Czech Technical University
Faculty of Nuclear Sciences and Physical Engineering

Department of Mathematics
Branch of Studies: Applied Information Technology

Design of an Information System for Support of Forensic Audit

Bachelor's Degree Project

Author: Edita Pešková
Adviser: Mgr. Karel Macek, Ph.D.
Language Adviser: Mgr. Hana Čápová
Academic Year: 2015

Před svázáním místo téhle stránky vložíte zadání práce s podpisem děkana (bude to jediný oboustranný list ve Vaší práci) !!!!

Declaration

I declare that this Bachelor Project is all my own work and I have cited all sources I have used in the bibliography.

In Prague .....

.....
Edita Pešková

Acknowledgements

I wish to thank to my supervisor for his inspiring feedback, my family for their patience and support in my studies and anyone who encouraged me in this project.

Edita Pešková

Název práce:
Návrh informačního systému pro podporu forenzního auditu

Autor: Edita Pešková

Obor: Applied Information Technology
Druh práce: Bakalářská práce

Vedoucí práce: Mgr. Karel Macek, Ph.D.
Oddělení ekonometrie, Ústav teorie informace a automatizace
Konzultant: —

Abstrakt: Tato bakalářská práce předkládá návrh systému a naznačuje požadavky, které jsou potřebné aby byl popsán smysl a cíle technik digitálního forenzního vyšetřování, vykonávaných forenzními auditory, účetními a inpektory firem. Pomocí různorodých postupů, nástrojů a technik rozpoznáváme v jakých případech mohou nástroje forenzního auditu poskytnout auditorům potřebné informace k provedení forenzního auditu. Bakalářská práce představuje požadavky, které musí splňovat vlastní informační systém použitelný pro podporu vyšetřování a také poskytuje detailní návrh tohoto systému.

Klíčová slova: Forenzní audit, Vyšetřování, Návrh systému, Databáze, Sběr dat

Title:
Design of an Information System for Support of Forensic Audit

Author: Edita Pešková

Abstract: This bachelor project proposes a system design and suggests requirements that are needed in order to describe the purpose and goals of the digital forensic investigation techniques carried out by the forensic auditors, accountants and examiners of companies. Using various procedures, tools and techniques we identify where the forensic audit tools and the system can provide the auditors necessary information to carry out forensic audit. This bachelor thesis provides requirements that our own information system usable to support forensic audit must follow and also provides a detailed design of this system.

Key words: Forensic audit, Investigation, System design, Database, Data collection

Contents

Introduction

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language. klicova slova: forenzni audit, unik penez, prosetreni spolecnosti, vyhledavani dukazu, pocitacova podpora, aplikace podporujici forenzni audit, vizualizace procesu vysetrovani, report o vysetrovanem pripadu, metodika forenzniho auditu, navrh informacniho systemu, ...

Chapter 1

Forensic audit and its computer support

na zacatek shrnout co vsechno obsahuje tato kapitola. asi tak takhle:

This chapter strives to define and explain the meaning of the term "forensic audit" as well as other therms related to this field. We demonstrate typical roles and outline the process. az bude kapitola dopsana, zkontrolovat, zda toto odpovida

1.1 Matters of forensic audit

nelibi se mi, pridat do jinych casti a zrusit Forensic audit is a specialization within a field of accounting that examines and evaluates evidence concerning unproven statements for possible use as evidence in court. Forensic audit is usually used in case there is a suspicion in certain company there is a crime being committed. The background of the investigated case is rather diverse. A customer can be, for example, a CEO who wants to examine the functioning of one of the sub-divisions of a controlling company. There can be a suspicion of some fraudulent activity or the need of forensic audit can be closely unspecified.

1.2 What is forensic audit

The term "forensic" can be defined in multiple ways. According to merriam-webster dictionary citace http://www.merriam-webster.com/dictionary/forensic the definition is "relating to the use of scientific knowledge or methods in solving crimes". The term "audit" is explained in the same dictionary as "a complete and careful examination of the financial records of a business or person". citace http://www.merriam-webster.com/dictionary/audit

The essence of forensic audit is to discover and investigate fraudulent intentions and fraudulent behavior.

