
Implementing Ethics Auditing Model: New Approach

Authors: Merle Rihma, Birgy Lorenz, Mari Meel, Anu Leppiman

The aims of this article are to test how does enhanced ethics audit model as a new tool for management in Estonian companies work and to investigate through ethics audit model the hidden ethical risks in information technology which occur in everyday work and may be of harm to stakeholders' interests. Carrying out ethics audit requires the diversity of research methods. Therefore throughout the research the authors took into account triangulation method. The research was conducted through qualitative approach and an analysis on a case study, which also included interviews, questionnaires and observations. Reason why authors audited ethical aspects of company's info technology field is due to the fact that info technology as such is an area which is not handled in any CSR reports but may cause serious ethical risks to company's stakeholders. The article concludes with suggesting an extension of the ethics audit model for evaluating ethical risks and for companies to help to raise employees'- awareness about safe internet using and responsibility towards protecting the organization's information technology and to prevent ethical and moral risks occurring.

Keywords: *Ethics audit, stakeholders, corporate rules and regulations, information technology (IT), internet safety*

Introduction

In various statements by numerous institutions (e.g. Estonian Ministry of Foreign Affairs, E-Estonia) Estonia is considered of one of the leading E-governance and a society that relies on technology and internet. This is a

weakness and strength at the same time. Estonia has lots of services which people can access through computers and mobile phones despite these online services being very time efficient, the services oftentimes result in raising a risk of becoming too open for exploiting the expected users' goodwill and resulting in violating the individuals' privacy. By words of Mietinen (2004) new economy is to a large extent a technological revolution involving the information and communication technologies and which affects almost all aspects of the economy, business and people's personal lives. In the current study the authors focus on the area which is in the middle of IT and ethics, as there are issues that neither field has (internet safety, espionage, business ethics, social manipulation, online behaviour and rules and regulations that focus on solving these issues for the companies). In this paper, IT is considered as a mean for using info technological equipment's like computers, phones, tablets, online and computer programs in everyday work. There are some previous researches (Ribble and Bayley 2004, Lessing 1999, Spinello 2010 etc.) conducted in the field responsible of technology use and cyber ethics. Discussion about setting new online rules and regulations have come up in several occasions to regulate advertisement (Nettleton, 2008, Jones, 2011) and data gathering (Eecke, 2009) which solely focus online client and business relations. Although there are lots of regulations and suggestions on how to survive and protect yourself or you company in computer using, there are always risks not to act according to rules. In Estonia there have been no previous attempts to carry out ethics audit in private sector.

The research gap is to find out whether the ethics audit model works in small Estonian company as ethics audit seems to be unknown within Estonian companies. A conceptual model was created in 2012 by Rihma and is displayed in current research. The research is aimed to discover the hidden ethical risks in the examined small Estonian company where, like in most of companies, IT is used as toolbox in everyday work.

Authors' goal is to investigate the ethical challenges regarding the use of IT at workplace. The auditing model was adapted for the current research in the minds only of internal stakeholders' (owners, employees and customers) expectations and by adding the information technology audit area that will be explained in more detail in the forthcoming chapter.

The research questions were:

- how will ethics audit contribute to the prevention of risks in information technology
- what have to change for modifying ethics audit model

By using the ethics audit in the technology field offers the company the insight and enables it to develop tools to protect the business and workers from hidden risks and ethical issues which may usually stay unnoticed when doing these two audits (ethics and IT) separately.

The auditing process in current research involves three components: ethical framework of auditing model (Kaptein, 1998; Rihma, 2012), elements form cyber security audit (Northcutt 2004); internal stakeholder's interests toward company. An auditing gives the overview on how company in its daily business' meets internal stakeholder's interests from the point of their expectations in IT field.

Theoretical clarification: stakeholder's theory, ethics audit and ethics of info technology

Business can be understood as a system of how to create value for stakeholders. For maintaining the organization it is essential to build strong relationships with stakeholders and fulfil their expectations (Mahoney, 1994; Ambler and Wilson, 1995). Each and every member of the organization has to remain ethically responsive in relationship to its different stakeholders (Morland 2008).

