it in courtroom. However, on the whole the proved DE cannot be sufficient to reconstruct a case completely, particularly in connecting people to the attacker's computer. Therefore, in addition to the proved DE, some physical artefacts and eyewitness statements are needed.

The CDFI KPI metrics must meet legal requirements for measuring reliability, authenticity and accuracy of the DE, based on properly applied scientific methodology and independent, repeated examinations. However, the DF KPI metrics have not yet been established comprehensively and precisely, and there is no industry standard to support them. Therefore, KPI metrics concepts from another research area must be adopted to build the CDFI KPI metric system. However, some metrics in the DF investigative process have already been proposed, such as the Forensic Traceability Measurement by authors Siti R. Selamat et al. [3]. Daniel Ayers [13] makes suggestions for the measurement of the computer forensic tools' efficacy and performance, including the following parameters: absolute (T) and relative (T1) speed; completeness (%); accuracy (100 %); reliability (100 %); auditability (%); repeatability (%); and limitations of first-generation tools (Y/N).

The CDFI KPI metrics should be implemented into the computer incident management system to encourage its performance improvement, effectiveness and efficiency of the internal security controls and the ISMS. This approach should provide quantitative assessment of gains in the main CDFI objectives, such as: (1) creation of the proved DE; (2) reduction of the cost and the CDFI cycle time; and (3) understanding attack activities and reconstruction of the computer incident/crime. The key elements of the CDFI KPI metrics in this approach should address alignment with the DF principles and SOPs, and meet the forensic and legal requirements.

Measuring the CDFI KPIs is of critical importance for improvement of their objectives, performances, effectiveness and efficiency. These parameters incorporate "best practices" of the measured KPIs, an appropriate risk analysis, and provide a quantitative assessment of new business values. The first step in developing the CDFI KPI metrics is to involve the DF stakeholders and other necessary resources, then to identify critical phases of the CDFI process, forensic requirements, objectives, key performances of the CDFI process, and finally the KPI metrics. Examples of independent category classification of the DE KPIs that are not mutually exclusive could involve content and variety of data (such as metadata, directory, configuration, log, backup, recovered and tampered data), and forensic interpretation, as well.

In general, to determine the quality of a particular KPI metric, the SMART (specific, measurable, attainable, realistic, and timely) test can be used. The importance of the KPI metrics' quality is well known, especially for assessment of the process trend and change management against known and new coming standards. In the CDFI KPI metrics, a Yes/No or TBD measure must very often be used, usually for establishing trends and baselines, such as: DE legal admissibility; performed DF analysis with/without SOP criteria; qualification of the DF examiner, etc. The CDFI KPI metrics can provide a quantitative assessment of forensic requester satisfaction and quality of CDFI performances and DF investigator's services.

According to ISOstandards, objectives are defined as wanted results and performances as accomplished results. They should have the same KPIs as much as possible [15]. Development of the CDFI KPIs and their objectives and metrics can best be specified when they are defined at the levels of objectives, criteria and KPI metrics. The key performance objectives, risks and recourses of the CDFI process are outlined in Tab. 1.

In Tab. 1 the phases and activities are selected according to the four-phase DF investigative model. Some activities such as planning and providing resources for the CDFI process are avoided, as they are mandatory in any process. The other items are selected as representatives of the key activities, following the idea of the CDFI key performance analysis. Among the many performances of the CDFI process, the authors have selected only the key ones among them that are critical for the effectiveness and efficiency of the CDFI process, including their risk, verification status and validation status. The risk factors have to be analyzed in any process, and therefore must be assessed in the CDFI process, as well. The verification status of the key activities reflects assessment of the SOPs and forensic technology application strictness in accordance with the CDFI process. The validation status of the CDFI process depends on legal judgement after cross-examination in the courtroom. The legal system's involvement includes providing a warrant for initiating the CDFI process, and extends into the trial process. In Tab. 1 an "expert" means one expert of the computer science without forensic knowledge who can tell only facts. Opposite, "an expert witness" is a digital forensic specialist who has legal licensee and can express facts and his/her own opinion.

