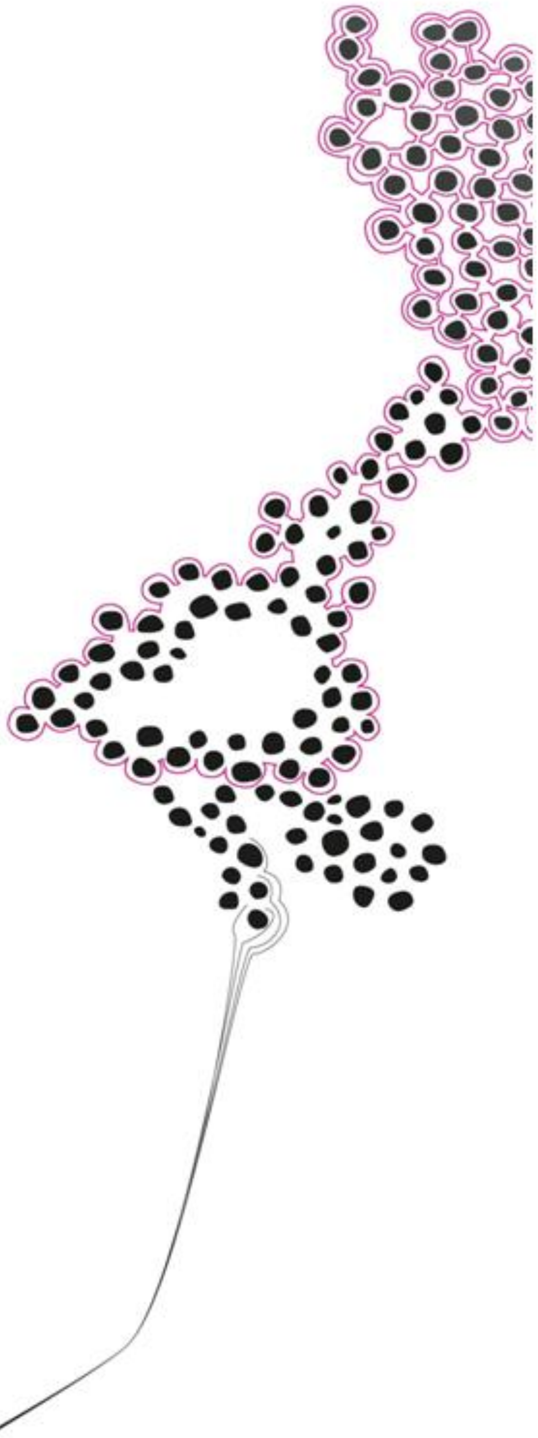
UNIVERSITY OF TWENTE.



Continuous Forensic Readiness

Master Thesis
By Jeroen de Wit

Continuous Forensic Readiness

Author:

Jeroen de Wit
Master Computer Science
Track Computer Security

Student number s0123277
jeroen@jeroendewit.nl
dewit.jeroen@kpmg.nl
Tel: +31 6 3096 7642

Faculty of EEMCS, University of Twente
P. O. Box 217, 7500AE Enschede
The Netherlands

Graduation Committee:

First supervisor

Dr. Pascal van Eck
Assistant Professor
Information Systems group
Faculty of EEMCS
p.vaneck@utwente.nl
Tel: +31 53 489 4648

Second supervisor

Dr. Hilda Folkerts
Lecturer IT Management
Industrial Engineering and Business Information Systems (IEBIS)
School of Management and Governance
h.f.folkerts@utwente.nl
Tel: +31 65240 0345

Third supervisor:

ir. Matthieu Pâques CISSP CISA
Manager
KPMG Advisory N.V.
Risk Consulting – Information Protection Services
paques.matthieu@kpmg.nl
Tel: +31 20 656 8409

Revision: 1.22
Date: 20 October 2013

Preface

This document contains my master thesis, the final document that I produced for the master Computer Science at the University of Twente. It describes the design, execution and results of my research on Continuous Forensic Readiness, which I carried out at KPMG IT Advisory. During my period at KPMG the subject caught the attention of both clients and colleagues. I hope the results of this research contribute to the knowledge on this subject within the company as well as in the academic literature.

This master thesis would not have been possible without the support of so many people, starting with my supervisors Pascal, Hilda and Matthieu. Despite the sometimes bumpy ride this thesis research has proven to be, they have helped me get the right research approach, continuously delivered high quality feedback and offered me great advice that provided guidance and direction for my thesis research.

I would also like to thank all my colleagues at KPMG for the formal and informal guidance through discussions, debates and the overall very pleasant working atmosphere. Lars and Thom, special thanks to the both of you for making available your forensic knowledge and ideas in the early stage of this research. Olga, our little intern team was tremendously fun, and it’s great to be able to continue to work together as advisors at KPMG.

A special note for my friends, family and my parents. They have supported and encouraged me throughout my entire life. This certainly includes my time in Enschede, where I had the privilege to take part in numerous great activities which made that period so very special. It’s something I will be able to look back upon with a smile for the rest of life.

Last, but definitely not least: A very, very special note for my girlfriend, Jamie-Dee. Despite the endless hours I spent on this research, and maybe even more despite the time I spent on matters besides this research, she has supported and inspired me throughout my entire study and thesis period and helped me to stay focused and finish my research.

I hope you will enjoy reading this master thesis about continuous forensic readiness. If at the end of this thesis you have any remaining questions or remarks, please feel free to contact me.

Jeroen de Wit

Amstelveen, October 2013

Management Summary

For years information security has focused on implementing preventive measures to avoid IT incidents. In recent years the realization has struck that only trying to prevent IT incidents is insufficient, as examples have shown that a determined attacker with sufficient resources will eventually be successful in breaking or circumventing any preventive measures taken. As such, organizations are now taking a more holistic approach to information security, implementing preventive, detective and responsive measures.

Depending on the organization and the nature of the IT incident, response to an incident can contain a forensic analysis. Upon successful completion, such an analysis reveals exactly how the incident occurred, which systems and data have been affected and potentially who is responsible. Upcoming legislation will force organizations to disclose such detailed information on IT incidents to supervisory authorities, in case of data breaches. Being prepared for forensic analysis is known as a state of forensic readiness. Currently there is no generally acknowledged model available on how organizations can achieve that state within the academic literature, nor in the professional market. Furthermore, the limited amount of available guidelines which describe how to (partly) achieve a state of forensic readiness do not describe how organizations can maintain it.

This research proposes the Continuous Forensic Readiness Framework (CFRF), based on literature studies and interviews, which allows organizations to reach and maintain a state of forensic readiness. The basis for the CFRF are 44 aspects and corresponding illustrative controls for achieving forensic readiness. These aspects are derived from academic literature and experts on forensic analysis. To allow a state of continuous forensic readiness to be reached, for each aspect the CFRF describes actions to be performed in a Plan-Do-Check-Act (PDCA) cycle, on the different management levels Strategic, Tactical and Operational. For each of these actions responsibilities are assigned to stakeholders, differentiating between Responsible, Accountable, Supportive, Consulted and Informed (RASCI).

The aspects within the CFRF are categorized in People, Process and Technology, and furthermore divided into three levels of importance. This allows the framework to be implemented in a layered manner starting on controls with the highest importance, as well as for each organization to determine on which level they are currently acting. Furthermore, the division in categories allows implementation and maintenance to be delegated within the organization while progress and status can be monitored by assessing the controls.

By implementing the CRFR organizations are able to achieve a state of continuous forensic readiness, and are thus prepared to perform forensic analyses at all times.

Table of Contents

List of Figures

List of Tables

1 Introduction

Cybercrime incidents are still increasing in number, magnitude and impact [56, 77, 78, 83, 137]. Despite efforts in trying to keep attackers out of critical systems, it has been deemed impossible to completely secure systems [18, 133]. In other words, with unlimited time and resources an attacker that is determined to gain unauthorized access to your systems will succeed sooner or later. This requires organizations to prepare beforehand for data leaks and IT incidents; mainly focusing on technological prevention techniques, such as currently often still done [39, 96], is no longer sufficient. Organizations will need to take other factors into account, such as people and processes. A method which does that is from here on called *holistic*.

In order to achieve such a holistic approach to security and offer a more thorough defense, organizations should focus on three main aspects of cybercrime: prevention, detection and response [69]. Prevention techniques are nowadays generally accepted even by consumers, with commonly installed anti-virus programs and firewalls put in place to defend against known viruses, malware and otherwise unwanted visitors to their system. Organizations and governments often have advanced variants in place. Furthermore, monitoring techniques to detect ongoing attacks, such as an Intrusion Detection System (IDS), are commonly implemented in large organizations. A more sophisticated attacker is able to circumvent most of these measures though, as has become clear to the general public as well due to several high impact incidents broadly discussed in the media such as the *Stuxnet* [110] malware and more recently the *Duqu* [108] and *Flamer* [82, 109] worms.

An inability to deal with attacks and remove or mitigate the risk can have considerable consequences for organizations. Most notable examples are the loss of vital (business, confidential, valuable) information, great financial implications as a result of brand damage and disruption of business processes. [3, 45, 74, 75]. Besides adequate prevention techniques it is thus of crucial importance for any organization to quickly and adequately detect and respond to IT incidents. Unfortunately this is currently not the case due to organizations' inability to perform decent, timely analysis on their systems and network after detection of an incident: they are not ready for analysis, let alone a forensically sound analysis. This can partly be explained due to some organizations' impression that the benefits do not compensate for the costs which need to be made to prepare for such cases. However, as explained more thoroughly in section 1.3, there are nowadays strong business cases as well as regulations which emphasize the need for forensic readiness, and show that being forensic ready can be a business enabler and save costs in the long run. Several organizations often encountering cybercrime recognize the benefits which being ready for forensic analysis would bring. They are however unaware of the requirements and how to incorporate controls into their organization to reach and maintain this state. There are no practical guidelines on how to do this either, and current academic literature on the subject is relatively scarce and does not have a holistic viewpoint.

This research aims to aid solve this challenge by providing the so-called *Continuous Forensic Readiness Framework*. This control framework describes how the basic elements, people, processes and technology, can be set up in a way to support performing timely and adequate analysis after a IT incident is detected. Furthermore, the framework supports to maintain this state.

With a control framework we refer to a data structure that organizes and categorizes an organization's internal controls, which are practices and procedures established to create business value and minimize risk.

In the remainder of this chapter, section 1.1 briefly mentions research and practice for additional security measures beyond the prevention controls. In section 1.2 the main goal of this research is elaborated, building upon the earlier observations. Section 1.3 describes in more detail the analyses as are meant in this research, including important drivers for forensic readiness.

1.1 Beyond prevention

Besides prevention techniques, detection and response controls will enhance security and help aim for adequate security measures and efficient mitigation of security incidents [40, 69, 74]. Detection mechanisms are occasionally implemented in the form of e.g. Intrusion Detection Systems (IDS) which detect anomalies within a system and/or network in order to determine a possible IT incident, and have so far received quite some interest from both the scientific and the corporate world resulting in several distinct approaches, as can be found in [11, 44, 63, 66-68, 71, 72]. Fortunately the response aspect has also been the subject of some serious thought and research, especially on the topic of Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs). Attention has risen in the area of business continuity as well, in which high impact IT incidents nowadays receive recognition as being crucial incidents [12, 33].

1.1.1 Still no perfect world

Any adequate response starts with an analysis of the current situation to define the actual problem and determine what has happened, or perhaps even still is happening, on your systems and networks. Once that information is known the most effective and efficient response plan can be chosen. Most organizations however find themselves without proper guidelines for these situations and fail to bring such an investigation to a productive conclusion [69, 97, 103]. Furthermore, when such an investigation is conducted most organizations realize they miss crucial data to accurately determine the root cause and impact of the IT incident, or would have been able to produce a much more efficient and complete investigation if certain information would have been available, or at least available earlier [47, 48]. Understandably, organizations put business process resumption at first place and therefore in response to high impact IT incidents, recovery teams often focus on retrieving data from backups, restoring systems to safe states and performing (security) patches and updates to prevent future instances of the situation. During these operations valuable information with regards to potential analysis may unfortunately be destroyed or rendered useless.

Forensic analysts, such as the KPMG Forensics team as well as the KLPD (Dutch National Police) High Tech Crime Unit, hired to (aid) investigate sophisticated attacks experience this lack of guidelines, data and processes at their clients as well, and it may keep them from being able to perform a complete and/or timely analysis.

1.2 Goal

In order to properly respond to incidents in a timely manner organizations need to be able to quickly and adequately determine what happened within their systems and networks. Also, to provide irrefutable evidence following a thorough forensic analysis as follow up to an IT incident, data needs to be appropriately extracted and safeguarded [37, 88, 117].

The main goal of this research is twofold. First, the research gives organizations handles to be able to have the required information available to

1. perform adequate preliminary analysis directly following the IT incident, and
2. perform adequate forensic analysis following the IT incident.

Adequate analysis in this research means an analysis where the conclusions are delivered with certainty: following the steps in the analysis solid evidence can be provided to come to that conclusion. An adequate forensic analysis means an analysis whereby next to certainty of the results, the collection and processing of the data is done in a forensically sound manner such that it will be accepted in a court of law.

As no (IT) environment is a static one, but rather more like a living organism, acquiring the required state once will not be enough to fulfill the demands in the future. Therefore this research secondly aims to incorporate the *forensic readiness controls* found in the first part into a governance framework, allowing organizations to *maintain* its state of forensic readiness.

1.3 (Forensic) Analysis

As described in the previous section this research is about preparing for two different types of analysis, both coping with the same problems. Seeing as most businesses have business continuity as main goal in case of an incident, numerous actions are performed on systems such as updating operating systems and applications, removing user accounts and changing access rights. As mentioned these actions may interfere with potential evidence trails.

The analyses differ from each other both in time of performing and in depth of research. After an incident, the initial analysis any organization performs is to as fast as possible determine what systems have been compromised and preferably also how, in order to allow them to take an adequate response leading to minimal business interruption and damage.

A more thorough analysis is required in order to completely clean one’s systems, to possibly prosecute attackers as well as to gain a more thorough insight into the situation as required by laws and regulations. It can also be performed out of own interest (for e.g. future situations) and as good business practice. This analysis often overlaps with the preliminary analysis and is aimed to give a complete view of amongst others how the attackers gained access, what systems they compromised, what data they extracted and if they are still inside the network. In fact, if evidence is to be used in a court of law, the preliminary analysis should already be performed in a forensically sound manner.

1.3.1 Compliance

Besides being 'just' an inconvenience, inadequate or missing controls which lead to an inability to perform adequate analysis could have much greater implications [14, 52, 76]. For example consider compliance with regulations such as the Sarbanes-Oxley act in the United States of America and comparable law in the European Union such as the 8th Company Law Directive on The Statutory Audit and the Company Reporting Directives issued by the European Union Council of Ministers.

Much of the attention, discussion and work regarding The Sarbanes-Oxley act, and corresponding European counterparts (sometimes teasingly called the EU SOX) focus on sections 302 and 404 of the act [30]. In short, Section 302 dictates that Chief Executive Officers (CEOs) and Chief Financial Officers (CFOs) must personally certify financial statements and the existence and effective operation of disclosure controls and procedures. Section 404 covers internal controls over financial reporting – the processes in place that are designed to ensure the reliability of the financial report process and the preparation of financial statements [30]. The CEO and CFO must once again personally certify the evaluation of the controls. Furthermore, section 302 requires the external auditor to independently attest to management's assertion on the effectiveness of internal controls, including IT controls, as they relate to financial reporting.

In the U.S., the Securities and Exchange Commission (SEC)'s rules for internal control compliance regarding the Sarbanes-Oxley act are clarified through three objectives [30, 118, 119]:

1. *"Records are maintained in a reasonable detail to accurately and fairly reflect the transactions and dispositions of the assets of the organization.*
2. *There is reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in accordance with generally accepted accounting principles (GAAP), and that receipts and expenditures of the organization are being made only in accordance with authorization of management and directors of the registrant.*
3. *There is reasonable assurance regarding prevention of unauthorized acquisition, use, or disposition of the organization's assets that could have a material effect on the financial statements."*

To comply to these rules organizations require adequate IT controls, and in times of being audited or after having experienced an IT incident, need to be able to prove the implemented controls are sufficient. Forensic readiness can aid in proving the controls taken were sufficiently effective [46, 48, 89].

Recently the *Telecommunicatiewet* [113] in the Netherlands has been revised, to include amongst others a duty for telecommunication providers to report data breaches. The law has significant implications and may lead to at a minimum severe image damage and its resulting financial losses in the case of a security breach [81]. In some exceptional cases, if according to the regulator appropriate security controls were applied, a provider will not have to report the breaches and can thus prevent potential damage [81]. Forensic analysis following a breach may aid in proving appropriate controls were indeed in place.

Furthermore, in the general case of a security breach, organizations have to report to the *Onafhankelijke Post en Telecommunicatie Authoriteit* (OPTA) on what happened, a notice for which the OPTA will not accept merely the notice *"We have been hacked."* [81]. Organizations will thus have to be able to investigate such IT incidents both fast and thorough.

Organizations that have adequate controls, guidelines and processes in place to retrieve required data from their systems and network quickly and efficiently can prove to auditors and regulators that they comply to regulations [30]. Besides the regulatory demands *"…forward-thinking companies and executives are seizing the opportunity and turning compliance into a competitive advantage. Companies that fail to act may pay a heavy price."* [30].

As a side note, working on and thinking about compliance will provide organizations with several other advantages as well, for starters it will enhance overall IT governance [43, 46, 48]. A short overview of compliance drivers, divided into positive and negative drivers, is shown in Table 1.

Table 1: Positive and negative drivers for compliance, adapted from [102] and extended.

Negative drivers	Positive drivers
Reduced risk to huge fines and lawsuits [5, 15, 81] Reduced risk to ruin the brand's reputation [5]	Brings better insight into processes and responsibilities. Processes can thus be optimized which as a result can transform into a competitive or financial advantage. [15, 43, 59] Business effectiveness increased because of the better control [15, 43] Business agility is increased [15, 43] Organizations gain more insight into risks, which can then be tackled [59] Prevent loss of resources and the probability of system breach [43] Contribute to the compliance of other regulatory requirements, such as those for privacy [43]

1.3.2 Business

As one might suspect, almost all drivers for compliance as listed in Table 1 have business implications. Therefore these are certainly 'business reasons' for forensic readiness as well. Besides it possibly being a good investment due to the implications mentioned above, there is however another reason businesses should strive for forensic readiness: investigative costs.

After an IT incident where investigation is required the amount of work to determine what happened is enormous. There are estimates of up to 40 billable hours of forensic identification for merely two hours of intruder time [111]. Considering that most intruders are on your network far longer than that, Mandiant[1] even determined a median of 416 days [75], the potential damage is enormous. Although we have to take into account the fact that the publishers are in some way favored by these numbers and thus the objectivity is not guaranteed, even if these numbers are somewhat exaggerated investigating hacked systems is still a very time consuming task, whereas investigating itself is becoming increasing important.

Ensuring the forensics experts do not waste their time trying to get the relevant data or waiting for mandates and have the necessary data available allows them to faster draw conclusions, preparing for such an investigation can lower these required hours and thus lower costs [111].

1.3.3 Law

Besides complying to laws and regulations, as described in detail in section 1.3.1, there are other aspects of the law to take into account. In certain cases such as e.g. child pornography, large-scale fraud or suspecting of a command & control server (such as with *"Bredolab"* [98, 107]), agencies can show up and claim computers (in some instances requiring a court order), or at a minimum bit-by-bit images of those computers, in order to investigate.

In order to minimize business disruption and also to cooperate smoothly with agencies, it would significantly help to be prepared to be able to supply data fast [97]. Again, (aspects of) forensic readiness can aid an organization in doing so [97].

1.4 Document structure

Chapter 2 introduces the research and methodology for this thesis. From chapter 3 and onwards this document is divided into five main parts. The first four correspond with the phases of this research namely Problem Investigation, Solution Design, Design Validation, Solution Evaluation. These phases are elaborated on in chapter 2.

In part 1, Problem Investigation, a literature study is performed to gain further insight into the topic. Experts were interviewed and the results of the literature studies and these interviews were analyzed, resulting in a list of aspects and demands for the continuous forensic readiness framework.

Part 2, Solution Design, uses the results from the first section to set up a continuous forensic readiness framework. Current available governance framework are briefly discussed, and approaches on how to set up the new framework discussed. An approach is chosen and finally the framework itself is discussed.

[1] An incident response organization with more than 30% of the Fortune 100 as its clients. http://www.mandiant.com

Part 3, Design Validation, describes the validation of the proposed framework using three different methods. First of all the requirements as identified earlier were mapped to the framework to check if all requirements are met. Secondly the framework was discussed with experts. Thirdly the framework was applied to a case, the University of Twente (UT), after which its Computer Emergency Response Team (CERT) was interviewed to check for usability and suitability of the framework for the University of Twente.

Part 4, Solution Evaluation, describes the evaluation of the entire process as well as the resulting framework.

In part 5 the final conclusion is stated and possible future research identified.

2 Research

This chapter introduces the research, and elaborates upon the approach used. This chapter contains the following information regarding the research:

- Contribution (section 2.1), both
  - Practical (section 2.1.1), and
  - Theoretical (section 2.1.2)
- Scoping (section 2.2)
- Research questions (section 2.3)
- Methodology (section 2.4)

2.1 Contribution

This section describes the contribution of this research from a practical and a theoretical viewpoint, and elaborate on its relevance.

2.1.1 Practical

Organizations are currently not ready to perform adequate analyses following an IT incident at all times, let alone in a forensically sound manner. This research provides them with a better insight and instructions to gain and maintain a state wherein they are able to do so. It delivers the necessary aspects to reach this state, which can subsequently be checked and measured by organizations to assess their current situation. Furthermore, the governance framework provided incorporates these aspects and provides handles on how to become and stay ready for forensic analysis. The resulting governance framework and process model provides organizations with useable, concrete actions to achieve and maintain a state of continuous forensic readiness.

2.1.2 Theoretical

Current academic literature on forensic readiness is relatively scarce, not all in agreement, focus on different aspects and fail to provide a complete view. Furthermore, research that does describe how to *become* (partly) forensic ready does not describe how to *maintain* this state. This research aims to fill the gaps in existing knowledge between both areas by providing a control framework.

2.1.3 Relevance

The research is guided by up-to-date information on cyber security threats, regulations and forensic analysis practices. The relevance of this project is therefore in significant extension of the existing knowledge base. We can see the desire of an organization to become and stay forensic ready as a compliance issue. Generally governance models like CobiT and ITIL describe *what* should be implemented in terms of compliance, but do not state *how* this should translate into real measures: this is left for the business to implement. In the case of forensic readiness neither what you have to do to be compliant nor how this should be done are conclusively known nor generally accepted. There is no governance or process model which handles forensic readiness in a structural way through governing all layers and aspects of the organization, including safeguarding for changing environments. This research fills these gaps. Figure 1 graphically depicts this as follows: The blue blocks are currently existing, when focusing on the governance frameworks the currently available frameworks are meant. The red blocks are the contribution of this research, namely a new governance framework to fulfill the need for forensic readiness, as well as a process model which is the detailed implementation of this framework.

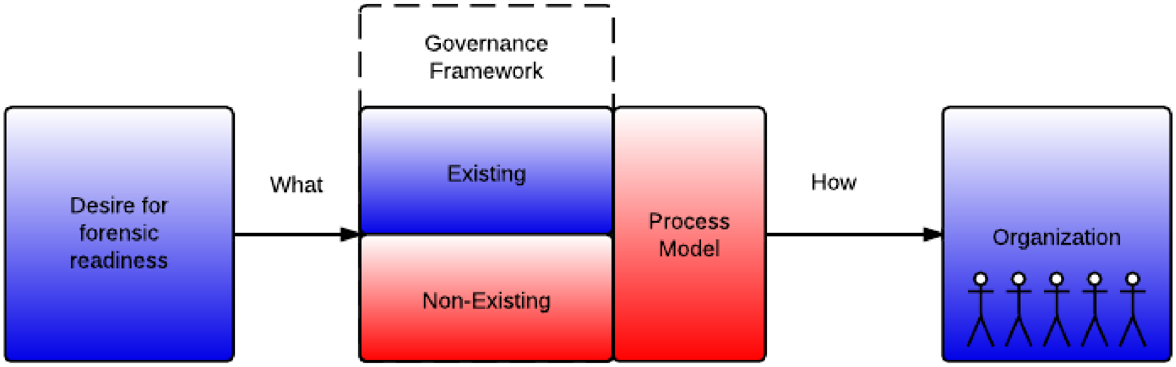


Figure 1: Research relevance

2.2 Scope

Despite the inevitability of being hacked, preventive measures still keep a lot of attackers out of networks and systems. And even though a sophisticated security program consists of a coherent set of preventive, detective and responsive controls, it can be argued that keeping out as much attackers as early as possible is the best starting point for a defensive mechanism. Preparing for a hack and more advanced security measures, such as preparing for a forensic analysis afterwards, are aspects of a highly developed security program.

This research thus has its focus on organizations with a mature IT environment, wherein security is already addressed at a certain level of sophistication and which is capable of detecting possible breaches. Most likely these environments can be found in bigger companies, multinationals, academia, etc. The research explicitly does not limit itself to organizations who perform the forensic analyses themselves: becoming forensically ready can be performed by and has benefits for most organizations, not just those that perform their own analyses. Although the resulting framework may to some degree be suited for less mature IT environments and perhaps even starting companies, these are outside the scope of this research.

Considering the goal of this research, how to *stay* forensic ready, current governance models are studied. The most popular existing models (commonly used in practice and/or in literature) are studied, of which the results are discussed in chapter 9.

2.3 Questions

As the overall goal of this research is to design a framework on continuous forensic readiness, the main research question is a *design* question (as explained later in section 2.4) and can be formulated as follows:

RQ: How to construct a framework on continuous forensic readiness such that organizations are capable to (let) perform adequate analyses following an IT incident?

The following sub questions will help in answering the main research question:

SQ 1. What do forensic analysts require for performing an adequate analysis?
SQ 2. Taken into account the requirements identified in SQ1, what additional demands do organizations impose on a continuous forensic readiness framework?
SQ 3. What forensic readiness models are currently available and to what extent do they help organizations to become continuously forensic ready?
SQ 4. What leading governance models are currently available and how are they suited for forensic readiness?
SQ 5. How do we fill the gap between the requirements/demands identified in SQ1/SQ2 and the solutions offered as identified in SQ3/SQ4?
SQ 6. Does the proposed solution in SQ5 fulfill the needs identified in SQ1/SQ2?

The circular nature and supportive function of these questions is depicted in Figure 2.

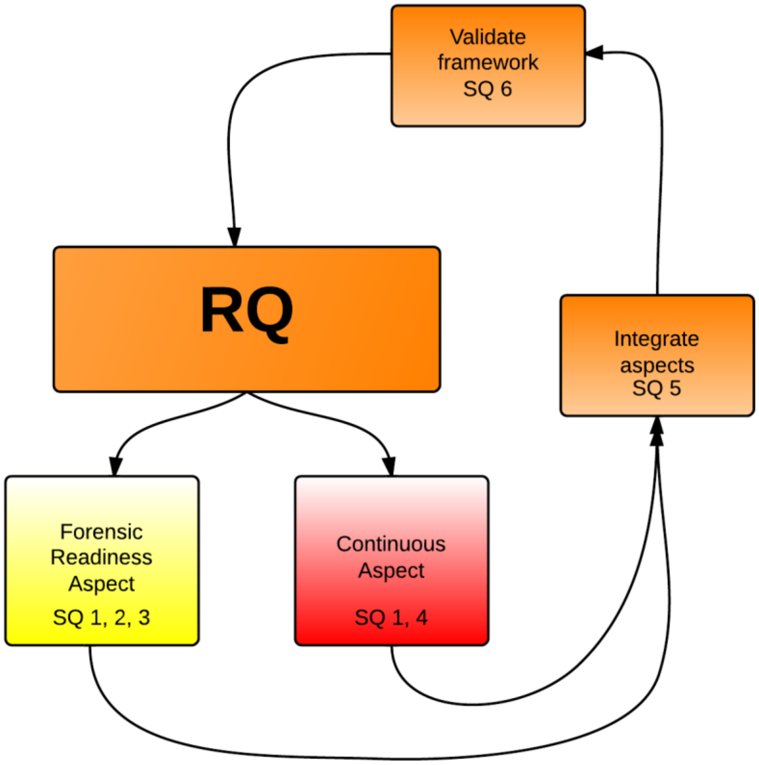

Validate framework SQ 6
RQ
Integrate aspects SQ 5
Forensic Readiness Aspect SQ 1, 2, 3
Continuous Aspect SQ 1, 4

Figure 2: Research questions

2.4 Methodology

Research can be classified into several categories. As the goal of this research is to produce a framework, it can be classified as a design-oriented research. The most appropriate methodology for this research is *Design Science* as described by Hevner et al [54] and later refined by Wieringa [131]. In this research the refined version is leading.

Wieringa notes that design and research are closely related activities. In design science problems can be divided between *practical* problems and *knowledge* problems. Practical problems call for a change of the world so that it better agrees with some stakeholders goals. Knowledge problems by contrast do not call for a change of the world but for a change of our knowledge about the world [131].

According to Wieringa, a design science project is a set of nested problems with at the top level a *practical* problem. This research's main question is indeed a practical problem, namely on designing a framework. Furthermore, Wieringa notes that practical problems can often be divided into sub problems of both knowledge and practical nature. This also shows at how the main research question (RQ) is divided in six sub questions (SQs). These are different kind of questions themselves and are categorized in Table 2.

Table 2: Sub questions by type of problems

Sub question	Type
1	Knowledge
2	Knowledge
3	Knowledge
4	Knowledge
5	Practical
6	Knowledge

Furthermore, Wieringa describes how each investigation is either problem-driven, goal-driven, solution-driven or impact-driven. In a problem-driven investigation stakeholders experience problems that need to be diagnosed before solving them. In goal-driven investigations there is a situation in which there may be no problem experienced by all stakeholders as of now, but where there are nevertheless reasons to change the world in agreement with some goals. In a solution-driven investigation technology is in search of problems that can be solved with it. Finally, impact-driven investigation (also called evaluation research) focuses on the outcome of past actions rather than preparing for the design of future solutions.

Due to e.g. new regulations and insights with regards to forensic readiness, as described in chapter 1, this research can be described as goal-driven. Following Wieringa, the research includes stakeholder goals to be achieved as main design principle to take into account.

2.4.1 Design Science Guidelines

According to Hevner et al [54], an effective design science research should follow seven guidelines. Wieringa [131] has supported four of these and elaborated on three. Concluding his paper, Wieringa gives eight guidelines for design science. These are used as handles for this research and are listed in Table 3.

Table 3: Design Science Guidelines

Guideline	Description
1	Distinguish practical problems from knowledge questions
2	Solve practical problems by the regulative cycle (see Figure 3)
3	Distinguish problem investigation from design validation
4	Problem investigation may be problem-driven, solution-driven, goal-driven, or impact-driven
5	When designing a solution, maintain the design argument
6	When validating a design, consider trade-offs and sensitivity
7	When validating a design, aim to incorporate conditions of practice
8	When solving a knowledge question in the regulative cycle by means of research, no research method is banned.