According to R. Edward Freeman (1984, 2010) the corporation should to be managed for the benefit of its stakeholders: shareholders, employees, customers, suppliers and local community. Domenec Melé (2012) argues that stakeholders are people affected by or who can affect the activity of the company. Managers have to ensure that stakeholder's interests are secure in every level of company's activity. Unethical behaviour or negligence attitude towards stakeholder may decrease trustworthiness between stakeholders

There are several definitions and principles on how to classify stakeholders. Even Freeman (2010) has no clear cut answers for how to notice internal or external stakeholders who belong to the abovementioned groups. Freeman considers internal stakeholders as owners (or shareholder), employees, managers, customer and suppliers. In current research authors based on the viewpoint of owners, employees/managers and customers for

reason that they are directly threatened risk which are caused from info technological issues. Ethical issues in info technology are directly related to general business ethics principles.

There is always a question on how to measure ethical business behaviour or what is business ethics at all. A generalizing business ethics definition by Lewis (1985) - after reviewing 158 textbooks - states that business ethics consists of rules, standards, codes or principles which provide guidelines for morally right behaviour and truthfulness in specific situations. To be more specific - empirical ethics developed by Musschenga (2004) states that the study of peoples actual beliefs, intuitions, behaviour and reasoning yields information that is meaningful for ethics and should be the starting point of ethics. The aim of empirical ethics is to improve the context-sensitivity of ethics. This approach is suitable for ethics audit as well; because ethics audit will highlight through the employees` company`s real microclimate and same time helps to raise employees` awareness of ethical behavioural risks.

Ethics audit can be used in different fields to analyse ethical risks in company. Ethics audit is flexible; it works according to company`s individual circumstances, including their size, type, legal structure or industrial sector of operation. Main structure and processes of ethics audit model should be followed.

According to Mackenzie (1998), Domingo (2005) and Kaptein (1998) ethics auditing reflect the extent to which the company meets the economic, social, and environmental demands on which the trust placed in it depends. Usually ethics audit involves compliance with stated rules or regulation (code of conduct, values statements etc.) or by other words comparison between actual employee behaviour provided in rules and procedures. According to the Stephen Northcutt (2004) the IT- audit functions allow professionals to perform review of the security risks and corresponding controls to incorporate changes to the business requirements and priorities. Auditing compares company`s policy and culture versus legal requirements and will try to compliance the aforementioned with real behaviour. The purpose of IT ethics audit is to carry out review of IT system, the controls and corresponding ethical security risks like leaking of confidential information, privacy and possible attacks towards company's stakeholders. Hereby auditing is considered through the lens of internal stakeholder`s expectation. In the current case study ethics audit was carried out to find

out shortcomings and risks which could be harmful in IT aspects and to be more focused in cyber ethics through stakeholder’s lenses.

As mentioned before the current ethics audit is based on qualitative research with a methodological triangulation being used. For clarifying auditing process visualization of auditing model in Figure 1 is given.

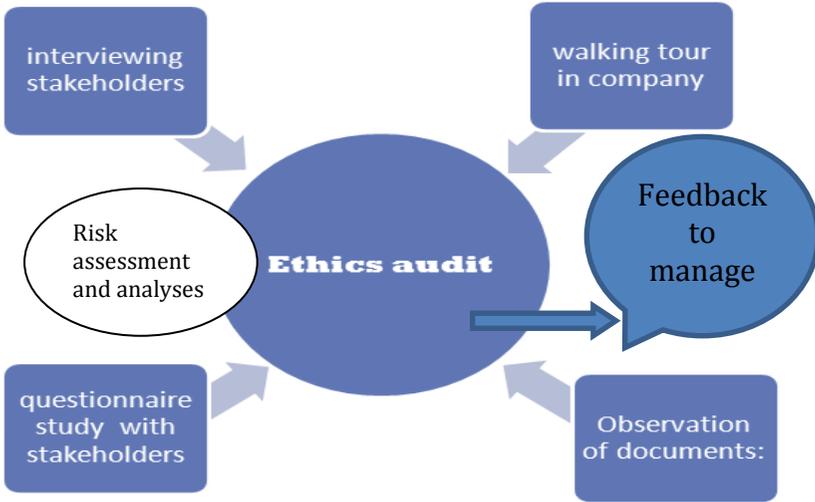


Figure 1: ethics audit model (compiled by authors)

There are four main data sources as input to auditing process: questionnaire, documents observation, working tour in company and interviews. All data will collected, categorized, analyzed and assessed through risk assessment matrix. Auditing committee gives feedback to management or stakeholder group.