Some examples of the CDFI KPI objectives and metrics are described in Tab. 2. Some of them are implicitly included, such as: compliance with the DF principles, methods, techniques and tools, and forensic request; CDFI cost optimization; quality of the DE and DF investigator's work; CDFI cycle time reduction; delivery time of the DE; forensic requester satisfaction, etc.

Table 1 Mapping objectives and resources of the CDFI process key performances

Key phases and activities of the DF investigation process	Key performances, risks and resources of the DF investigationprocess								
	Risk factors	Digital traces/ data sources	Identification & traceability consistency	Digital evidence	Digital forensic examiner	Forensic tool	Verification status	Legal system	Validation status
1. Preparation & identification	1	2	3	4	5	6	7	8	9
1.1. DD collection, transportation & storage	*	*	*		*		*	*	
1.2. Protection of DD/DE source integrity	*	*	*		*		*		
1.3. Creating the forensic case hypothesis	*	*	*		*				
2. Logical acquisition of DD & potential DE									
2.1. Forensic imaging/cloning of DD/DE	*	*	*		*	*	*		
3. Digital evidence analysis									
3.1. Discovery &extraction of the hidden DE& patterns	*	*	*		*	*	*		
3.2. Analysis & corroborativebuilding of proved DE	*	*	*	*	*	*	*		
3.3. Hypothesis verification	*		*	*	*				
4. Digital evidence presentation									
4.1. Expert / Expert witness testimony of the DE	*		*	*	*		*	*	
4.2. Hypothesis validation in cross-examination	*		*		*			*	*
Legend: DF – Digital Forensics; DD – Digital Data; DE – Digital Evidence									

Table 2 Examples of the CDFI KPIs objectives and metrics

No.	Key performance, risk, activity & resources of the CDFI process	Key performance objectives of the CDFI process	KPI (key performance indicator)	Metric
1	Preparation & Identification			
	1.1 DD/DE collection, transportation & storage			
	Risk factors	Incomplete/unclear forensic request	Inutility of DE for case	L, M, H*
		Anti-forensic activity	Anti-forensic activity verified	L, M, H
		Communication failure among stakeholders	Relevant DE uncovered	L, M, H
		Inadequacy of DD sources/content	Insufficient coverage of DE for case	L, M, H
		Lack of search & seizure SOP	DE contamination	L, M, H
		Lack of forensic case context assessment	Wrong direction of CDFI process	L, M, H
		Delay of the forensic request	Impossibility of DE extraction	L, M, H
	Digital data/traces sources	Completeness & comprehensiveness	Relative number** of DD/DE sources related to forensic case	Total N
		Ranking levels of DD/traces sources	Most evidentially significant DD/traces and lowest cost of those ranked	% of N
	Identification & traceability consistency	Level of identification and marking in the search & seizure process	Number of marked computer system components related to case	% of N
		Level of record traceability	Relative number of documented activities related to total executed	%/TBD
		Level of snapshot traceability	Relative number of relevant snapshots related to total executed	%/TBD
		Level of DD integrity protection	Relative number of verified image hash values related to total executed	%/TBD
		Level of forensic triage and prioritization	Number of performed triages & prioritizations related to examined DD sources	%/TBD
			Cost-benefit ratio (CBR) and ROI of CDFI	