A common mistake in the definition of forensic audit is to confuse it with financial audit. The aim of financial audit is to verify whether financial statements are fairly stated in accordance with accounting standards. Financial auditors search for material errors or other misstatements in the accountancy.

On the other hand the ultimate goal of forensic audit is to examine existing or gained suspicion and procure evidence concerning possible fraudulent behavior. Deceptive scenarios are discovered in the process of forensic audit and evidence together with a documentation that is usable for subsequent course of action is gathered. As a matter of principle forensic auditors are not expected to express their opinion on the guilt or innocence of suspects.

1.3 When to use forensic audit

asi spis nez priklady popsat za jakych situaci... Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

1.4 How to prepare for a forensic audit

v hrubych rysech jak to probiha (to co uz mam sem patri), na zaklade toho, co jsem zjistila, FA funguje takto:...

On the basis of what we have found the process of forensic audit works as follows. When it is decided that certain situation will be investigated in forensic audit it is important to prevent all investigated individuals to access all related documents and electronic evidence. It is also recommended to limit their access to corporate information systems.

Next step is to formulate properly the assignment. To define the extent and expectations on the outcome of forensic audit. To prevent a misunderstanding the assignment should be as specific and detailed as possible. It is best to choose the right audit company according to references and their experience with similar cases as the one we have specified.

When a client contacts an audit company with an assignment they usually schedule a meeting together formulate and sign and accept the assignment. The ordering party should be prepared to provide access to corresponding electronic and paper-like documentation as well as accept the fact that auditors are going to question employees and case-related person. On the other hand the audit company undertakes

to refrain from sharing all the confidential information with third parties.A team of specialists that are convenient to the assignment is formed and the inspection is launched.

The following steps of the precise method of forensic audit are not definite. The ability to adapt in new situations is one of many essential capabilities for the team of forensic auditors. The variety of investigated cases is so vast that there is no universally valid and precise course of action in the same time. Therefore on this place we present only general methodology of forensic audit. Several selected methods of forensic audit will be described later in this document. link na spravne misto!

1.5 General methodology of forensic audit

In this section we present basic phases that are used while performing forensic audit. This process is most commonly divided into four stages: Accumulation, Examination, Analysis and Reporting. This basic methodology starts after the selection of the audit company and after the specification of the assignment; at the same time when the real work of forensic auditors begins.

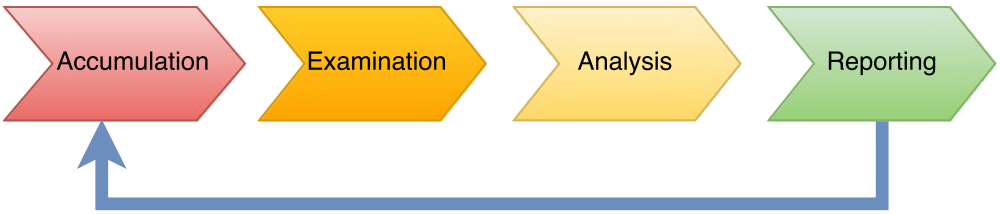


Figure 1.1: General methodology of forensic audit

Accumulation: The main purpose of this stage is to acquire as much usable data as possible. It means recognize possible sources of data and provide backup record. All the sources of data and information, including necessary cross examination and other sources of evidence, should be utilized in this phase. All the information from the conceivable sources of pertinent information should be gained.

Examination: Examinations include forensically preparing all the gathered data. This can be done using a blend of computerized and manual systems to survey and concentrate specifically compelling information.

Analysis: The following period of the procedure is to investigate the consequences of the examination, using legitimately reasonable routines and systems. The aim is to infer helpful data that addresses the inquiries that were the impulse for performing the accumulation and examination. grrrrrr...

Reporting: The last stage is reporting the consequences of the investigation, which may include depicting the activities utilized, clarifying how devices and methods were chosen, figuring out what different activities should be performed and giving proposals to change to approaches, rules, techniques, apparatuses, and different parts of the measurable procedure.