Organizations have a responsibility to act ethically in everyday use of info technology. IT related cyber ethics has gone long way since 1950 when this issue was first mentioned. In the beginning there was the fear about artificial intelligence and database privacy, which was later followed by the concern intellectual property, software piracy and computer crime. At 1990 people started to talk about free speech, anonymity and virtual communities. Taking into account the constant development and innovation happening in the information technology sector, it is likely that in the future there will probably be even more discussion about artificial electronic agents, such as ethical matters with regard to robotics (Tavani,

2004). According to Gotterbarn (2001) IT professionals have opportunities to do well or cause harm and enable or influence others to do so. The only way to restrict it to happen is to implement professional codes of ethics or relay on company's shared values. Challenges that companies face are related to various issues with regards to privacy (Regan 2002), keeping track of confidential information (Rowe 2006) and the freedom of speech (Spinello 1999). It is evident that internet has opened doors for everyone to post and comment on all kinds of matters on the Worldwide Web and has enabled its users to be approachable at any time and any place. However, despite the numerous positive opportunities internet has offered to its users, it should be born in mind that these same opportunities may also be taken advantage of and thus may be of a potential concern for the possible limitation of freedom of speech. Risks in IT field usually involve phishing, modifying systems or data, counter fiction, distributed denial of service attacks or simply making them ineffective. The most problematic aspect for the organization is to discover its weaknesses in cyber security that concern management, resources, documentation, security measurements (Hanson, 2009). That is why our study focuses on more legal justification and ethical behavior of humans that are using software and webs to interact with each other inside the company.

Methodology

As auditing process involves different research methods, authors hereby found the best and most qualitative method is a triangulation. Triangulation means integration of different methods, empirical research material or frameworks into research (Denzin 1988). There are differentiated (Denzin & Lincoln, 1998) four types of triangulations: multiple data sets, multi investigator, and multiple theory and multi method. The multi method contains two subtypes (Leppiman, 2010) an inner and an external triangulation. Also another advantage of this method is that the particular weakness of one method could be compensated by the particular strength of another (Denzin, 2006), for the same reason this method is widely used in social sciences. In current survey the authors used multi method as questionnaire, interviews, observation of documents and working environment to be more specific authors used case study which is known as a triangulated research strategy as well. Whilst conducting case study, Yin

(1994) recommends three tasks that must be carried out for a successful project: preparation for data collection, distribution of the questionnaire, and conducting interviews.

To test our ethics audit model the auditors carried out a six stages study in one small printing company (38 workers) which got a prize from Responsible Business Forum Index 2011 (RBF) in Estonia. Company was selected from top companies in the RBF list which has Estonian background (all the shareholders are Estonian). The audit in the information technology field was firstly agreed with the management of the investigated company in a preliminary manner since the company had not conducted any investigations – including ethical risk and threat assessments- itself in the aforementioned field, yet the ethical behavior and matters related to responsibility were already investigated in the company through CSR reports. The auditors chose an Estonian company since all the big international companies are by default meant to follow the headquarters requirements. Also the selection of participants in our research was a matter of convenience – in other words much of it depended on the availability of the company to allow the auditors to conduct this research.

The auditing was carried out by auditing committee. As settled in auditing model for Estonian big and middle size companies (Rihma 2012) there were three basic restrictions for committee experts:

- He or she has to be an active researcher in business ethics; publishing one to two scientific articles per year in a reviewed journal or has given presentations in conferences.
- He or she should have practical experience in corporate government.
- He or she should not have any kind of interest towards the organization being audited.

All this requirements were met by auditors. The auditing committee consisted of two auditors, supervised by associated professor. Two authors of current article were the auditors and another author participated as supervisor.