No.	Key performance, risk, activity & resources of the CDFI process	Key performance objectives of the CDFI process	KPI (key performance indicator)	Metric
			calculated	CBR>1
	Digital forensic investigator	Level of education Level of experience and skillfulness	Proof of competency and skillfulness Total number CDFIs executed Relative number of cases admitted by judge related to total executed	Y/N M % (M)
	Verification status	Compliance of DE sources to forensic requirement Level of CDFI return-on-investment (ROI) Level of CDFI cost-benefit (CBR)	Level of compliance (Gain from investment – cost of CDFI investment)/cost of CDFI investment Cost of CDFI/relevance of DE	%/TBD >1 <1
	Legal system	Legality of DD/DE collection	Manager's decision or warrant for CDFI	Y/N
	1.2.	Protection of DD/DE source integrity		
	Risk factors	Wrong application of SOP Forensic examiner/tool failure	DE chain of custody interrupted DE sources corrupted	L, M, H L, M, H
	Digital data/ traces sources	Physical & logical protection of digital devices & media	Documented DE chain of custody	Y/N (TBD)
	Identification & traceability consistency	Level of DD/DE source identification Level of DD/DE source record traceability	Relative number of identified relevant DE sources related to total number of sources Relative number of documented activities related to total executed	%/TBD %/TBD
	Digital forensic examiner	Level of education Level of experience and skillfulness	Proof of competency and skillfulness Total number of CDFIs executed by DF examiner Relative number of cases admitted by judge related to total executed	Y/N M % (M)
	Verification status	Level of DD/DE source authenticity	Relative number of verified hashes related to total number of imaged/cloned files	%/TBD
	1.3.	Creating the forensic case hypothesis		
	Risk factors	Insufficient number of DD traces Incomplete reasonable suspicion Wrong assessment of obviously inapplicable data ejection Relevant data losses due to log files filtration	Impossibility of DE extraction Wrong leading digital data Inconsistency of corroborative digital evidence False positive of digital evidence	L, M, H L, M, H L, M, H L, M, H
	Digital data/traces sources	Completeness of DE sources and case coverage	Level of compliance with forensic requirement	%/TBD
	Identification & traceability consistency	Ejected obviously inapplicable DD Documented & complied to reasonable suspicion	Ejected digital data related to full volume Level of documented DD supporting or opposing hypothesis	% %/TBD
	Digital forensic examiner	System engineering & investigation competency	Proof of competency and skillfulness Level of successfully predicted hypotheses related to executed ones	Y/N %/TBD
2	Logical acquisition of DD and potential DE			
	2.1.	Forensic imaging/cloning of DD/DE		
	Risk factors	Wrong application of SOP forensic examiner or tool failure Anti-forensic activity	Contamination of DE Number of blocked tools during imaging/ cloning process Incomplete media imaging/cloning	L, M, H L, M, H L, M, H
	Digital data/traces sources	Completeness & case coverage of DD sources Level of snapshots and extracted DD from running computers	Level of DD sources without forensic traces related to executed ones Relative number of relevant DD for case related to total executed	%/TBD %/TBD
	Identification & traceability consistency	Level of documented imaging/cloning of DD/DE	Relative amount of traceable DE related to imaged/cloned DD	%/TBD
	Digital forensic examiner	Level of imaging/cloning tool knowledge and choice Efficiency & effectiveness of imaging/cloning process	Adequacy of forensic tool chosen Relative time of imaging/cloning related to specified time for tool applied	%/TBD T(s/m/h)
	Forensic tools	Imaging/cloning speed by GB Level of imaging/cloning reliability	Absolute time of imaging/cloning Repeated imaging/cloning compliance	T(s/m/h) %/TBD
	Verification status	Level of image/clone integrity	Positive verification of image hash	Y/N
3	Digital evidence analysis			
	3.1	Discovery & extraction of hidden DE & patterns		