2.4.2 Design Science Phases

According to guideline 2 practical problems should be solved by the regulative cycle. This cycle is given in Figure 3. The cycle actually consists of five stages, namely “Problem investigation”, “Solution Design”, “Design Validation”, “Solution Implementation” and “Implementation validation”. The first and the last stage are essentially the same state (as you can see in Figure 3), but are different in time. The former stage is at commencement of the design research, whereas the latter is after (every) implementation of the designed solution: In practice, during a practical problem solving process the regulative cycle is performed iteratively with designers start matching an incompletely specified solution to an incompletely understood problem and then jointly elaborate their solution specification and problem understanding [131].

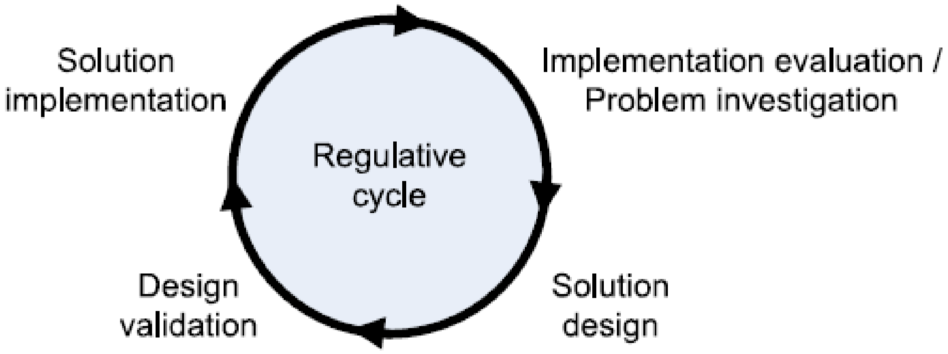


Figure 3: The regulative cycle, adapted from [131]

As Wieringa mentions it is often infeasible to perform the entire cycle within one research, let alone one Master thesis’ research, and this research is no different [132]. In this research no actual implementation is performed, therefore the stage “Solution Implementation” is absent. Considering the proposed solution is evaluated though, “Implementation Evaluation” is replaced by “Solution Evaluation”. All stages for this research are shown in Figure 4.

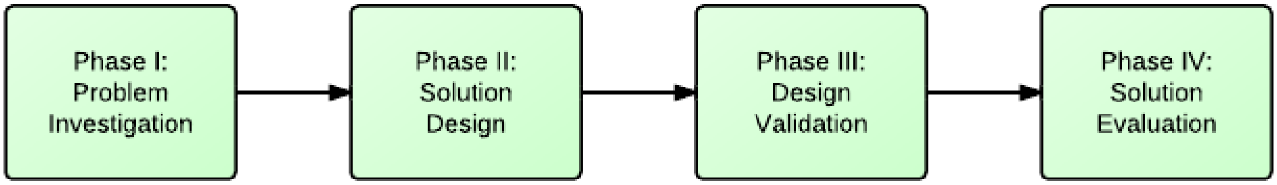

Phase I: Problem Investigation
Phase II: Solution Design
Phase III: Design Validation
Phase IV: Solution Evaluation

Figure 4: Research model overview

The next sections briefly describe what activities were performed in each phase.

Phase I: Problem Investigation

1. Consult literature on incident response, forensic analysis and forensic readiness.
2. Interview forensic experts on forensic analysis, forensic readiness, experience from practice.
3. Extract needs for forensic readiness from interviews and literature.
4. Extract demands for forensic readiness framework from interviews and literature.
5. Validate identified needs for forensic readiness.

Phase II: Solution Design

6. Consult existing governance models for suitability with forensic readiness.
7. Extend, adapt or create a new governance model to include forensic readiness.

Phase III: Design Validation

8. Check whether resulting framework from 7 matches the requirements as found in 4.
9. Validate the framework with experts.
10. Implement framework for CERT-UT.
11. Check usability of the framework for CERT-UT.

Phase IV: Solution Evaluation

12. Evaluate the process of setting up the framework.
13. Evaluate the framework for generic usage, beyond the CERT-UT.

A detailed overview of the research model is given in Appendix A: Detailed Research Model.

2.5 Information sources

This section briefly describes the information sources that were used during the research in order to answer the research question and sub questions.

2.5.1 Literature review

The problem analysis phase is dedicated to gathering, assessing and synthesizing knowledge through a substantial literature review. As Wieringa mentions a good design science research should drawn upon an existing knowledge base [131]. Therefore answers to the corresponding knowledge questions are partly answered by literature.

2.5.2 Interviews

A series of semi-structured interviews were held to extract information from experts. Face-to-face conversations helped to gain greater detail and context, and to provide a more solid base for a future framework.

Forensic experts

Forensic experts from different organizations were interviewed to extract information on how forensic analyses are performed. Knowledge on the forensic analysis process helped in determining requirements for such an analysis, which could thus be translated to forensic readiness demands. Furthermore, another group of experts was used to validate the resulting framework.

The forensic experts were sought in leading organizations on the area of forensic analysis, both national and worldwide. For this research experts from amongst others the Dutch National Forensic Institute (NFI), the KLPD High Tech Crime Unit, Fox-IT and members of the ‘big four’ (KPMG, Deloitte, PwC and Ernst & Young) were contacted. The experts interviewed are described in chapter 5.

Governance experts

Experts on governance from different organizations were interviewed in order to get a feeling with the currently most important governance models, as well as the main principles of these which could serve as a basis for the Continuous Forensic Readiness Framework.

Implementers

In order to help validate the framework, a variety of organizations was visited. Security managers and (internal) audit employees were interviewed to get their view on the framework, its usability and applicability. Furthermore, KPMG employees often encountering (control) frameworks were interviewed for the same purpose.

2.5.3 Case study

The University of Twente has its own CERT, namely CERT-UT, which collaborates intensively with SURFcert, the CERT of SURFNet[2]. The CERT-UT has agreed to act as a tester, or a ‘light version’ of a case study for this research. Considering incident response is a main responsibility of any CERT, the members of such teams are often the first at the scene and the actual responders. This makes gathering data in a forensically sound manner a practice which is, or should be, performed by them.

The resulting framework was not directly implemented, but they cooperated in the research steps to see if and how this could be incorporated in their organization. For this purpose the University of

[2] SURFnet helps researchers, professors and students work together with ICT. http://www.surfnet.nl

Twente acted as a client for the framework, providing input such as their current situation and requirements. As a client they also aided in validating the framework.

2.6 Summary

In this chapter the research methodology, different stages of the research, the actions taken and information sources used for this research have been described. The research is described in four different parts: *Problem Investigation, Solution Design, Design Validation* and *Solution Evaluation*. In the next part of this thesis *Problem Investigation* will be elaborated upon.

I – Problem Investigation

3 Introduction – Problem Investigation

This part of the thesis discusses the first stage in this research. It investigates the core problems, current literature and extracts requirements for a possible solution. It is the first of four phases in the actual research, as shown in Figure 5.

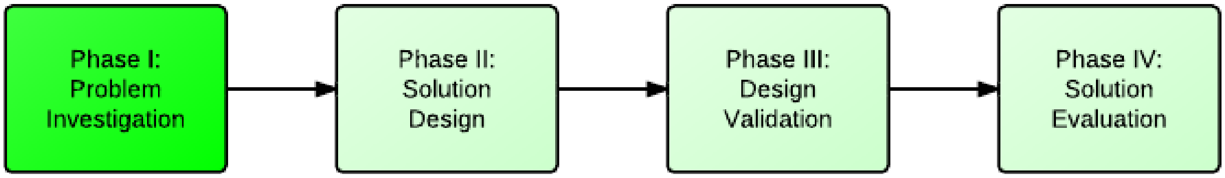

Phase I: Problem Investigation
Phase II: Solution Design
Phase III: Design Validation
Phase IV: Solution Evaluation

Figure 5: Phase I – Problem Investigation

In order to get a good feeling for the field within which this research was performed, as well as to identify relevant aspects with regards to forensic readiness, an extensive literature review was performed. Chapter 4 gives a concise overview of the relevant scientific literature with regards to this research, and elaborates on the main trends and realizations from the fields of incident response, forensic analysis and forensic readiness. Next to a literature study, forensic experts were interviewed. Chapter 5 describes the forensic analysis expert interviews. Furthermore, organizational demands for the framework extracted from interviews are described as well. Resulting from the literature study and interviews, in chapter 6 the list of applicable controls and their relevance for the Continuous Forensic Readiness Framework is derived and validated. This part of the thesis is summarized in chapter 7.

4 Background

In order to answer SQ 1, *"What do forensic analysts require for performing an adequate analysis?"* ,one of the actions performed was an extensive literature study. By searching for relevant keywords on scientific databases *Web of Science* and *Scopus* top cited articles were selected for initial review on the topics of *Incident Response, Forensic Analysis* and *Forensic Readiness.* By cited reference searching the list of relevant literature was extended to 151 articles, selected based on their abstract. These articles were read and analyzed for aspects which could be relevant for achieving a state of forensic readiness.

The following sections 4.1, 4.2 and 4.3 provide a concise overview of the three topics. For each of these topics the trends and notions from the literature analyzed are described. Furthermore, the main aspects relating to success according to the literature are given. Please note that due to the unpreventable variety of wording different authors use in their publications, the aspects identified in the coming sections are named by myself. Aspects which had no fundamental difference besides naming are combined, otherwise a different aspect was identified and added to the list. For a more elaborate overview of the literature analyzed for each topic, please see my earlier publication on this topic [31]. Section 4.4 provides the reader with additional relevant definitions used in this research.

4.1 Incident response

Seeing as (forensic) analysis as defined in this thesis is performed with a least a presumption that something unwanted occurred within the organization, it seems trivial to include incident response as a topic which has coherence with forensic readiness: Incident response procedures are followed in such cases. In this section, incident response is described by three different important aspects: *Business Continuity Management*, wherein incident response finds its origin, *IT incident response* and *Computer Security Incident Response Teams*.

4.1.1 Business Continuity Management

Responding to devastating incidents was once the field of ad hoc solutions, with management deciding right there and then on what to do. Following the saying *"To be prepared is half the victory"*, the field of Business Continuity Management (BCM) emerged to prepare organizations for such situations. Generally, the goal of BCM is to reduce risk posed by service disruptions. Looking at the academic literature, the field has received considerably more attention after the tragedy of the terrorist attack on the Twin Towers, at the 11th of September 2011, where next to the thousands of lives lost also dozens of organizations went bankrupt.

BCM originally focuses on disasters causing a disruption in your business process. A Business Continuity Plan (BCP) is created to determine how an organization should continue operations under adverse conditions. These conditions range from local events such as building fires, theft and vandalism, to regional incidents like earthquakes and floods as well as (inter)national scenarios such as pandemic illnesses. Any event that could impact operations should be considered for such plans.

These plans thus identify potential impacts that threaten an organization and provide a framework for building resilience and the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activities. There have been numerous publications on this topic. For details please see the earlier publication [31].

Throughout the BCM literature, the main focus is on continuity of the business processes. Whereas this focus has not changed, the possible scenarios to take into account while developing such a plan have. The field of BCM gradually moved from anticipating merely environmental disasters to include (terrorist) attacks, but also lower impact incidents with higher frequencies. With the increase in cybercrime incidents, Brettle [12] published a short editorial explicitly adding IT security breaches to the scenarios to take into account. Literature on responses specifically for those incidents is described in the next paragraph.

The main aspects for effective BCM, as identified in the publications on BCM studied [10, 12, 13, 76, 85, 93, 130, 134], are shown in Table 4.

Table 4: Main aspects Business Continuity Management literature

Aspect	Description	% of papers mentioned
Risk analysis	A thorough risk analysis should be performed to determine which elements of the organization are most important, to develop an adequate plan accordingly.	88%
Test plan	The plan has to be tested up front and regularly.	75%
Team	A skilled and knowledgeable team has to be available to execute the BCM plan.	63%
Policies & Procedures	Policies have to be defined regarding all BCM aspects, and procedures have to be developed correspondingly.	63%
Determine goals up front	Goals should be defined such that the plan can be tested and trained for efficiency and adequacy.	63%
Redundant hardware	Redundant hardware has to be available for the most critical system to ensure maximum response and minimum business disruption.	63%

4.1.2 IT Incident Response

The rising number of IT incidents caused the need to be able to properly respond to grow. There have been several leading publications on this topic, including standards from the International Organization for Standardizations (ISO) and U.S. National Institute of Standards and Technology (NIST).

Publications in the field of IT incident response are not in agreement on the exact interpretation of the response process, number, naming and content of stages/phases within this process nor the precise actions to take (or when to perform these). However, some specific aspects mentioned can count on consensus or are supported by most of them. While creating such an incident response plan is an act of preparation in itself, most frameworks also identify the need to add preparation as a phase in these plans. In such a phase essential matters can be taken care of before an incidents occurs, which will aid in performing the actual response during an incident. Furthermore, in the papers discussed (forensic) analysis is mentioned albeit not always in the same phase, using the same preconditions or goals, nor discussed in depth. Despite these differences it is clear that forensic analysis is deemed of interest within the field of incident response. An extensive overview of IT incident response literature and their models as analyzed for this thesis is described in [31].

The main aspects for an effective IT Incident Response, as identified in the 10 publications on IT incident response studied, are shown in Table 5.

Table 5: Main aspects IT Incident Response literature

Aspect	Description	% of papers mentioned
Team	The team should be multidisciplinary, thus besides technical expertise include delegates from e.g. management, HR and legal departments.	70%
Policies & procedures	Policies have to be defined regarding all BCM aspects, including IT incident responses, and procedures have to be developed correspondingly.	70%
Prepare standard documents	Certain acts, which include filing reports or requests will have to be done in each investigation, which is always the start of incident response. Prepare such standard documents to avoid forgetting important aspects and saving time.	60%
Document actions taken	Document all actions taken during response, not just for documentation reasons as before but also to be able to reproduce the result, if required for evidence in a court of law.	60%
Toolkit	Tools are required for any type of response, ensure these are available on a secure medium.	60%
Logs	Logs are the most essential aspect and source of information for determining what happened. Ensure the proper actions are logged.	60%

4.1.3 Computer Security Incident Response Team (CSIRT)

One top aspect identified both in BCM literature as well as IT Incident Response literature is the team performing the action. As the names imply, Computer Security Incident Response Teams (CSIRTs, also known as Computer Emergency Response Teams, CERTs) are teams dedicated to one task: computer incident response. As the team performing the response was deemed important, a limited set of 3 leading papers regarding these specific teams were analyzed as well. These articles describe a variety of possible structures for such teams, depending on the organization and its needs. Furthermore, although incident handling is the core task of any CSIRT there are nowadays many other services such a team may offer, depending on their structure, time and budgets. Publications thereby note that, taking appropriate budgeting and staffing into account, CSIRTs have room to provide additional services. A more detailed overview of the CSIRT literature studied is given in [31].

The main aspect identified in CSIRT literature, besides the important note regarding possible additional services above, regards the team's members. Not only does the team require a multidisciplinary staffing, also selecting who in (or outside of) the organization is part of the CSIRT is of great influence. The team should not (necessarily) overlap with the IT team doing maintenance and configuration. In fact a team with too much overlap may struggle during incident response.

4.2 Forensic Analysis

Computer forensics is a part of the forensic sciences. The notion of computer forensics initially knew two different supported views: Legal specialists commonly refer to only the analysis, instead of including the collection, of data. By contrast computer scientists define computer forensics as the validity of tools and techniques applied against computer networks, systems, peripherals, software, data and/or users to identify actors, actions and/or states of interest.

Peisert et al [92] borrow two more complete definitions: By Steve Hailey of the Cyber Security Institute[3], *"The preservation, identification, extraction, interpretation and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found."*. The second originates from the first Digital Forensics Research Workshop[4] held in 2001: *"The use of scientifically derived and proven methods towards the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions shown to be disruptive to planned operations."*

Both definitions show a link between the technical analysis and its final goal, which is to offer indisputable conclusions which may be used as evidence in a court of law.

A total of 37 papers regarding forensic analysis and possible methods in this respect were analyzed. From this analysis it became clear that despite the general goal the models have in mind, namely to provide indisputable evidence applicable in a court of law, the proposed models for the process of forensic analysis are not in agreement. Besides different naming, which is obviously no fundamental difference, models are not analogous regarding the number of phases as is elaborated upon in [31]. Furthermore, for the detailed reader my earlier publication [31] will show that for some models the entire process, phase and what actions (not) to perform in what phase differ as well. Although the general goal is a commonly accepted one, models have different viewpoints, different level of detail and occasionally disagree on specific aspects. This is likely the result of forensic analysis being a broad, multidisciplinary process with a lot of different professions being involved.

The main aspects for an effective forensic analysis, as identified in the 37 publications on forensic analysis studied, are shown in Table 6.

Table 6: Main aspects Forensic Analysis literature

Aspect	Description	% of papers mentioned
Toolkit	Tools are required for any type of response, including forensic analysis.	68%

[3] http://www.csisite.net/
[4] http://www.dfrws.org/

Legal	The plan has to be tested against legislative demands.	57%
Chain of custody	A chain of custody has to be kept to raise the value of evidence in a court of law.	57%
Maintain integrity of original data	Restoration or analysis should not violate the integrity of the original data when performing a forensic analysis.	57%

4.3 Forensic Readiness

As we've similarly seen with the emergency of BCM in 4.1.1, a need arose to prepare for possible unwanted situations an organization may encounter. Some of the publications regarding *Forensic Analysis* have hinted towards preparing for analysis to ensure the process will be able to be executed more efficiently and successfully. There have been limited publications on *Forensic Readiness*: a total of 15 publications were found and analyzed. From these publications 7 provide either a proactive approach as part of their forensic analysis, or are a (process) model for forensic readiness as meant in this research. The other publications 8 discuss relevant viewpoints and aspects of forensic readiness.

Whereas Grobler et al [47] advocate forensic readiness as an aspect of information security best practice, literature seems to be in disagreement on how to achieve a state of forensic readiness. As is the case with forensic analysis, different models prescribe different steps and other most notable aspects of forensic readiness. The one (process) model by Rowlingson [101] available for forensic readiness is limited with regards to the aspects an organization has to take into account, compared to those identified in the earlier literature described. Furthermore, the model does not describe how to maintain the state it identifies as forensically ready. The main aspects for an effective forensic analysis, as identified in the 15 publications on forensic readiness studied, are shown in Table 7.

Table 7: Main aspects Forensic Readiness literature

Aspect	Description	% of papers mentioned
Policies & Procedures	Policies have to be defined regarding all forensic aspects, and procedures have to be developed correspondingly, in order to embed forensic readiness into the organization.	67%
Legal	The plan has to be tested against legislative demands, ensuring that resulting evidence adheres to required legislation.	67%
Training	The team should keep up to date with threats and tools, and receive regular training.	60%
Determine interesting data up front	Following the risk analysis, determine where in your IT landscape the most interesting data with regards to analysis can be found.	60%
Risk analysis	A thorough risk analysis should be performed to determine which elements of the organization are most important, to develop an adequate plan accordingly.	60%

4.3.1 Digital Evidence

The main result any forensic analyst is looking for is indisputable evidence, collected from the near infinite pool of data which computers and network(s) can nowadays become. Indisputable digital evidence in case of an IT incident is the result an organization is aiming for when attempting to becoming forensic ready. Whereas aspects regarding the process of incident response, forensic analysis and preparing therefore have been identified in the previous sections, characteristics of the ultimate end goal have not yet been explicitly mentioned.

Not a lot can be noted about digital evidence which does not apply to 'regular' evidence in a normal court of law. Digital evidence will, just as regular evidence, need to be indisputable *'enough*' to convince a judge and/or jury (depending on your legislation) of its correctness. In general, there are some basic principles regarding digital evidence which all forensic literature seems to agree upon [126]:

1. Acquire the evidence without altering or damaging the original;
2. Authenticate the recovered evidence as being identical to the originally seized data;
3. Analyze the data without modifying it.

4.4 Definitions

This section provides a definition for two main elements in the remainder of this thesis, which have so far not been explicitly defined: *Governance* and *Management*.

4.4.1 Governance

In literature several types of governance are defined. Dictionaries mention the following:

Governance (noun)

> **1**. The persons (or committees or departments etc.) who make up a body for the purpose of administering something; "the governance of an association is responsible to its members". [95]
> **2**. The act of governing; exercising authority. [95]
> **3**. Exercise of authority; control; government; arrangement [128].

The definitions above, albeit abstract, show that governance is on how control is arranged within an organization. Seeing as this is exactly how governance is intended in this research, the clear and concise definition as provided by Smits et al [104] is leading in this thesis:

"Governance: The arrangement of the control"

4.4.2 Difference between governance and management

An important issue to recognize is that governance is not the same as management. In short, within a hierarchy management deals with responsibilities and authority, direct with or carry on business or affairs. Governance on the other hand is about ensuring the right mechanisms are in place which *enable* one to manage, ensuring the organization can be run or managed *well*. In the Cobit 5 framework [61] this is described as follows:

“Governance ensures that enterprise objectives are achieved by evaluating stakeholder needs, conditions and options; setting direction through prioritisation and decision making; and monitoring performance, compliance and progress against agreed-on direction and objectives.

Management plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives”

4.5 Summary

This chapter has provided the reader with a concise background, as a minimal required knowledge for the remainder of this thesis. Literature on Incident Response, Forensic Analysis and Forensic Readiness have been described, and main trends and top aspects identified in those fields have been mentioned.

Concluding, a forensic analysis is or should be part of incident response (procedures), where the team performing the incident is likely to be involved. To what matter they are involved depends on decisions made when composing the team and describing its role in the organization. Forensic analysis models available are not in exact agreement regarding required aspects and their importance, but they all serve the same goal and have several similarities. Current models for forensic readiness are scarce and those available are limited in their applicability and scope. Furthermore, none of the currently available models provides the reader handles on how to become and stay forensic ready.

All literature combined provided a list of 42 relevant aspects for forensic readiness.

5 Expert interviews

Whereas chapter 4 describes the literature study performed to aid in answering SQ 1, *"What do forensic analysts require for performing an adequate analysis?"*, this chapter describes the second step for answering SQ 1. Semi-structured interviews were conducted with experts on the subject of forensic analysis. The following sections describe the goals and questions for the interviews, the people interviewed and the analysis performed afterwards.

5.1 Goals and questions

The goals of the interviews with forensic experts were the following:

- Determine how a forensic analysis is performed, including concrete requirements for that process;
- Determine current best practices in the field for forensic analysis;
- Determine current best practices in the field for becoming forensically ready;
- Determine stakeholders involved in these processes;
- Determine business demands encountered for proactive forensic actions.

These goals served as the basis for the questions asked during the interviews. After initial talks with a forensic expert at KPMG about the problems often facing analysis, and the thorough literature review described in chapter 4 the questions were prepared. The list of questions is available in Appendix F: Interviews.

5.2 People interviewed

The people interviewed were selected based on their profession and experience within the field. A variety of organizations contributed to this first part of the research, with the average working experience of the interviewed analysts being 9 years.

Meetings of an hour were scheduled with the experts, wherein the context was outlined and then the prepared questions were discussed. An overview of the interviews is shown in Table 8.

Table 8: Forensic analysts group 1 interviewed

#	Date	Organization	Job title	Years of experience
1	07/05/2012	KLPD High Tech Crime Unit (HTCU)	Projectleader, Digital Specialist	18
2	12/06/2012	Nationaal Forensisch Instituut (NFI)	Data Analysis Researcher	6
3	12/06/2012	NFI	Data Analysis Researcher	4
4	22/06/2012	Fox-IT	Senior Forensic Analyst	13
5	06/08/2012	National Cyber Security Centre (NCSC)	Senior Security Specialist	12
6	06/08/2012	NCSC	Security Specialist	8

7	06/08/2012	NCSC	Security Specialist	4

5.3 Analysis

The interviews were recorded – if allowed by the interviewed person. Extensive notes were taken during the interviews as well. The answers to questions were processed afterwards. Although questions had been prepared, not all of these were explicitly asked due to many of the interviewed persons unknowingly answered questions while talking about their own experiences and best practices. Considering how these semi-structured interviews were conducted, the explicit answers are not incorporated in this document. It was agreed with each interviewed person to send them a short report of the interview such that they could check for factual accuracy.

5.3.1 Forensic readiness aspects

One of the goals of the interviews was to determine relevant aspects for forensic readiness. This was done in steps, first determining the forensic analysis process and its specific requirements, then distilling these into aspects one can prepare for (in the context of forensic readiness). Following the literature review described in chapter 4 an initial list was available, however this list was not shown or mentioned to the experts to avoid influencing them.

During the interview, if certain aspects mentioned by the interviewed person were unclear or ambiguous, an explicit definition or explanation was asked. While processing the answers, the same methodology was used as when processing literature: if an aspect mentioned had no fundamental difference to an existing aspect other than naming, they were denoted as the same. Otherwise, a new aspect was added to the list.

The main relevant aspects for forensic readiness identified in the interviews with the forensic experts are shown in Table 9.

Table 9: Main aspects from interviews

Aspect	Description	Mentioned in % of interviews
Chain of custody	In order to ensure evidence stands up in court, a thorough chain of custody is vital. A chain of custody is a chronological documentation showing the seizure, custody, control, transfer, analysis and disposition.	100%
Logs	Logs are the most essential aspect and source of information for determining what happened.	100%
Team	The team should be multidisciplinary, thus besides technical expertise include delegates from e.g. management, HR and legal departments.	71%
Legal	Any plan for forensic readiness should be tested for adequacy with regards to legal demands.	71%
Situational awareness	Organization have to be aware of their IT landscape to be able to develop an efficient plan. This will also greatly aid an investigator during	71%

	an analysis.	
Bit by bit copy	To ensure all potential evidence is captured, including those in hidden/deleted volumes or 'corrupt' sections of the system, a bit-by-bit copy is required.	71%
Hashing	Hashing has several uses, most importantly to provide proof of integrity after creating copies: By creating a hash of the original and then comparing it to the copy, its integrity can be proven.	71%
Maintain integrity of original data	Restoration or analysis should not violate the integrity of the original data.	71%

5.3.2 Relevant stakeholders

Some of the literature, especially publications on incident response and a limited number on forensic analysis, discuss different stakeholders to be involved during such a process. In the interviews relevant stakeholders with regards to forensic analysis and forensic readiness were identified. These stakeholders as identified are listed in Table 10.

Table 10: Stakeholders identified by interviews

Name	Description
CSIRT	Performs the initial incident response, where a lot of forensic (preparatory) work should be done.
Helpdesk employees	Often receive first notice of a potential incident, and should inform person reporting the incident on what to do.
Business owners	Achieving forensic readiness will, depending on the implementation, impose some restrictions on availability right after an incident as well as possible performance constraints. Buy-in from this group is often required to perform an analysis efficiently.
Top management	Accountable for all daily operations of an organization. Furthermore, their support will significantly aid analyses with getting things done.
Head of IT department	Achieving forensic readiness will, depending on the implementation and current situation, impose technical adjustments to the infrastructure and systems, for which the head of IT department is responsible.
Legal department	Besides helping to determine whether the resulting evidence with proposed adjustments will lead to acceptable evidence in a court of law, the legal department will have to check current contracts with employees, customers and/or suppliers for clauses which may or may not interfere with the collection of data for forensic analysis.
Internal audit	Internal audit can help to periodically verify whether the forensic readiness components proposed are adequately implemented.
Employees	Employees will need to be informed with basic forensic rules and how to act in case of a potential incident.

5.3.3 Organizational demands

The interviewed persons for this part of the research were all experts on forensic analysis. In their profession they have encountered numerous organization struggling with forensic analysis, partly due to being unprepared. One of the goals of the interviews was to determine business demands with regards to proactive forensic activities, e.g. preparing for forensic analysis, the experts had encountered in their professional career. Three main reasons were agreed upon by our experts, for which we also find support in literature previously studied. These are:

1. To minimally interrupt business [79];
2. To minimize the costs of forensics on incident response [79];
3. Ensure investigations are cost efficient [46, 111].

University of Twente's demands

The Universty of Twente agreed to act as a case study for this research. Their main drivers, organizational characteristics and the case itself will be described in more detail in chapter 17. For now it suffices to note that besides the forensic experts, interviews were also conducted with employees of the University of Twente. The list of interviews is shown in Table 11.

Table 11: Interviews at the University of Twente

#	Date	Job title
1	06/07/2012	Security Manager, CERT-UT officer and team lead
2	30/08/2012	Internal IT Auditor

During these interviews it became clear that the CERT-UT currently has a limited role, with a main focus on continuity in incident responses. Obviously, this is often the case for any CERT. As we saw in chapter 4, the main purpose of a CERT is incident handling which due to business demands often comes down to returning to normal operation as soon as possible. However, as was noted additional services may be offered by CERTs, and in 1.3 several reasons for organizations to pursue forensic readiness are given. In line with this reasoning, the CERT-UT indicated they are interested to see if and how the University of Twente can incorporate forensic readiness practices into their organization and incident response. However, in order for the University of Twente to actually implement such a framework, the employees interviewed made it clear the framework would have to take into account the following three demands:

Demand 1: Business continuity remains a main issue, thus forensic analysis should cost as little as time as possible.
Demand 2: Due to limited budgets, the monetary costs for investigations should be limited.
Demand 3: The response should be in proportion: Analysis should have a decent chance of leading to a successful prosecution or otherwise satisfactory result.

These demands correspond well with the demands our forensic experts generally encountered, as described in section 5.3.3.

6 Forensic Readiness Requirements

In this chapter the requirements to achieve forensic readiness are described. Section 6.1 describes how the requirements as identified by literature and experts were validated. Section 6.2 elaborates on the resulting aspects which form the basis for the Continuous Forensic Readiness Framework.

6.1 Validation of aspects

The forensic readiness requirements are interpreted as the aspects identified for the relevant academic literature fields described in chapter 4, combined with the aspects identified by expert interviews as described in chapter 5.

A total of 45 aspects was identified in the combined literature study and expert interviews. Considering the research question of this thesis and the conclusion of incomplete models currently available in literature, all 45 were initially selected as aspects of forensic readiness. These aspects were submitted for validation to 15 forensic experts, different than the ones used to extract requirements. A total of 9 experts participated in the validation, from a variety of organizations with an average experience of 8 years. These experts are listed in Table 12.

Table 12: Forensic experts interviewed for validation

#	Organization	Job title	Years of experience
1	Ernst & Young	Senior Manager Forensics	14
2	KPMG	Technical Forensics Investigator	3
3	KPMG	Technical Forensics Investigator	3
4	CC Bill	Lead security Analyst	17
5	Fox-IT	Senior Forensic IT expert	4
6	Fox-IT	Forensic IT expert	5
7	NFI	Data Analysis Researcher	15
8	CZ	Advisor Information Security	2
9	Van Landschot	Security Manager	6

First, individual interviews were held with available experts to collect their detailed feedback. The experts were further asked to give their opinion on the completeness and effect of these demands, using the form added in Appendix G – Validation form. In this form they had the option to add or remove aspects. Furthermore, they were asked to rate the effectiveness of each aspect on a scale from 1 to 5.