1.6 use case diagram

komentar k diagramu

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

1.7 co sem jeste zahrnout:

VIZE: Rozdelit obecne druhy odhalovaneho chovani. Zahrnout vseobecne veskerou tresnout cinnost - nejspis podle zakona? Z techto oblasti vyelimimovat vsechny, pro ktere nema cenu uvazovat pocitacovou podporu (nasilne ciny, prepadeni, kradeze hmotneho majetku, pravni dokumenty? atd.).
Zbyle tak nejak rozdelit do skupin podle toho, jaky druh pocitacove podpory je obecne vyuzitelny. Pak se mozna pokusit k sobe priradit dany precin a metodu. Z metod nechci zminovat konkretni SW, ale spise obecne oblasti reseni - jak vyuzivame data mining, fuzzy logiku, strojove uceni (nebo alespon co to je a ze se take muze vyuzit), kvantitativne analyticky SW, forenzni toolkity na obnovu dat a podobne.
DOTAZ: Z predchozi vize chci prejit v dalsi kapitole zpet k obecne metodologii a diagramu z ARISu. Nevim, jak na to plynule navazat aby to davalo celkove hlavu a patu. Snad me jeste neco napadne.

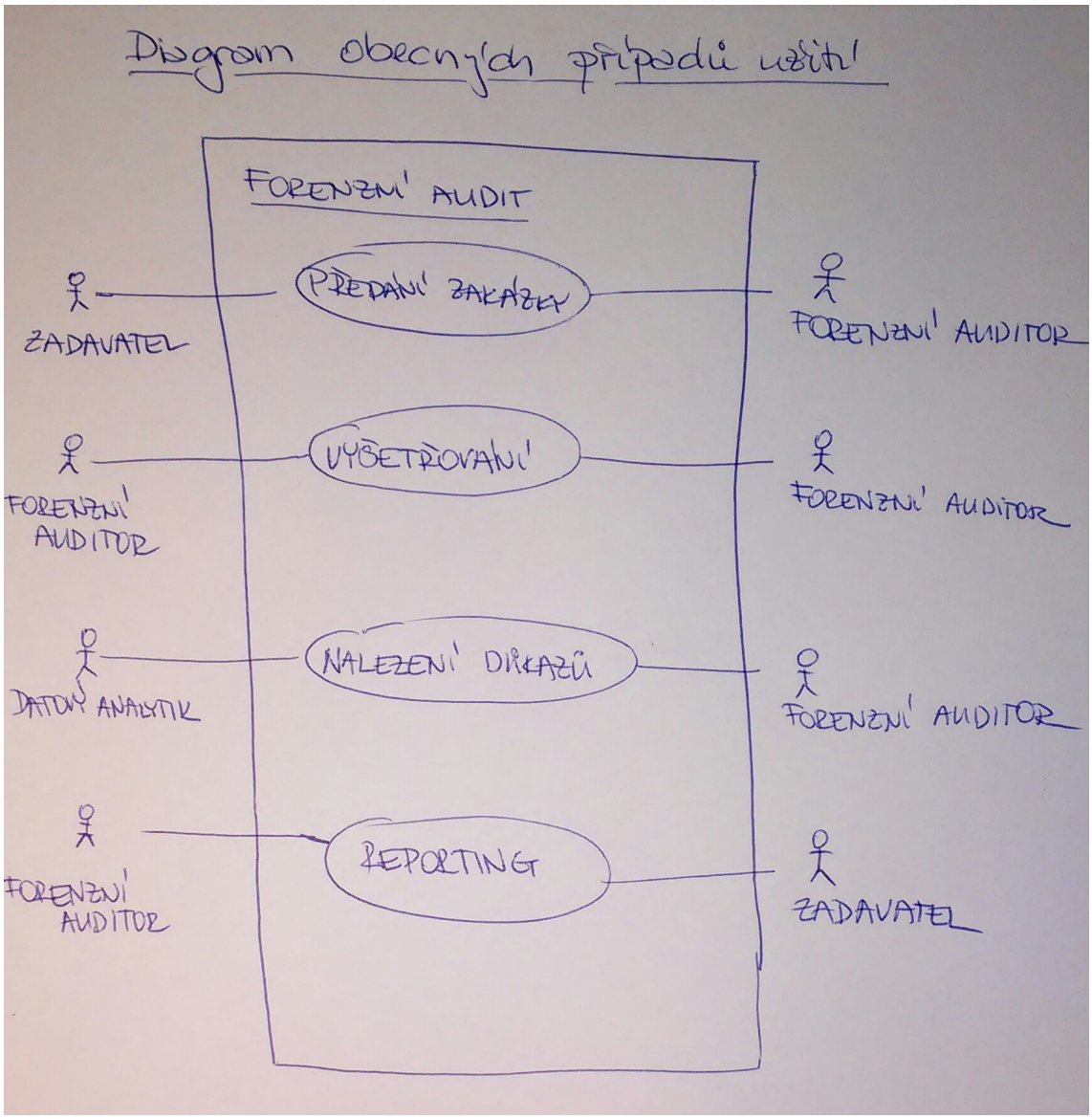


Figure 1.2: Velky obrazek vsech zainteresovanych stran - f.auditor, datovy analytik pro FA, zakaznik (zadavatel, materska spolecnost)

Chapter 2

Original methodology for a computer aided forensic audit

Jsem si vedoma, ze jsem clovek, ktery to nikdy nedelal (= omezena znalost). Toto je jak to chapu. Toto neni jak by to nekdo mel delat. Toto je seriozni pokus popsat proces forenzniho auditu. PROCESNI DIAGRAMY!!!

vystupem = okomentovany obrazek, ktery dava hlavu a patu

s Use case diagrammem pak kontaktovat praxi

We are aware to have only limited knowledge of forensic audit and no practical experience. This chapter should not be considered as a manual explaining how forensic audit should be done. However, this is rather a serious attempt to describe the process of forensic audit.

2.1 The phase of preparation of the forensic-audit process

Before the process of forensic audit starts there is a block of organizational or administrative affairs that needs to be [AJ!] done . It all starts in a institution where there is a suspicion of an act that is not following required rules. The institution might be of various kinds. A example can be an international corporation suspecting one of local branches from a money leakage. dalsi priklady?

The rules might be either internal regulation or corporate policies or even given by law. Basically any kind of misbehavior can be investigated by forensic audit. Given the background of the case the ordering party might also be of multiple kinds and from various branches of economy. They usually suspect possible internal or external risks that can be represented by fraudsters or people committing some other type of crime. Generally the ordering party is the head of a given company. Some specific cases are: CEO of certain company, new holder of an existing company, authorized representative of a supervisory board etc.. However forensic audit can be also assigned by a court or the police.