It is crucial that during planning and implementing ethics audit the authors would develop mutually supportive and collaborative relations with the company being investigated. First of all auditors started introducing the principles of ethic audit, since all the auditors were a pioneers in the aforementioned field in Estonia. All ethical parameters of the research

methods and confidentiality issues were mutually agreed between both parties –the researchers and the company. The aim of auditing from company side was to get overview about ethical issues and threats connected to info technology.

The auditors got a primary data about company before the auditing process from public media, annual report and some informal sources (friends, familiar businessmen).

Ethics audit in current research was built up as it was given in figure 1 and settled as follows:

Stage I – questionnaires conducted amongst the company's employees. There were no special written regulations, rules or codes of conduct to which to rely on (except some contracts) during the auditing process. The aim of the questionnaire was to get first information about employees' awareness about ethical issues in information technology. The survey was carried out within half of the company employees who volunteered (n=17, ~ 50% of employees) in May 2013. Survey was provided both electronically or on paper and consisted of four parts: overall background (12 questions), IT usage (10 questions), ethical dilemmas (8 questions) and ethical risks (7 questions). Questions were both open and closed; in addition the liker scale was being used. Survey gave us overview about the overall background of the company, people's knowledge about IT area and on various ethical issues. Data was analyzed in excel and auditors used this data as preformation for providing an input to interviews and case study analyses. These results gave auditors' the basic informational starting point for the forthcoming auditing process.

Stage II – A tour at the company's work space was conducted during the work hours (offices, preprint area, leisure area etc.) for getting information about the physical evidences which could support or deny the results of interviews or surveys. The auditors took photos and videos to save all data from this stage of the survey. This method was considered as non-participatory observation which allows following the ordinary working conditions and environment.

Stage III – Focus group interview (Valtonen 2005, 223; Leppiman 2010, 119) with company workers moderated by the auditors.

Auditors decided to use interview as research method mainly for two reasons: firstly, as mentioned before the topic and ethic audit was new for all involved persons and the interview enabled the researchers to clarify the questions or reformulate the issues immediately when needed and to get better understanding of subject. Secondly, in this survey as in qualitative research persons attitude and opinions have significant meaning in whole process (Laherand 2008).

The purpose of the interviews was interrogating the essence of the ethical climate in everyday work conditions tied to IT. Whilst preparing and conducting the interview, the auditors were aware of the possible biases and questions organized with special care. Auditors used open-ended semi-structured interviews to expand the depth of data gathering, and to increase the number of sources of information. Participants were two individuals from the management level and three specialists were also present with voluntary base different occupations such as sales manager and accountant; secretary, designer, new employee from printing area to be represented those from the company that directly are using technology, internet, company servers etc. Interview consisted of 14 questions which were divided to IT and ethical areas and was done in pairs (management) and threes (specialists) during their extended lunch time (1 hour) as a group interview. The interview questions were semi-structured and developed from the literature survey. The survey was not anonymous, but all employees knew that their interviews were confidential and that honest answers will help to improve their everyday work in this company. The analysis was carried out as a qualitative content analysis (Mayering, 2000; Leppiman 2010, 124-125).

Interviews recorded (prior permission was given by the participants); after several time listening all text was transcribed. As suggested by Laherand (2008) written text was read many times before categorizing raised issues: IT issues, ethical issues and general issues. The appeared risks were marked in the colors of traffic light: red – highly critical, amber – medium and green as best practice or good sign.

Stage IV – discussion was conducted about ethical dilemmas with two people from management and two specialists, with one person being the same who participated in interview (the company aside organizer). The auditors used two cases: one was about company secretary that used computer as a public computer (everyone could use it and get access to

client's private data) and another one was about a photographer that mixed up work and private life by putting client's data on social network. Discussions varied from 45 minutes to 1 an hour. Participants were first asked to read the story and to discuss it then with peers; participants marked out ethical, IT and privacy related challenges and then presented the findings to others. After that they discussed whether these kinds of problems emerge at their company and what may be the best policy to avoid these. This method also raised several extra questions from the company's side on how to deal with IT ethical dilemmas or even how to manage technical system better.

The auditors collected data from employees and managers, but the discussion involved also predictions on how other stakeholder groups (clients and owners) are directly affected in their behavior around technology. Results of the interviews and discussion were transcribed and analyzed as described in stage three.