The experts were unanimous in their opinion that the set of requirements covers requirements for organizations to become forensic readiness. Nearly all defined the list as complete, comments lead to minor rephrasing and/or re-ordering of the aspects mostly for sake of maintaining a clearer overview. The average effectiveness ratings from all experts were:

- an average for all aspects of 3.7;
- a minimum of 2.3;
- a maximum of 4.6.

The essential elements were in line with what was expected after examining the research and earlier interviews with experts. Based on these expert validations and ratings no aspects were added. It was noted by experts that one of the aspects, *Preparing infrastructure for forensics*, is (or should) actually be incorporated within *Policies & Procedures*, and then further separated in several technical implementations. This recommendation was followed. The resulting total amount of aspects was 44.

6.2 Aspects

In order to be able to grasp all 44 aspects to be incorporated into the framework, structure needed to be applied. An overview of all aspects shows that three main categories can be identified, namely:

- People, containing 4 aspects;
- Process, containing 20 aspects;
- Technology, containing 20 aspects.

During the validation each aspect was rated for effectiveness on a scale from 1 to 5. This rating, combined with relevance the literature study assigned the aspect measured by number of references, allowed us to further divide these aspects in terms of importance. Three layers of importance were defined, layer 1 being the most important and layer 3 the least important. Layer 1 aspects scored > 4, layer 2 contains the aspects with a score between 3 and equal or smaller to 4, and layer 3 contains all aspects with a score equal to or lower than 3. The first layer contains 15 aspects, the second layer 21 and the third layer contains 8 aspects. Dividing the aspects in importance allows organizations to:

- Determine where they are in their current situation, and;
- Apply focus on certain areas to improve based on this assessment.

All aspects, divided by category and importance, are shown in Table 13. These aspects essentially form the controls for the governance framework. Most aspects are self-explanatory, however Table 14, Table 15 and Table 16 provide illustrative controls for each aspect of the respective categories people, process and technology.

An extensive mapping of each identified aspect to its source is given in Appendix H: Mapping of aspects to sources.

Table 13: Aspects by category and importance

	People	Process	Technology
Layer 1	RQ1: Team	RQ5: Risk analysis	RQ24: Time synchronization
	RQ2: Training	RQ6: Policies & procedures	RQ25: Logs: What is logged
		RQ7: Budgeting	RQ26: Bit-by-bit copy
		RQ8: Prioritize incidents	RQ27: Collect volatile to less volatile
		RQ9: Chain of custody	RQ28: Hashing
		RQ10: Investigative actions	RQ29: Maintain integrity of original data
			RQ30: Never work on original or primary copy
Layer 2	RQ3: Awareness	RQ11: Determine interesting data sources up front	RQ31: Toolkit
	RQ4: Senior Management Level Support	RQ12: Determine purpose of investigation up front	RQ32: Logs: Remote logging
		RQ13: Legal	RQ33: Logs: Log retention time
		RQ14: Test plan	RQ34: Normal behavior network, systems, applications
		RQ15: Situational awareness	RQ35: Write blocker
		RQ16: Describe mandate to incident responder	RQ36: Isolate compromised systems
		RQ17: Contact list whom to escalate to	RQ37: Backups
		RQ18: Prepare standard documents	RQ38: Storage of evidence
		RQ19: Include lessons learned	RQ39: Packaging for transport
			RQ40: Periodic review of data source configuration
Layer 3		RQ20: Maintain and use knowledge base	RQ41: Logs: Ensure dynamic logging capability
		RQ21: Contact with law enforcement	RQ42: Compare trusted state of systems
		RQ22: Secure communication available	RQ43: Proactively collecting useful data
		RQ23: Continually review security threats (external)	RQ44: Redundant hardware

Table 14: Controls - People category

ID	Layer	Aspect	Illustrative control
Pe.1	1	Team	A multidisciplinary team is available for incident response. If chosen for a third party providing incident response capabilities, the organization shall ensure an in-house team (albeit smaller) is available for providing internal knowledge and direct communication within the organization. The team shall consist of sufficient objective members, i.e. it will not contain too much system administrators performing everyday business in comparison to other members. The team shall be capable of handling incident response from a broad perspective, containing skills ranging from legal knowledge and public relations to technical, forensic analysis capabilities.
Pe.2	1	Training	The team performing forensic analysis as part of incident response shall be trained on knowledge of and capabilities with tools, best practices regarding collecting and handling evidence and forensic analysis.
Pe.3	2	Awareness	All personnel shall be made aware of existing policies and procedures regarding how to respond to a potential compromised computer. Such policies will typically include not touching the system and reporting to the appropriate contact within the organization as soon as possible.
Pe.4	2	Senior Management Level Support	Senior management shall support implementation of a forensic readiness program in the organization. This support shall not be limited to allocation of budget and defining policies. Top management shall *practice what they preach* by assigning the subject to a member of their decision-making body (typically the CIO or CISO), setting the example and ensuring the program is accepted throughout the company.

Table 15: Controls - Process category

ID	Layer	Aspect	Illustrative control
Pr.1	1	Risk analysis	The organization shall perform a risks analysis and determine its risk appetite. Depending on the acceptable risk as defined, the organization shall establish its forensic capability accordingly. It is essential determine what systems, data and/or processes are vital to the organization. Ask yourself the question: *"What are your crown jewels?"*.
Pr.2	1	Policies & Procedures	The organization shall define and/or adjust existing policies to incorporate forensic readiness. These policies should amongst others describe matters such as under which conditions to investigate, how to handle privacy sensitive data in an investigation, allowance of anti-forensic tools, when to escalate incidents to law enforcement and

			how forensic readiness requirements influence outsourcing decisions/negotiations also with regards to SLAs. Procedures regarding forensic analysis shall be described, following the earlier defined policies. Furthermore, procedures for reporting suspicious activities potentially leading to forensic analysis shall be described.
Pr.3	1	Budgeting	Top management shall ensure sufficient budget is available to design and implement forensic readiness within the organization.
Pr.4	1	Prioritize incidents	During incident response, the response team shall prioritize incidents based on the risk analysis. In case multiple incidents occur simultaneously, high risk incidents shall be given priority for investigation.
Pr.5	1	Chain of custody	To ensure resulting evidence from an investigation is accepted in a court of law, the response team shall maintain a thorough chain of custody for all evidence. The chain of custody shall provide a detailed timeline stating when, how and by whom the evidence was gathered, collected, moved, kept or analyzed and for what purpose.
Pr.6	1	Investigative actions	To ensure resulting evidence from an investigation is accepted in a court of law, every step in the investigation shall be documented for reproducibility. This includes every command executed at every file or bit location on hard disk during investigation, such that the result can be verified. This may be automated, e.g. using screen scrapers.
Pr.7	2	Determine interesting data sources up front	Based on the risk analysis, data sources containing potential interesting data in case of an IT incident shall be identified and documented. This overview shall be reviewed periodically.
Pr.8	2	Determine purpose of investigation up front	Based on policies, and if thereby required in consultation with the responsible individual/board, the purpose of each investigation as part of incident response shall be decided up front. This purpose shall partly determine the required forensic approach.
Pr.9	2	Legal	The forensic procedures followed during investigation shall adhere to legislative demands. The procedures shall periodically be reviewed against legislative compliance, including breach notification and privacy laws.
Pr.10	2	Test plan	Forensic procedures shall regularly be tested for usability and practicability. A simulation containing a practical scenario may be part of such a test.
Pr.11	2	Situational awareness of network, systems and data	The organization shall identify and classify data, systems and segments within its network, including connections amongst systems and data flows and a mapping of crucial business data to systems. This overview shall be reviewed periodically.
Pr.12	2	Describe mandate to incident	A detailed mandate shall be described for the incident response team indicating what decisions they are authorized to take, including shutting down (web)services.

		responder	
Pr.13	2	Contact list whom to escalate to/ask help	An escalation contact within and/or outside the organization who can be contacted 24/7 shall be described, in case of critical incidents, new insights requiring immediate attention and/or an identified lack of knowledge. Furthermore, backup contact(s) shall be appointed.
Pr.14	2	Prepare standard documents	Standard documents shall be prepared to ensure smooth handling of often occurring situations in investigations, such as data requests from third parties (ISPs), maintaining a chain of custody, documenting investigative actions, waivers to be signed by employees allowing investigations.
Pr.15	2	Include lessons learned	For each investigation the plan of action shall include a lessons learned session to allow improvement at a next occurrence.
Pr.16	3	Maintain and use knowledge base	A knowledge base shall be created, maintained and used such that identical or similar incidents and investigations encountered earlier can effectively be performed at a next occurrence.
Pr.17	3	Contact with law enforcement	Contact with law enforcement shall be established and maintained to ensure a quick and smooth response and investigative capability in case of escalation to law enforcement.
Pr.18	3	Secure communication available	Secure communication shall always be available for the incident response team, including fall-back options in case of a compromised network, potentially containing the organization's mail server.
Pr.19	3	Continually review security threats (external)	New security threats, exploits and their characteristic shall be known to the incident response team to ensure adequate investigative means, as an addition to the regular training. Besides consuming relevant information themselves, the incident response team can use publication from national public sources such as the National Cyber Security Centre (NCSC), who often publish factsheets on new threats.

Table 16: Controls - Technology category

ID	Layer	Aspect	Illustrative control
Te.1	1	Time synchronization	All systems within the organization's network shall be synchronized to one unique time source. Deviations shall be checked periodically.
Te.2	1	What is logged	Systems identified as important shall enable audit logging, containing for every user each actions performed. Logs shall include timestamps. Security logging shall be fully enabled, on the network, system and application layer.
Te.3	1	Bit-by-bit copy	During collection of potential evidence a bit-by-bit copy shall be made, to avoid unwanted changes to original data and ensure integrity of resulting evidence can be verified. The primary copy shall be kept safely for reproducing more bit-by-bit copies in a later stage, required for investigation.

Te.4	1	Collect volatile to less volatile	During collection of potential evidence, most volatile data sources shall be collected first. In order to be able to do so, the volatility of data sources shall be determined and required hardware and software shall be in place.
Te.5	1	Hashing	Cryptographic hash functions shall be applied to ensure the integrity of at least log files (e.g. both per line and of the complete file) and collected potential evidence (e.g. hash value of entire disk).
Te.6	1	Maintain integrity of original data	During investigation the integrity of the original data shall be maintained, unless it is otherwise impossible to perform critical investigation. In such case, measures shall be taken to ensure the validity of the investigation's result, e.g. by filming the entire process.
Te.7	1	Never work on original/primary copy	Investigation shall never occur on the original or primary data copy of evidence, unless it is otherwise impossible to perform critical investigation. In such case, measures shall be taken to ensure the validity of the investigation's result, e.g. by filming the entire process. In all other cases, new bit-by-bit copies shall be made before investigative actions are taken. Sufficient hardware and/or storage shall be available for this means.
Te.8	2	Toolkit	An adequate toolkit shall be available for the incident response team, such that they will always be able to rely on safe versions of required tools.
Te.9	2	Remote logging	Logs shall be saved both locally and at a remote, secured system to ensure log content can be trusted even if a single system has been compromised. Inconsistencies between local and remote logs can be indicators of compromise.
Te.10	2	Log retention time	Logs shall minimally be kept for the amount of time required to oblige with local legislation. Furthermore, log retention time for each system shall be determined based on the risk associated with that system, resulting from the risk analysis.
Te.11	2	Normal behavior networks, systems, applications	The organization shall determine a safe baseline of behavior its network(s), systems and applications.
Te.12	2	Write blocker	During collection and (static) analysis integrity of disks and files shall be maintained by utilizing a write blocker. Depending on the media under investigation, both software and hardware solutions may be used.
Te.13	2	Isolate compromise systems	The organization shall posses the capability to easily and quickly isolate systems from its internal network.

Te.14	2	Backups	Regular backups shall be made, keeping both ‘hot’ and ‘cold’ copies, to ensure swift return to daily operations after potential evidence has been collected. A differentiation may be made between daily, weekly, monthly and yearly backup tapes. Keeping several of each type of backups increases the chance of being able to deliver required data to forensic investigators performing historical comparison.
Te.15	2	Storage of evidence	Evidence shall be stored securely, such that damage or alteration of (digital) data is avoided. Furthermore, evidence shall be stored for a minimum period of time as required by local legislation.
Te.16	2	Packaging for transport	Evidence shall be transported securely, such that damage or alteration of (digital) data is avoided.
Te.17	2	Periodic review of data source configuration	Data source’s configuration shall be reviewed periodically, to ensure correct settings for e.g. logging.
Te.18	3	Ensure dynamic logging ability	A dynamic logging ability shall be implemented on network, system and application level to ensure more detailed logging can be captured if an object is suspected of being compromised.
Te.19	3	Compare trusted state of systems	A trusted baseline of all system(s) (roles) and its cryptographic signature shall be kept, containing amongst others main executables and libraries, to allow comparison to trusted states for suspected compromised systems.
Te.20	3	Proactive collecting useful data	For high risk systems, potential evidence shall be collected periodically to ensure evidence is available if an incident is detected.
Te.21	3	Redundant hardware	Redundant hardware shall be available to replace originals after an incident has been detected, allowing the original disks to be used as evidence. Accurate backup (and restore) capabilities are required to support this.

7 Summary

In this phase of the research, sub questions 1, 2 and 3 were answered:

SQ 1. *What do forensic analysts require for performing an adequate analysis?*
SQ 2. *Taken into account the requirements identified in SQ1, what additional demands do organizations impose on a continuous forensic readiness framework?*
SQ 3. *What forensic readiness models are currently available and to what extent do they help organizations to become continuously forensic ready?*

To answer SQ 1, literature was studied as described in chapter 4. Furthermore, forensic experts were interviewed. A total of 45 aspects were identified, validated, categorized, prioritized and finally listed in chapter 6. A detailed description of all these aspects, as well as illustrative controls which serve as controls for the final goal namely the Continuous Forensic Readiness framework, are provided in Table 14, Table 15, and Table 16 for the respective categories people, process and technology.

Besides the demands from forensic analysts, SQ 2 relates to demands coming from the organizations. In order to determine these demands, forensic experts were asked on their experiences. Combined with demands as described in literature and the demands mentioned by the case study of this research, the University of Twente, this resulted in 3 demands which the Continuous Forensic Readiness Framework will have to adhere to, as mentioned in section 5.3.3.

To answer SQ 3, in section 4.3 currently available models for forensic readiness were discussed. This issue was also discussed during the interviews with forensic experts. There are some models currently available but they do not suffice for an holistic approach to forensic readiness. Furthermore, the approaches elaborated upon work towards becoming forensic ready in some point in time, but disregard what to do from there on.

The requirements and demands identified as answers to SQ1, SQ2 and SQ3 form the starting point for the Continuous Forensic Readiness Framework. In phase “II – Solution Design” we continue with designing the framework.

II – Solution Design

8 Introduction – Solution Design

In this part of the thesis the creation of the actual Continuous Forensic Readiness Framework is discussed, based on the analysis presented in the first part. This second phase of the research is known as 'Solution Design', as shown in Figure 6.

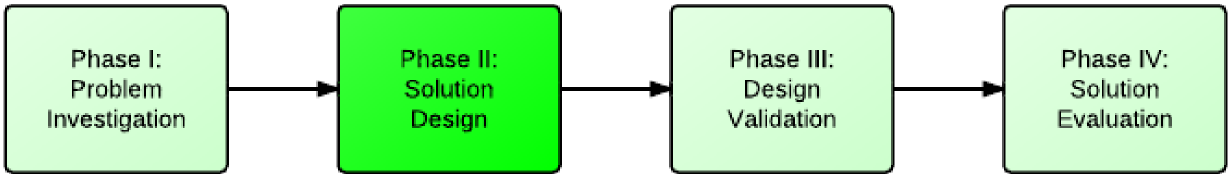

Phase I: Problem Investigation
Phase II: Solution Design
Phase III: Design Validation
Phase IV: Solution Evaluation

Figure 6: Phase II – Solution Design

Currently available governance models together with their key components are elaborated on in chapter 9. In order to create a framework several different approaches were possible, and these as well as the approach chosen are discussed in chapter 10. After having looked at these currently available models, their key aspects and the choice on how it was performed in this research has been made, the actual framework is introduced in a high level overview in chapter 11. In chapter 12 the framework is looked at in a more detailed manner. This phase of the research is summarized in chapter 13.

9 Existing Governance Models

In order to answer SQ 4, *What leading governance models are currently available and how are they suited for forensic readiness?*, a limited set of commonly known and accepted governance models was studied. These models are:

- COBIT 5
- COSO
  - Internal Control Framework (ICF)
  - Enterprise Risk Management Framework (ERMF)
- ITIL v3
- ASL/BiSL
  - ASL
  - BiSL
- ISO 2700x
- Information Security Governance Framework (ISGF)

The purpose of this literature study was to, for each model, determine how the governance model works and explore its possible relation with and/or use for forensic readiness. In order to achieve this each governance model was analyzed to extract its main elements. Section 9.1 provides brief general descriptions for each model, after which section 9.2 discusses notable observations from this study. For a more detailed summary of the building blocks of each governance model we refer to Appendix I: Basic Building Blocks Governance Models.

9.1 General descriptions

This section provides brief descriptions for each model.

9.1.1 COBIT [61]

Control OBjectives for Information and related Technologies (COBIT) is a framework created by ISACA for information technology management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks. COBIT 5 is based on five key principles:

1. Meeting stakeholder needs;
2. Covering the enterprise end-to-end;
3. Applying a single integrated framework;
4. Enabling a holistic approach;
5. Separating governance from management.

The framework divides the practices and activities into two main domains: governance and management. It furthermore defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. These enablers are divided into seven categories, which are:

1. Principles, policies and frameworks;
2. Processes;
3. Organizational structures;
4. Culture, ethics and behavior of individuals and of the enterprise;
5. Information;
6. Services, infrastructure and applications;
7. People, skills and competencies.

The framework defines a total of 37 generic processes to manage IT, to support governance of IT by defining and aligning business goals with IT goals and IT processes.

9.1.2 COSO ICF [28]

This framework is an internal control framework, initially aimed at the reliability of financial statements and furthermore aids in increasing efficiency, minimizing risks and comply with laws and regulations [27]. The framework identifies five components of internal control, namely:

1. Control Environment;
2. Risk Assessment;
3. Control Activities;
4. Information & Communication;
5. Monitoring Activities.

Furthermore, the framework is geared to achieving objectives related to (1) operations, (2) compliance and (3) reporting. Lastly the framework identifies different operating units and other structures within the entity.

A direct relationship exists between the objectives, the components and the operating units, legal entities, and other structures within the entity. The framework was updated on the 14th of May 2013. In this final updated version of the framework the core objectives, components and structure remained the same, although not only financial reporting but also internal and external non-financial reporting is now included [27, 28]. Furthermore an additionally 17 principles were identified as important enough to be embedded in the original framework, and were added to the existing components.

9.1.3 COSO ERMF [26]

In addition to the Internal Control Framework, in 2004 COSO published a framework to allow management to evaluate and improve their organization's enterprise risk management [26]. COSO believes *Enterprise Risk Management – Integrated Framework* expands upon the Internal Control Framework, providing a more robust and extensive focus on the broader subject of enterprise risk management. The principles of the Internal Control Framework remain the same, and the framework is still build up around objectives, components and structures within the entity. This framework however includes four categories:

1. Strategic;
2. Operations;
3. Reporting;
4. Compliance.

The five original components are encompassed by eight components within the new framework. These components are Internal Environment, Objective Setting, Event Identification, Risk Assessment, Risk Response, Control Activities, Information & Communication and Monitoring.

9.1.4 ITIL [62]

Information Technology Infrastructure Library (ITIL) is not a model or framework for delivering quality IT services by itself, but more a set of best practices for achieving this same goal. ITIL thus offers practical design criteria. ITIL v3 is focused on the continuous improvement of service management. ITIL provides broad guidance documentation covering IT Service Delivery, Management, Support, elements of IT Infrastructure, and Security and Application Management. ITIL distinguishes between five phases:

1. Service Strategy;
2. Service Design;
3. Service Transition;
4. Service Operation;
5. Continual Service Improvement.

At the core is the service strategy, surrounding it the service design, transition and operation operating circularly. As the name suggests, Continual Service Improvement is performed continuously. These phases are further specified into 26 processes.

9.1.5 ASL / BiSL [6]

ASL and BiSL were created as a response to gaps that were present in ITIL version 2. They are both considered complementary to ITIL v2, and therefore discussed together Generally speaking, ICT management can be divided into Technical/Infrastructure Management, Application Management and Information Management. Herein ITIL v2 was used to describe technical management, ASL for application management and BiSL for functional and information management.

ASL

The Application Services Library (ASL) is a public domain standard, describing a standard for processes within Application Management. It is named a library because the standard is based on descriptions of best practices from industry. Two main categories of support are defined:

1. Descriptions of the processes for Application Management, plus the use of best practices;

2. Standard terminology, avoid the pitfall of talking about the same thing whilst using different words.

ASL is structured in different management levels, namely strategic, tactical and operational, and further defines six clusters of processes, namely:

1.	Organization Cycle Management	(Strategic)
2.	Applications Cycle Management	(Strategic)
3.	Management Processes	(Tactical)
4.	Maintenance Processes	(Operational)
5.	Enhancement and Renovation Processes	(Operational)
6.	Connecting Processes	(Operational)

BiSL

BiSL is a framework for information management, also based on best practices. ITIL and ASL focused on the supply side of information and BiSL on the demand side, arising from the end-user organization. BiSL has a focus the demand side: the business that wants to use IT to its maximum. It is aimed at translating business processes to IT systems and processes, in order to support business. Like ASL it describes its processes on three different management levels, and defines seven clusters of processes:

1.	Develop I-organization strategy	(Strategic)
2.	Develop information strategy	(Strategic)
3.	Information coordination	(Strategic)
4.	Management processes	(Tactical)
5.	Use management	(Operational)
6.	Alignment processes	(Operational)
7.	Functionality Management	(Operational)

9.1.6 ISO 27000 - *A Code of Practice for Information Security Management [58, 59]*

The ISO 27000 series, or family, describes information security matters. The most important standards within this series are the 27001, which specifies an Information Security Management System (ISMS) meant to bring information security under explicit management control, and the 27002, which provides an extended list of 133 controls organizations can implement. These standards are included here on advice of governance experts interviewed for two main reasons. First, they provide thorough controls and second, forensic analysis as part of incident response has an obvious alignment with security.

ISO 27001 underlines the fact that management is responsible for security, as it is not only a technical issue. A major component of information security should therefore be risk management. In essence, ISO 27001 describes a process of how to select the controls specified in ISO 27002. This is needed because just ‘blindly’ implementing all controls is generally considered bad practice, because not all controls are equally relevant for all organizations. The standard is based on the Plan-Do-Check-Act cycle, which is shown in Figure 7.

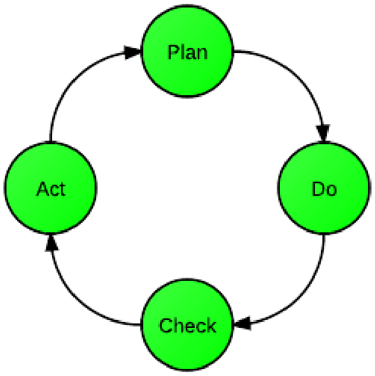


Figure 7: Plan-Do-Check-Act (PDCA) or Deming Cycle

As the name and shape suggest this is a cyclic process. In the *Plan* phase objectives and processes necessary to deliver the expected output are established. In the *Do* phase the plan is implemented, the processes executed and data is collected for the following phases. In the *Check* phase the actual results are measured, collected and compared against the expected results. In the *Act* phase corrective actions are taken if needed to overcome significant differences between actual and planned results.

ISO 27001 helps to gain an overview of all controls, which are often otherwise just implemented ad hoc, and align them to strategic choices made on the topic of information security. For this information security requirements and expectations are used as input for the PDCA cycle, from where eventually a managed information security environment will arise. ISO 27001 describes the required states to achieve these as to establish, implement, operate, monitor, review, maintain and improve. These are fit into a PDCA cycle.

ISO 27002 identifies three categories for its controls, namely management, technical and physical aspects. These controls rely on each other like a pyramid, which represents the breakdown from management controls to operational controls.

9.1.7 Information Security Governance Framework [124]

The Information Security Governance (ISG) Framework, defined by von Solms and von Solms, has as basis the Direct-Control cycle as shown in Figure 8. Von Solms & Von Solms argue that any governance has a direct-control cycle at its core, which in its simplest form ‘prescribes’ and ‘checks’. Using just basic governance theory the authors provide a framework for a specific means, namely for information security. In their model, they distinguish between different management levels (strategic, tactical, operational), and combine these together with the direct-control cycle to enforce specific controls meant for information security.

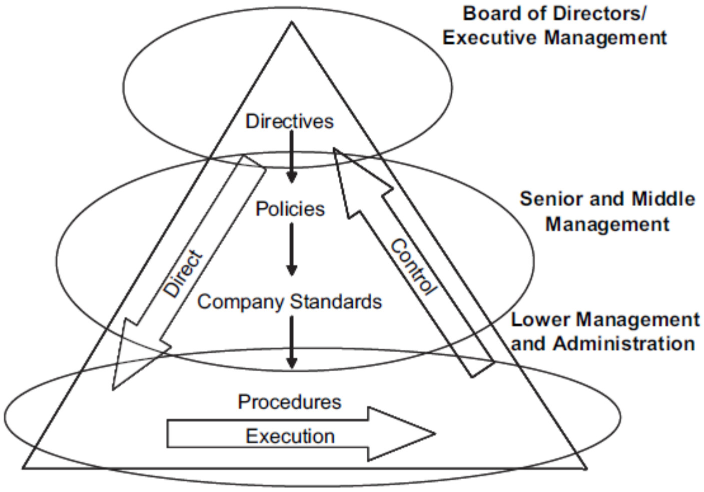


Figure 8: Von Solm's Direct & Control cycle, adapted from [124]

In Appendix I: Basic Building Blocks Governance Models an overview of the main findings of the study to governance models is provided, namely the building blocks for each model. For a more elaborate description of each model we refer to its respective publication.

9.2 Observations

Despite different goals and configuration that these governance models have, taking a further look at these models, their setup, structure and basic building blocks, there are some important general observations to note here:

Continuous aspect

All frameworks contain an aspect referring to either an continual improvement or a periodic check with regards to the implementation. The naming is not identical, and the exact implementation / amount of steps in such a cycle do not always align. However, whether we are looking at the Monitoring Activities as defined in the COSO frameworks, governance-management cycle in COBIT, Continual Service Improvement in ITIL, the cyclic setup of processes in ASL/BiSl, the PDCA in ISO27000 or the Direct-Control cycle in ISGF, they all imply a cyclic working where the actual situation is compared with desired, and then if needed correctments/adjustments are made in order to satisfy the goal.

Categorization of controls

The controls defined in order to reach the goal intended are often categorized, arguably this is done for easier usability of the framework.

Management levels

A distinction is often made between different management levels, within which controls (or categories of controls) are then divided.

Stakeholders

A distinction is often made between stakeholders to be involved in certain processes or controls.

10 Solution approach

In order to create the Continuous Forensic Readiness Framework several different options were available. Experts on governance and governance models were interviewed to gain a deeper understanding of these topics, as well as discuss the project itself and possible approaches to take. The experts interviewed are listed in Table 17.

In 10.1 the different approaches are discussed. Next in 10.2 the method chosen is presented and arguments are given for this choice. Section 10.3 discusses an important aspect of this choice..

Table 17: Interviewed persons for governance

#	Organization	Function
1	Considerati	Managing Partner
2	KPMG	Manager Information Protection Services
3	CapGemini	Compliance Consultant

10.1 Different approaches

We can generally differentiate between four different approaches when attempting to incorporate certain aspects into an organization:

1. Use an existing governance model
2. Extend an existing governance model
3. Build a completely new governance model
4. Build a new governance model based on basics from other models

The main advantages and disadvantages of each for this research are shown in Table 18.

Table 18: Advantages and disadvantages of solution approaches

#	Approach	Advantages	Disadvantages
1	Use an existing model	Literature and practical experience exists Already validated	Not specific enough, with a different focus than forensic readiness
2	Extend an existing model	Literature and practical experience exists Relatively easy to validate	Not specific enough, not only focused on forensic readiness but too broad
3	Build completely new model	Can be completely designed for this goal Have the exact right focus	Hard to validate Unlikely to be accepted
4	Build new model based on basics from others	Literature and practical experience for the parts exists Suitable aspects can be chosen, thus improving specificity	More difficult to validate than using existing model Choice for aspects can be hard

10.2 Chosen approach

There is no governance model available which focuses on forensic readiness. There are some models which have security elements, from which in turn certain aspects might be closely related, but these simply do not suffice to reach a state of forensic readiness. Therefore, approach 1 was no realistic option.

Approach 2 requires us to add the forensic readiness aspects to an already existing model. The result will thus be able to count on a thorough basis, but still be specific enough to support forensic readiness.

Building a complete new model, approach 3, would allow us to construct a very specialized framework completely focused on forensic readiness. It would however be very hard to validate, both scientifically and in practice. Furthermore, it is unlikely to be accepted by organizations.

Approach 4 allows to 'selectively shop' from existing frameworks to find basics which fit the forensic readiness needs. As a result a completely new model arises, but the basic elements are still related to existing governance frameworks.

After consolidating governance experts, approach number 4 was chosen. Elements from existing governance models are combined to provide the Continuous Forensic Readiness Framework. Approach 2 was abandoned because the forensic readiness aspects differ too much from any other demands. The extension of an existing model would require adding a large amount of new components, making a new framework based on existing basic building blocks seem a more appropriate choice.

10.3 Plan-Do-Check-Act (PDCA) Cycle

One of the main aspects mentioned by governance experts, but also something noted in all governance models and earlier studies with regards to implementing and securing controls within organizations [13, 58], is an implementation cycle. The one often encountered and also recommended by experts during interviews is the Plan-Do-Check-Act Cycle, or Deming Cycle. This cycle was briefly introduced earlier, in section 9.1.6, and is for repetition shown in Figure 9.

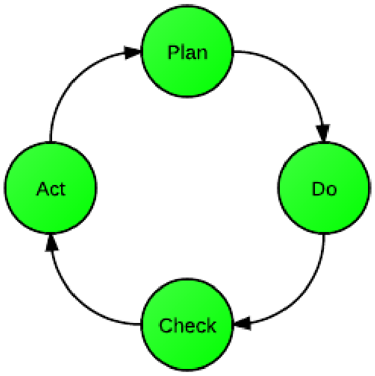


Figure 9: Plan-Do-Check-Act (PDCA) or Deming Cycle

11 The Continuous Forensic Readiness Framework

In this chapter the Continuous Forensic Readiness framework is introduced on a high level. First the building blocks selected are introduced in section 11.1. Section 11.2 then provides an overview of the framework, and in section 11.3 the working is explained.