After the decision to perform forensic audit the ordering party contacts the audit company and they negotiate with a business representative about the sphere of the contract, price and deadlines. If there is no agreement it is probable that the ordering party contacts another audit company. It is important to familiarize the ordering party with the fact that while conducting forensic audit the auditors might need access to various confidential information concerning the ordering company. On the other hand the audit company undertakes not not to manipulate with this data in a protective way and not to expose it to the risk of misuse. If both parties agree with the conditions the contract is made and the case is accepted.

In the audit company there is a team of specialists established according to the character of the case. It is important to be aware of conflict of interest in this phase. Members of the team must not be related in any way to the original case. Members of the team can be forensic auditors, data analytics, specialists in any particular field (biometry, data recovery, criminology, law, etc.), consultants and assistants.

When the team of auditors is established the next thing is creating a document for record of the investigation. It also serves as a documentation. It is also common to create a nickname for important subjects and for the case to provide security of the confidential information. This is the end of all the administration that needs to be done before the actual forensic audit.

2.2 Accumulation of data

In the beginning of the investigation the team needs to gain an insight into the background situation of the case. They can learn it from materials they have been provided by the client. An appropriate strategy for investigation is created. It means, that all the relevant methods are taken account of and the best are chosen.

In all the cases it is important to secure all the documents, data repositories and all other possible sources of (digital) evidence. Any unauthorized person must not have a chance to manipulate with any possible evidence. For this reason backups of all the digital information are made. According to a FBI statistics the average investigated case size is approximately 500 GB. citace (ariu- paper, zdroj 13) In fact there are usually two copies of the data. The first is utterly for backup and the second can be used for analysis and work with the data.

The investigating team needs to evaluate all possible available sources of important information, access and gain the data. If the case is somehow special it might be needed to authorize an specialist to collect specific pieces of evidence. An example could be a case when fingerprint recording is needed.