Stage V – documents analysis on contracts between workers, clients and information technology service provider and company; basic information that is displayed at company website to guide workers, clients (mission, CSR principles, portfolio of services). This gave us information on standards and regulations that are already implemented in the company and provided an input for the foundation in the model compared to what auditors will analyze in the results. As some of the materials were confidential auditors were not able to get a hold of all of the documents, but auditors were able to contact to the person who was responsible for the documents and who gave us the insight of the content in the papers. Auditors used this information as only material for compliance with further research.

Stage VI – The auditors analyzed risks and gave feedback to company management. As indicated before several time in this article and based on Rihma auditing model (2012), risk analyses is connected to auditing process as a new instrument. The risk analysis was based on risk assessment matrix where the likelihood of a risk appearance and risk significance has been identified in four quadrants. It is visualized through heat map where I quadrant "Prevent at Source" includes risks which are classified as primary risks and are rated "high" priority.) In II quadrant called "Detect and Monitor" risks are significant, but they are less likely to occur. III quadrant

“Monitor” risks are less significant, but have a higher likelihood of occurring and in last quadrant “Low Control” group risks are both unlikely to occur and not significant.

Analyzing auditing process and results

Authors approach to analyze implemented ethics audit model is structured according the stages of auditing process and in every stage there are results in three level - first best practices of auditing process will described, then parts of auditing process which could be improve will be pointed out and in third part failed actions will be analyzed. In this article authors do not demonstrate real finding about IT shortcomings because of the silent agreement with company 's mangers and due to of the small business society in Estonia the company could be identified. After the audit substantive feedback was given to company's management.

Questionnaire

Starting from questionnaire, ordinary written anonymous questionnaires give the most honesty answer to questions and gives the best basic awareness of company's' real business behavior however in this case the sample size was not reliable enough.

In fact employees have a large amount of information that the public, the media and even managers are not aware of. Not every breach of ethics is illegal, either, and employees can be an insightful source of information on legal breaches of ethics occurring on a regular basis. This is the reason why well prepared questionnaire is best source of information. The authors are not satisfied with a sample size in the present auditing process which was rather small to point out any findings. As mentioned before all the data we got from the questionnaire was used as preliminary information. In the future for the auditors to carry out ethics audit auditors should have to get reliable sample size.

Walking tour

A lot of information is available by simply observing the company during working hours. Many routine activities or special operations will provide

adequate picture about the actual work environment within company. The organizational culture will be better understood by seeing the physical evidences. Looking same things and issues from another point of view could be help to discover new nuances and hidden risks. Usually people are not aware of the risk or forget to act properly in a workplace to protect this kind of information (both physically and virtually). No restriction for photographing was set by the company, meaning that all guests can easily take photographs or videos without limitations and by doing so, posing serious risk to the security of the company.

Interviews and dilemmas

Conducting the interviews and solving ethical dilemmas gave valued information for auditing process. Experienced interviewer can interpret body language, an attitude, a microclimate and interviewee's feelings (Gillham 2009) besides to simply analyzing the verbal answers of the interviewees. During interviews there was appearance that employees were loyal and had strong unity. In same way all negative aspects appeared which could indicate to further risks.

Representing interviewees in a group gave us the impression that they could not talk about everything what was going on in detail, but gave us good overview of the current situation and of the basic challenges, whilst having the possibility of being able to support other employees arguments. Results from this area gave information which was later compared to documentation; it also gave a lot of information on work process, cyber security issues, ethical understanding and sustainability. Auditors used content analyses to understand more precisely all interviewees' statements and data between the lines (Richards 2009).

Using stories in solving ethical dilemmas can be used as the silent teacher which raised a new understanding among interviewees' about the possible risks and opportunities.

Lessons the auditors learned indicate that to get more reliable audit results employees should be interviewed individually as there were some signs which indicated that experienced workers were more loyal than the new ones. After the auditors realized that interviewing the shareholder of the company is inevitable, because the many thing which appeared or was confirmed during interview and look like not problematic issue to

employees or managers but definitely may harm shareholders' interests (like hackwork with employer's tools, easy access to confidential files etc.).