11.1 Building blocks selected

Based on the interviews with governance specialists and the governance models studied and described in chapter 9 a total of four building blocks were selected:

- Management (11.1.1)
- Stakeholder (11.1.2)
- Internal Control (11.1.3)
- Plan-Do-Check-Act (11.1.4)

11.1.1 Management

During interviews with experts, both governance and forensics, it became clear that in order to ensure measures are implemented thoroughly it is vital for any framework to be used in all aspects of an organization. This also means the framework needs to be applied throughout all management levels of an organization. We also see this in the implementation of ASL, BiSL, the ISG framework and mentioned in the Code of Information Security Management. The management levels commonly accepted and widely used are:

- Strategic
- Tactical
- Operational

11.1.2 Stakeholder

The actions which have to be performed in order to become forensic ready are not just divided among management levels, but find their corresponding owner in different stakeholders as well, as discussed in chapter 5. We therefore differentiate actions to take under stakeholders which have to perform them, and add this building block as well. Cobit mentions ‘meeting stakeholder needs’ as a key principle. Furthermore, both COSO’s Internal Control Framework and COSO’s Enterprise Risk Management Framework separate their activities per stakeholder as well.

One essential stakeholder for any organization with regards to forensic analysis is the CERT. Following the literature and interviews with experts it has become clear that a CERT is, or should definitely be, the actual first responder to any IT incident. Seeing as preparing for forensic analysis should certainly be accounted for during the initial actions, in this framework the CERT has a prominent role. This will also become clear in chapter 12.

11.1.3 Internal Control

Another block of the framework is the *Internal Control*. It is in this block that the actual activities are defined which need to be in place, or have *controls* for them, in order to achieve a state of continuous forensic readiness. Each of these activities have to be performed on a certain management level by a certain stakeholder. These activities aim to achieve the requirements as specified in chapter 6, and are therefore grouped in the same way, namely by People, Process and Technology.

11.1.4 Plan-Do-Check-Act Cycle

The entire framework functions using the Plan-Do-Check-Act Cycle, which we've discussed earlier in section 10.3. As mentioned, it is observed that many governance framework consists of a similar cycle. COBIT has the Evaluate, Direct and Monitor equivalent. ITIL contains a Continual Service Improvement phase which is nearly the same, and both ASL and BiSL contain several cycles within the processes. The ISO 27000 family uses the PDCA cycle itself, and the ISG Framework works with a Direct-Control cycle. Seeing as the PDCA is the well known, broadly accepted and often used, it is used in the to be constructed framework.

11.2 High level overview

In Figure 10 we see the Continuous Forensic Readiness Framework as a whole. The Management block is on the front, describing the different managerial levels. On the side we can see the Stakeholders block, while the Internal Control block is visible at the top. The block are related as follows: for every demand regarding achieving and maintaining forensic readiness in the Internal Control block, there is a stakeholder who has to perform an action, which takes place at a certain management level.

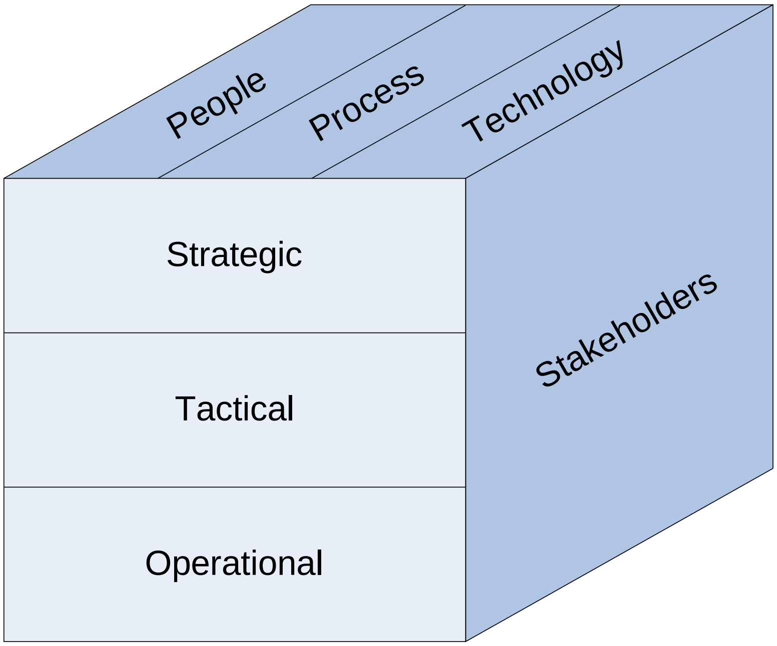


Figure 10: Continuous Forensic Readiness Framework

11.3 In practice

In Figure 10 we see the framework in a high level. Based on the building blocks described earlier, we are missing the PDCA Cycle in the overview. The cycle becomes essential during the actual working of the framework. The PDCA cycle is present at different layers within the framework. As discussed in section 10.3, PDCA cycles are often implemented on top of one another. This allows for a continual improvement cycle, as well as the ability to go up or down in abstraction levels, meanwhile keeping the essence of the activity consistent. This difference in abstraction level is graphically depicted in Figure 11.

As explained, each category within the Internal Control block contains activities. These activities follow the Plan-Do-Check-Act cycle, in order to ensure achieving and more importantly maintaining forensic readiness. This however does not mean that all actions of the cycle take place at the same management level, e.g. a ‘plan’ action at the strategic level may lead to one or more ‘do’ actions at the tactical or operational level.

All these activities are elaborated upon in chapter 12. Surrounding these activities we see one big PDCA cycle in Figure 11, this is the top PDCA cycle, which is defined in Table 19.

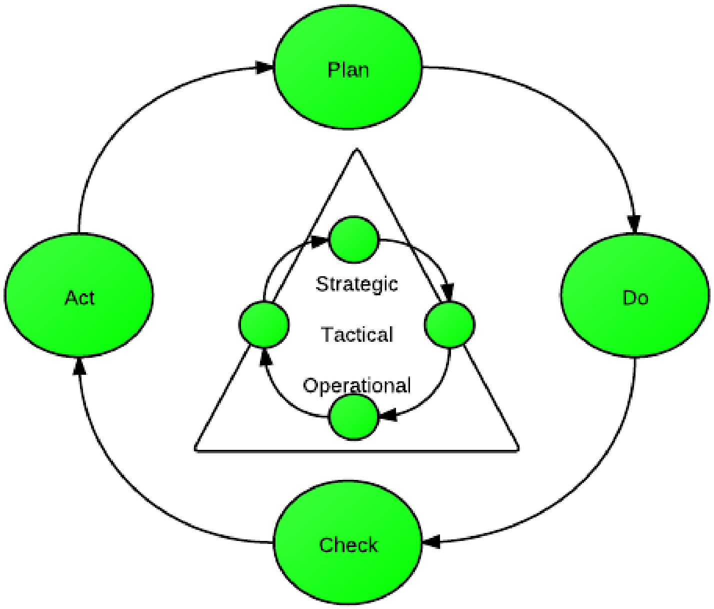


Figure 11: PDCA Cycle in and around the framework

Table 19: Main PDCA cycle

Phase	Activity	Description
Plan	Create a plan for continuous forensic readiness	A strategic plan must be made to achieve forensic readiness
Do	Implement measures to achieve the plan	Once the plan has been made, concrete actions have to be performed in order to execute it

Check	Check whether the organization is in a state of forensic readiness	The controls implemented can be measured to determine their effectiveness
Act	Adapt the plan and/or measures if needed	If the organization does not fulfill the forensic readiness requirements, adjustments should be made

12 Detailed view into the Continuous Forensic Readiness Framework

In this chapter we look at the Continuous Forensic Readiness Framework in more detail. For each element in the Internal Control building block we look at how the PDCA cycle works. In section 12.1 we look at the People category, followed by Process in section 12.2. In section 12.3 the activities with regards to Technology are elaborated upon.

For all the activities in the framework, a RASCI table is suggested to assign responsibilities for each stakeholder. The abbreviations and their meaning are shown in Table 20.

Table 20: RASCI table

Abbreviation	Description	Task
R	Responsible	Owner of the activity
A	Accountable	Person to whom “R” is accountable, authority who approves
S	Supportive	Can provide resources or play a supporting role in implementation
C	Consulted	Provides information and/or expertise necessary to complete the project
I	Informed	Needs to be notified but not necessarily consulted

Responsibilities can differ a great deal for each organization, and depend on amongst others stakeholders involved at the organization, and the incident response process currently in place. To ensure the framework in itself can be broadly applied, the general stakeholders are used in the next paragraphs. The RASCI table is left empty, seeing as responsibilities are highly dependent on the environment. As with any framework, the proposed Continuous Forensic Readiness will need to be specified for each unique organization during actual implementation, which includes determining responsibilities. Some activities require such a specific expertise and/or authorization that defining these responsibilities will be easy, whereas others will most likely require more time and discussion.

12.1 People

The People block regards activities relating to the human aspect of forensic readiness. The requirements for this dimension are discussed in section 6.2. In Table 21 an overview is given of the relevant stakeholders and their responsibilities for the People aspect.

Table 21: Stakeholder responsibilities with regards to People aspect

Stakeholder	Responsibility
Top management	Accountable for daily operations, including staffing
Head of IT department	The CSIRT is often part of the IT department
Business Owners	Establish desired awareness of employees w.r.t. forensics demands
Legal Department	Should be aware of certain forensic practices and demands
CSIRT	Ensure members, helpdesk employees and all other employees are aware and if needed have required skills for their actions.
Helpdesk employees	Should be aware of forensic demands
Employees	Should be aware of certain forensic practices and demands.

The activities together are shown in Table 22. As mentioned, the responsibilities will have to be uniquely determined for every organization. The management level mentioned for each action (denoted in the final column with a *S* for Strategic, *T* for Tactical and *O* for Operational) is therefore to be interpreted as a suggestion, based on the experience from interviews, rather than a final decision. The level on which the action will take place is obviously influenced by the organization implementing the framework. The Layer-column denotes which importance layer the action belong to, as discussed in section 6.2.

Table 22: Activities related to the People dimension

Phase	#	Activity	Stakeholders							S/T/O?	Layer
			Top management	Head of IT department	Business Owners	Legal department	CSIRT	Helpdesk employees	Employees		
Plan	Pe.P1	Ensure forensic readiness ambition as agreed upon can be carried out within the organization								T	1
	Pe.P2	Ensure team is adequately trained								T	1
	Pe.P3	Create/modify an awareness plan								S	2
	Pe.P4	Ensure top management commits to forensic readiness								S	2
Do	Pe.D1.1	Determine required team skills, based on forensic readiness ambition of organization								T	1
	Pe.D1.2	Assign and/or hire staff to team								T	1
	Pe.D2.1	Determine training requirements								T	1

Do	Pe.D2.2	Develop or buy training (materials)								T	1
	Pe.D2.3	Schedule trainings								T	1
	Pe.D2.4	Attend trainings								O	1
	Pe.D3.1	Develop awareness initiative								T	2
	Pe.D3.2	Attend awareness initiative								O	2
	Pe.D4.1	Commit to forensic readiness and display this commitment								S	2
	Pe.D4.2	Follow policies and procedures as determined for forensic readiness								S	2
	Pe.D4.3	Create level of equality between CIO (or if present: CISO) and rest of executive board								S	2
Check	Pe.C1	Evaluate if team can effectively perform required tasks								T	1
	Pe.C2.1	Evaluate training suitability w.r.t. goal								T	1
	Pe.C2.2	Check team members attended trainings								T	1
	Pe.C3.1	Evaluate awareness initiative's efficiency								T	2
	Pe.C3.2	Check attendees awareness initiative								T	2
	Pe.C4.1	Monitor perceived top management commitment								T	2
	Pe.C4.2	Check 'balance' within executive board								S	2

Act	**Pe.A1**	Adjust team formation								T	1
	Pe.A2.1	Adjust training								T	1
	Pe.A2.2	Enforce more trainings								T	1
	Pe.A3.1	Adjust initiative								T	2
	Pe.A3.2	Enforce attending awareness initiative								T	2
	Pe.A4.1	Adjust commitment and involvement where needed								S	2
	Pe.A4.2	Adjust composition of executive board if required								S	2

12.2 Process

The Process block relates to the process side of forensic readiness. The requirements for this dimension are discussed in section 6.2. In Table 23 an overview is given of the relevant stakeholders and their responsibilities for the Process aspect.

Table 23: Stakeholder responsibilities with regards to Process aspect

Stakeholder	Responsibility
Top management	Accountable for all daily operations
Head of IT department	Responsible for incorporate adequate processes surrounding the ICT environment, and ultimately responsible for the CSIRT.
Business Owners	Responsible for incorporating adequate processes into their departments
Legal department	Should test processes for legal adequacy
Internal audit	Audits the processes against internal policies as well as regulations and laws
CSIRT	Does most of the actual work regarding (preparing for) forensic analysis
Helpdesk employees	Have to follow procedures as defined

The activities are shown in Table 24.

Table 24: Activities related to the Process dimension

Phase	#	Activity	Stakeholders							S/T/O?	Layer
			Top Management	Head of IIT Department	Business Owners	Legal Department	Internal Audit	CSIRT	Helpdesk Employees		
Plan	Pr.P1	Determine forensic readiness ambition								S	1
	Pr.P2	Ensure forensic readiness is embedded in organization's policies								S	1
	Pr.P3	Ensure forensic readiness policy is incorporated into procedures								T	1
	Pr.P4	Ensure forensic readiness has sufficient monetary resources to be performed in the organization.								S	1
	Pr.P5	Ensure forensic procedure can be performed efficiently and adequately								T	1
	Pr.P6	Plan tests of forensic procedures								T	2
	Pr.P7	Ensure forensic readiness activities adhere to legislative demands matching the organization's ambition								S	2
	Pr.P8	Ensure the organization learns from (earlier) incidents								S	2
	Pr.P9	Ensure the organization has external situational awareness								T	3

Plan	**Pr.P10**	Ensure communication remains secure during an incident								T	3
Do	**Pr.D1.1**	Perform a risk assessment								T	1
	Pr.D1.2	Determine risk appetite								S	1
	Pr.D1.3	Decide what the organization wants to achieve w.r.t. forensic readiness, taking into accounts its internal and external environment								S	1
	Pr.D2	Create forensic readiness policy & update existing policies with forensic readiness aspects								S	1
	Pr.D3.1	Determine procedures influenced by forensic readiness								T	1
	Pr.D3.2	Update/create procedures for forensic readiness								T	1
	Pr.D3.3	Define forensic procedures (acquisition, analysis, handling of evidence)								T	1
	Pr.D4	Assign sufficient budget for forensic readiness, in line with ambition.								S	1
	Pr.D5.1	Prioritize events during incidents								T	1
	Pr.D5.2	Prepare documents and facilities required for a thorough chain of custody and notes during analysis								T	1
	Pr.D5.3	Determine purpose of investigation up front								S/T	2
	Pr.D5.4	Determine interesting data sources up front, based on identified risks and risk appetite								T/O	2

Do	**Pr.D5.5**	Describe mandate for incident responder								S	2
	Pr.D5.6	Describe contact list w.r.t. escalation								T/O	2
	Pr.D5.7	Describe escalation process and decision mandate								T	2
	Pr.D5.8	Prepare standard documents								T	2
	Pr.D5.9	Acquire internal situational awareness of networks, system and data								O	2
	Pr.D5.10	Establish and maintain contact with law enforcement								O	3
	Pr.D6	Perform test of forensic procedures								T/O	2
	Pr.D7	Determine legal suitability of forensic readiness policyndprocedures								T	2
	Pr.D8.1	Facilitate 'lessons learned' sessions								T	2
	Pr.D8.2	Participate in 'lessons learned' sessions								O	2
	Pr.D8.3	Facilitate usage of knowledge base								T	3
	Pr.D8.4	Update knowledge base after incidents								O	3
	Pr.D9	Research external security threats								O	3
	Pr.D10	Prepare fallback options for communication								T	3
Check	**Pr.C1.1**	Review if risk assessment is up to date and adequate								T	1
	Pr.C1.2	Review if risk appetite suffices								S	1

Check	**Pr.C1.3**	Review if forensic readiness ambition is (still) adequate and suits the organization								S	1
	Pr.C2	Evaluate policies for organization's forensic readiness goal and effectiveness								S	1
	Pr.C3	Check if procedures align with the defined policy								T	1
	Pr.C4	Evaluate forensic readiness effectiveness w.r.t. budget								T	1
	Pr.C5.1	Evaluate if process is focusing on correct events according to priority								O	1
	Pr.C5.2	Evaluate if a thorough chain of custody and investigative log is kept consistently								O	1
	Pr.C5.3	Evaluate actions taken align with purpose								T	2
	Pr.C5.4	Review data sources against risk assessment								O	2
	Pr.C5.5	Review if escalation contact list is up to date								O	2
	Pr.C5.6	Evaluate if incident responder mandate suffices								T	2
	Pr.C5.7	Evaluate escalation process and mandate description for effectiveness and correctness								T	2
	Pr.C5.8	Review if all relevant documents are present								T	2
	Pr.C5.9	Review if knowledge of networks, system and data matches the real life situation								O	2
	Pr.C5.10	Evaluate if contact with law enforcement is still correct and 'warm'								O	3

Check	**Pr.C6**	Validate that forensic procedure tests were successfully completed								T	2
	Pr.C7	Evaluate if legal suitability matches the ambition level								T	2
	Pr.C8.1 **Pr.C8.2**	Review lessons learned minutes								T	2
	Pr.C8.3 **Pr.C8.4**	Evaluate usage of knowledge base								T	3
	Pr.C9	Review current security threats known for completeness								T	3
	Pr.C10	Review availability and suitability of fallback communication methods								T	3
Act	**Pr.A1.1**	Update identified risks								T	1
	Pr.A1.2	Reconsider risk appetite								S	1
	Pr.A1.3	Adjust ambition level								S	1
	Pr.A2	Adjust policies where required								S	1
	Pr.A3	Adjust (forensic) procedures								T	1
	Pr.A4	Adjust budget								S	1
	Pr.A5.1 **Pr.A5.3**	Adjust actions taken								O	1 2
	Pr.A5.2	Adjust prepared documents and facilities								T	1
	Pr.A5.4	Update list with data sources								T	2
	Pr.A5.5	Update contact list								O	2
	Pr.A5.6	Adjust mandate described								S	2
	Pr.A5.7	Adjust escalation process								T	2

Act	**Pr.A5.8**	Update document base								T	2
	Pr.A5.9	Re-acquire situational awareness								O	2
	Pr.A5.10	Adjust contact frequency								O	3
	Pr.A6	Re-schedule tests / Adjust forensic readiness procedure								T	2
	Pr.A7	Update forensic readiness policies and procedures								S/T	2
	Pr.A8.1 **Pr.A8.2**	Schedule additional lessons learned meetings								T	2
	Pr.A8.3	Adjust enforcement of knowledge base								T	3
	Pr.A9	Adjust situational awareness research method / frequency								T	3
	Pr.A10	Adjust fallback communication options								T	3

12.3 Technology

The Technology block regards activities relating to the technological side. The requirements for this dimension are discussed in section 6.2. In Table 25 an overview is given of the relevant stakeholders and their responsibilities for the People aspect.

Table 25: Stakeholder responsibilities with regards to Technology aspects

Stakeholder	Responsibility
Top management	Accountable for daily operations
Head of IT department	Responsible for the IT landscape within the university
Business Owners	Could experience hinder from new technological solutions
Legal Department	Can consult on admissibility of evidence collected in a certain manner
Internal Audit	Audits the IT infrastructure
CSIRT	Uses technological solutions for incident response and possibly forensic analysis
Helpdesk employees	Use technological solutions for initial incident response
Employees	Use the IT infrastructure of the organization

The activities are shown in Table 26.

Table 26: Activities related to the Technology dimension

Phase	#	Activity	Stakeholders							S/T/O?	Layer
			Top management	Head of IT department	Business Owners	Legal Department	Internal Audit	CSIRT	Helpdesk Employees		
Plan	Te.P1	Ensure infrastructure is prepared for forensic analysis								T	1
	Te.P2	Ensure initial response can be performed by the team in a forensically sound manner								T	1
	Te.P3	Ensure analysis can be performed efficiently and in a forensically sound manner								T	1
	Te.P4	Ensure crucial data is collected periodically								T	3
Do	Te.D1.1	Activate time synchronization of clocks on network								O	1
	Te.D1.2	Make list of data to be logged, determined by accepted risk and decided goals and policies								T	1
	Te.D1.3	Technically implement logging process based on prescribed procedure								O	1
	Te.D1.4	Implement remote secure logging								O	2
	Te.D1.5	Implement a long log retention time								O	2

Do	**Te.D1.6**	Implement a dynamic logging capability								O	3
	Te.D1.7	Derive safe baseline of networks, systems and applications (behavior)								T	2
	Te.D1.8	Implement ability for (instant) network segregation								O	2
	Te.D1.9	Enforce only known configurations on systems								O	2
	Te.D1.10	Create hash values for trusted system states								O	3
	Te.D2.1	Provide team with required data acquisition tools								T	1
	Te.D2.2	Determine all-round forensic toolkit requirements								T	2
	Te.D2.3	Compose forensic toolkit								O	2
	Te.D3.1	Provide team with required forensic analysis tools								T	1
	Te.D3.2	Setup the backup/restore process such that relevant backups (e.g. logging) can be restored in a short period of time								T	2
	Te.D3.3	Prepare packaging for storage and transport of evidence								O	2
	Te.D3.4	For crucial systems, prepare redundant hardware to replace original in case of analysis								T/O	3
	Te.D4.1	Identify high risk systems								T	3
	Te.D4.2	Implement proactive collection of crucial (system)								O	3

Check	**Te.C1.1**	Evaluate if time deficiencies are within predetermined limit								O	1
	Te.C1.2	Evaluate if data logged aligns with decided list								T	1
	Te.C1.3	Review if logging completes successfully								O	1
	Te.C1.4	Review if secure remote logging works adequately								O	2
	Te.C1.5	Review if log retention time is sufficient as agreed upon								O	2
	Te.C1.6	Review if dynamic logging works adequately								O	3
	Te.C1.7	Review if baseline is still adequate and up to date								O	2
	Te.C1.8	Review and test network segregation capability								O	2
	Te.C1.9	Review system states and documented deviations								O	2
	Te.C1.10	Review completeness of list of hash values								O	3
	Te.C2.1	Evaluate if data acquisition tools are adequate								O	1
	Te.C2.2	Review determined toolkit requirements for adequacy and alignment with business goal								T	2
	Te.C2.3	Review if toolkit contains agreed upon tools								O	2
	Te.C3.1	Evaluate if forensic analysis tools are adequate								O	1

Check	**Te.C3.2**	Test response of restore process for relevant files								O	2
	Te.C3.3	Review if packaging is adequate and sufficient								O	2
	Te.C3.4	Review if hardware stored is correct for the target systems								O	3
	Te.C4.1	Evaluate if high risk systems match risk assessment and situational awareness								T	3
	Te.C4.2	Review proactive collection effectiveness								T	3
Act	**Te.A1.1**	Update time synchronization								O	1
	Te.A1.2	Update list with data to be logged								O	1
	Te.A1.3 **Te.A1.4** **Te.A1.5** **Te.A1.6**	Update logging process								O	1 2 2 3
	Te.A1.7	Update safe baseline								O	2
	Te.A1.8	Update network segregation capability								O	2
	Te.A1.9	Update standard configuration or restore systems								O	2
	Te.A1.10	Update list of hash values								O	3
	Te.A2.1	Adjust data acquisition tools								T	1
	Te.A2.2	Update toolkit requirements								T	2
	Te.A2.3	Adjust toolkit								O	2

Act	**Te.A3.1**	Adjust forensic analysis tools								T	**1**
	Te.A3.2	Adjust backup/restore process								O	**2**
	Te.A3.3	Adjust packaging stock								O	**2**
	Te.A3.4	Adjust redundant hardware stored								O	**3**
	Te.A4.1	Update list of high risk systems								T	**3**
	Te.A4.2	Adjust proactive collection schedule								T	**3**

13 Summary

In this phase two sub questions were answered, namely SQ 4 and SQ5:

SQ 4. *What leading governance models are currently available and how are they suited for forensic readiness?*
SQ 5. *How do we fill the gap between the requirements/demands identified in SQ1/SQ2 and the solutions offered as identified in SQ3/SQ4?*

SQ4 was answered in chapters 9 and 10, mentioning the most relevant aspects of current governance models and noting their misfit if aiming for forensic readiness. The basic building blocks of governance models were however deemed useful and could be used to create a new framework with a specific focus on forensic readiness.

The newly created Continuous Forensic Readiness Framework, which answers SQ5, was introduced on a high level in chapter 11 where the building blocks used and the framework's overall working are presented. The process model containing the detailed activities following the PDCA cycles within the framework was elaborated upon in chapter12.

The next part, "III – Design Validation", describes the validation process of the framework.

III – Design Validation

14 Introduction – Design Validation

In this part of the thesis the design of the Continuous Forensic Readiness framework is validated. This third phase of the research is named 'Design Validation', as shown in Figure 12.

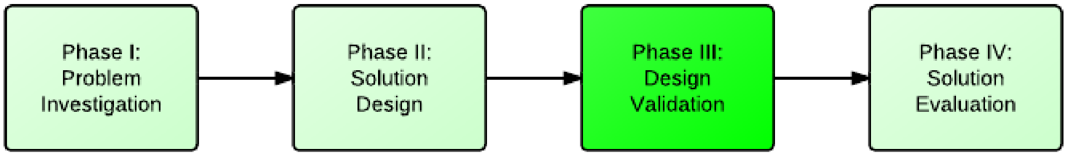


Figure 12: Phase III - Design Validation

The requirements regarding achieving forensic readiness themselves have already been validated, as discussed in section 6.1. The validation of the proposed method to achieve *continuous* forensic readiness, using the framework as described in chapters 11 and 12, is however still to be discussed.

This validation was done in three different ways. First off all, the requirements and demands as determined in chapters 5 and 6, were matched with the framework, which is described in chapter 15. Furthermore chapter 16 discusses validation of the framework by experts. In chapter 17 the case study, the University of Twente, is introduced and the framework applied to them, to see how and if it fits their organization and may help them become and stay forensic ready. The validation process is then summarized in chapter 18.

15 Requirements

In this chapter the framework is validated based on its initial demands and requirements. These requirements and demands for the Continuous Forensic Readiness Framework were derived in chapters 5 and 6. In order to check whether the framework adheres to all of these, a mapping is made to see where each requirement finds its way in the framework. This mapping is shown in Table 27.

Table 27: Mapping of requirements to framework

#	Requirement	Framework			
People					
		Plan	Do	Check	Act
RQ1	Team	Pe.P1	Pe.D1.1, Pe.D1.2	Pe.C1	Pe.A1
RQ2	Training	Pe.P2	Pe.D2.1, Pe.D2.2, Pe.D2.3, Pe.D2.4	Pe.C2.1, Pe.C2.2	Pe.A2.1, Pe.A2.2
RQ3	Awareness	Pe.P3	Pe.D3.1, Pe.D3.2	Pe.C3.1, Pe.C3.2	Pe.A3.1, Pe.A3.2
RQ4	Senior Management Level Support	Pe.P4	Pe.D4.1, Pe.D4.2, Pe.D4.3	Pe.C4.1, Pe.C4.2	Pe.A4.1, Pe.A4.2
Process					
		Plan	Do	Check	Act
RQ5	Risk analysis	Pr.P1	Pr.D1.1, Pr.D1.2, Pr.D1.3	Pr.C1.1, Pr.C1.2, Pr.C1.3	Pr.A1.1, Pr.A1.2, Pr.A1.3
RQ6	Policies & Procedures	Pr.P2, Pr.P3	Pr.D2, Pr.D3.1, Pr.D3.2, Pr.D3.3	Pr.C2, Pr.C3	Pr.A2, Pr.A3
RQ7	Budgeting	Pr.P4	Pr.D4	Pr.C4	Pr.A4
RQ8	Prioritize incidents	Pr.P5	Pr.D5.1	Pr.C5.1	Pr.A5.1
RQ9	Chain of custody	Pr.P5	Pr.D5.2	Pr.C5.2	Pr.A5.2
RQ10	Investigative actions	Pr.P5	Pr.D5.2	Pr.C5.2	Pr.A5.2
RQ11	Determine interesting data sources up front	Pr.P5	Pr.D5.4	Pr.C5.4	Pr.A5.4
RQ12	Determine purpose of investigation up front	Pr.P5	Pr.D5.3	Pr.C5.3	Pr.A5.3
RQ13	Legal	Pr.P7	Pr.D7	Pr.C7	Pr.A7
RQ14	Test plan	Pr.P6	Pr.D6	Pr.C6	Pr.A6
RQ15	Situational awareness	Pr.P5	Pr.D5.9	Pr.C5.9	Pr.A5.9
RQ16	Describe mandate to incident responder	Pr.P5	Pr.D5.6	Pr.C5.6	Pr.A5.6
RQ17	Contact list whom to escalate to	Pr.P5	Pr.D5.5 Pr.D5.7	Pr.C5.5, Pr.C5.7	Pr.A5.5, Pr.A5.7

RQ18	Prepare standard documents	Pr.P5	Pr.D5.8	Pr.C5.8	Pr.A5.8
RQ19	Include lessons learned	Pr.P8	Pr.D8.1 Pr.D8.2	Pr.C8.1 Pr.C8.2	Pr.A8.1 Pr.A8.2
RQ20	Maintain and use knowledge base	Pr.P8	Pr.D8.3 Pr.D8.4	Pr.C8.3 Pr.C8.3	Pr.A8.3
RQ21	Contact with law enforcement	Pr.P5	Pr.D5.10	Pr.C5.10	Pr.A5.10
RQ22	Secure communication available	Pr.P10	Pr.D10	Pr.C10	Pr.A10
RQ23	Continually review security threats (external)	Pr.P9	Pr.D9	Pr.C9	Pr.A9
	Technology				
		Plan	Do	Check	Act
RQ24	Time synchronization	Te.P1	Te.D1.1	Te.C1.1	Te.A1.1
RQ25	What is logged	Te.P1	Te.D1.2, Te.D1.3	Te.C1.2, Te.C1.3	Te.A1.2, Te.A1.3
RQ26	Bit-by-bit copy	Te.P2	Te.D2.1	Te.C2.1	Te.A2.1
RQ27	Collect volatile to less volatile	Te.P2	Te.D2.1	Te.C2.1	Te.A2.1
RQ28	Hashing	Te.P2, Te.P3	Te.D2.1, Te.D3.1	Te.C2.1, Te.C3.1	Te.A2.1, Te.A3.1
RQ29	Maintain integrity of original data	Te.P2, Te.P3	Te.D2.1, Te.D3.1	Te.C2.1, Te.C3.1	Te.A2.1, Te.A3.1
RQ30	Never work on original or primary copy	Te.P3	Te.D3.1	Te.C3.1	Te.A3.1
RQ31	Toolkit	Te.P2, Te.P3	Te.D2.2, Te.D3.1	Te.C2.2, Te.C3.1	Te.A2.2, Te.C3.1
RQ32	Remote logging	Te.P1	Te.D1.4	Te.C1.4	Te.A1.4
RQ33	Log retention time	Te.P1	Te.D1.5	Te.C1.5	Te.A1.5
RQ34	Normal behavior network, systems, applications	Te.P1	Te.D1.7	Te.C1.7	Te.A1.7
RQ35	Write blocker	Te.P3	Te.D3.1	Te.C3.1	Te.A3.1
RQ36	Isolate compromise systems	Te.P1	Te.D1.8	Te.C1.8	Te.A1.8
RQ37	Backups	Te.P3	Te.D3.2	Te.C3.2	Te.A3.2
RQ38	Storage of evidence	Te.P3	Te.D3.3	Te.C3.3	Te.A3.3
RQ39	Packaging for transport	Te.P3	Te.D3.3	Te.C3.3	Te.A3.3
RQ40	Periodic review of data source configuration	Te.P1	Te.D1.9	Te.C1.9	Te.A1.9
RQ41	Ensure dynamic logging ability	Te.P1	Te.D1.6	Te.C1.6	Te.A1.6
RQ42	Compare trusted state of systems	Te.P1	Te.D1.10	Te.C1.10	Te.A1.10
RQ43	Proactive collecting useful data	Te.P4	Te.D4.1, Te.D4.2	Te.C4.1, Te.C4.2	Te.A4.1, Te.A4.2
RQ44	Redundant hardware	Te.P3	Te.D3.4	Te.C3.4	Te.A3.4

Besides these requirements, there were an additional three demands. These were:

1. To minimally interrupt business;
2. To minimize the costs of forensics on incident response;

3. Ensure investigations are cost efficient.

In essence, these demands indicate that we have to ensure forensic analysis can be performed efficiently (both in terms of time and money) while minimally disrupting business processes. Because of the risk-based nature of the framework each organization is able to determine for itself which parts it wants to include in forensic readiness. The framework as proposed adheres to all three demands:

Regarding demand 1, *to minimally interrupt business*: Forensic readiness is, as we've seen, in itself meant to prepare for the forensic analysis process by ensuring data and processes required are already available and defined instead of performing analysis as part of an incident response in an ad hoc manner. Besides this overall remark applicable to the first demand, there are several specific controls in the framework which ensure minimum business interruption. For example, identifying the most relevant data sources, based on your risk assessment, and then in a periodic, proactive manner collecting these as well as having redundant hardware in place provides researchers with valuable data to analyze whilst allowing the business to continue quickly.