It might be useful to visit the workplace of the investigated company and check if there are some other possible sources of evidence. After having all the data secured in some cases it can be also beneficial to perform a cross examination. It can be done even by mere conversation with involved persons, but it should be recorded.

It is possible that already in the end of collection of data the forensic audit team

has a idea or even hypothesis about what happened in the chase. Having this idea might be useful in further investigation, but auditors should beware of jumping into conclusions. All the actions and also the potential hypothesis should be documented in the case documentation.

2.3 Examination

The phase of examination comes when all the data is collected. Methods of examination are very different according to the character of the case, the sources of data and also the field that is investigated.

In the examination phase it is necessary at first to assess the data and mine the relevant pieces of information from all the collected data. It starts by identification of the data files that contain information of interest. Forensic auditors must not be discouraged by the size of data. After those files are identified it is often demanded to filter the extraneous information and leave only the coarsely filtered data.

2.4 Analysis

After the data being pre-filtered there comes the most extensive part of the investigation. The aim of analysis is to study and analyze the data to draw conclusions from it or to determine that no conclusion can be drawn. By the end of analysis most important subjects, events, people, and people and relationships between them should be recognized. In order to find the conclusion it is required to unite information gained from multiple sources of data.

However first of all to obtain the information hidden in the data, specific sources of data need to be analyzed by a competent specialist. For example provided that a file contains billing data the task is delegated to accountancy specialists. They can use appropriate accounting software, or extract only data of particular interest and use some quantitative software. If the data contain log files, or deleted files it is a job for information technology specialists to recover or examine the data.

Several methods the team of investigators might use are: quantitative software analysis, analysis of relationships between persons, making use of analytical software. In case of suspicion from corruption a investigation of decisions made by the management of the company might be needed. Investigators might pose questions similar to following. Who are the suppliers of the investigated company? In what business the company invests and who decides about it? Who does have an access to (financial) resources?

There might be cases when specialists in various sub-branches of forensics might be needed. Even an external company might be hired to solve a particular problem. Examples of auxiliary specialists can be experts in computer forensics, forensic dactylography, digital forensics, forensic biometry, forensic psychiatry, forensic linguistic etc. According to all available expert's opinions the situation in the case is

gradually revealed.

All the steps proceeded in the analysis result in understanding of the situation in the case. According to the information investigators gained a verdict is pronounced and retrospectively supported by the data collected in the beginning of the process.

2.5 Reporting

After having investigated the assigned case the team of forensic auditors has some results to show. Either they have found what undesirable actions happened or there might be cases when they have not discovered any signs of such behavior. In both cases proper results are presented to the ordering party.

There are multiple possible results of previous investigations. Basically either a crime has been discovered or it has not. If the investigation discovered a crime in the report must be mentioned the exact methods that lead to the discovery together with the evidence supporting the result. The report should clarify if there is enough evidence. If there is not enough evidence the type of data needed to prove the result should be described and reasoned. The explanation why there is no evidence yet should be also given.

If no crime has been discovered in the reporting stage there still must be explained what data has been investigated and how the investigation was conducted. Everything that has been find out about the case should be in an appropriate form presented. Special effort should be made in explanation of an alternative solution. One explanation might be that there has not been enough time to process all available data. In that case it leads to customers decision. They decide whether they want to continue the investigation in more details or whether they are content with the result and they already believe that no crime has been committed. This situation is very case-specific.

According to the result of the investigation several additional information might be suggested. This might be for example an advise about subsequent actions preventing repetition of the undesirable behavior. While investigating the case sometimes forensic auditors might discover completely new problem in the investigated company. This additional information should be also included in the report.

The actual reporting is affected by many factors. When preparing the final presentation these factors should be considered. First, the presentation should be prepared with regard tho the audience the speaker is going to have. The extent of professional details regarding the methods used in the process should be adjusted to the anticipated knowledge of the audience. However, if asked, the speaker should be prepared to explain the details. The presentation should be easily comprehensible and explain everything discovered in the investigation.