Observation of document

To avoid hypocrisy practices must not contradict the company's proclamations (Rihma 2013; Wagner et al. 2009; Brande 2010). Compliance document and real behavior are crucial aspects in trust creating process because both are preceded mainly from company's decisions and real behavior. What is once settled should be followed.

As mentioned before there were not many documents to have based for compliance especially talking about IT related documents or procedures. The auditing process should be supplemented with minimum requirements of compliance mechanism. Meaning that during the auditing process one should follow compliance with certain basic box of moral values or cyber ethics, but in this case there was not possible to use a checklist for basic requirements (excepted different kinds of contracts). In this case neither of the auditors followed the compliance of Estonian RBF index questionnaire as it appears to have very little to do with IT ethics and responsibilities.

However, auditors can assume that the contracts between employee and employer regulate confidentiality clauses and detail instances such as the employers right to read employees e-mail etc.

Risk assessment, analyses and giving feedback

For summarizing the auditing results all identified risks were assessed which occurred in the I quadrant are given in the Table 1. Risks in that quadrant "Prevent at Source" are classified as primary risks. These are the critical risks that threaten the achievement of company objectives. These risks are both significant in consequence and are likely to occur and should be reduced or eliminated with preventative controls. It is also agreed that these risks should also be subject to control evaluation.

Risks were estimated by auditors based on the collected information. Nevertheless, there was the possibility that some risks seem to the auditors bigger or - on the contrary - are underestimated, thus it would be beneficial to have a dialog with the management during risk mapping.

After auditing a written feedback and full ethical risk analyze with suggestion to the company's management was given. In the report every finding was supported with at least one example drawn from the facts determined in the auditing process. Results of auditing process (questionnaire, documentation survey, interviews, and workplace survey) auditors analyzed all answers according to internal stakeholders' interest - how these hidden risks can affect their expectations towards company and whether there are any risks which would reduce trustworthiness amongst stakeholders.

Feedback contains company's description of audit methodology, interpreting data; best practices, hidden ethical and IT related risks were pointed out. Feedback document was structured by stakeholders group: employees, managers, customer and shareholder. Management of audited company accepted proposals of auditing committee. After receiving feedback a telephone conference was held on the matters as well. Results of risk analyses help managers to prevent hidden risk. A relationship based on mutual trust and respect enabled the ethics audit to be conducted and reported in a way which would create the most efficient response. Results indicated that in the company under the survey there were no contradictions between the declared values and actual values.

Since hereby described and used ethics audit process includes methodological triangulation which easily brings out hidden risks in selected area. All used methods were familiar to auditing subjects and authors can assume that the first attempt to pioneering ethics auditing in Estonian business environment was successful for both party - for the auditors and for the management. Linking ethics audit to risk assessment gives to the model a specific value. Ethics audit does not only discovers the hidden risks but also categorizes risk by significance and likelihood. Ethics audit will easily discover risks from the grassroots level and bring out the contradiction between declared regulations, documents and real environment. Oftentimes problems are being caused by the inexperience of employers with regard to data leaks since these instances have not been allegedly apparent in most companies. Throughout the use of ethics audit these kinds of risks and shortcomings can be discovered in time and will give the opportunity to manage risks proactively and systematically.

Limitations of auditing process

Despite of successful auditing process there are some shortcomings and limitation for improving auditing model. On one hand the multiplicity of the research methods may have caused a situation where the interviewees did not interpret the questionnaire unanimously. On the other hand it was possible to check the coherence and to increase the reliability of data.

First, as mentioned before questionnaire is a valuable source in the general data gathering stage. Reliable sample size gives auditors the quantitative information which will be used whilst comparing auditing results in different period. In current research auditors lost that opportunity. Qualitative data has proved to be difficult compare in follow up activities. Secondly, interviews held in groups could deface information because of fear to tell something wrong or unexpected. In same time the genuine opinion from every member of organization is important for putting together the big picture. Besides the group interviews, confidential individual interviews should be part of auditing in future as well.