Regarding demand 2, *to minimize the costs of forensics on incident response*: The framework mentions several low cost options which already greatly aid forensic investigators, essentially saving time and thereby money. Although without budget nothing can be achieved (as the saying goes, *"money makes the world go round"*), even just being able to perform a (targeted) bit-by-bit copy as an organization saves investigators work. Preparing for this measure comes at a minimal cost. The user of the framework is able to determine its own mix of activities to take based on the risk assessment, its risk appetite and budget made available.

Regarding demand 3, *ensure investigations are cost efficient*: By establishing and maintaining the situational awareness of one's own network, deciding up front which response is adequate for what systems and keeping track of their logging processes through the defined logging policy, organizations are able to quickly give an estimate as to what information can be found, how vital the system breached really is. Using this information they can conclude whether or not analysis is interesting for them. These are all processes/procedures advised in the framework but are very useful for regular ICT maintenance and management as well, and may to some extent even already exist.

15.1 Identical mapping

As the attentive reader may have noticed, some of the requirements map to the same actions in the framework. This indicates a certain kind of generalization which is worth looking into here.

In the *Process* category, we find two identical mappings worth mentioning. The first of which are shown in Table 28.

Table 28: Identical mapping #1 in Process category

#	Requirement	Framework			
		Plan	Do	Check	Act
RQ8	Prioritize incidents	Pr.P5	Pr.D5.1	Pr.C5.1	Pr.A5.1

RQ9	Chain of custody	Pr.P5	Pr.D5.2	Pr.C5.2	Pr.A5.2
RQ10	Investigative actions	Pr.P5	Pr.D5.2	Pr.C5.2	Pr.A5.2
RQ11	Determine interesting data sources up front	Pr.P5	Pr.D5.4	Pr.C5.4	Pr.A5.4
RQ12	Determine purpose of investigation up front	Pr.P5	Pr.D5.3	Pr.C5.3	Pr.A5.3
RQ15	Situational awareness	Pr.P5	Pr.D5.9	Pr.C5.9	Pr.A5.9
RQ16	Describe mandate to incident responder	Pr.P5	Pr.D5.6	Pr.C5.6	Pr.A5.6
RQ17	Contact list whom to escalate to	Pr.P5	Pr.D5.5, Pr.D5.7	Pr.C5.5, Pr.C5.7	Pr.A5.5, Pr.A5.7
RQ18	Prepare standard documents	Pr.P5	Pr.D5.8	Pr.C5.8	Pr.A5.8
RQ21	Contact with law enforcement	Pr.P5	Pr.D5.10	Pr.C5.10	Pr.A5.10

The identical mappings are all with regards to the *Plan* action to be performed, which is *Ensure forensic procedure can be performed efficiently and adequately*. As we see, this is a broadly defined *Plan* action. The reason for this is to increase the readability of the framework, as otherwise every requirement mentioned above would have its own *Plan* action, increasing the size of the table with all actions significantly. Seeing as all aspects are meant to ensure an efficient and adequate execution of the forensic procedure, they are combined here.

The second identical mapping In the *Process* block is shown in Table 29.

Table 29: Identical mapping #2 in Process category

#	**Requirement**	**Framework**			
	People				
		Plan	Do	Check	Act
RQ9	Chain of custody	Pr.P5	Pr.D5.2	Pr.C5.2	Pr.A5.2
RQ10	Investigative actions	Pr.P5	Pr.D5.2	Pr.C5.2	Pr.A5.2

The actions these are mapped to are shown in Table 24, but for ease of reference these are mentioned below

Pr.P5: Ensure forensic procedure can be performed efficiently and adequately

Pr.D5.2: Prepare documents and facilities required for a thorough chain of custody and notes during analysis

Pr.C5.2: Evaluate if a thorough chain of custody and investigative log is kept consistently.

Pr.A5.2: Adjust prepared documents and facilities

In contrast with the first identical mapping in the *Process* category, these aspects are mapped to identical actions in all four steps of the PDCA cycle. The reason for this is that despite their importance and thereby big aspect *during* the forensic analysis, there are only limited steps one can take to *prepare* for this, which is the what the Continuous Forensic Readiness Framework intends to do. Seeing as both aspects require certain documents and possible other facilities (if e.g. performed digitally; a system or application) they were combined in order to avoid entering duplicate actions. Other important actions which can be taken are already covered by other aspects, such as training.

In the *Technology* block, we find another two sets of identical mappings, which are shown in Table 30 and Table 31.

Table 30: Identical mapping #1 in Technology category

#	Requirement	Framework			
		People			
		Plan	Do	Check	Act
RQ26	Bit-by-bit copy	Te.P2	Te.D2.1	Te.C2.1	Te.A2.1
RQ27	Collect volatile to less volatile	Te.P2	Te.D2.1	Te.C2.1	Te.A2.1
RQ28	Hashing	Te.P2, Te.P3	Te.D2.1, Te.D3.1	Te.C2.1, Te.C3.1	Te.A2.1, Te.A3.1
RQ29	Maintain integrity of original data	Te.P2, Te.P3	Te.D2.1, Te.D3.1	Te.C2.1, Te.C3.1	Te.A2.1, Te.A3.1
RQ30	Never work on original or primary copy	Te.P3	Te.D3.1	Te.C3.1	Te.A3.1
RQ35	Write blocker	Te.P3	Te.D3.1	Te.C3.1	Te.A3.1

The actions these are mapped to are shown in Table 24, but for ease of reference these are mentioned below:

Te.P2:	Ensure initial response can be performed by the team in a forensically sound manner
Te.D2.1:	Provide team with required data acquisition tools
Te.C2.1:	Evaluate if data acquisition tools are adequate
Te.A2.1:	Adjust data acquisition tools
Te.P3:	Ensure analysis can be performed efficiently and in a forensically sound manner
Te.D3.1:	Provide team with required forensic analysis tools
Te.C3.1:	Evaluate if forensic analysis tools are adequate
Te.A3.1:	Adjust forensic analysis tools

As we see, the requirements are mapped to actions related to either data acquisition tools or forensic analysis tools. Again, most of these aspects are vital to perform during a forensic investigation. However, in the context of preparing for them there is an organization can only perform limited actions. Ensure the usage of these principles is laid out in policies & procedures, is trained and people are aware of their needs are covered in other aspects of the framework (respectively the *People* and the *Process* category). From a technical point, an organization can only ensure proper tools are available.

Table 31: Identical mapping #2 in Technology category

#	Requirement	Framework			
People					
		Plan	Do	Check	Act
RQ38	Storage of evidence	Te.P3	Te.D3.3	Te.C3.3	Te.A3.3
RQ39	Packaging for transport	Te.P3	Te.D3.3	Te.C3.3	Te.A3.3

The reason for storage and packaging to be combined is nearly identical to the explanations above, so I do not elaborate on this more than needed. They are combined because as a preparation for these actions, ensuring the proper casings/packages are available suffices.

15.2 Additional observation

An additional observation which becomes clear when taking a look into the identical mappings described above, is the fact that whereas the aspects have been categorized in *People*, *Process* and *Technology*, they are still very much intertwined. A lot of the preparatory actions which can be taken in the Technology category do not suffice with the technical preparation alone, but should definitely be taken into account when training people as well. As an example, the aspects mentioned in Table 30 are all vital to ensure the evidence resulting from an investigation is forensically sound. However, just having the technological tools in place to enforce these practices will not suffice if the employees performing the actions are not made aware of and/or trained on these actions. The importance of an holistic viewpoint is thereby once again underlined.

16 Expert validation

This chapter describes the second method used to validate the framework. By performing another round of interviews with experts, different than the governance experts interviewed beforehand, the framework was validated. For this round, a total of 7 experts were interviewed from a variety of organizations, all experienced with governance and process models. The interviewed persons are listed in Table 32.

Table 32: Validation interviews Framework

#	Organization	Job title	Years of experience
1	CZ	Advisor Information Security	2
2	Van Landschot Bankiers	Security Manager	6
3	Booking.com	Corporate Security Officer	14
4	FrieslandCampina	Senior Manager Internal Audit	15
5	KPMG	IT Auditor, IT Risk Consultant, Governance Consultant	4
6	KPMG	IT Auditor, IT Risk Consultant, Governance Consultant	4
7	KPMG	IT Auditor, IT Risk Consultant, Governance Consultant	5

The framework together with the control descriptions and a filled in framework used for the case study (will be discussed in chapter 17) were first send to each expert. They were asked to rate the perceived effectiveness of the framework and the ease of implementation on a scale from 1 to 5. Individual interviews were then held with each to collect detailed feedback. These interviews were recorded – if allowed – and later processed. A short report of each interview was send to the interviewed person for checking factual accuracy.

16.1 Perceived effectiveness

For *perceived effectiveness* of the framework, the experts were asked to focus mainly on the set up of the framework itself: the effectiveness of the controls which filled the framework were already validated as described in chapter 6.

The average perceived effectiveness was rated at nearly 4 out of 5. Especially the combination of assigning responsibilities to stakeholders, the management level and the incorporated PDCA was considered a very strong point of the framework. The experts expected, given the effectiveness of the controls for forensic readiness itself as validated earlier, the framework to be effective in allowing an organization to become and stay forensic ready.

16.2 Ease of implementation

For *ease of implementation* of the framework, the experts were asked to focus merely on how easy the framework would be to implement in an organization, taking into account the prerequisite of a mature IT environment as mentioned in section 2.2.

The first version of the framework which was send to the experts did not include the notion of different levels of importance for the aspects. The average rating for implementation was just over 2 out of 5, indicating the experts foresaw great issues implementing the framework. During the interviews held this was one of the main topics in each interview.

In general, the framework was described as large. Considering the amount of actions to be taken, experts expected issues with focus and a great deal of "Where to start". Experts mentioned that adding different layers in the aspects would allow organizations to implement the framework one layer at a time, instead of a full blown implementation. Adding different such layers ensures that organizations can:

- Determine in what state they are in currently;
- Easier apply focus during implementation;
- Work towards forensic readiness in a stepwise fashion.

Based on these conversations as well as discussions with my supervisors, the levels of importance were added as have been presented in the framework in chapter 6 and applied to the actions to take, as discussed in chapter 12.

After adding these layers, the experts were again send the framework and asked to give a new rating on the ease of implementation. As expect, the average rating was now higher, with an average of 3.6**.**

17 Case study: Current UT model

In this chapter the third validation method is described, namely that by use of a case study. First the demands the UT had towards the framework are validated in section 17.1. In section 17.2 the current situation at the UT is analyzed, which allowed us to complete the framework for the UT. In order to assess the usability and practicality of the framework for the University of Twente (UT), a last interview was held with a member of the CERT-UT and with an Information Manager and Security Officer. The summary of this validation is given in section 17.3.

17.1 Demands

The employees of the UT interviewed formulated three demands for the Continuous Forensic Readiness Framework.

Demand 1: Business continuity remains a main issue, thus forensic analysis should cost as little as time as possible.

Demand 2: Due to limited budgets, the monetary costs should be limited.

Demand 3: The response should be in proportion: Analysis should have a decent chance of leading to a successful prosecution or otherwise satisfactory result.

As we've seen in section 5.3.3, these demands were essentially the same way as the general demands which forensic experts had experienced before. These demands have been met, as concluded in chapter 15. Here we therefore briefly explain why these specific instances of the demands are met as well.

In essence, the UT's demands indicate that we have to work with limited time and money to achieve an "as good as possible" result. Because of the risk-based nature of the framework each organization is able to determine itself which parts it wants to include in forensic readiness.

Regarding demand 1, *Business continuity remains a main issue, thus forensic analysis should cost as little as time as possible*: Forensic readiness itself is aimed at ensuring forensic analysis can be performed more efficiently. Furthermore, there are measures identified which allow evidence to be collected in such a manner that business continuity can be performed in the same way, e.g. by having redundant hardware in place.

Regarding demand 2, *Due to limited budgets, the monetary costs should be limited:* The framework mentions several low cost options which already greatly aid forensic investigators. Furthermore, the implementer of the framework is able to determine its own mix of activities to take based on the risk assessment, its risk appetite and available budget.

Regarding demand 3, *The response should be in proportion: Analysis should have a decent chance of leading to a successful prosecution or otherwise satisfactory result:* The University of Twente explicitly mentioned it is not interested in investigating breaches where they are very unlikely to have any success, which actually derives from the 1st and 2nd demands, and is thus caused by a shortage of time and money. By establishing and maintaining the situational awareness of its own network, deciding up front which response is adequate for what systems and keeping track of their logging processes through the defined logging policy, they are able to quickly give an estimate as to what information can be found, how vital the system breached really is and conclude whether or not analysis is interesting for them.

17.2 Analysis

Before the framework could be applied for the UT, initial research had to be performed on the organizational aspects, stakeholders involved, current method for incident response, (internal) compliance to security policies and control framework used within the UT. This information was used to determine relevant parts of the framework, and to see if (and if so, how) we could implement the framework's activities into the existing situation.

The complete analysis can be found in Appendix J: Analysis University of Twente. For now it suffices to note the following key conclusions:

- The University of Twente has its own CERT, namely CERT-UT;
- The incident response procedure is two staged, where the CERT-UT comes into response after so called *First Line Responders* have informed them;
- The UT is implementing an ITIL-like model for governance, tweaked for its own preferences;
- They are still regularly applying changes in this model.

Furthermore, following the analysis of their organization, processes and interviews with CERT-UT and an Information Manager and Security Officer (see Appendix F: Interviews), 9 stakeholder(s) (groups) for the UT with regards to forensic readiness were identified. The stakeholders and their description are listed in Table 33.

Table 33: Stakeholders UT

Stakeholder	Description
CERT-UT	The CERT team does the actual incident response and handling, and is in the current situation given a certain mandate. Incorporating forensic readiness and forensic analysis as a goal of incident response would certainly influence their work.
First line responders	The first line responders determine what happens with each incoming incident. As we've seen in the earlier discussions, initial actions taken in a response can be crucial for forensic analysis and adequacy: their response will certainly be influenced.
Business owners	Business owners may see a certain decrease in the service level with regard to downtime if, higher in the organization, it is decided that forensic analysis is deemed necessary. Furthermore, the business owners will likely be responsible for translating certain policies into measures in order to assure compliance.
Executive Board	Top management is ultimately responsible for management and administration of the organization, which includes actions taken in case of criminal intent and issues such as compliance (as discussed in 1.3.1). These are all relevant with regards to forensic readiness.

Head of Infra department	The head of the infra department is end responsible for the CERT, and decides whether or not to report a crime and press charges.
Director of ICTS	The ICTS is responsible for all ICT related matters at the University of Twente. Forensic readiness will surely influence their current IT systems, infrastructure, procedures, etc.
Legal Council	The staff jurist aids and informs the Secretary of the Executive Board on legal issues, which includes compliance with applicable laws. This would include compliance with laws relevant for forensic readiness, as mentioned earlier in 1.3.1. Furthermore, forensic analysis needs to adhere to certain legislative principles which may change over time, which the jurist should have and keep an overview of. If adjustments need to be made due to legislative changes the staff jurist can communicate this to other relevant parties.
Operational Audit – ICT	The operational audit performs checks on the internal controls, including those on ICT. Although mostly focused on financial systems, other automated systems are more and more included as well [120]. With regards to forensic readiness, the operational audit should certain check for these.
Employees / Students	Although both employees and students will unlikely be actively involved in a forensic analysis, or the preparation for it, they are often the ones who first mention discrepancies by reporting them to the ICT helpdesk. They will thus need a certain acquaintance or knowledge on the matter.

We can map the stakeholders for this particular case to our general stakeholders as identified in section 5.3.2. This mapping is shown in Table 34.

Table 34: General stakeholders vs specific stakeholders

General stakeholders	Specific stakeholders University of Twente
Computer Security Incident Response Team (CSIRT)	• CERT-UT • Head of Infra department
Helpdesk employees	First line responders
Business owners	Business owners
Top management	Executive board
Head of IT department	• Director of ICTS • Head of Infra department
Legal department	Staff jurist
Internal audit	Operational Audit – ICT
Employees	Employees / Students

In line with their demands, and due to the just finished reorganization of ICTS, the UT is not planning on implementing the framework at this moment. It was however made clear that if they were to implement it, they would do so in a stepwise manner. Due to the levels of importance introduced in the framework, this is feasible. As such, it was decided to for this case only fill in the responsibilities for all actions of importance layer 1. After consultation with CERT-UT the responsibilities for each action were determined, and the framework was thus filled in. This result can be found in Appendix K: Completed framework for the UT.

17.3 Validation

The framework was first send to the involved employees to allow them to study it thoroughly. Then the completed framework was discussed with them. Personal interviews were held to receive detailed feedback. The interviews were processed afterwards, and a short note was send for checking the factual accuracy of the result.

Both employees concluded that the framework met the demands as decided up front. Furthermore, they expected the framework to be effective once implemented. Both awarded the framework with a 4 out of 5.

Based on the levels of importance and overall composition of the framework, combined with the experience the UT already has tweaking frameworks to its own environment, ease of implementation was perceived as do-able. Although implementing such frameworks continues to be a tricky process, and including the current wave of budget cuts and reorganizations, commitment to an implementation was not considered very likely. However, the incentive put aside, if the UT decided to implement the framework its ease of implementation was considered to be a 3,5 out of 5.

18 Summary

In this phase one sub question was answered, namely SQ6:

SQ 6: Does the proposed solution in SQ5 fulfill the needs identified in SQ1/SQ2?

This validation has been performed in three different ways.

In chapter 15 the demands mentioned in chapter 5 and the requirements as specified in chapter 6 were mapped to the Continuous Forensic Readiness Framework. All requirements were successfully mapped to the framework, and it was argued that all organizational demands were met with the proposed framework.

Secondly a group of experts were interviewed to validate the framework, of which the results were discussed in chapter 16. They rated the perceived effectiveness nearly 4 out of 5, and the ease of implementation a 3.6 out of 5.

Finally employees of the University of Twente were interviewed to determine their opinion on the applicability and usability of the framework for the university, as discussed in chapter 17. They concluded that the framework first of all adhered to the demands the University of Twente drafted. Furthermore, they rated the perceived effectiveness as 4 out of 5, and the ease of implementation – if the UT would agree to do so – with a 3,5 out of 5.

In the next part we evaluate the solution and the research process as followed during this thesis.

IV – Solution Evaluation

19 Introduction – Solution Evaluation

In the previous phase, the framework was validated by checking the requirements and demands, as well as through interviews with experts. In this phase of the research method, Phase IV (as can be seen in Figure 13), the solution is evaluated.

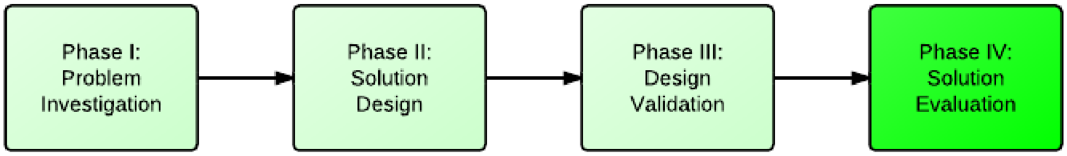

Phase I: Problem Investigation
Phase II: Solution Design
Phase III: Design Validation
Phase IV: Solution Evaluation

Figure 13: Phase IV – Solution Evaluation

First the general applicability of the framework, beyond the University of Twente, is discussed in chapter 20. Then the process of creating the framework and the framework itself are evaluated in chapter 21. In chapter 22 this phase is summarized.

20 Usability beyond University of Twente

Within Design Science, Wieringa [131] specifies two types of validation. The first, *Internal Validation*, is about the here and now. We've seen this validation already in phase three of this research: Design Validation. The second type is *External Validation*, and should also be considered according to Design Science guideline 6 (section 2.4.1).

External validation itself considers two aspects: trade-off and sensitivity.

20.1 Trade-off

Trade-off is about whether a changed treatment will still be valid. This is based on the fact that customers often implement the proposed treatment only up to a certain point, combine the treatment with others, or adjust the treatment to fit their organizational needs better.

For the first goal of the framework, to ensure organizations are able to perform (forensic) analysis following an IT incident, we can confidently state that considering the trade-off characteristics described above the treatment will still be valid *up to a certain point*. The entire framework is set up such that organizations can decide up to what importance layer they want to implement the framework. In theory it is even possible to limit their choice to for which organizational asset they decide to anticipate forensic analysis. Furthermore, the forensic readiness aspects which serve as the basis for the framework were broadly determined, with each aspect in itself adding to the forensic readiness capability. In other words, applying just some of these will still aid in achieving forensic readiness, albeit less than if all are implemented. Combining the treatment with others – assuming they do not have conflicting views or goals – does not diminish this ability either. In short, the trade-off validation holds. The validation of the forensic aspects with experts also indicates this.

The second goal of the framework, to enable organizations to *maintain* the state of forensic readiness, is harder to evaluate. Seeing as maintaining a state requires organizations to periodically review their implemented measures against the described measures (IST-SOLL comparison), only implementing the framework partially will certainly negatively influence the ability to maintain this state. How this might be achieved without the exact implementation of the proposed framework will vary for every organization in which it is conducted: e.g. an organization with a strong internal audit department will most likely find it easier to enforce aspects are implemented than organizations where such internal control is not present.

20.2 Sensitivity

Sensitivity is about whether the proposed treatment will still be internally valid in a changed context. Context here being the environment in which it was 'implemented'; the University of Twente. Looking at the framework in chapter 17, it is clear the stakeholders identified and the responsibilities assigned will need to be changed. These changes are however not with the actual controls to be implemented, as we've determined earlier that these were extracted and validated in a more general sense than just for this case. Furthermore, the framework itself is set up in a broad sense, with the intention to be specified for the environment in which it will be implemented.

Another important characteristic for the context within which the framework can be implemented is the size of the organization. As noted in 2.2, this research focuses on organizations with a mature IT environment. For sake of sensitivity, it is important to touch upon other size organizations as well.

As can be expected from a design with mature IT environments as one of the starting points, the Continuous Forensic Readiness Framework is mostly suited for larger organizations. Implementing the (periodic) activities is simply easier than if you're looking at small- to medium sized organizations. That having said, the activities described can also be implemented by such organizations, if they are interested in achieving continuous forensic readiness.

All things considered, the controls identified are in any situation relevant and can thus still be applied to achieve continuous forensic readiness.

21 Process evaluation

In this chapter the process of the research performed for this master's thesis is evaluated. First the process in general is evaluated in 21.1. Some points regarding the framework itself are then touched upon in 21.2. Two main topics are described in specific; the case study in 21.3 and the research methodology in 21.4.

21.1 General process

This research's goal was to create a framework enabling organizations to achieve a state of Continuous Forensic Readiness. Seeing as in the first weeks of performing this Master's research the scope was more on incident response in general, knowledge from that broader area was gained. Soon after the forensic readiness focus was applied it became clear that the result could, and actually needed, to be incorporated into an incident response process to ensure the most efficient result. For this, the CERT-UT was contacted.

Performing the research for and writing my master's thesis has occasionally been one of trial and error. In hindsight I've realized that clearly determining the scope and thereby picturing what needs to be done is essential. For instance, in order to create a framework allowing a continuous state of forensic readiness, first what is required to achieve forensic readiness needed to be determined.

This first research turned out to embrace quite some more work than was initially considered. As a result, two validation steps needed to be performed: one for the basis of the framework, and one for the framework itself. (To be completely honest: this could've been combined, however then experts with knowledge on both forensic analysis/readiness and implementing governance frameworks are required, which are even harder to find).

Another point surrounding my master thesis research is communication. In specific, it involves communication with the university on the assessment of this work, appointing the supervisors and providing deliverables for review to them. Although in the end it all worked out, as communication went more smoothly once a predefined and agreed upon planning was maintained, the research and writing this thesis has been delayed by well over a year in total. If there would be just one thing to take with me from this experience, it is to clearly define and agree on goals, planning and deadlines up front for an efficient way of working. Luckily, I've learned way more than just this one thing on this journey.

Furthermore, although the framework is already rather practical due to its setup and the research methodology chosen (on which more in 21.4), I would have liked to have seen the framework actually implemented in order to assess its usability in yet an additional way. That having said, it is my understanding that this is not common for Master thesis research. What alleviates this urge is the knowledge that professionally, organizations have shown interest in the concept due to amongst others upcoming legislation, as discussed in 1.3. Perhaps I'll have a chance to guide an implementation in the not too far future.

21.2 The Framework

Seeing as the framework has been validated by various methods already, as discussed in the previous phase, and the conclusion was that it adheres to the requirements and demands it won't be discussed in too much detail here again. However, there are two additional topics worth mentioning here: physical and broader aspects.

21.2.1 Physical aspects

We've seen the framework and its underlying aspects validated by amongst others experts, and concluded that the framework succeeds in offering handles to achieve continuous forensic readiness without lacking any aspects. However, in hindsight I've realized the physical aspect is not mentioned in the framework.

By physical aspects we deem requirements for forensic readiness in the physical world. The most notable of these are the availability of a 'war room' where the responsible team is situated during incident response, and enough water/food to be brought in for this team once it is clear the incident will require substantial hours to be worked in the night.

These requirements are not included in the framework since these are not vital for *forensic readiness*. They are most definitely important for an efficient incident response, but are not essential for the forensic analysis as part of such a response following an IT incident. Furthermore, taking into account the mature IT environment as starting point, an incident response plan, facilities and procedures such as these should already be in place.

21.2.2 Broader aspects

On the other hand, taking another look at the framework it can be argued that some aspects are for a broader goal than just forensic readiness, such as *lessons learned* and *use knowledge base*. These aspects are mainly for an efficient team process, but not specific for forensic readiness and thus support a broader goal than the goal of this framework.

These requirements are included in the framework because they were deemed as important aspects for an efficient forensic analysis both by literature and experts. Therefore, besides their general contribution to more efficient incident response and any team process, they have a direct contribution to forensic readiness.

21.3 Case study

After several conversations via e-mail and in person it became clear that the university was willing to participate in the research, by acting as a 'light' case study. Although this initially seemed like a great addition – and I still find it fantastic to have had the time and ideas of all employees who participated and answered my questions – after some time it became clear to me that this kind of case study was not ideal. Whereas the framework was constructed to be broadly applicable and with the intention and need to refine it for every organization, which is common for more frameworks, the actual implementation was missing in this case study. The effectiveness and ease of implementation for the framework was validated as described in phase 3 of this research. However, whereas a case study is generally meant to show a proof of concept for a design, in this case the proof of concept was limited to a perceived ease of implementation by an organization instead of an actual implementation.

21.4 Research methodology

The research methodology chosen, Design Science as last refined by Wieringa, proved very promising at first. I was familiar with the methodology due to courses I followed in the Master program, and based on the subject I was researching it seemed like a perfect fit.

In all honesty, it was a good fit. When you want to design something, a scientific design method seems fair. The problem I experienced with the methodology though, is that at times it feels like a self-fulfilling prophecy. The first time I found it to work against me was when the rightful question was raised of what the failure criteria would be for this research, and if the research still had a right of existence in case of a failure. Of course, any research *can* fail.

Based on the Design Science principles, if you fail to meet the goals/desired future state then the research fails. However, these goals and/or desired state are all that will decide between success or failure. By defining these goals and/or future states yourself, in theory one can guarantee the research always succeeds.

Despite this inherent weakness, I feel comfortable stating that given the setup of the research and the validations that the quality of the validation phase was not impacted. Thereby its conclusion is also still valid, namely that the framework enables organizations to achieve continuous forensic readiness.

22 Summary

This phase of the research did not have any specific sub-questions which needed to be answered. Instead, this phase focused on evaluating the research performed.

In chapter 20 the usability of the framework beyond the University of Twente was discussed. Two essential aspects in the validation step according to design science, trade-off and sensitivity, were discussed. The conclusion is that the framework is still applicable both in a partial or alongside other frameworks implementation as well as in other environments than the University of Twente.

Chapter 21 evaluated the process followed in this research, as well as some topics regarding the framework itself which were not discussed in the validation phase. Briefly, essential lessons learned while performing the research were noted. Shortcomings and hindsight insight in both the framework and the process were discussed. Despite these shortcomings, the performed validation remains valid and the Continuous Forensic Readiness Framework does indeed support organizations in reaching and maintaining a state of continuous forensic readiness.

In the next part of this thesis, the final conclusion is provided.

V – Conclusion

23 Final Conclusion

Forensic readiness is the state of being prepared for forensic analysis. This thesis describes the research on the continuous forensic readiness framework, which allows an organization to achieve and moreover maintain a state of forensic readiness.

Despite business, legal and compliance reasons for organizations to pursue forensic readiness, academic publications on this topic are scarce. Publications which are available often do not describe steps how to reach such a state, but merely focus on a subset of relevant issues. In one paper steps are provided for reaching a state of forensic readiness, the aspects included are limited and do not mention how to maintain this state in the reality of an ever changing (IT) environment. Thus, this research set out to design a framework which gives organizations handles for how to achieve a state of forensic readiness and moreover maintain this state, as an holistic approach towards information security. Such a state is called continuous forensic readiness.

The goal for this research is therefore twofold: Firstly to enable organizations to have the required information available to perform adequate and timely analysis following IT incidents in a forensically sound manner, and secondly, to incorporate the forensic readiness controls identified in a governance framework to ensure organizations can maintain the state of forensic readiness.