No.	Key performance, risk, activity & resources of the CDFI process	Key performance objectives of the CDFI process	KPI (key performance indicator)	Metric
	Risk factors	Digital forensic examiner failure Inadequate forensic tool choice	Incompleteness of extracted DE	L, M, H
	Digital data/traces sources	Level of DE traces discovered Level of leading DD in single search	Relative number of DE traces per source of DD Relative number of digital traces per single search	%/TBD %/TBD
	Identification & traceability consistency	Level of relevant DE trace identification Level of relevant DE trace consistency	Relative amount of unidentified leading DE related to total executed Relative amount of inconsistent leading DE related to total executed	%/TBD %/TBD
	Digital forensic examiner	Efficiency and effectiveness of leading DE extraction	Relative amount of leading DE extraction related to total executed	%/TBD
	Forensic tools	Relative speed of leading DE extraction per GB of searched data Leading data extraction reliability	Relative time of leading DE extraction Relative number of corroboratively proofed DE traces related to total executed	T(s,m,h) %/TBD
	Verification status	Level of leading DD compliance to forensic case	Relative number of DE nonconformities to forensic case related to total executed	%/TBD
	3.2.	Analysis & corroborative building of proved DE		
	Risk factors	Digital forensic examiner failure Digital forensic tool failure Inconsistency in leading DD Anti-forensic activities Margin of error at each layer of abstraction DD consideration in isolation from system	Relative amount of false DE interpretation related to total executed Relative number of forensic tools blocked in analysis process Relative amount of DE missing related to total executed Impossibility of building DE corroboratively Impossible access to layer inputs, rule set and outputs to verify translation Influence of forensic tool error on DD integrity	L,M,H L,M,H L,M,H L,M,H L,M,H L,M,H
	Digital data/traces sources	Level of relevancy of DE traces per DD source	Relative number of leading DE traces per source related to total executed	%/TBD
	Identification & traceability consistency	Level of identified & documented leading DD Level of leading DD consistency	Relative amount of identified leading DD related to total executed Relative amount of consistent leading DD related to total executed	%/TBD %/TBD
	Digital evidence	Completeness & coverage of DE for case proof Level of corroboratively proved DE Level of proved principle of DE consistency Level of proved DE association, context, access, intent & validation to DF request	Relative amount of DE discovered, recovered and opened for case related to total executed Relative amount of corroboratively proved DE related to total executed Relative amount of proved principle of DE consistency related to total executed Relative amount of DE association, context, access, intent & validation to the DF request related to total executed	%/TBD %/TBD %/TBD %/TBD
	Digital forensic examiner	Level of DF examiner's knowledge & experience	Relative amount of rejected proved DE by lawsuit related to total executed	%/TBD
	Forensic tools	Absolute analysis speed Relative analysis speed Level of repetitiveness of verified DE test Level of rendering raw DD into readable & searchable formats Level of decryption, recovery & presentation in a useable format Level of reliability & repetitiveness of the analysis test	Time required to finish analysis DE processing time required to read data as on original media Relative number of testsverified by another forensic tool related to total executed Relative time of rendering raw DD related to specified time Relative time of translation into usable format related to specified time Relative number of tests with same results related to total executed	T(s,m,h) T_1(s,m,h) %/TBD % (N) T_2(s,m,h) T_3(s,m,h) %/TBD
	Verification status	Proved DE compliance to forensic request Level of forensic image integrity at any access point	Relative amount of inconsistent DE related to forensic request Relative number of unverified hashes related to total executed	%/TBD %/TBD
	3.3.	Hypothesis verification		