Biggest challenge in this process was the absence of compliance material like codes of conduct or codes of ethics or standards. It could be more successful process if in auditing preparatory stage the auditors can come to agreement with the management in certain basics requirements in what the managers would like to find out in the results. This is an overall issue in Estonian business environment that there is lack of behavioral standards, ethics code or other regulations.

It could be valuable to work out special auditing model for CSR reports used in RBF indexes to avoid the discrepancy between declared values and responsibility and real ethical behavior of companies. Authors would like to stress once again that in CSR reports or in another reports there are no places where one could report about these particular issues such as IT or public relations. Secondly, companies may have the opportunity to keep silent about inconvenient incidents or circumstances compiling CSR reports.

Conclusions

This study was the first attempt to provide ethics audit in an Estonian company. Whilst conducting the ethics audit, analyzing results and auditing

processes it became clear that the model and process need to improve and validate audit model and process for Estonian company.

Authors see continuing problem with compliance instruments, because major Estonian companies do not have a code of conduct or ethics or regulations to which compare real behavior.

Current pioneering auditing study investigates a special part of a small company. To test ethics auditing model more comprehensively there is need to practice this model all-around company and in different type companies (retailers, selling, servicing etc.).

Although the ethics audit process is time-consuming because of the amount of information and selecting relevant data it is effective and valuable management tool to provide sustainable trust between stakeholders. The authors would like to emphasize that microclimate inside the organization was mutually supporting, an attitude towards auditing process was contributory and the management was obviously interested in getting a constructive feedback. This encourages authors to continue to conduct ethics audit in Estonian companies and to work on improving the ethics audit model.

References

- [1]. AuditNet, The Global Resource for Auditors (2010). Risk assessment survey and risk mapping tool. [Online] Available: <http://www.auditnet.org/docs/risk1.doc> (July 5, 2011)
- [2]. Brande, M. (2010) *Corporate Social Responsibility: "Does the End Justify the Motive? The Influence of the Sincerity of the Motive and the Consistency of the Actions on Customers' Perceptions and Intentions*, Maastricht University School of Business & Economics, theses, [Online] Available: <http://delosfuegos.com/Thesis.pdf> (30. January 2013)
- [3]. Crane, A., Matten, D. (2010). *Business Ethics Managing Corporate Citizenship and Sustainability in the Age of Globalization*, Third Edition, Oxford University Press
- [4]. Domingo, G. M. (2005). *Trust and Dialogue: Theoretical Approaches to Ethics Auditing*. *Journal of Business Ethics*, 57, 209-219.

- [5]. Denzin, N.K. (1988). *Triangulation*. In: Keeves, J.P. (Edit.) Educational Research, Methodology and Measurement. An International Handbook.
- [6]. Denzin, N. K. & Lincoln, Y.S. (1998). *Entering the Field of Qualitative Research*. In: Denzin, N. K. & Lincoln, Y.S. (Edit.) Collecting and Interpreting Qualitative Materials. Sage. CA
- [7]. Denzin, N. K. (2006). *Sociological Methods: A Sourcebook (Methodological Perspectives)* Transaction Publishers
- [8]. Eecke, P., Truyens, M. (2009). *Social networking self-regulation initiative*. Journal of Internet Law, 1094-2904, 13 (1),
- [9]. E-Estonia the Digital Society (2014). [Online] Available: http://ccdcoe.org/cycon/2012/workshops/e-Estonia_03.2012.pdf (January 12, 2014)
- [10]. Estonian Ministry of Foreign Affairs, [Online] Available: <http://www.vm.ee/?q=node/18935> (January 12, 2014)
- [11]. Freeman, R. E. (1984). *Strategic Management: A Stakeholder Approach*, Boston: Pitman
- [12]. Freeman, R.E. (2010). *Strategic Management: A Stakeholder Approach*, New York: Cambridge University Press
- [13]. Gillham, B. (2000). *Developing a Questionnaire*, London: Continuum
- [14]. Gotterbarn, D. (2001). *Informatics and professional responsibility. Science and Engineering Ethics*, 7(2), 221-230.
- [15]. Greenwood, M. and Van Buren, H. J. III (2010). *Trust and Stakeholder Theory: Trustworthiness in the Organisation–Stakeholder Relationship*. Journal of Business Ethics, Volume 95, Issue 3, pp 425-438.
- [16]. Hanson, V. et al (2009). *Infosüsteemide turve I Turvarisk*, Cybernetica AS.
- [17]. Jones, R., Tahri, D. (2011). *Online selling and contracting: An overview of EU rules*, *Computer Law and Security Review: The International Journal of Technology and Practice*, 2011, Volume 27, Issue 4, pp. 402 – 406.
- [18]. Kaptein, M. (1998). *Ethics Management: Auditing and Developing the Ethical Content of Organization*. Kluwer Academic.
- [19]. Laherand, M. L. (2008). *Kvalitatiivne uurimisviis*, Tallinn: Infotrükk.