In order to achieve these goals, the following questions were answered:

SQ 1. What do forensic analysts require for performing an adequate analysis?

By performing an academic literature study and conducting expert interviews, as described in chapters 4 and 5, a total of 44 aspects were identified, validated, categorized, prioritized and finally listed in chapter 6. A detailed description of all these aspects, as well as illustrative controls which serve as controls for the final goal namely the Continuous Forensic Readiness framework, are provided in section 6.2.

SQ 2. Taken into account the requirements identified in SQ1, what additional demands do organizations impose on a continuous forensic readiness framework?

As described in chapter 5, three main demands were identified by experts interviews and academic literature study, namely:

1. To minimally interrupt business;
2. to minimize the costs of forensics on incident response;
3. ensure investigations are cost efficient.

SQ 3. What forensic readiness models are currently available and to what extent do they help organizations to become continuously forensic ready?

Derived from literature study and expert interviews, as described in chapter 5, there are a limited amount of models currently available. However, these models do not suffice for an holistic approach to forensic readiness. Furthermore, the available models aim to become forensic ready as an endpoint, but disregard what to do from there on.

SQ 4. What leading governance models are currently available and how are they suited for forensic readiness?

The leading governance models COBIT 5, COSO ICF, COSO ERMF, ITIL v3, ASL/BiSL, ISO 2700x and ISGF were discussed in chapter 9. In itself these models were deemed unfit for forensic readiness, as described in chapter 10. However, the basic building blocks of governance models were considered useful and could be used to create a new framework with a specific focus on forensic readiness.

SQ 5. How do we fill the gap between the requirements/demands identified in SQ1/SQ2 and the solutions offered as identified in SQ3/SQ4?

To overcome the gaps, the Continuous Forensic Readiness Framework was introduced on a high level in chapter 11, where the governance building blocks used and the framework's overall working are presented. The process model, which contains the detailed activities following the PDCA cycles within the framework, was elaborated upon in chapter 12. A high level overview is shown in Figure 14.

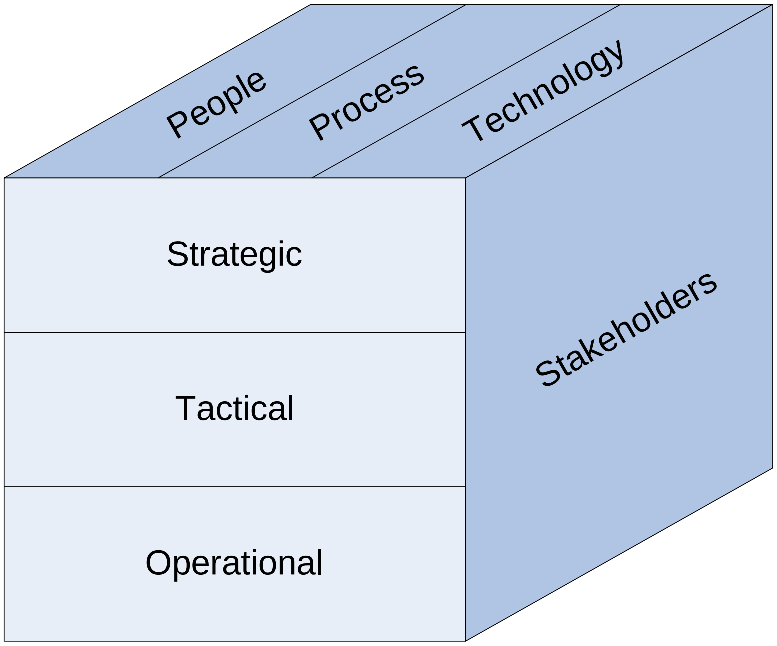


Figure 14: Continuous Forensic Readiness Framework

SQ 6. Does the proposed solution in SQ5 fulfill the needs identified in SQ1/SQ2?

The designed framework has been validated in three different ways. Firstly, the identified requirements were mapped to the solution as described in chapter 15, secondly, a round of interviews was held with a different set of experts, as described in chapter 16, and thirdly, chapter 17 describes the explorative case study which was performed at the University of Twente.

The main research question could then be answered:

How to construct a framework on continuous forensic readiness such that organizations are capable to (let) perform adequate analyses following an IT security incident?

The framework was designed as follows: First, requirements for forensic readiness were derived from literature and through experts interviews (chapters 4, 5 and 6), both from the forensic analysis point of view (SQ1) as well as organizational demands (SQ2). Currently available forensic readiness models were analyzed and determined how they aid in achieving a continuous state of forensic readiness (SQ3, chapters 4 and 5). Leading governance models were then analyzed and their fit for forensic readiness was determined (SQ4, chapters 9 and 10). The forensic readiness models available were denoted as incomplete and furthermore did not allow for a continuous state of forensic readiness. Currently available governance models were deemed unfit for forensic readiness. These identified gaps between SQ1/SQ2 and SQ3/SQ4 were filled by designing the Continuous Forensic Readiness Framework (SQ5, chapters 10, 11 and 12), which was then validated (SQ6, chapters 15, 16 and 17).

This research has contributed to academic literature by identifying a complete set of forensic readiness aspects and rating them to their importance. Furthermore, the Continuous Forensic Readiness Framework describes how organizations can maintain this state. The research's practical contribution is exactly this: by describing the forensic readiness controls and designing the control framework to go with it, it gives organizations concrete handles and instructions on how to achieve and maintain a state of forensic readiness.

The framework resulting from this research has reached the goals it set out to achieve: Based on the validation performed, it allows organizations to reach and maintain a state of forensic readiness.

23.1 Limitations and Future work

Every research has its limitations, this research is no exception.

Implementation

The main limitation of the research would be the lack of an actual implementation. Whereas the framework was validated in a variety of ways, no actual conclusion can be drawn from a real life implementation where minor and perhaps major issues may arise that were not noted by the experts interviewed. Therefore, in order to further validate the framework's workings and extract valuable lessons from practice, multiple case studies should be performed to determine how well an implementation will occur.

Other important aspects related to implementation are *cost* and *time*. During this research there has not been a focus on determining costs and time required for the implementation of the work. Although it has been noted that eventually costs for e.g. forensic analysis will drop if the preparations as laid out in the framework are performed, a quantitative measurement for implementation itself has and could not be made. For future research, this would be very interesting aspects to consider.

Additional validation

The amount of interviews conducted for this research has been substantial. Nonetheless, the validation interviews for each round (forensic aspects and the governance framework itself) were relatively limited (to respectively 9 and 7 interviews). Although the validation was performed in a qualitative manner rather than a statistical analysis with a quantitative approach, and no anomalies occurred in these, additional expert interviews could provide an even stronger basis for the framework.

Controls

The identified controls are described in a single dimension. They are sufficiently detailed for experts and our case implementers to make an assumption on ease of implementation. However, most control descriptions can be extended upon such that each control itself will actually have different maturity levels. Whereas this is currently not required, if the framework will be adopted by an organization it can certainly be of added value during implementation.

Different maturity level per control will also aid determining how well a certain control is implemented. Furthermore, a concrete test plan has not yet been defined. For an actual implementation and review of this implementation, the implementer will have to be able to measure when exactly controls are met.

Appendix A: Detailed Research Model

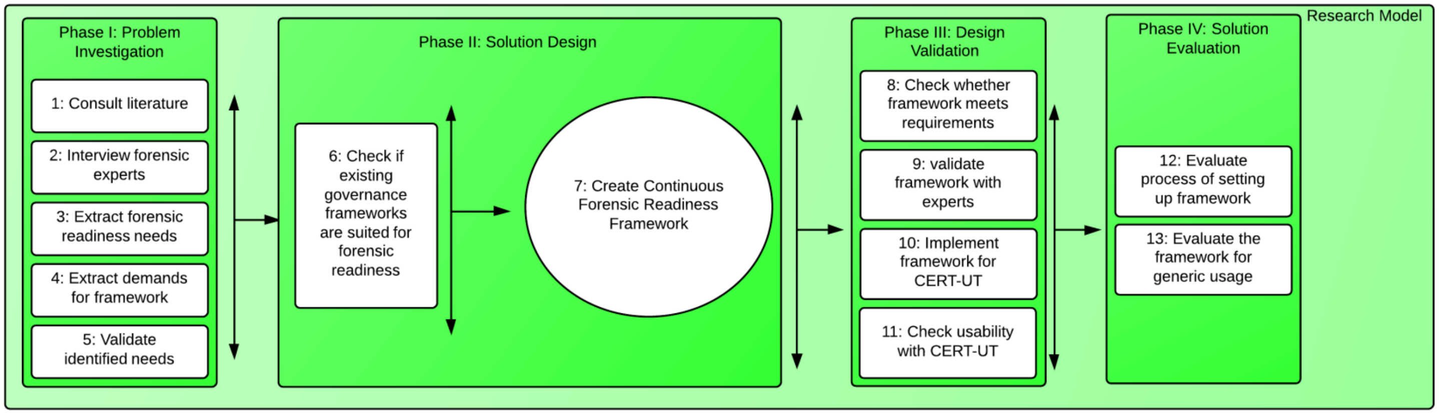

Research Model
Phase I: Problem Investigation
1: Consult literature
2: Interview forensic experts
3: Extract forensic readiness needs
4: Extract demands for framework
5: Validate identified needs
Phase II: Solution Design
6: Check if existing governance frameworks are suited for forensic readiness
7: Create Continuous Forensic Readiness Framework
Phase III: Design Validation
8: Check whether framework meets requirements
9: validate framework with experts
10: Implement framework for CERT-UT
11: Check usability with CERT-UT
Phase IV: Solution Evaluation
12: Evaluate process of setting up framework
13: Evaluate the framework for generic usage

Figure 15: Detailed Research Model

Appendix B: BCM aspects mapped to literature sources

Table 35: BCM aspects mapped to literature sources

Aspect	British Standards BS2599 [13]	Contingency Planning Guide for Federal Information Systems [85]	Business Continuity Management & Guidelines [93]	Optimization strategy for disaster recovery [130]	Business Continuity - Is it expensive and hard? [134]	Business Continuity and mission critical applications [10]	New Considerations for Security Compliance, Reliability and Business Continuity [76]	Business Continuity Planning (BCP) Methodology [33]
Team	✓	✓	✓	✓				✓
Training	✓	✓	✓				✓	
Awareness	✓	✓						✓
Policies & Procedures	✓	✓	✓	✓				✓
Risk analysis	✓	✓	✓	✓	✓		✓	✓
Determine goals up front	✓	✓	✓	✓	✓		✓	✓
Budgeting	✓	✓					✓	✓
Senior Management Level Support	✓	✓	✓				✓	
Legal						✓	✓	
Test plan	✓	✓	✓	✓			✓	✓
Prioritize incidents	✓	✓						
Situational awareness		✓		✓	✓			✓
Describe mandate to incident responder	✓	✓					✓	
Contact list whom to escalate to		✓	✓					

Document performed actions				✓			✓	
Include lessons learned	✓			✓				
Redundant hardware	✓	✓	✓			✓	✓	
Backups	✓	✓			✓		✓	

Appendix C: Incident response aspects mapped to literature sources

Table 36: IT incident response aspects mapped to literature sources

Aspects	Responding to Intrusions [18]	Incident Handling: An orderly response to unexpected events [100]	A framework for incident response [32]	Computer Security Incident Handling Guide [84]	ISO 27035 - Information security incident management [60]	On incident handling and response: A state-of-the-art approach	Security Situation Assessment and Response Evaluation (SSARE) [29]	An integrated approach to security incident management [42]	Preparation, detection and analysis: the diagnostic work of IT incident response [129]	Information security incident response [1]
Team		✓	✓	✓	✓	✓			✓	✓
Training	✓			✓	✓					
Awareness	✓	✓		✓	✓					
Policies & procedures	✓		✓	✓	✓	✓	✓			✓
Determine interesting data up front		✓			✓		✓		✓	✓
Risk analysis										
Determine goals up front				✓						✓
Budgeting			✓	✓						
Senior Management level support	✓			✓	✓	✓				
Legal	✓			✓	✓	✓				✓
Test plan	✓			✓	✓	✓				
Prioritize incidents				✓						

Maintain and use knowledge base				✓	✓				✓	
Situational awareness				✓					✓	
Describe mandate to incident responder	✓	✓	✓			✓			✓	
Contact list whom to escalate to		✓		✓	✓	✓				✓
Contact law enforcement	✓	✓								
Prepare standard documents	✓	✓	✓	✓	✓	✓				
Chain of custody	✓		✓		✓	✓				✓
Document actions taken		✓		✓	✓	✓		✓		✓
Secure communication available									✓	
Include lessons learned	✓	✓		✓	✓					
Time synchronization				✓						
Toolkit	✓		✓	✓	✓	✓			✓	
Logs	✓			✓	✓	✓			✓	✓
Remote logging				✓						
Log retention time				✓						
Compare trusted state of systems	✓			✓	✓	✓				

Normal behavior networks systems, applications				✓					✓	
Prepare infrastructure for response and analysis							✓			
Bit by bit copy			✓	✓	✓	✓				
From volatile to less volatile				✓						
Hashing	✓		✓	✓	✓	✓				
Maintain integrity of original data	✓		✓	✓	✓	✓				
Never work on primary copy	✓			✓	✓	✓				
Write blocker						✓				
Isolate compromised systems	✓			✓		✓				
Redundant hardware	✓		✓							
Backups	✓					✓				
Storage of evidence	✓		✓							

Appendix D: Forensic analysis aspects mapped to literature sources

Table 37: Forensic analysis aspects mapped to literature sources

Aspect	Advanced Framework for Digital Forensic Technologies and Procedures [115]	Digital Evidence Management Plan [46]	An Ad Hoc Review of Digital Forensic Models [94]	Two models of digital forensic examination [25]	Conducting Incident Post Mortems [105]	Specifying digital forensics: A forensics policy approach [112]	Research and review on Computer Forensics [51]	Policies to enhance computer and network forensics [138]	Computer Forensics In Forensis [92]	Guide to Integrating Forensic Techniques into Incident Response [87]	The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation [55]	A Control Framework for Digital Forensics [125]	A hierarchical, objectives-based framework for the digital investigations process [9]	Categories of digital investigation analysis techniques based on the computer history model [20]	A Formalization of Digital Forensics [70]	Management strategies for implementing forensic security measures [135]	Internet forensics: Legal and Technical Issues [65]	Methodological Frameworks of Digital Forensics [24]	Adding the Fourth "R": A Systems Approach to Solving the Hacker's Arms Race [34]
Team				✓	✓			✓		✓	✓	✓	✓			✓			
Training					✓		✓	✓		✓	✓	✓	✓			✓			
Awareness							✓	✓				✓				✓			
Policies & procedures	✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓		✓	✓			
Determine interesting data sources up front	✓	✓					✓			✓	✓	✓	✓			✓		✓	

Risk analysis	✓	✓					✓			✓	✓	✓	✓			✓		✓	
Determine purpose of investigation up front			✓			✓	✓			✓			✓						
Budgeting				✓	✓		✓				✓					✓			
Senior Management level support								✓		✓						✓			
Legal	✓	✓		✓		✓			✓	✓	✓	✓	✓		✓	✓	✓		✓
Test plan							✓			✓		✓							
Prioritize incidents					✓		✓						✓						
Maintain and use knowledge base															✓				
Situational awareness		✓				✓		✓			✓						✓		
Describe mandate to incident responder										✓		✓	✓			✓			
Contact list whom to escalate to												✓	✓			✓			
Contact law enforcement	✓																✓		
Prepare standard documents	✓		✓												✓	✓			
Chain of custody			✓				✓	✓		✓		✓	✓			✓	✓		✓
Investigative Actions							✓									✓		✓	
Include lessons learned			✓										✓		✓	✓			
Continually review security threats (external)																✓			
Time synchronization		✓	✓									✓	✓						
Toolkit	✓	✓	✓				✓		✓	✓	✓	✓	✓			✓	✓	✓	
Logs	✓			✓	✓			✓	✓	✓		✓		✓		✓	✓	✓	
Remote logging									✓	✓									
Log retention time													✓				✓		
Compare trusted state of systems			✓							✓			✓						
Proactive collecting useful data	✓					✓		✓		✓									
Bit by bit copy			✓		✓		✓	✓		✓		✓		✓		✓			

Collect volatile to less volatile			✓		✓					✓	✓	✓				✓			
Hashing	✓			✓			✓	✓	✓	✓		✓	✓			✓		✓	✓
Maintain integrity of original data	✓		✓				✓	✓		✓		✓				✓	✓	✓	
Never work on primary copy							✓	✓				✓						✓	
Write blocker							✓					✓	✓						
Backups													✓						
Storage of evidence	✓						✓	✓				✓	✓						
Periodic review of data source configuration										✓									

Aspect	Electronic Crime Scene Investigation First Responders [116]	Forensic Examination of Digital Evidence [117]	A Digital Forensic Investigative Model for Business Organisations [41]	Getting Physical with the Digital Investigation Process [21]	Computer Forensics Investigations in a Corporate Environment [103]	An Overview of Digital Security Forensics Approach and Modelling [53]	Defining a Process Model for Forensic Analysis of Digital Devices and Storage Media [4]	The Enhanced Digital Investigation Process Model [8]	An Examination of Digital Forensic Models [99]	Computer Forensics Model Based on Evidence Ring and Evidence Chain [73]	IS Auditing Guideline G28: Computer Forensics[57]	Guidelines for best practice in the forensic examination of digital technology [36]	Principles-Driven Forensic Analysis [91]	Digital Forensics Works [19]	RFC 3227 - Guidelines for Evidence Collection and Archiving [88]	An evaluation of agreement and conflict among computer forensics experts [16]	Deskundig en praktisch juridisch advies[37]	The question of organizational forensic policy [136]
Team		✓		✓	✓			✓		✓		✓						✓
Training	✓	✓	✓	✓				✓	✓			✓						
Awareness			✓		✓							✓						
Policies & procedures	✓	✓			✓				✓		✓	✓						✓
Determine interesting data sources up front						✓			✓				✓					
Risk analysis						✓			✓				✓					

Determine purpose of investigation up front			✓					✓	✓		✓	✓				✓		
Budgeting		✓																✓
Senior Management level support																		✓
Legal					✓	✓	✓		✓	✓		✓				✓	✓	
Contact list whom to escalate to					✓													
Contact law enforcement		✓			✓													
Prepare standard documents	✓	✓			✓			✓	✓		✓					✓		
Chain of custody	✓	✓	✓		✓				✓	✓		✓		✓	✓	✓	✓	✓
Investigative Actions	✓	✓	✓		✓			✓				✓				✓		✓
Time synchronization		✓	✓	✓			✓	✓							✓			
Toolkit		✓	✓	✓	✓		✓	✓	✓		✓	✓	✓	✓	✓	✓		
Logs			✓	✓	✓	✓	✓				✓		✓	✓				
Remote logging			✓	✓														
Ensure dynamic logging ability				✓														
Compare trusted state of systems				✓														
Prepare infrastructure for forensics				✓				✓			✓			✓				
Bit by bit copy		✓	✓	✓	✓		✓	✓	✓		✓	✓		✓	✓	✓		
Collect volatile to less volatile											✓				✓			
Hashing			✓	✓			✓	✓				✓			✓	✓	✓	✓
Maintain integrity of original data	✓	✓	✓	✓		✓		✓			✓	✓		✓	✓	✓		✓
Never work on primary copy			✓					✓						✓	✓	✓		
Write blocker		✓					✓				✓					✓		
Redundant hardware		✓	✓	✓	✓						✓					✓		
Backups																✓		
Storage of evidence							✓					✓						
Packaging for transport	✓																	

Appendix E: Forensic readiness aspects mapped to literature sources

Table 38: Forensic readiness aspects mapped to literature source

Aspect	The Proactive and Reactive Digital Forensics Investigation Process: A Systematic Literature Review [2]	Examining the state of preparedness of Information Technology Management in New Zealand for events that may require forensic analysis [97]	Digital Forensic Readiness: An insight into Governmental and Academic Initiatives [80]	Case study: Network intrusion investigation - lessons in forensic preparation [22]	Digital Forensic Readiness as a Component of Information Security Best Practice [47]	A multi-component view of Digital Forensics [49]	Embedding Forensic Capabilities into Network [35]	A framework to guide the implementation of Proactive Digital Forensics in organizations [48]	A Ten Step Process for Forensic Readiness [101]	Forensic Readiness [111]	Measures of retaining digital evidence to prosecute computer-based cyber-crimes [126]	Information Assurance and Forensic Readiness [90]	The importance of Corporate Forensic Readiness in the information security framework [89]	Six Mistakes of Log Management [23]	Guide to Computer Security Log Management [86]
Team		✓		✓	✓	✓		✓	✓			✓			
Training		✓	✓	✓	✓	✓	✓	✓	✓				✓		
Awareness		✓			✓	✓	✓						✓		
Policies & Procedures		✓	✓	✓	✓	✓	✓	✓	✓				✓		✓
Determine interesting data up front	✓		✓		✓	✓	✓	✓	✓			✓	✓		
Risk analysis	✓		✓		✓	✓	✓	✓	✓			✓	✓		

Determine purpose of investigation up front			✓	✓					✓						
Budgeting		✓				✓									
Senior Management level support					✓				✓				✓		
Legal			✓		✓	✓	✓	✓	✓		✓	✓	✓		✓
Test plan			✓		✓		✓					✓			
Prioritize incidents				✓											
Maintain and use knowledge base			✓	✓		✓		✓							
Situational awareness			✓	✓						✓					
Describe mandate to incident responder						✓		✓							
Contact list whom to escalate to			✓	✓											
Contact law enforcement				✓					✓						
Chain of custody			✓		✓	✓	✓			✓	✓		✓		

Investigative Actions				✓		✓									
Secure communication available									✓						
Include lessons learned				✓											
Time synchronization										✓					
Toolkit				✓	✓	✓	✓	✓		✓	✓				
Logs		✓		✓		✓			✓	✓	✓			✓	✓
Remote logging									✓	✓					✓
Log retention time									✓	✓				✓	✓
Ensure dynamic logging ability															✓
Proactive collecting useful data	✓								✓				✓		
Prepare infrastructure for forensics			✓			✓						✓			
Bit by bit copy				✓						✓	✓				
Collect volatile to less volatile										✓					
Hashing				✓		✓				✓	✓	✓			
Maintain integrity of original data			✓			✓	✓		✓		✓	✓			

Never work on primary copy										✓	✓				
Isolate compromised systems			✓												
Redundant hardware										✓					
Backups										✓		✓			
Storage of evidence		✓		✓		✓			✓	✓					

Appendix F: Interviews

Introduction

Besides literature, interviews were conducted for both the creation and the validation stage in this research. For these interviews, the following had to be performed:

1. Define goals
2. Set up the questions
3. Find appropriate people to interview
4. Analyze the results

These steps are discussed in the following sections.

Goals

The following goals were defined:

For every interview:

- Extract demands for the continuous forensic readiness framework;
- Determine business demands for the framework.

Additionally, for interviews with CERT-UT:

- Determine current organization and approach to forensic analysis & forensic readiness.

For the interviews with forensic experts:

- How a forensic analysis is performed, and extract requirements following those steps;
- Current best practices to become forensic ready.

Interview questions

The goals for the interviews served as the basis for the questions. Together with initial talks with a forensic expert at KPMG about the problems often facing analysis and a thorough literature review the questions were setup. The total list of questions is available at the end of this appendix.

People interviewed

The people interviewed were contacted based on their profession and experience within the field. Different type of experts were needed for this research. Firstly a CERT-UT employee was needed to determine the current situation at the Universiteit Twente. Secondly forensic experts were needed to determine how they handle forensic analysis and what they need for those actions, as well as another group of forensic experts to validate the findings. These experts were found in a variety of companies.

Thirdly governance experts were needed to get a feeling for the framework. A list of people interviewed is given in Table 39, sorted by for what purpose they were spoken.

Table 39: Interviews

Date	#	Organization	Job title	Topic of interview
		Framework Requirements		
06/08/2012	1	NCSC	Senior Security Specialist	Incident response, forensic analysis
06/08/2012	2	NCSC	Security Specialist	Incident response, forensic analysis
06/08/2012	3	NCSC	Security Specialist	Incident response, analysis, (forensic) tools
07/05/2012	4	KLPD High Tech Crime Unit	Projectleader, Digital Specialist	Forensic analysis
12/06/2012	5	Nationaal Forensisch Instituut (NFI)	Data Analysis Researcher	Forensic analysis
12/06/2012	6	Nationaal Forensisch Instituut (NFI)	Data Analysis Researcher	Forensic analysis
22/06/2012	7	Fox-IT	Senior Forensic Analyst	Forensic analysis
		University of Twente/UT-CERT Case		
06/07/2012, 01/07/2013	8	Universiteit Twente	CERT-UT Officer, Security Manager	CERT-UT setup, IT governance at UT, requirements.
30/08/2012	9	Universiteit Twente	IT Auditor	Governance models, IT governance at UT, internal audits, controls
14/08/2013	10	Universiteit Twente	Information Manager, Security Officer	Policies at and applicability for UT.
		Governance		
29/05/2012	11	Considerati	Managing Partner	Governance, regulation, forensics
27/08/2012	12	KPMG	Manager IT Advisory	Governance, governance models
27/04/2012	13	CapGemini	Consultant	Governance, governance models
		Framework validation		
03/09/2012	14	Ernst & Young	Senior Manager Forensics	Validate forensic demands
24/08/2012	15	KPMG	Technical Forensics Investigator	Validate forensic demands
24/08/2012	16	KPMG	Technical Forensics Investigator	Validate forensic demands
23/05/2013	17	CC Bill	Lead security Analyst	Validate forensic demands
28/06/2013	18	Fox-IT	Senior Forensic IT expert	Validate forensic demands
26/09/2012	19	Fox-IT	Forensic IT expert	Validate forensic demands
08/07/2013	20	Nationaal Forensisch	Data Analysis Researcher	Validate forensic demands

		Instituut (NFI)		
08/03/2013, 17/07/2013	21	CZ	Adviseur Informatie-beveiliging	Validate forensic demands & control framework
17/07/2013	22	Van Landschot Bankiers	Security Manager	Validate forensic demands & control framework
11/06/2013	23	Booking.com	Corporate Security Officer	Validate control framework
04/07/2013	24	FrieslandCampina	Senior Manager Internal Audit	Validate control framework
01/07/2013	25	KPMG	Advisor Information Protection Services	Validate control framework
05/08/2013	26	KPMG	Advisor Information Protection Services	Validate control framework
05/07/2013	27	KPMG	Manager Information Protection Services	Validate control framework

Questions

The following topics were discussed during the semi-structured interviews.

- Naam, functie, bedrijf
- Toestaan met naam en toenaam in verslag op te nemen, of liever anoniem?
- Omschrijving werkzaamheden als professional
- Hoe lang al actief als forensisch analist?
- Wat voor forensische analyses doet u? (Reactief/pro-actief)
- Ingeroepen na incident / Proactief naar bedrijven toe na eigen constatering?
- Na oproep, wat komt u zoal tegen – chaos of structurele response?
- Wat zou een bedrijf allemaal klaar moeten hebben zodat u direct aan forensische analyse kan beginnen?
- Welke aspecten horen hierbij? (Zelf denk aan Technische, Beleidsmatig/Process, Legal)
- Technisch (zoals bijv: Logging (Host, Applicatie, OS, Netwerk, Firewall, Router, Etc.), Tooling?, Bit-by-bit copies bijv, als bedrijf zijnde zelf al maken?, In literatuur een 'emergency kit' met schone laptop, etc?, Iets anders?)
- Beleidsmatig / process? (Bijv; beslissing uitzetten ja/nee, business of IT? Pre-defined of ad-hoc?, Forensische analyse opgenomen in response plan bijvoorbeeld?, Überhaupt, verantwoordelijkheid over forensic readiness?)
- Legale issues/keuzes? (As-in, wel of niet vervolgen?)
- Behandeling bewijs goed omschreven (chain of custody preservation)
- Zijn er dingen vaak niet aanwezig?
- Reden waarom bekend?
- Kosten?
- IT vs Business (= geen alignment)?
- Hoe gaat u bij een forensische analyse te werk?
- Standaard procedure/checklist?

- Wat voor gegevens kijken jullie naar?
- Wat voor data zouden jullie graag naar willen kijken maar is er vaak niet?
- Andere benodigdheden?
- Tools?
- Overige resources die bedrijf moet leveren?
- Veel voorkomende situaties?
- Specifieke eisen aan data?
- Bijv, hoe lang logs worden bewaard?, Van welke data wil je logs?, Alle systemen of alleen de bekende gecomprimeerde?, Etc.
- Legale issues?
- Belangrijke aspecten indien als bewijs moet/wil worden gebruikt?
- Dingen die daarin mis gaan bij bedrijven?
- Voor zover bekend, regelgeving die bedrijven verplicht ‘forensic ready’ (of iets dergelijks) te zijn?
- Al tools die bewijsmateriaal ‘veilig stellen’?
- Welke?
- Hoe efficiënt?
- Aanbevelingen a.d.h.v. situaties die u reeds gezien heeft?
- Idee hoe forensic readiness te enforcen bij bedrijven? (Bijv; business value aantonen?)
- Bedrijfsstructuur van belang? (rol CIO / CISO, bijvoorbeeld?)

Appendix G – Validation form

Introduction

Dear reader,

First off all: thank you for participating in the validation for (part of) my master thesis! For this validation you will need this document together with the description of the requirements, in the *Forensic Readiness Aspects.pdf* file.

My thesis research is about *Continuous Forensic Readiness*, where we are looking at forensic analysis as part of an incident response. This is an action for which we can prepare, which is known as becoming *forensically ready*. In order to create a control framework achieving this goal, I have determined a list of requirements for forensic readiness based on a thorough literature review and interviews held with forensic analysts. Some of the requirements you will encounter may however not be specific requirements for a forensic analysis, but are more closely related to incident handling. These were specifically mentioned by experts or literature as essential aspects, and were thus added for this overview.

Please read the document *Forensic Readiness Aspects* and then answer the questions below. The filled in form can be returned to j.a.w.dewit@student.utwente.nl. Thank you! -Jeroen

Personal Information	
Name	
Organization	
Job title	
Work experience	

In my thesis I will, due to previous request, only mention your organization, job title and work experience. Your name is purely for my own administration and will not be disclosed. If you would like other aspects to not be disclosed, please let me know.

Instructions

Starting on the next page, you'll find the requirements divided in the categories People, Process and Technology. Please check the list for completeness. If you feel there are aspects missing, please add them. If you feel that elements are superfluous and do not belong to the requirements for forensic analysis or are of no added value, please indicate that they should be removed and provided a reason why. Please take into account that these requirements are not meant as a minimum baseline to be achieved, but rather aim for preparing for forensic analysis as much as possible. In your view, some may thus add only a very limited aspect, but still add something to the level of preparedness nonetheless.

In the last column, 'effectiveness', please indicate on a scale from 1 – 5 how effective you think each requirement is with regard to preparing for a forensic analysis, aka becoming forensically ready.