No.	Key performance, risk, activity & resources of the CDFI process	Key performance objectives of the CDFI process	KPI (key performance indicator)	Metric
	Risk factors	Forensic hypothesis assessment failure Insufficient DE for hypothesis verification	Relative amount of inapplicable DE related to total executed Relative amount of unacceptable DE related to total executed	L,M,H L,M,H
	Identification & traceability consistency	Level of identified, consistent & documented DE to support hypothesis Level of identified, consistent & documented DE to deny hypothesis	Relative amount of DE to support hypothesis related to total executed Relative amount of DE to deny hypothesis related to total executed	%/TBD %/TBD
	Digital evidence	Level of consistent DE for hypothesis verification Level of relevancy and weight of DE for hypothesis verification	Amount of verified DE supporting hypothesis Relative number of proved DE supporting/opposing hypothesis	N % (N)
	Digital forensic examiner	Level of digital forensic examiner competency	Relative amount of supporting DE unverified related to total executed	%/TBD
4	Digital evidence presentation			
	4.1 Expert/ Expert witness testimony of the DE			
	Risk factors	Level of DE relevancy to case Insufficient weight of DE to be accepted by manager/court suite Biased testimony of expert/expert witness Unclear and complex terminology of the expert / expert witness	Relative amount of DE rejected by judge related to total presented Relative amount of insignificant DE for case related to total presented Relative number of biased statements related to total testified Relative number of terms requested to be clarified related to total presented	L, M, H L, M, H L, M, H L, M, H
	Digital forensic examiner	Level of testimony efficiency & effectiveness Level of DF examiner honesty, integrity & neutrality	Relative number of accepted testimonies related to total presented Relative number of rejected testimonies related to total executed	%/TBD %/TBD
	Identification & traceability consistency	Level of DE traceability & consistency presentation Level of reliability, principles and methods of testimony application	Relative number of consistent & traceable facts related to DE Relative number of rejected testimonies related to total executed	%/TBD %/TBD
	Digital evidence	Level of presentation of DE relevancy and weight for case	Relative number of rejected DE related to total presented	%/TBD
	Legal system	Level of admitted DE testimony from CDFI process	Relative number of admitted DE related to total presented	%/TBD
	Validation status	Level of failed DE testimony	Relative number of failed DE testimonies related to executed ones	%/TBD
	4.2. Hypothesis validation in cross-examination			
	Risk factors	Hypothesis disproved by other side Level of DE incompleteness Unclear/complex DE presentation Identified DE inconsistency	Relative number of failed hypotheses related to total predicted	L, M, H
	Identification & traceability consistency	Level of consistency & traceability of DE for hypothesis validation	Relative amount of rejected DE related to total validated	%/TBD
	Digital forensic examiner	Level of validated DE per case	Relative amount of validated DE related to total presented	%/TBD
	Legal system	Level of validated hypothesis by manager/judge per case	Relative number of validated hypotheses relating to total presented	%/TBD
	Validation status	Level of satisfaction of all stakeholders	Relative number of cases closed by final verdict related to total executed	Y/N
	Legend: DF – Digital Forensics; DD – Digital Data; DE – Digital Evidence; SOP – Standard Operating Procedure; *TBD – To be done in future research; Y/N – Yes or No decision; L, M, H – Low, Medium, High risk; CBR – Cost-Benefit Ratio; ROI – Return of Investment; SE – System engineering; **Relative number … – ratio of measured amount to total executed amount (% or TBD)			

4 Integrated management model of the corporate DF investigation

The effectiveness of a CDFI management system can be measured by levels of its performance objective achievement. The main purpose of establishing a CDFI management system is to define the following: management methodologies of its policy and objectives; risk factors influencing them; and the resources and CDFI process activities to fulfil stakeholders' forensic requirement needs and expectations [16]. Any organization conducting a CDFI process must ensure that it is supported by forensically sound and legally admissible procedures. The CDFI process must implement a quality management system to apply CDFI methodologies, techniques and tools.