One part of the report might be focused on alternative explanations of what happened. This may happen if the information that has been found about an event is incomplete. Alternatively it may happen if there are more plausible explanations

about what happened. Each of these explanations should be analyzed in the previous steps and an attempt to prove or disprove them

Besides an oral presentation the output of the assignment should be also a written document describing all the important facts about the case. This document should be handed over to the ordering party and should contain:

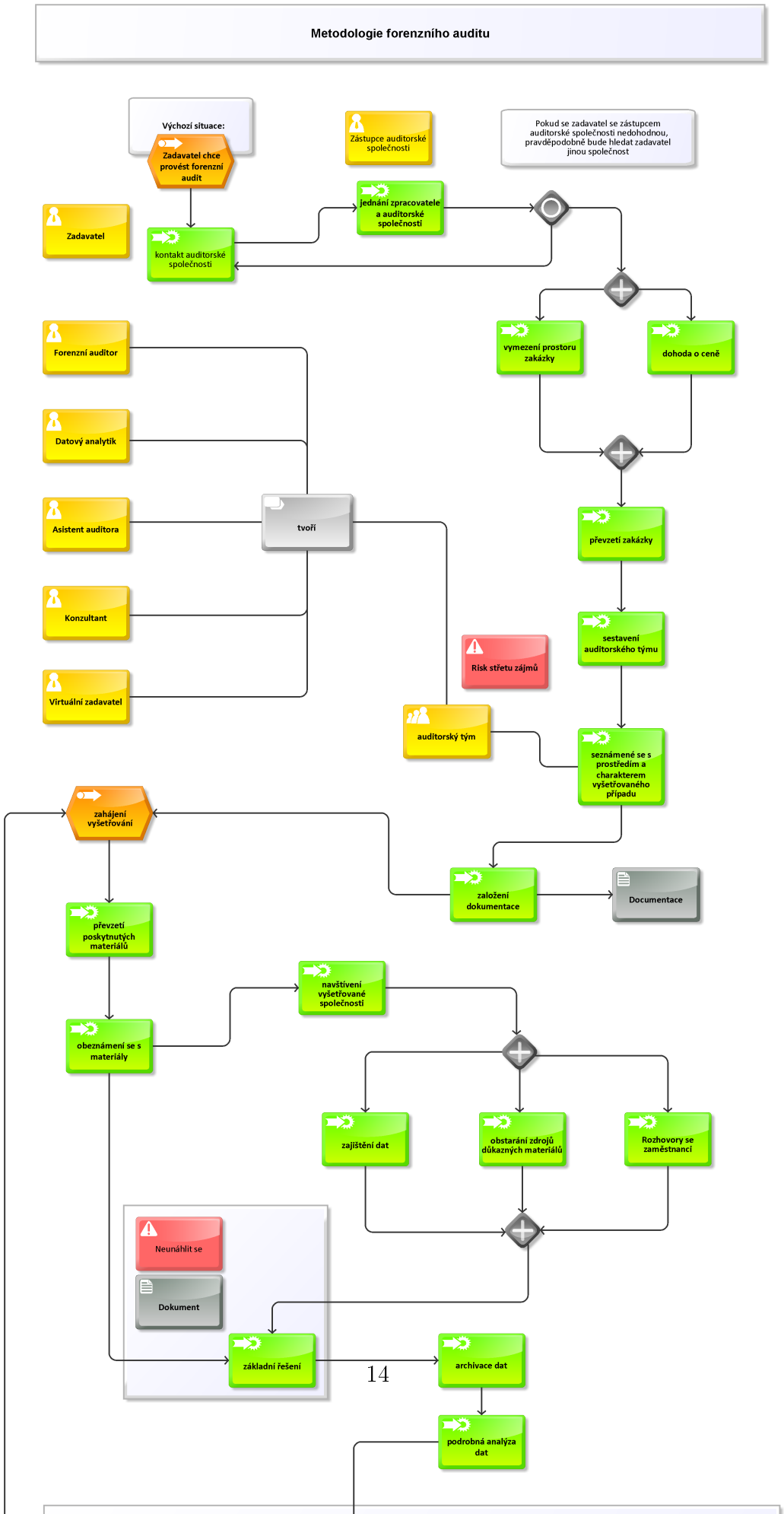
- information about the agreement between the two sides
- list of sources of evidence in the investigation
- description of methods used in the investigations
- the sequence of important evidence found in the data
- explanation of the evidence
- summarization of what the evidence result in
- recommendation on how to prevent similar further actions
- optionally a suggestion what steps should be made to improve the current state
- conclusion of the case