- [20]. Lessing, L., (1999). *Code and Other Laws of Cyberspace*. Version 2.0, Basic Book,
- [21]. Leppiman, A. (2010). *Arjen elämyksiä – Leiri- ja elämispohjainen Arkipäivät-perhepalvelu sosiaalisen kokemuksen tuottajana/Everyday Experiences- Camp- and Experience-Based Weekdays Family Service as a producer of Social Experiences*. Acta Universitatis Lapponiensis 182. Lapland University Press.
- [22]. Mackenzie, C. (1998). *Ethics auditing and Ethical Knowledge*, Journal of Business Ethics, 17(13), 1395-1402.
- [23]. Mayring, P. (2000). *Qualitative Content Analysis, Qualitative Methods in Various Disciplines I: Psychology.*, 1 (2) June, Forum: Qualitative Social Research Sozialforschung, retrieved from: (<http://www.qualitative-research.net/index.php/fqs/article/view/1089/2385>).
- [24]. Melé, D. (2012). *Management Ethics: Placing Ethics at the Core of Good Management*
- [25]. Morland, M. P. (2008). *Business Ethics as Practice: Ethics as the everyday business of business*. Cambridge University Press.
- [26]. Musschenga A.W (2005). *Empirical Ethics, Context-Sensitivity, and Contextualism*. Journal of Medicine and Philosophy 30 (5):467 – 490.
- [27]. Nettleton, K. (2008). *Is more regulation needed online?* Campaign (London. 1968) (0008-2309), p. 12.
- [28]. Northcutt, S (2004). *IT's Ethics Handbook: Right and Wrong for IT Professionals*
- [29]. Regan, P. M. (2002). *Privacy as a Common Good in the digital world*. Information, Communication & Society, 5(3), 382-405.
- [30]. Ribble, M., Bailey, G (2004). *Monitoring Technology Misuse & Abuse*, T.H.E Journal, Kansas State University.
- [31]. Richards, L. (2009). *Handling Qualitative Data: A Practical Guide (2nd Edition)*. Thousand Oaks: Sage.
- [32]. Rihma (2012). *Ethics Auditing Model for Estonian Big and Middle Size Companies*, China-USA Business Review, Vol. 11, No. 8, 1146-1158.
- [33]. Rihma, M., Meel, M. (2013). *The discrepancy between declared values and real ethical behaviour of companies (Estonian case)*. European Scientific Journal, 9(16), 26 - 42.

-
- [34]. Spinello, R. A (2010). *Cyberethics: Morality and Law in Cyberspace*, Jones and Bartlet Learning.
- [35]. Spinello, R. A. (1999). *Ethical reflections on the problem of spam*. *Ethics and Information Technology*, 1(3), 185-191.
- [36]. Tavani, H. T. (2004). *Ethics and technology: Ethical issues in an age of information and communication technology*. New York: Wiley.
- [37]. Valtonen, A. (2005). *Ryhmäkeskustelut-millainen metodi?* In: Ruusuvuori, J. & Tiittula, L.(Edit.) *Haastattelu: tutkimus, tilanteet ja vuorovaikutus*. Tampere: Vastapaino.
- [38]. Wagner, T., R. J. Lutz, et al. (2009). *Corporate Hypocrisy: Overcoming the Threat of Inconsistent Corporate Social Responsibility Perceptions*. 37(2): 170-180. *Journal of Marketing*
- [39]. Yin, R. (1994). *Case study research: Design and methods* (2nd ed.). Thousand Oaks, CA: Sage Publishing.