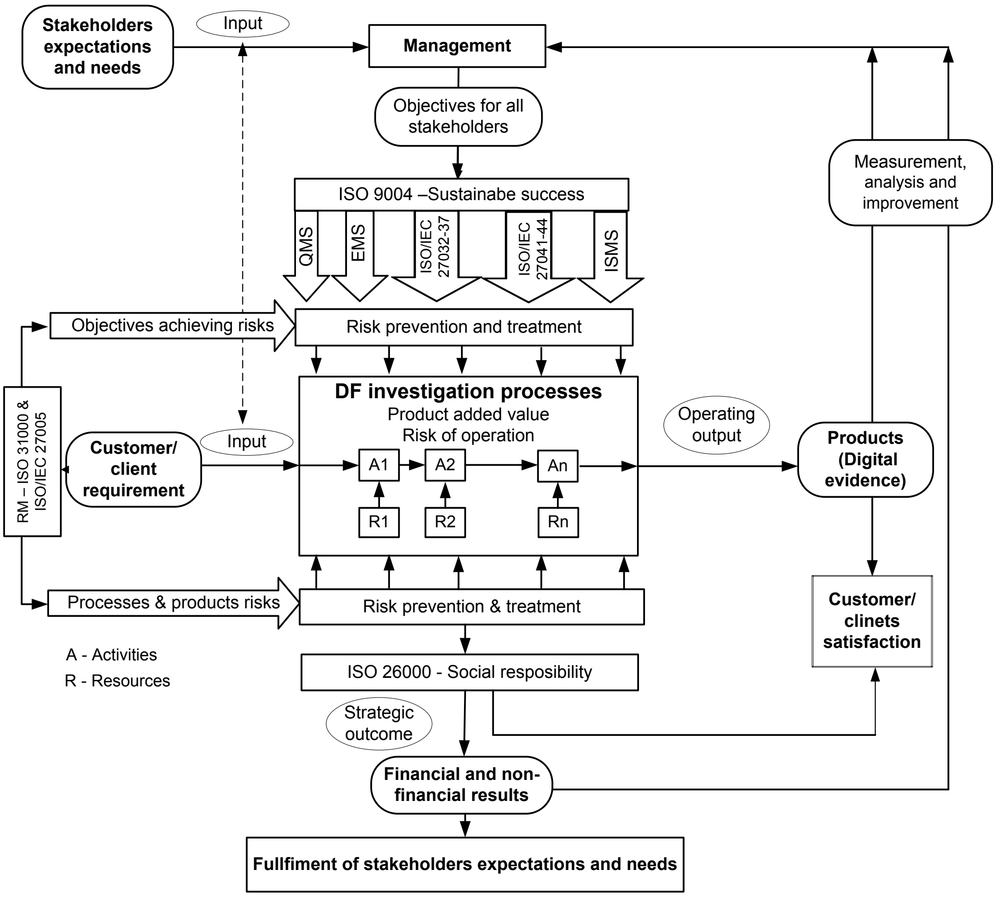
Stakeholders expectations and needs
Input
Management
Objectives for all stakeholders
Measurement, analysis and improvement
ISO 9004 –Sustainabe success
QMS
EMS
ISO/IEC 27032-37
ISO/IEC 27041-44
ISMS
Objectives achieving risks
Risk prevention and treatment
RM – ISO 31000 & ISO/IEC 27005
DF investigation processes
Product added value
Risk of operation
Customer/ client requirement
Input
A1
A2
An
R1
R2
Rn
Operating output
Products (Digital evidence)
Processes & products risks
Risk prevention & treatment
Customer/ clinets satisfaction
A - Activities
R - Resources
ISO 26000 - Social resposibility
Strategic outcome
Financial and non-financial results
Fullfiment of stakeholders expectations and needs

Figure 2 Integrated management model of the CDFI process

The objectives of the CDFI management process can cover many functions, such as: manage legal and ethical requirements for education, security training and awareness; define security/forensic policies and procedures; perform incident investigation [18]; identify and collect DE; examine, analyse and manage DE; manage third parties; and document, report and present DE [7]. In the integrated model of the CDFI process management system, forensic requirements are input values. The needs and expectations of the stakeholders – who may include the client and the legal system, DF and law enforcement investigators, and suspected/convicted persons – are the objectives that management must identify. For the clients and the other stakeholders, the outputs of the integrated CDFI process management model are products/services of the CDFI process phases and activities. Results of the outputs can be defined as the KPIs of achieved objectives of DF investigation process performances. The functional structure of the integrated model of the CDFI process management system, providing application of the IMPROP model [16] to the DF investigation process, is shown in Fig. 2.

The detailed structure of partial management systems (e.g. ISMS), shown vertically in Fig. 2, can be defined by establishing individual management systems according to corresponding standards. However, many forensic standards are still missing. Some of them are in draft form, and a few of them have been already published. There is also a lack of standardized data sets that are available for research purposes [17].

In this model, the main purpose of ISO/IEC standards is to promote techniques and methods of good practice in the DF investigation process. The results of a standardized DF investigation process could facilitate easier comparison and acceptance of the obtained DE by different people in the CDFI process, or in different legal systems. Once adopted into CDFI practice, these forensic standards require the CDFI process management system to be integrated into ISMS and TQM systems within the organization. In addition to the existing forensic standards, general QMS (ISO 9001) and EMS (ISO 14001) standards must also be included in this model. The QMS standard can help in defining the DF investigation process input transformation and its product value, anti-forensic risk prevention, and quality achievement of the CDFI process objectives. The EMS standard, focused on environmental risk prevention and achievement of environmental objectives, as well as the other general and information security standards, such as ISO 9004, ISO 31000, ISO 26000, ISO/IEC 27001, 27032, 27033, 27034, and 27035, should also be applied in the model.