Requirement	Remove	Reason for removal	Effectiveness
People			
Team			
Training			
Awareness			
Senior Management Level Support			
Process			
Before			
Policies & Procedures			
Determine interesting data sources up front			
Risk analysis			
Determine purpose of investigation up front			
Budgeting			
Legal			
Test plan			
Prepare infrastructure for forensics			
Begin			
Prioritize incidents			
Maintain and use knowledge base			
Situational awareness			
Describe mandate to incident responder			
During			
Contact list whom to escalate to			
Contact with law enforcement			
Prepare standard documents			
Chain of custody			
Investigative actions			
Secure communication available			
After			
Include lessons learned			

Other			
Continually review security threats (external)			
Technology			
Before			
Time synchronization			
Toolkit			
What is logged			
Remote logging			
Log retention time			
Ensure dynamic logging ability			
Compare trusted state of systems			
Normal behavior network, systems, applications			
Proactive collecting useful data			
Begin			
Bit-by-bit copy			
Collect volatile to less volatile			
Hashing			
During			
Maintain integrity of original data			
Never work on original or primary copy			
Write blocker			
Isolate compromise systems			
After			
Redundant hardware			
Backups			
Storage of evidence			
Packaging for transport			
Other			
Periodic review of data source configuration			

In the table below, please indicate your top 5 of most relevant requirements.

#	Requirement
1	
2	
3	
4	
5	

Further feedback

If you have any further feedback, please feel free to provide it below:

Appendix H: Mapping of aspects to sources

In Table 40 the aspects are mapped to their sources. The numbers A through G indicate experts interviewed (see Appendix F: Interviews).

Table 40: Mapping of requirements to sources

#	Requirement	Source							
		Literature	A	B	C	D	E	F	G
People									
Layer 1									
RQ1	Team	[1, 8, 9, 13, 17, 21, 22, 25, 32, 33, 36, 47-50, 55, 60, 64, 73, 79, 84, 85, 87, 90, 93, 97, 100, 101, 103, 105, 106, 114, 117, 123, 125, 129, 130, 135, 136, 138]	✓	✓		✓	✓		✓
RQ2	Training	[8, 9, 13, 17, 18, 21, 22, 35, 36, 41, 47-51, 55, 60, 76, 80, 84, 85, 87, 89, 93, 97, 99, 101, 105, 116, 117, 125, 135, 138]	✓					✓	✓
Layer 2									
RQ3	Awareness	[13, 17, 18, 33, 35, 36, 41, 47, 49, 51, 60, 84, 85, 89, 97, 100, 103, 123, 125, 127, 135, 138]		✓	✓	✓			
RQ4	Senior Management Level Support	[13, 17, 18, 47, 50, 60, 64, 76, 79, 84, 85, 87, 89, 93, 101, 106, 123, 135, 136, 138]			✓			✓	✓
Process									
Layer 1									
RQ5	Risk analysis	[1, 2, 9, 13, 17, 24, 29, 33, 35, 46-49, 51, 53, 55, 60, 76, 80, 85, 87, 89-91, 93, 99-101, 106, 114, 115, 123, 125, 129, 130, 134, 135]	✓	✓					
RQ6	Policies & Procedures	[1, 7, 9, 13, 17, 18, 22, 25, 29, 32, 33, 35, 36, 46-51, 57, 60, 64, 70, 79, 80, 84-87, 89, 92-94, 97, 99, 101, 103, 106, 112, 114-117, 123, 125, 130, 135, 136, 138] [8, 19, 21, 29, 49, 57, 80, 90, 114, 123]		✓	✓		✓	✓	✓
RQ7	Budgeting	[13, 25, 32, 33, 49-51, 55, 76, 84, 85, 97, 105, 117, 123, 127, 135, 136]			✓				
RQ8	Prioritize incidents	[9, 13, 17, 22, 51, 64, 84, 85, 105]		✓	✓				
RQ9	Chain of custody	[1, 9, 16-19, 32, 34-37, 41, 47, 49, 51, 60, 65, 73, 79, 80, 87-89, 94, 99, 103, 111, 116, 117, 125, 126, 135, 136, 138]	✓	✓	✓	✓	✓	✓	✓
RQ10	Investigative actions	[1, 8, 16, 22, 24, 36, 41, 42, 49, 51, 60, 64, 76, 79, 84, 100, 103, 116, 117, 130, 135, 136]			✓			✓	✓
Layer 2									

RQ11	Determine interesting data sources up front	[1, 2, 9, 13, 17, 24, 29, 33, 35, 46-49, 51, 53, 55, 60, 76, 80, 85, 87, 89-91, 93, 99-101, 106, 114, 115, 123, 125, 129, 130, 134, 135]	✓	✓					
RQ12	Determine purpose of investigation up front	[1, 8-10, 13, 16, 17, 22, 33, 36, 41, 51, 57, 80, 84, 85, 87, 94, 99, 101, 112, 130]	✓	✓	✓			✓	
RQ13	Legal	[1, 4, 9, 10, 16-18, 25, 34-37, 46-49, 53, 55, 60, 65, 70, 73, 76, 79, 80, 84, 86, 87, 89, 90, 92, 99, 101, 103, 112, 114, 115, 125, 126, 135]	✓	✓		✓		✓	✓
RQ14	Test plan	[13, 17, 18, 33, 35, 47, 51, 60, 76, 79, 80, 84, 85, 87, 90, 93, 125, 130]	✓						✓
RQ15	Situational awareness	[22, 33, 46, 55, 65, 80, 84, 85, 106, 111, 112, 114, 129, 130, 134, 138]	✓	✓	✓			✓	✓
RQ16	Describe mandate to incident responder	[9, 13, 18, 32, 48-50, 76, 79, 85, 87, 100, 125, 129, 135]		✓		✓		✓	
RQ17	Contact list whom to escalate to	[1, 9, 17, 22, 60, 79, 80, 84, 85, 100, 103, 125, 135]		✓	✓	✓	✓		
RQ18	Prepare standard documents	[8, 16-18, 32, 57, 60, 70, 79, 84, 94, 99, 100, 103, 115-117, 135]							
RQ19	Include lessons learned	[9, 13, 18, 22, 60, 64, 70, 84, 94, 100, 106, 130, 135]				✓	✓	✓	
Layer 3									
RQ20	Maintain and use knowledge base	[22, 48, 49, 60, 64, 70, 80, 84, 129]				✓	✓	✓	
RQ21	Contact with law enforcement	[18, 22, 65, 100, 101, 103, 115, 117]		✓	✓	✓	✓		
RQ22	Secure communication available	[17, 101, 129]						✓	✓
RQ23	Continually review security threats (external)	[135]		✓	✓	✓	✓		
Technology									
Layer 1									
RQ24	Time synchronization	[4, 8, 9, 21, 41, 46, 84, 88, 94, 111, 117, 125]				✓	✓	✓	✓
RQ25	What is logged	[1, 4, 17-25, 41, 49, 53, 57, 60, 65, 79, 84, 86, 87, 91, 92, 97, 101, 103, 105, 111, 115, 125, 126, 129, 135, 138]	✓	✓	✓	✓	✓	✓	✓
RQ26	Bit-by-bit copy	[4, 8, 16, 17, 19-22, 32, 36, 41, 51, 57, 60, 79, 84, 87, 88, 94, 99, 103, 105, 111, 117, 125, 126, 135, 138]	✓	✓			✓	✓	✓
RQ27	Collect volatile to less volatile	[55, 57, 84, 87, 88, 94, 105, 111, 125, 135]					✓		
RQ28	Hashing	[4, 8, 9, 16-18, 21, 22, 24, 25, 32, 34, 36, 37, 41, 49, 51, 60, 79, 84, 87, 88, 90, 92, 111, 115, 125, 126, 135, 136, 138]	✓	✓			✓	✓	✓

RQ29	Maintain integrity of original data	[8, 16, 18, 19, 21, 24, 32, 35, 36, 41, 49, 51, 53, 57, 60, 65, 79, 80, 84, 87, 88, 90, 94, 101, 115-117, 125, 126, 135, 136, 138]	✓	✓			✓	✓	✓
RQ30	Never work on original or primary copy	[8, 16, 18, 19, 24, 41, 51, 60, 79, 84, 88, 111, 125, 126, 138]	✓						
Layer 2									
RQ31	Toolkit	[4, 8, 9, 16-19, 21, 22, 24, 32, 35, 36, 41, 46-49, 51, 55, 57, 60, 64, 65, 79, 84, 87, 88, 91, 92, 94, 99, 103, 111, 115, 117, 123, 125, 126, 129, 135]		✓			✓	✓	✓
RQ32	Remote logging	[21, 41, 84, 86, 92, 101, 111]	✓				✓	✓	✓
RQ33	Log retention time	[9, 23, 65, 84, 86, 101, 111]	✓	✓					
RQ34	Write blocker	[4, 9, 16, 51, 57, 79, 117, 125]					✓		
RQ35	Isolate compromise systems	[18, 79, 80, 84]							✓
RQ36	Backups	[9, 13, 16, 18, 76, 79, 85, 90, 111, 114, 134]	✓					✓	✓
RQ37	Storage of evidence	[4, 9, 18, 22, 32, 36, 49, 51, 97, 101, 111, 115, 125, 138]					✓		
RQ38	Packaging for transport	[116]							
RQ39	Periodic review of data source configuration	[87]						✓	✓
Layer 3									
RQ40	Ensure dynamic logging ability	[21, 86]							✓
RQ41	Compare trusted state of systems	[9, 17, 18, 21, 60, 79, 84, 87, 94, 114]						✓	
RQ42	Normal behavior network, systems, applications	[84, 129]	✓						✓
RQ43	Proactive collecting useful data	[2, 87, 89, 101, 112, 115, 138]							✓
RQ44	Redundant hardware	[10, 13, 16, 18, 21, 32, 41, 57, 76, 85, 93, 103, 111, 117]							✓

Appendix I: Basic Building Blocks Governance Models

Table 41: Governance Frameworks building blocks

Framework	Building block	Description
COBIT	Evaluate, Direct and Monitor (EDM)	Ensure governance framework setting and maintenance, benefits delivery, risk optimization, resources optimization and stakeholder transparency. Ensures needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved, sets direction and monitors performance and compliance against the objectives.
	Align, Plan and Organize (APO)	Manages the IT management framework, strategy, enterprise architecture, innovation, portfolio, budget and costs, human resources, relationships, services agreements, suppliers, quality, risk and security. Concerns identification of how IT can best contribute to achievement of the business objectives.
	Build, Acquire and Implement (BAI)	In order to realize the IT strategy, this dimension manages programs and projects, requirements definition, solutions identification and build, availability and capacity, organizational change enablement, changes, change acceptance and transition, knowledge, assets and configuration.
	Deliver, Service and Support (DSS)	Concerned with actual delivery of required services, domain manages operations, services requests and incidents, problems, continuity, security services and business process controls.
	Monitor, Evaluate and Assess (MEA)	Monitors, evaluates and assesses the performance and conformance, system of internal control and compliance with external requirements.
COSO ICF	Operations, Financial Reporting, Compliance	The objectives the framework tries to achieve
	Stakeholders	Stakeholders that are involved to create internal control
	Control Environment	The foundation of the organization, including ethical values, integrity and competence of people
	Risk Assessment	Identification and analysis of relevant risks to the achievement of an organizations' objectives
	Control Activities	Policies and procedures that help ensure activities are performed correctly
	Information & Communication	Relevant information must be identified and communicated, also includes reports generated by IT systems.
	Monitoring	Monitoring of the internal controls.
COSO ERMF	Strategy, Operations, Reporting, Compliance	The objectives the framework tries to achieve

	Stakeholders	Stakeholders that are involved to create internal control
	Internal Environment	Describes the tone of an organization and sets the basis for how risk is viewed and addressed.
	Objective Settings	Objectives must exists before potential events affecting their achievement can be identified.
	Event Identification	Internal and external events affecting the achievement of objectives must be identified, whereby distinguishing between risks and opportunities.
	Risk Assessment	Risks are analyzed looking at their likelihood and impact, to determine how to manage them.
	Risk Response	Risk response is selected – avoiding, accepting, reducing or sharing – by developing action aligning with the organization's risk tolerance and risk appetite.
	Control Activities	Policies and procedures are established and implemented to ensure the responses are effectively executed.
	Information & Communication	All relevant information is identified, capture and communicated in a form and time frame such that people are capable to carry out their responsibilities.
	Monitoring	Monitoring of the internal controls.
ITIL	Service Strategy	The achievement of strategic goals or objectives requires the use of strategic assets
	Service Design	Design IT services, along with the governing IT practices, processes and policies, to realize the strategy and facilitate the introduction of services into the live environment ensuring quality service delivery, customer satisfaction and cost-effective service provision
	Service Transition	The development of capabilities for transitioning new and changed services into operations, ensuring the requirements of Service Strategy, encoded in Service Design, are effectively realized in Service Operations while controlling the risks of failure and disruption
	Service Operation	Achieving effectiveness and efficiency in the delivery and support of services to ensure value for the customer and the service provider
	Continual Service Improvement	Creating and maintaining value for customers through better design, introduction and operation of services, linking improvement efforts and outcomes with Service Strategy, Design, Transition and Operation
ASL	Strategic, Tactical, Operational	Management levels within which the model works
	Organization Cycle Management	Aimed at development of future vision, and translation of that vision to policy. Elements are defining Account & Market, Supplier, Technology, Capabilities and finally Service Delivery
	Applications Cycle Management	Strategy for customer organizations, ICT developments and customer environment, application portfolio management and application life cycle management
	Management Processes	The translation of policy into actions. Contract Management, Planning and Control, Quality

		Management, Financial Management and Supplier Management
	Maintenance Processes	Aimed at the day-to-day optimal use of applications. User Support, Continuity Management, Operational ICT Control, Configuration Management
	Enhancement and Renovation processes	Ensures necessary adjustments to applications. Impact Analysis, Design, Realization, Test, Implementation
	Connecting processes	Change Management, Program Management and Distribution
BiSL	Strategic, Tactical, Operational	Management levels within which the model works
	Develop I-organization strategy	Meant to define how control of information is organized. Manage user organization relations, define strategy I-organization, manage supplier relations, manage partner chain relations
	Information coordination	Meant for alignment on a strategic level
	Develop information strategy	Meant to translate developments in the organization and its environment into a strategy on information for the mid and long term. Define partner chain developments, define technological developments, manage information lifecycle, manage information portfolio, define business process developments
	Management processes	Planning & Control, Financial Management, Demand Management, Contract Management
	Use management	Provide an optimal and continuous support of the business processes. Support Users, Manage Business Data, Manage IT Supplier
	Alignment processes	Meant for alignment on an operational level through Change Management and Transition Management
	Functionality management	Aim is to guide and realize changes in information services. Specify requirements, Design non-automated information system, Prepare transition, Review and test
ISO 27000 family	Plan-Do-Check-Act Cycle	Cycle acting as the basis for implementation and is applied to structure all ISMS processes
	Establish, implement, operate, monitor, review, maintain, improve	Important states relating to the implementation cycle
	Security policy	Provide management with direction and support for information security in accordance with business requirements and relevant laws and regulations
	Organizing Information Security	To manage information security within the organization, as well as maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties
	Asset Management	To achieve and maintain appropriate protection of organizational assets

	Human Resources Security	To ensure employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities. Covers phases prior to, during and after employment
	Physical and Environmental Security	To prevent unauthorized physical access, damage and interference to the organization’s premises and information as well as prevent interruption to the organization’s activities
	Communications and Operations Management	To ensure the correct and secure operation of information processing facilities and minimize risk of failure and protect integrity of software and information.
	Access Control	Ensure authorized user access and to prevent unauthorized access to information systems and information
	Information Systems Acquisition, Development and Maintenance	To ensure security is an integral part of information systems, and to prevent errors, loss, unauthorized modifications or misuse of information in applications
	Information Security Incident Management	Ensure information security events and weaknesses are handled effectively and consistent
	Business Continuity Management	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption
	Compliance	To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements with regards to organizational policies and standards
ISGF	Direct & Control	Together with ‘Execute’, these elements form the main cycle upon which the entire governance framework is build
	Strategic, Tactical, Operational level	The management levels requiring action for implementing the framework
	People/Actions/Leveled risk	These are important aspects with regards to information security, and not discussed in detail the paper but merely mentioned as important aspects. However, their meanings are clear from a security perspective
	Best Practices	
	Organization	
	Awareness	

Appendix J: Analysis University of Twente

In this appendix the current situation at the University of Twente, and in specific the CERT-UT is described. Furthermore, relevant stakeholders for the University of Twente with regards to forensic readiness are identified. Also the governance framework used within the UT is discussed.

Incident response

The University of Twente has its own Computer Emergency Response Team, the CERT-UT, which handles all IT incidents. The team consists of seven core members, which serve as the second line responders in rotation shifts with 1 – 4 hours per week each, and five operators which are the first line responders available during office hours. These operators are students who respond to notifications to the ICT support desk, which can include security incidents. All second line responders have a technical background, but with a variety in specialties. The CERT's current work consists mostly of reactive tasks and a minor amount of education.

In case of a security incident the operator decides whether to put this through to the CERT-UT or handle it himself by putting the computer in Quarantainenet[1]. If the incident is too complicated to be handled by a first line responder, it is put through to the CERT-UT, the officer on duty will handle the response. Depending on the nature of the incident he will either take care of it himself or put it through to another CERT-UT member with the proper skills. In case the internal knowledge is insufficient, contact is sought with SURFCERT, an overarching CERT for all institutions connected to SURFNet.

The CERT-UT is commissioned by the Executive Board to take care of all IT incidents [122]. As such, they are allowed to decide themselves how to solve and handle incidents, including the decision whether to prosecute or not. However, the main focus of the CERT-UT is continuity. In order to set clear goals they have made agreements with the business owners of systems about certain response times and incident resolving times. For instance, the education information systems Blackboard and Osiris have different response necessities than the e-mail server. Furthermore, systems such as Blackboard may have different response necessities for different moments in time, e.g. near test weeks these systems have higher priorities than at the beginning of the teaching quartile.

The CERT-UT has so far had limited experience with forensic investigations. In the past they have provided law enforcement with data and a memory dump of a victim computer, but as mentioned they mostly just mitigate the problem as soon as possible without worrying about forensic analysis. A partial reason is the limited time and budget they have: just acquiring the needed data might already take their maximum of 4 hours in the week, thus making it infeasible for an adequate analysis. Therefore for each incident, in the consideration to further investigate the responder's opinion on whether or not it will have any use to potentially prosecute the attacker will strongly count in the final decision. The decision to report a crime, press charges and/or investigate further is made by the head of Infra, their direct boss, who relies on advice given by the CERT-UT. In all these cases law enforcement is contacted: they

[1] A network management and control system which can separate computers from the rest of the network http://www.quarantainenet.nl/

do not perform forensic analysis themselves either. As a result, they also do not specifically prepare for forensic analysis. The IT Incident Response Process as described above is graphically depicted in the flowchart in Figure 16.

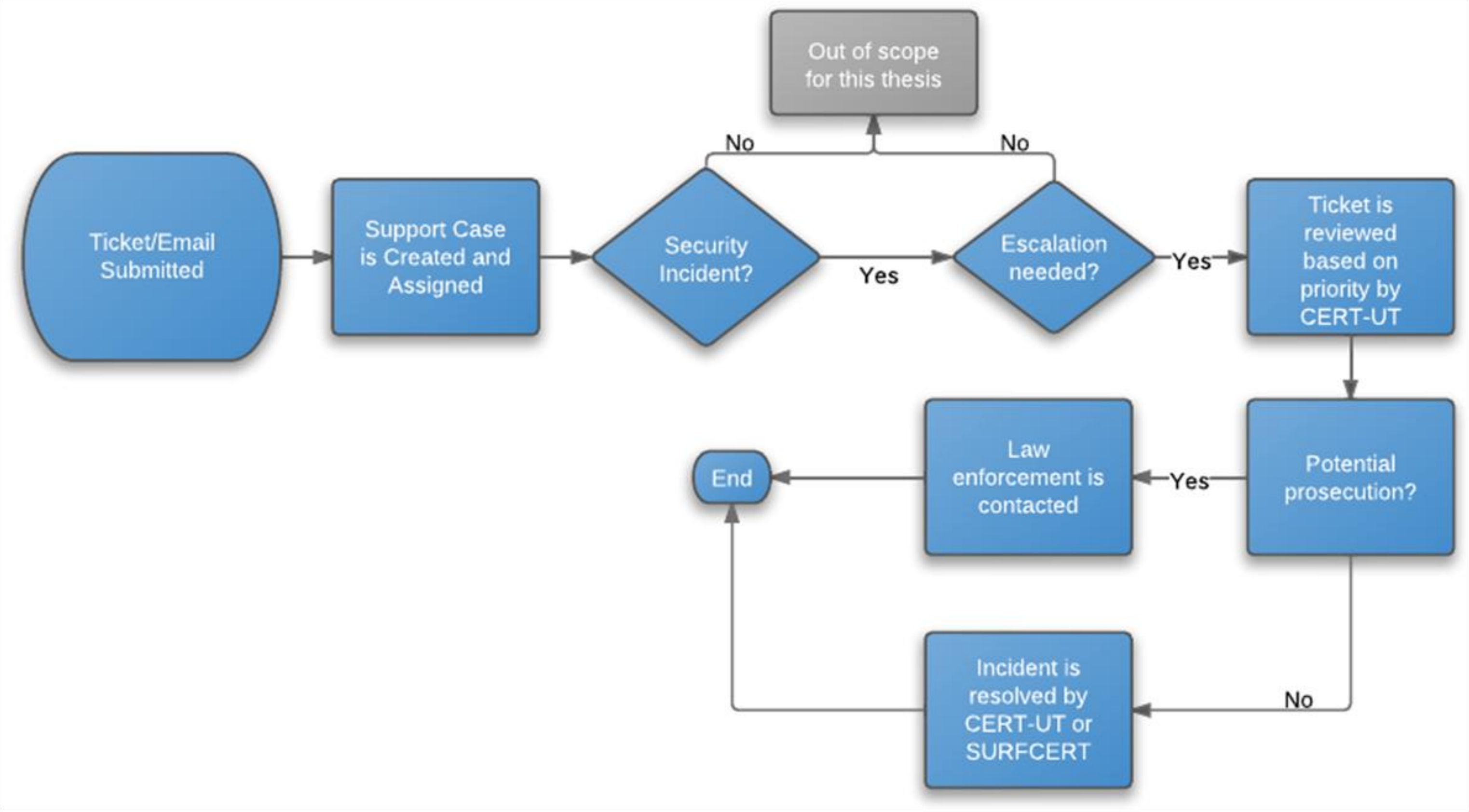
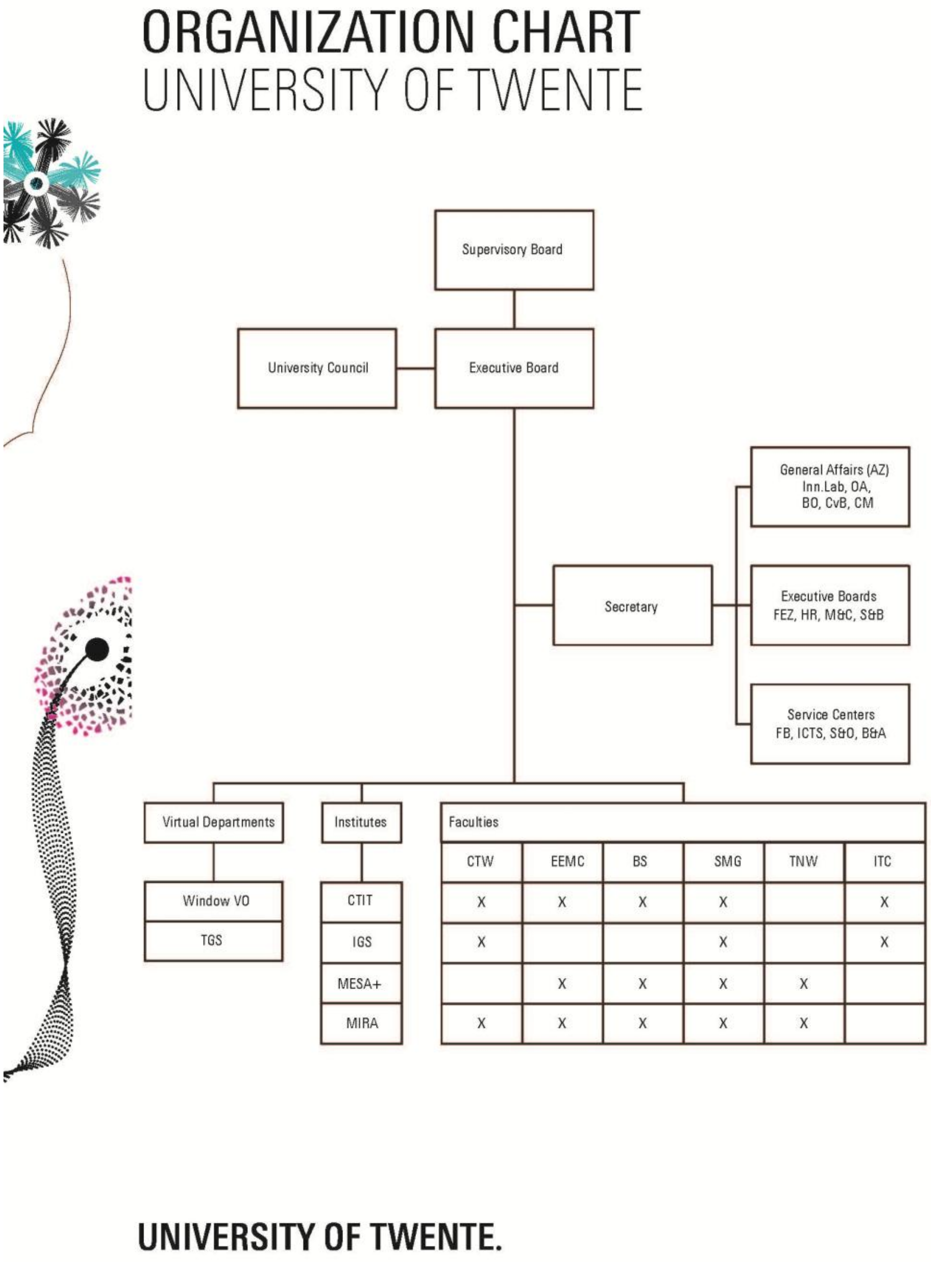

Ticket/Email Submitted
Support Case is Created and Assigned
Security Incident?
No
Yes
Out of scope for this thesis
No
Escalation needed?
Yes
Ticket is reviewed based on priority by CERT-UT
Potential prosecution?
Yes
Law enforcement is contacted
End
No
Incident is resolved by CERT-UT or SURFCERT

Figure 16: Flowchart for Incident Response at University of Twente

Organizational composition and stakeholders

In order to find all relevant stakeholders we first look at the organization itself. Figure 17 shows the organizational chart for the University of Twente.



Institutes	CTW	EEMC	BS	SMG	TNW	ITC
CTIT	X	X	X	X		X
IGS	X			X		X
MESA+		X	X	X	X	
MIRA	X	X	X	X	X	

Figure 17: Organization Chart University of Twente

The CERT-UT falls directly under the ICTS, the ICT Service centre, which is a service centre supporting Secretary as we can see in Figure 17.

The ICTS' own organizational chart is shown in Figure 18.

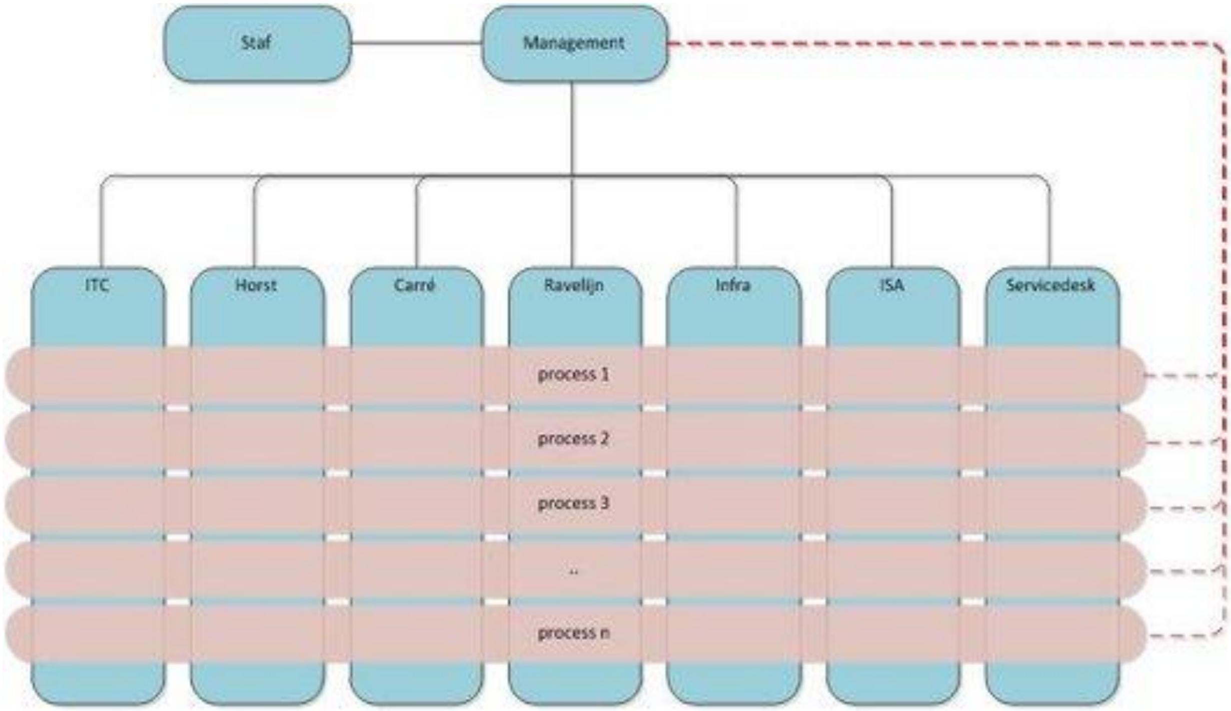


Figure 18: Organization Chart of the Utwente ICTS, adapted from [121]

As we can see the ICTS is a matrix shaped organization, with a hierarchical division in departments each at their own location (which are different buildings on the campus). Furthermore there is a functional coordination of the different work and management processes across all locations, which creates the matrix.

Furthermore there are two back office departments: *Infra*, for Network Administration, Server Administration and Telephony, and *ISA* for Information Services, System Development and Application Support. Although ICTS will soon be reorganizing, the CERT-UT currently falls under the responsibility of the head of the Infra department.

Following the organizational charts above and the interviews with CERT-UT we can identify the following stakeholders for forensic readiness within University of Twente:

- CERT-UT
- First line responders
- Business owners
- Executive Board
- Head of Infra department
- Director of ICTS
- General Affairs, in particular:
    - Legal Council

    - Operational Audit – ICT
- Employees / Students

CERT-UT

The CERT team does the actual incident response and handling, and is in the current situation given a certain mandate. Incorporating forensic readiness and forensic analysis as a goal of incident response would certainly influence their work.

First line responders

The first line responders determine what happens with each incoming incident. As we've seen in the earlier discussions, initial actions taken in a response can be crucial for forensic analysis and adequacy: their response will certainly be influenced.