2.6 [AJ!] Work following after a forensic audit

- posledni faze
- priprava na prezentaci vysledku
- vytvoreni alternativnich reseni (pokud mame nekompletni informace o tom, co se stalo)
- zvazeni komu budou vysledky prezentovane
- navrhy opatreni vzhledem k vysledkum forenzniho auditu
- oznameni jinych problemu na ktere se mimochodem pri vysetrovani prislo
- navrhy ve vylepseni procesu a smernic (ve firme)

DALE:
- rozsireni expertizy auditorske spolecnosti, ale s ohledem na citlivos dat v danem pripadu - sledovani trendu v technologiich a novelach zakonu

timhle diagramem bude problem, budu ho muset primutit aby se rozdelil na vic stran


Metodologie forenzního auditu
Výchozí situace:
Zadavatel chce provést forenzní audit
Zástupce auditorské společnosti
Pokud se zadavatel se zástupcem auditorské společnosti nedohodnou, pravděpodobně bude hledat zadavatel jinou společnost
Zadavatel
kontakt auditorské společnosti
jednání zpracovatele a auditorské společnosti
Forenzní auditor
Datový analytik
Asistent auditora
Konzultant
Virtuální zadavatel
tvoří
vymezení prostoru zakázky
dohoda o ceně
převzetí zakázky
sestavení auditorského týmu
Risk střetu zájmů
auditorský tým
seznámené se s prostředím a charakterem vyšetřovaného případu
zahájení vyšetřování
založení dokumentace
Documentace
převzetí poskytnutých materiálů
navštívení vyšetřované společnosti
obeznámení se s materiály
zajištění dat
obstarání zdrojů důkazných materiálů
Rozhovory se zaměstnanci
Neunáhlit se
Dokument
základní řešení
archivace dat
podrobná analýza dat

Chapter 3

tato kapitola by asi mela obsahovat oduvodnene pozadavky na vlastni metodiku, pouzitelnou ve FA s ohledem na ostatni pristupy a metodiky

jaky je rozdil mezi metodikou, kterou uz mam vytvorenou v arisu a touto vlastni metodikou?-> je to totez

3.1 Pribuzne metodiky

3.1.1 Obecny project management (zde je projektem FA projekt)

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

3.1.2 Obecne zpracovani objednavky (zde je objednavkou FA projekt)

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like "Huardest gefburn"? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression

of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

3.2 Specificke pozadavky pro FA

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

3.2.1 Zohledneni rizik

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

3.2.2 Zohledneni ruznych dat

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information. Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

3.2.3 Zohledneni ruznych zpusobu zpracovani a intepretace dat

Hello, here is some text without a meaning. This text should show what a printed text will look like at this place. If you read this text, you will get no information.

Really? Is there no information? Is there a difference between this text and some nonsense like “Huardest gefburn”? Kjift – not at all! A blind text like this gives you information about the selected font, how the letters are written and an impression of the look. This text should contain all letters of the alphabet and it should be written in of the original language. There is no need for special content, but the length of words should match the language.

Chapter 4

Design of an information system for support of forensic audit

vsechno o tom systemu jako takovem, ale tak, aby to navazovalo na predchozi...?

prostredi webu + silne zabezpeceni, reporty, export, pdf
maly informativni obrazek, ktery poskytne uzivateli informaci o tom, co se stalo
! pripojit pripady uziti vcetne zavislosti

jedna se o aplikaci, ktera provazi celym projektem (zadanim) forenzniho auditu. sice existuji i jiny nastroje pro podporu takovychto projektu, ale projekt ma useky a nam jde o integraci porizenych vysledku

Chapter 5

Discussion

5.1 Further improvements

- pokryt dalsi administrativni casti (zacatek, konec)
- detailnejsi navrh a implementace
- detailnejsi osetreni rizik
- zamysleni nad sdilenim zkusenosti (duvernost vs. rust expertyzy auditorske spolecnosti)
- vyuziti mimo FA - jina administrativa + moduly pro vyuziti policii / soudy

pouzitelne technologie!

Attachment A

Contents of the CD

The text of this bachelor project in pdf

The text of this bachelor project is saved as `BP_Peskova.pdf` in root folder.