Current industry standards cover only three components of the DF investigation process: acquisition, preservation and analysis [2]. Existing nationally created DE acquisition procedures for cross-border computer crimes may not be accepted by another country's legal system. Therefore, the newly published ISO/IEC 27037 standard for acquiring DE must be included in the integrated model. This standard provides guidance on integrity preservation of the identified, collected, acquired, marked, stored and transported DE. It harmonizes acquisition activities across borders so that cyber criminals can be prosecuted accordingly. This standard is not technically oriented and avoids using jurisdiction-specific terminology. The main purpose of the ISO/IEC 27041 standard is to describe mechanisms, methods and processes used in the first response and investigation of computer incidents or crimes, providing relevant DE for a successful DF investigation later on. It gives guidance on the validation of the DF investigative processes. The main focus is on security of the DF processes, methods and tools used in the DF investigation. The scope and purpose of ISO/IEC 27042 describes guidance on the processes of analysing, interpreting and corroboratively constructing the proved DE. This standard emphasizes the integrity of these processes in such a way that different investigators, working on the same DE, must get essentially the same results. Any differences in results, due to use of different tools or forensic techniques, should be traceable and explainable. It introduces the basics of forensic tool selection and use, as well as proficiency and competency of the investigators. A harmonized DF process is presented in the ISO/IEC 27043 standard. The scope and purpose of this standard concerns the DF principles and the processes involved in investigating incidents, providing proactive counter-processes to an incident, including retrieving DE from storage or dissemination of any DF investigation experience. These forensic standards are the drivers for standardization of the DF investigative process, application of good practices, lessening of the complexity of DE, and use of common terminology and forensically sound approaches to any computer incident or crime.

Therefore, it is possible to apply the IMPROP model in the case of using one or more management system standards, including ISMS and CDFI process management systems that are mutually complementary. These standards support the effectiveness and efficiency of security and CDFI management systems. It is recommended to use them simultaneously. In the application of this model to the CDFI, it is very important to emphasize the significance of teamwork, due to the multidisciplinary knowledge and experiences that are required in DF science.

5 Conclusion

Quantitative measurement of CDFI KPIs may provide corporate digital forensic investigators and managers, law enforcement DF examiners and judges with vital information for monitoring and verifying the consistency of the CDFI process, enabling the most appropriate judgment in the courtroom and focusing CDFI resources on the areas of greatest business value. Some metrics, such as financial metrics, are well established and, to a great extent, dictated by regulatory bodies worldwide. In the DF community there are no such broadly accepted standards to establish a consistent KPI metric system of the DF investigative process. The authors of this article suggested some of the key CDFI process performances and their KPI metrics, based on available references and original research. Beyond these suggested CDFI KPI measures, it is up to each DF investigative entity, each CDFI team and the individuals involved to define the right metrics for their environment and DF investigative processes. More practice and experience in CDFI KPI metric implementation could contribute to this insufficiently defined forensic area. All relevant stakeholders in the CDFI process can benefit from well-conceived and implemented CDFI KPI metrics.

In this research the authors proposed a theoretical integrated CDFI process model, its key performances and their KPI metrics. Further research, developing and implementing the CDFI process model and KPI metrics in real systems, is an extremely important step toward maturing the field of the CDFI process itself, corporate forensic readiness and computer incident management systems, which are also a vital part of an organization's proactive network security, incident management, ISMS and TQM systems. Finally, it would provide further promotion and standardization of DF as a forensic science.

6 References

[1] Cohen, F. Metrics for Digital Forensics. // Proceedings of the MiniMetriCon Conference / San Francisco, 2011, pp. 1-22.

[2] Andrew, M. W. Defining a Process Model for Forensic Analysis of Digital Devices and Storage Media. // IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering / Seattle, 2007, pp. 16-30. DOI: 10.1109/SADFE.2007.8

[3] SSelamat, S. R.; Sahib, S.; Hafeizah, N.; Yusof, R.; Abdollah, M. F. A Forensic Traceability Index in Digital Forensic Investigation. // Journal of Information Security. 4, 1(2013), pp. 19-32. DOI: 10.4236/jis.2013.41004

[4] Selamat, S. R.; Yusof, R.; Sahib, S. Mapping process of digital forensic investigation framework. // International Journal of Computer Science and Network Security. 8, 10(2008), pp. 163-169.