Business owners

Business owners may see a certain decrease in the service level with regard to downtime if, higher in the organization, it is decided that forensic analysis is deemed necessary. Furthermore, the business owners will likely be responsible for translating certain policies into measures in order to assure compliance.

Executive Board

Top management is ultimately responsible for management and administration of the organization, which includes actions taken in case of criminal intent and issues such as compliance (as discussed in 1.3.1). These are all relevant with regards to forensic readiness.

Head of Infra department

The head of the infra department is end responsible for the CERT, and decides whether or not to report a crime and press charges.

Director of ICTS

The ICTS is responsible for all ICT related matters at the University of Twente. Forensic readiness will surely influence their current IT systems, infrastructure, procedures, etc.

Legal Council

The staff jurist aids and informs the Secretary of the Executive Board on legal issues, which includes compliance with applicable laws. This would include compliance with laws relevant for forensic readiness, as mentioned earlier in 1.3.1. Furthermore, forensic analysis needs to adhere to certain legislative principles which may change over time, which the jurist should have and keep an overview of. If adjustments need to be made due to legislative changes the staff jurist can communicate this to other relevant parties.

Operational Audit – ICT

The operational audit performs checks on the internal controls, including those on ICT. Although mostly focused on financial systems, other automated systems are more and more included as well [120]. With regards to forensic readiness, the operational audit should certain check for these.

Employees / Students

Although both employees and students will unlikely be actively involved in a forensic analysis, or the preparation for it, they are often the ones who first mention discrepancies by reporting them to the ICT helpdesk. They will thus need a certain acquaintance or knowledge on the matter.

Internal compliance and governance

Interviews with Ron Velthoen were held to determine how the University of Twente currently upholds (internal) compliance with regards to their security policies. Currently, the university is in the process of implementing a control framework based on ITIL v3. This process has been running for several years now, from 2010 onwards aided by the acquisition of the APM (Alignability Process Model)[1] which helps in implementation of ITIL by providing more specific processes, procedures, work instructions and tool settings. Despite these well meant specifications the university obviously still needs to adjust and tweak the controls to fit their own needs. The APM does help in providing more guidance though.

The team performing the implementation consists of four members, taking up their duty with regards to this plan on a part-time basis. So far they have completely implemented five processes:

- Incident Management
- Problem Management
- Change Management
- Configuration Management
- Service Level Management

During the interviews it was however underscored time and time again that there is an important continuous aspect, in other words, the implementation is never done. Improvements are still regularly made to already implemented controls. Another important note to quickly recap is that although ITIL is in fact at the basis of these controls, the controls are thoroughly adjusted to fit the university's organization and needs.

Due to the current circumstances, which can in short be described as tumultuous, it is deemed of no use to 'hook' the framework's activities into the ITIL-like model the UT uses now. Therefore it was decided to propose the framework as-is to the UT. Furthermore, it is clear that the UT is used to tweaking frameworks and controls to their own situation, something which is an important aspect for any framework, and can be helpful in implementation here.

[1] http://www.alignability.com/

Appendix K: Completed framework for the UT

People

The relevant stakeholders identified for the UT with regards to the People category are shown in Table 42. The activities and proposed responsibilities are shown in Table 43.

Table 42: UT Stakeholders for People category

Stakeholder	Responsibility
Executive Board	Accountable for daily operations, including staffing
Director of ICTS	The CERT falls under this business unit
Head of Infra department	Head of, amongst others, the CERT and its staff
Business Owners	Establish desired awareness of employees w.r.t. forensics demands
Staff jurist	Should be aware of certain forensic practices and demands
CERT-UT	Ensure members, first line responders and all employees are aware and if needed have required skills for their actions.
First Line responders	Should be aware of forensic demands
Employees & Students	Should be aware of certain forensic practices and demands.

Table 43: Framework layer 1 completed for UT - People

Phase	#	Activity	Stakeholders								S/T/O?
			Executive board	Directors of ICTS	Head of Infra department	Business Owners	Legal Council	CERT-UT	First Line responders	Employees & Students	
Plan	**P1**	Ensure forensic readiness ambition as agreed upon can be carried out within the organization	A	R	C		C	S			T
	P2	Ensure team is adequately trained	I	A	R		C	S	S		T
Do	**D1.1**	Determine required team skills, based on forensic readiness ambition of organization		AR	S		S	S			T

	D1.2	Assign and/or hire staff to team		A	R			C			T
	D2.1	Determine training requirements		I	AR			S	C		T
	D2.2	Develop or buy training (materials)		C	AR		S	S			T
	D2.3	Schedule trainings		I	AR			I			T
	D2.4	Attend trainings			A			R			O
Check	**C1**	Evaluate if team can effectively perform required tasks	I	AR	I			S	S		T
	C2.1	Evaluate training suitability w.r.t. goal		I	I			AR			T
	C2.2	Check team members attended trainings			AR			I			T
Act	**A1**	Adjust team formation		A	R			C			T
	A2.1	Adjust training			AR			S	C		T
	A2.2	Enforce more trainings			AR			I			T

Process

The relevant stakeholders identified for the UT with regards to Process People category are shown in Table 44. The activities and proposed responsibilities are shown in Table 45.

Table 44: UT Stakeholders for Process category

Stakeholder	Responsibility
Executive Board	Accountable for all daily operations
Director of ICTS	Responsible for incorporate adequate processes surrounding the ICT environment
Head of Infra department	Head of, amongst others, CERT
Business Owners	Responsible for incorporating adequate processes into their departments
Legal Council	Should test processes for legal adequacy
Operational Audit – ICT	Audits the processes against internal policies as well as regulations and laws
CERT-UT	Does most of the actual work regarding (preparing for) forensic analysis
First Line responders	Have to follow procedures as defined

Table 45: Framework layer 1 completed for UT - Process

Phase	#	Activity	Stakeholders								S/T/O?
			Executive Board	Director of ICTS	Head of Infra department	Business Owners	Legal Council	Operational Audit – ICT	CERT-UT	First Line responders	
Plan	P1	Determine forensic readiness ambition	AR	S	C		C		C		S
	P2	Ensure forensic readiness is embedded in organization's policies	A	R	S	I	C	I	C	I	S
	P3	Ensure forensic readiness policy is incorporated into procedures		AR	S	I	C	I	C	I	T
	P4	Ensure forensic readiness has sufficient monetary resources to be performed in the organization.	AR	S	C						S
	P5	Ensure forensic procedure can be performed efficiently and adequately	I	AR	S				C		T
Do	D1.1	Perform a risk assessment	A	R	S	S	S	C	C		T
	D1.2	Determine risk appetite	AR	C		C	C				S
	D1.3	Decide what the organization wants to achieve w.r.t. forensic readiness, taking into accounts its internal and external environment	AR	S	C	S	S	C			S
	D2	Create forensic readiness policy & update existing policies with forensic readiness aspects	AR	C	C		S		S		S
	D3.1	Determine procedures influenced by forensic readiness		AR	S	C			C		T

	D3.2	Update/create procedures for forensic readiness	I	AR	I	I	I	I	I	I	T
	D3.3	Define forensic procedures (acquisition, analysis, handling of evidence)		AR	S		C		S		T
	D4	Assign sufficient budget for forensic readiness, in line with ambition.	AR	C		C					S
	D5.1	Prioritize events during incidents			AR	I			S	S	T
	D5.2	Prepare documents and facilities required for a thorough chain of custody and notes during analysis			AR				S	S	T
Check	**C1.1**	Review if risk assessment is up to date and adequate	A	R	S	S	S		S		T
	C1.2	Review if risk appetite suffices	AR	S		S	S				S
	C1.3	Review if forensic readiness ambition is (still) adequate and suits the organization	AR	S		S	S				S
	C2	Evaluate policies for organization's forensic readiness goal and effectiveness	AR	C	C						S
	C3	Check if procedures align with the defined policy	I	AR	S	C			C		T
	C4	Evaluate forensic readiness effectiveness w.r.t. budget	AR	C	S				C		T
	C5.1	Evaluate if process is focusing on correct events according to priority		AR	S				C		O
	C5.2	Evaluate if a thorough chain of custody and investigative log is kept consistently		A	R				S	S	O
Act	**A1.1**	Update identified risks	A	R	S	S	S	C	C		T
	A1.2	Reconsider risk appetite	AR	C		C	C				S
	A1.3	Adjust ambition level	AR	S	C	S	S	C			S
	A2	Adjust policies where required	AR	C	C		S		S		S
	A3	Adjust (forensic) procedures		AR	S	C			C		T
	A4	Adjust budget	AR	C		C					S
	A5.1	Adjust actions taken			A	I			R	S	O

	A5.2	Adjust prepared documents and facilities			AR				S	S	T

23.1.1 Technology

The relevant stakeholders identified for the UT with regards to Process People category are shown in Table 46. The activities and proposed responsibilities are shown in Table 47.

Table 46: UT Stakeholders for Technology category

Stakeholder	Responsibility
Executive Board	Accountable for daily operations
Director of ICTS	Responsible for the IT landscape within the university
Head of Infra department	Head of CERT, may help determine tools used
Business Owners	Could experience hinder from new technological solutions
Legal Council	Can consult on admissibility of evidence collected in a certain manner
Operational Audit – ICT	Audits the IT infrastructure
CERT-UT	Uses technological solutions for incident response and possibly forensic analysis
First Line responders	Use technological solutions for initial incident response

Table 47: Framework layer 1 completed for UT - Technology

Phase	**#**	**Activity**	**Stakeholders**								**S/T/O?**
			Executive board	**Director of ICTS**	**Head of Infra department**	**Business Owners**	**Legal Council**	**Operational Audit – ICT**	**CERT-UT**	**First line responders**	
Plan	**P1**	Ensure infrastructure is prepared for forensic analysis		A	R		C	I	S		T
	P2	Ensure initial response can be performed by the team in a forensically sound manner		AR			C		C	C	T
	P3	Ensure analysis can be performed efficiently and in a forensically sound manner		AR			C		C		T

Do	**D1.1**	Activate time synchronization of clocks on network		A	C				R		O
	D1.2	Make list of data to be logged, determined by accepted risk and decided goals and policies		AR		C		I	C		T
	D1.3	Technically implement logging process based on prescribed procedure		A	R				I		O
	D2.1	Provide team with required data acquisition tools		I	AR				C	C	T
	D3.1	Provide team with required forensic analysis tools		I	AR				C	C	T
Check	**C1.1**	Evaluate if time deficiencies are within predetermined limit		AR					C		O
	C1.2	Evaluate if data logged aligns with decided list	I	AR							T
	C1.3	Review if logging completes successfully		I	AR						O
	C2.1	Evaluate if data acquisition tools are adequate		I	AR		S		C		O
	C3.1	Evaluate if forensic analysis tools are adequate		I	AR		S		C		O
Act	**A1.1**	Update time synchronization	I	AS	S				R		O
	A1.2	Update list with data to be logged	I	AS		S			R		O
	A1.3	Update logging process		I	AR						O
	A2.1	Adjust data acquisition tools		I	AR				C		T
	A3.1	Adjust forensic analysis tools		I	AR				C		T

References

[1] Abimbola A. Information security incident response. *Network Security* 2007: 10-13, 2007.

[2] Alharbi S., Weber-Jahnke J., and Traore I. The proactive and reactive digital forensics investigation process: A systematic literature review. *International Journal of Security and its Applications* 5: 59-72, 2011.

[3] Andoh-Baidoo F.K., and Osei-Bryson K.M. Exploring the characteristics of Internet security breaches that impact the market value of breached firms. *Expert Systems with Applications* 32: 703-725, 2007.

[4] Andrew M.W. Defining a process model for forensic analysis of digital devices and storage media. In: *International Workshop on Systematic Approaches to Digital Forensic Engineering*. Bell Harbor, WA: 2007, p. 16-30.

[5] Ashley P., Powers C., and Schunter M. From privacy promises to privacy management: a new approach for enforcing privacy throughout an enterprise. In: *Proceedings of the 2002 workshop on New security paradigms*. Virginia Beach, Virginia: ACM, 2002, p. 43-50.

[6] ASL BiSL Foundation. ASL BiSL Foundation http://www.aslbislfoundation.org/. [Online; accessed 14/08/2012].

[7] Baker W.H., and Wallace L. Is information security under control?: Investigating quality in information security management. *IEEE Security and Privacy* 5: 36-44, 2007.

[8] Baryamureeba V., and Tushabe F. The Enhanced Digital Investigation Process Model. *Asian Journal of Information Technology* 5: 790-794, 2006.

[9] Beebe N.L., and Clark J.G. A hierarchical, objectives-based framework for the digital investigations process. *Digital Investigation* 2: 147-167, 2005.

[10] Bertrand C. Business continuity and mission critical applications. *Network Security* 2005: 9-11, 2005.

[11] Bitter C., North J., Elizondo D.A., and Watson T. An introduction to the use of neural networks for network intrusion detection. 2012, p. 5-24.

[12] Brettle P. Real world response to business continuity. *ITNOW* 48: 8-9, 2006.

[13] British Standards. BS2599. 2006.

[14] Burkett J.S. Business Security Architecture: Weaving Information Security into Your Organization's Enterprise Architecture through SABSA®. *Information Security Journal* 21: 47-54, 2012.

[15] CA Technologies. The role of Security Management in achieving Continuous Compliance. 2007.

[16] Carlton G.H., and Worthley R. An evaluation of agreement and conflict among computer forensics experts. In: *Hawaii International Conference on System Sciences*. Waikoloa, HI: 2009.

[17] Carnegie Mellon Software Engineering Institute. Handbook for Computer Security Incident Response Teams (CSIRTs). 2003.

[18] Carnegie Mellon Software Engineering Institute. Responding to Intrusions. 1999.

[19] Carrier B.D. Digital forensics works. *IEEE Security and Privacy* 7: 26-29, 2009.

[20] Carrier B.D., and Spafford E.H. Categories of digital investigation analysis techniques based on the computer history model. *Digital Investigation* 3: 121-130, 2006.

[21] Carrier B.D., and Spafford E.H. Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence* 2: 2003.

[22] Casey E. Case study: Network intrusion investigation - Lessons in forensic preparation. *Digital Investigation* 2: 254-260, 2005.

[23] Chuvakin A. Six mistakes of log management. *Computer Security Journal* 23: 38-41, 2007.

[24] Čisar P., and Čisar S.M. Methodological frameworks of digital forensics. Subotica: 2011, p. 343-347.

[25] Cohen F. Two models of digital forensic examination. Berkeley, CA: 2009, p. 42-53.

[26] Committee of Sponsoring Organizations of the Treadway Commission. Enterprise Risk Management - Integrated Framework Executive Summary. 2004.

[27] Committee of Sponsoring Organizations of the Treadway Commission. Internal Control Integrated Framework - Draft for Information Only. 2011.

[28] Committee of Sponsoring Organizations of the Treadway Commission. An Update of COSO's Internal Control - Integrated Framework. 2012.

[29] D'Ambrosio B., Takikawa M., Fitzgerald J., Upper D., and Mahoney S. *Security Situation Assessment and Response Evaluation (SSARE)*. Los Alamitos: IEEE Computer Soc, 2001, p. 387-394. isbn: 0-7695-1212-7

[30] Damianides M. Sarbanes-oxley and IT governance: New guidance on IT control and compliance. *Information Systems Management* 22: 77-84, 2005.

[31] de Wit J.A.W. Preparing for Incident Response - Forensic Analysis. In: *EWI*. Enschede: University of Twente, 2012, p. 51.

[32] DePaul University. A Framework for Incident Response. 2002.

[33] Dey M. Business Continuity Planning (BCP) methodology essential for every business. In: *IEEE GCC Conference and Exhibition*. Dubai: 2011, p. 229-232.

[34] Endicott-Popovsky B., and Frincke D. Adding the fourth "R". In: *IEEE System, Man and Cybernetics Information Assurance Workshop*. West Point, NY: 2004, p. 442-443.

[35] Endicott-Popovsky B.E., and Frincke D.A. Embedding forensic capabilities into networks: Addressing inefficiencies in digital forensics investigations. In: *IEEE Workshop on Information Assurance*. West Point, NY: 2006, p. 133-139.

[36] ENFSI. Guidelines for best practice in the Forensic Examination of Digital Technology, Version 6. 2009.

[37] Engelfriet A. *Security - Deskundig en praktisch juridisch advies*. Ius Mentis, 2011. isbn:

[38] European Commission. Directive 2006/43/EC of the European Parliament and of the Council 17 may 2006 on statutory audit of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC. 2006.

[39] Fenz S., Ekelhart A., and Neubauer T. Information security risk management: In which security solutions is it worth investing? *Communications of the Association for Information Systems* 28: 329-356, 2011.

[40] Forrester. Planning for Failure. 2011.

[41] Forrester J., and Irwin B. A Digital Forensic Investigative Model for Business Organisations. In: *Information Security for South Africa Conference*. Sandton: 2006.

[42] Forte D.V. An integrated approach to security incident management. *Network Security* 2008: 14-16, 2008.

[43] Fox C., and Zonneveld P. IT Control Objectives for Sarbanes-Oxley. IT Governance Institute, 2003.

[44] Gil Pérez M., Gómez Mármol F., Martínez Pérez G., and Skarmeta Gómez A.F. RepCIDN: A Reputation-based Collaborative Intrusion Detection Network to Lessen the Impact of Malicious Alarms. *Journal of Network and Systems Management* 1-40, 2012.

[45] Goel S., and Shawky H.A. Estimating the market impact of security breach announcements on firm values. *Information and Management* 46: 404-410, 2009.

[46] Grobler C.P., and Louwrens C.P. Digital evidence management plan. In: *Information Security for South Africa Conference*. Johannesburg: 2010.

[47] Grobler C.P., and Louwrens C.P. Digital forensic readiness as a component of information security best practice. In: *New Approaches for Security, Privacy and Trust in Complex Environments*, edited by Venter, Eloff, Labuschagne, and Solms. Published: 2007, p. 13-24.

[48] Grobler C.P., Louwrens C.P., and Von Solms S.H. A framework to guide the implementation of proactive digital forensics in organizations. In: *International Conference on Availability, Reliability, and Security*. Krakow: 2010, p. 677-682.

[49] Grobler C.P., Louwrens C.P., and Von Solms S.H. A multi-component view of digital forensics. In: *International Conference on Availability, Reliability, and Security*. Krakow: 2010, p. 647-652.

[50] Grobler M., and Bryk H. Common challenges faced during the establishment of a CSIRT. In: *Information Security for South Africa Conference*. Johannesburg: 2010.

[51] Guo H., Jin B., and Huang D. Research and review on computer forensics. In: *Forensics in Telecommunications, Information and Multimedia*. Published: Shanghai: 2011, p. 224-233.

[52] Hedström K., Kolkowska E., Karlsson F., and Allen J.P. Value conflicts for information security management. *Journal of Strategic Information Systems* 20: 373-384, 2011.

[53] Hellany A., Achi H., and Nagrial M. An overview of digital security forensics approach and modelling. In: *International Conference on Computer Engineering and Systems*. Cairo: 2008, p. 257-260.

[54] Hevner A.R., March S.T., Park J., and Ram S. Design science in information systems research. *MIS Quarterly: Management Information Systems* 28: 75-105, 2004.

[55] Hunton P. The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. *Computer Law and Security Review* 27: 61-67, 2011.

[56] Information Security Forum. ISF Threat Horizon 2014. 2012.

[57] Information Systems Audit and Control Association. Guideline G28: Computer Forensics. 2000.

[58] International Organization for Standardization. ISO 27001 - Information security management systems - Requirements. 2005.

[59] International Organization for Standardization. ISO 27002 - Information Technology - Security techniques - Code of practice for information security management. 2005.

[60] International Organization for Standardization. ISO 27035 - Information security incident management. 2011.

[61] ISACA. COBIT 5. 2012.

[62] IT Service Management Forum. *An Introductory Overview of ITIL v3*. itSMF UK, 2007. isbn: 0-9551245-8-1

[63] Jaisankar N., Ganapathy S., Yogesh P., Kannan A., and Anand K. An intelligent agent based intrusion detection system using fuzzy rough set based outlier detection. 2012, p. 147-153.

[64] Kabay M.E. CSIRT Management. 2009.

[65] Karyda M., and Mitrou L. Internet forensics: Legal and technical issues. Karlovassi, Samos: 2007, p. 3-12.

[66] Kavitha B., Karthikeyan D.S., and Sheeba Maybell P. An ensemble design of intrusion detection system for handling uncertainty using Neutrosophic Logic Classifier. *Knowledge-Based Systems* 28: 88-96, 2012.

[67] Kheir N., Debar H., Cuppens-Boulahia N., Cuppens F., and Viinikka J. Cost evaluation for intrusion response using dependency graphs. Paris: 2009.

[68] Kiuchi M., and Onoda T. Intrusion detection in control systems using sequence characteristics. *IEEE Transactions on Electronics, Information and Systems* 132: 14-20+11, 2012.

[69] KPMG Advisory N.V. Nieuwe perspectieven vragen om actie. 2012.

[70] Leigland R., and Krings A.W. A Formalization of Digital Forensics. *International Journal of Digital Evidence* 3: 2004.

[71] Li J.S., Hsieh C.J., and Lin H.Y. A hierarchical mobile-agent-based security operation center. *International Journal of Communication Systems* 2012.

[72] Liu X., Peng L., and Li C. Research on the BM algorithm based on the intrusion detection system. Beijing: 2012, p. 309-315.

[73] Ma G., Wang Z., Zou L., and Zhang Q. Computer forensics model based on evidence ring and evidence chain. In: *International Conference on Advanced in Control Engineering and Information Science*. Dali, Yunnam: 2011, p. 3663-3667.

[74] Mandiant. M-trends 2011. 2011.

[75] Mandiant. M-trends 2012. 2012.

[76] McDonald R. New considerations for security compliance, reliability and business continuity. In: *IEEE Rural Electric Power Conference*. Charleston, SC: 2008, p. B11-B17.

[77] Ministerie van Veiligheid en Justitie. Cybersecuritybeeld Nederland. 2011.

[78] Ministerie van Veiligheid en Justitie. Veiligheid in Cyberspace. 2012.

[79] Mitropoulos S., Patsos D., and Douligeris C. On Incident Handling and Response: A state-of-the-art approach. *Computers and Security* 25: 351-370, 2006.

[80] Mouhtaropoulos A., Grobler M., and Li C.T. Digital forensic readiness: An insight into governmental and academic initiatives. In: *European Intelligence and Security Informatics Conference*. Athens: 2011, p. 191-196.

[81] Mr. F.J. Zuiderveen Borgesius. De meldplicht voor datalekken in de Telecommunicatiewet. 2011.

[82] Nationaal Cyber Security Centrum. Factsheet afluisterwalmare Flamer lang onder de radar https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/factsheets/factsheet-afluistermalware-flamer-lang-onder-de-radar.html. [Online; accessed 22/06/2012].

[83] Nationaal Cyber Security Centrum. Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010.

[84] National Institute of Standards and Technology. Computer Security Incident Handling Guide. 2008.

[85] National Institute of Standards and Technology. Contingency Planning Guide for Federal Information Systems. 2010.

[86] National Institute of Standards and Technology. Guide to Computer Security Log Management. 2006.

[87] National Institute of Standards and Technology. Guide to Integrating Forensic Techniques into Incident Response. 2006.

[88] Network Working Group, Brezinski D., and Killalea T. RFC 3227 - Guidelines for Evidence Collection and Archiving. 2002.

[89] Pangalos G., Ilioudis C., and Pagkalos I. The importance of Corporate Forensic Readiness in the information security framework. Larissa: 2010, p. 12-16.

[90] Pangalos G., and Katos V. Information Assurance and Forensic Readiness. In: *Next Generation Society Technological and Legal Issues*, edited by Sideridis AB, and Patrikakis CZ. Published: Springer Berlin Heidelberg, 2010, p. 181-188.

[91] Peisert S., Bishop M., Karin S., and Marzullo K. Principles-driven forensic analysis. In: *New Security Paradigms Workshop*. Lake Arrowhead, CA: 2005, p. 85-93.

[92] Peisert S., Bishop M., and Marzullo K. Computer forensics in forensis. In: *International IEEE Workshop on Systematic Approaches to Digital Forensic Engineering* 2008, p. 102-122.

[93] Peterson C.A. Business Continuity Management & guidelines. In: *Information Security Curriculum Development Annual Conference*. Kennesaw, GA: 2009, p. 114-120.

[94] Pollitt M.M. An ad hoc review of digital forensic models. Bell Harbor, WA: 2007, p. 43-52.

[95] Princeton University. Wordnet http://wordnet.princeton.edu/. [Online; accessed 29/08/2012].

[96] PWC. Key findings from the 2012 Global State of Information Security Survey. 2012.

[97] Quinn S. Examining the state of preparedness of Information Technology management in New Zealand for events that may require forensic analysis. *Digital Investigation* 2: 276-280, 2005.

[98] Reijerman D. Nationale Recherche haalt Bredolab-botnet uit de lucht http://tweakers.net/nieuws/70424/nationale-recherche-haalt-bredolab-botnet-uit-de-lucht.html. [Online; accessed 22/06/2012].

[99] Reith M., Carr C., and Gunsch G. An Examination of Digital Forensic Models. *International Journal of Digital Evidence* 1: 2002.

[100] Rollason-Reese R.L. Incident Handling: An Orderly Response to Unexpected Events. In: *ACM's SIGUCCS Conference*. San Antonio, TX: 2003, p. 97-102.

[101] Rowlingson R. A Ten Step Process for Forensic Readiness. *International Journal of Digital Evidence* 2: 2004.

[102] Schot J. The privacy governance framework : effectively dealing with privacy legislation. Enschede: Universiteit Twente, 2009.

[103] Sinangin D. Computer forensics investigations in a corporate environment. *Computer Fraud and Security* 2002: 11-14, 2002.

[104] Smits D., Bast C., van Beele J., Bloem J., Coenen T., Hassoldt W., Hofman C., van Leeuwen J., Peters R., Pol C., van Puffelen J., Schekkerman J., van Steen L., Verhoef C., Vincent M., and de Weme H. *Focus op IT-bestuur*. Den Haag: SDU uitgevers, 2008. isbn:

[105] Stephenson P. Conducting incident post mortems. *Computer Fraud and Security* 2003: 16-19, 2003.

[106] Sveen F.O., Torres J.M., and Sarriegi J.M. Learning from your elders: A shortcut to information security management success. Nuremberg: 2007, p. 224-237.

[107] Symantec. Trojan.Bredolab http://www.symantec.com/security_response/writeup.jsp?docid=2009-052907-2436-99. [Online; accessed 22/06/2012].

[108] Symantec. W32.Duqu http://www.symantec.com/security_response/writeup.jsp?docid=2011-101814-1119-99. [Online; accessed 22/06/2012].

[109] Symantec. W32.Flamer http://www.symantec.com/security_response/writeup.jsp?docid=2012-052811-0308-99. [Online; accessed 22/06/2012].

[110] Symantec. W32.Stuxnet http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99. [Online; accessed 22/06/2012].

[111] Tan J. Forensic Readiness. Cambridge, 2001.

[112] Taylor C., Endicott-Popovsky B., and Frincke D.A. Specifying digital forensics: A forensics policy approach. *Digital Investigation* 4: 101-104, 2007.

[113] Telecommunicatiewet. http://wetten.overheid.nl/BWBR0009950/Opschrift/geldigheidsdatum_25-06-2012. [Online; accessed 25/06/2012].

[114] Trček D. An integral framework for information systems security management. *Computers and Security* 22: 337-360, 2003.

[115] Trček D., Abie H., Skomedal Å., and Starc I. Advanced framework for digital forensic technologies and procedures. *Journal of Forensic Sciences* 55: 1471-1480, 2010.

[116] U.S. Department of Justice. Electronic Crime Scene Investigation: A Guide for First Responders. 2008.

[117] U.S. Department of Justice. Forensic Examination of Digital Evidence: A Guide for Law Enforcement. 2004.

[118] U.S. Securities and Exchange Commission. Appendix C: Safeguarding of Assets http://www.sec.gov/rules/pcaob/34-49544-appendixc.pdf. [Online; accessed 26/06/2012].

[119] U.S. Securities and Exchange Commission. PCAOB Rulemaking: Public Company Accounting Oversight Board; Notice of Filing of Proposed Rule on Auditing Standard No. 2, An Audit of

Internal Control Over Financial Reporting Performed in Conjunction with an Audit of Financial Statements http://www.sec.gov/rules/pcaob/34-49544.htm. [Online; accessed 26/06/2012].

[120] University of Twente. ICT-Audits http://www.utwente.nl/az/oa/ict/ictaudits.doc/. [Online; accessed 21/08/2012].

[121] University of Twente. Organization ICTS http://www.utwente.nl/icts/en/about_icts/organization/. [Online; accessed 21/08/2012].

[122] University of Twente. Security Policies ICT Beheer http://www.utwente.nl/sb/beleidsterreinen/informatiemanagement/documenten/security_policies_ict_beheer/index.html. [Online; accessed 21/08/2012].

[123] Von Solms B., and Von Solms R. The 10 deadly sins of information security management. *Computers and Security* 23: 371-376, 2004.

[124] von Solms R., and von Solms S.H. Information Security Governance: A model based on the Direct-Control Cycle. *Computers and Security* 25: 408-412, 2006.

[125] Von Solms S., Louwrens G., Reekie G., and Grobler T. A control framework for digital forensics. In: *Advances in Digital Forensics II*. Published: 2006, p. 343-355.

[126] Wang S.J. Measures of retaining digital evidence to prosecute computer-based cyber-crimes. *Computer Standards and Interfaces* 29: 216-223, 2007.

[127] Wang T., and Hsu C. The impact of board structure on information security breaches. Taipei: 2010, p. 1687-1694.

[128] Webster Dictionary. http://www.merriam-webster.com/. [Online; accessed 29/08/2012].

[129] Werlinger R., Muldner K., Hawkey K., and Beznosov K. Preparation, detection, and analysis: The diagnostic work of IT security incident response. *Information Management and Computer Security* 18: 26-42, 2010.

[130] Wiboonrat M., and Kosavisutte K. Optimization strategy for disaster recovery. In: *IEEE International Conference on Management of Innovation and Technology*. Bangkok: 2008, p. 675-680.

[131] Wieringa R. Design science as nested problem solving. In: *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology*. Philadelphia, Pennsylvania: ACM, 2009, p. 1-12.

[132] Wieringa R. Writing a Report About Design Research. 2007.

[133] Wiik J., and Gonzalez J.J. Limits to Effectiveness in Computer Security Incident Response Teams. In: *The System Dynamics Society* 2005.

[134] Windsor C. Business continuity - Is it expensive and hard? *ITNOW* 48: 12-13, 2006.

[135] Wolfe-Wilson J., and Wolfe H.B. Management strategies for implementing forensic security measures. *Information Security Technical Report* 8: 55-64, 2003.

[136] Wolfe H. The question of organizational forensic policy. *Computer Fraud and Security* 2004: 13-14, 2004.

[137] World Economic Forum. Global Risks. 2012.

[138] Yasinsac A., and Manzano Y. Policies to Enhance Computer and Network Forensics. In: *IEEE Workshop on Information Assurance and Security*. United States Military Academy, West Point, NY.: 2001.