[5] Grobler, C. P.; Louwrens, C. P.; von Solms, S. H. A multi-component view of digital forensics. // Availability, Reliability, and Security, ARES'10 IEEE International Conference / Krakow, 2010, pp. 647-652. DOI: 10.1109/ARES.2010.61

[6] Alharbi, S.; Moa, B.; Weber-Jahnke, J.; Traore, I. High performance proactive digital forensics. // Journal of Physics: Conference Series. 385, 1(2012), pp. 15. DOI: 10.1088/1742-6596/385/1/012003

[7] Nnoli, H.; Lindskog, D.; Zavarsky, P.; Aghili, S.; Ruhl, R. The Governance of Corporate Forensics Using Cobit, Nist and Increased Automated Forensic Approaches. // Privacy, Security, Risk and Trust (PASSAT), 2012 International Conference on and 2012 International Confernece on Social Computing IEEE / Amsterdam, 2012, pp. 734-741.

[8] Khatir, M.; Hejazi, S. M.; Sneiders, E. Two-dimensional evidence reliability amplification process model for digital forensics. // Digital Forensics and Incident Analysis / Malaga, 2008, pp. 21-29

[9] Overill, R. E.; Silomon, J. A. Digital meta-forensics: Quantifying the investigation. // Proceedings 4th International Conference on Cybercrime Forensics Education & Training / Canterbury, 2010,

[10] Sibiya, G.; Venter, H. S.; Ngobeni, S.; Fogwill, T. Guidelines for procedures of a harmonised digital forensic process in network forensics. // Information Security for South Africa (ISSA) / Johannesburg, Gauteng, 2012, pp. 1-7.

[11] Carrier, B.; Spafford, E. H. Getting physical with the digital investigation process. // International Journal of digital evidence. 2, 2(2003), pp. 1-20.

[12] Smith, D. C.; Petreski, S. A New Approach to Digital Forensic Methodology // DEF CON / Las Vegas, 2007

[13] Ayers, D. A second generation computer forensic analysis system. // Digital Investigation. 6, (2009), pp. 34-42. DOI: 10.1016/j.diin.2009.06.013

[14] Heleta, M.; Grubor, G.; Veljković, S. Model for Integrated Management of the Processes, Objectives, Risks and Performances. // International Journal of Scientific and Research Publications. 3, 10(2013). pp. 1-9.

[15] Heleta, M.; Heleta-Milošević, A. Integration of the objectives indicators and organization's key performances // International Convention on Quality, JUSK ICQ / Belgrade, 2010.

[16] Garfinkel, S.; Farrell, P.; Roussev, V.; Dinolt, G. Bringing science to digital forensics with standardized forensic corpora. // Digital Investigation 6(2009). pp. 2-11. DOI: 10.1016/j.diin.2009.06.016

[17] Kent, K.; Chevalier, S.; Grance, T.; Dang, H. Guide to integrating forensic techniques into incident response. // NIST Special Publication. (2006), pp. 800-86. DOI: 10.6028/nist.sp.800-86

Authors' addresses

Gojko Grubor, PhD, Assistant professor
Sinergija University,
Raje Baničića bb, 76300 Bijeljina, B&H
E-mail: ggrubor@sinergija.edu.ba

Milenko Heleta, PhD, Assistant professor
Singidunum University,
Danijelova 32, 11000 Belgrade, Serbia
E-mail: mheleta@singidunum.ac.rs

Nenad Ristić, PhD student
Sinergija University,
Raje Baničića bb, 76300 Bijeljina, Bosnia and Herzegovina
E-mail: nristic@sinergija.edu.ba

Ivan Barać, PhD student
Singidunum University,
Danijelova 32, 11000 Belgrade, Serbia
E-mail: ivan.barac@yahoo.com