Tampere University

Anni Kovanen

RISKS OF INTELLIGENT AUTOMATION AND THEIR IMPACT ON INTERNAL AUDIT

Faculty of Management and Business
Master's thesis
April 2020

ABSTRACT

Anni Kovanen : Risks of intelligent automation and their impact on internal audit
Thesis supervisor : Lasse Koskinen
Master's thesis
Tampere University
Degree Programme in Business Studies : Insurance science
April 2020

New technologies are driving transformative changes in all industries. Organizations are adopting new technologies seeking more efficiency and ways to capture value. The role of risk management as a part of organization's decision-making process is emphasized especially now when organizations are facing increasing uncertainty due to the opportunities and risks presented by new technology. Also, increasing uncertainty makes regulatory environment more complex and increases requirements of reporting organizational risks to external stakeholders.

Emerging technologies bring significant opportunities, which sometimes can overshadow their risks. Emerging technologies can complicate existing risks and create risks that organizations have not experienced before. To reach the full potential of technology investments, organizations are seeking new ways to manage their risks. One of the technologies transforming businesses in all industries is artificial intelligence, which can be combined with Robotic process automation.

Robotic process automation (RPA) alone can have significant impacts to organization's processes but has certain limitations. RPA can only automate specific rule-based tasks. When artificial intelligence capabilities are added to RPA, organizations are able to automate entire workflows. Artificial intelligence capabilities combined to RPA is called intelligent automation. With intelligent automation, predictions and decisions requiring human perception can be automated. Opportunities are clear but intelligent automation creates new kind of risks.

As organizations are seeking new ways to manage risks of intelligent automation, internal audit faces need to develop as well. In general, development of internal audit, the third line of defense, is actual topic. Especially opaque nature of intelligent systems makes understanding them more difficult and artificial intelligence is often referred as "black box". The objective of this research is to find out the key risks intelligent automation creates to organizations, what kind of challenges they pose to internal audit and what can internal audit do to keep up and stay relevant. The research is multi-method research, consisting expert interviews as qualitative method and survey as quantitative method.

Based on the interviews and survey conducted, five most relevant risk categories were identified. They are technology risks, cyber-risks, people related risks, risks related to strategy of intelligent automation and risks related to design and implementation of intelligent automation. Many of the key risks of intelligent automation are related to competence gaps in organization, increased reliance in intelligent systems and opacity of algorithmic decision-making. In addition, the big amounts of data used by intelligent automation and new access points it crates make cyber-risks relevant especially concerning this technology.

The key challenges, which risks of intelligent automation forces internal audit to face are increasing competence requirements, internal audits role and position in intelligent automation adoption and methods monitoring and auditing intelligent automation. Four key ways to tackle these challenges are improving internal audit's competences when possible, flexible resourcing models and internal audit's early involvement in intelligent automation adoption process. Based on the interviews and survey conducted, increased competence requirements is the biggest challenge to internal audit, especially in small internal audit organizations. In addition to technical skills required, internal auditors should have adequate understanding of many other aspects of intelligent automation, like regulation and ethicality questions.

Keywords: Artificial intelligence, intelligent automation, risk management, internal audit

TABLE OF CONTENTS

1 INTRODUCTION

1.1 Subject matter introduction

The purpose of risk management is to identify, monitor, and manage the risks that may affect business to help the organization achieve its business objectives. (Niemi 2018, 322) Thus, the purpose of risk management is not just to set limits to business, but to contribute to achieving the goals of the organization by ensuring that it exploits business opportunities as much as it is reasonable concerning organization's risk appetite.

Understanding risk is the primary function of risk management, as organizations make business decisions based on their risk portfolio. The role of risk management as a part of organization's decision-making process is emphasized especially now when organizations are facing increasing uncertainty due to the opportunities and risks presented by new technology. Also, increasing uncertainty makes regulatory environment more complex and increases requirements of reporting organizational risks to external stakeholders. (Niemi 2018, 322-328)

As risks of organizations change, internal audit as an assurance function changes as well. The mission of Internal Audit is to provide objective assurance, advice and insights to secure and enhance the value of the company. Internal Audit evaluates and improves the organization's risk management, internal control and governance processes. (www.IIA.fi 2019a) As a result of the use of new technology, the risks of companies and thus the role of internal audit and the auditing practices are changing (Niemi 2018, 121)

Internal Audit development has come a long way from when internal audit was only audit's supportive function. The birth of internal auditing can be traced to the founding of Institute of Internal Auditors (IIA) in 1941. After that, big turning point was Sarbanes Oxley act, which had big impact on accounting profession and, also to internal auditing. After Sarbanes Oxley act, COSO framework and new capabilities like IT-audit and data-analytics helped to push the profession forward. Now, however, we are experiencing fourth industrial evolution and organizations are forced to face new and constantly evolving risks. The strategies, practices,

and technologies are new and internal audit must adopt new vision and methods to stay relevant and accomplish its core idea to create value to organizations. (Hatherell 2018, 1)

The need for research about development of internal audit function has been noticed especially by companies that provide external internal audit services, like the big four companies, which have developed lot of publications around the subject. Also, Institute of Internal auditors (IIA) identifies new trends and risks concerning organizations and internal audit. IIA publishes Risk in Focus -reports yearly. The reports tell the stage of internal audit function and profession based on survey to Chief Audit Executives (CAEs) across Europe.

Studies such as ECIIA's Risk in Focus 2020 -report (2019) have found that companies consider risks caused by new technologies relevant. The European Institutes of Internal Auditors publishes an annual Risk in Focus -report. The purpose of the study is to highlight the key business risks identified by audit leaders in their organizations across Europe. In the Risk in Focus 2020 study, CAEs were asked what risk they perceive to be the greatest for their organization. The most popular answer (21%) was cyber and data security, followed by digitalization, disruptive technologies and other innovations (18%).

Gartner's 2019 Audit Plan Hot Spots (Christofferson et al. 2018) also aims to identify and analyze the risks auditors are preparing to focus on next year. Gartner's 12 risks highlighted include cybersecurity, the importance of data, business changes caused by digitalization, and the impact of automation on strategic workforce planning

One of the technologies that is changing businesses is intelligent automation. Intelligent automation combines software robotics and artificial intelligence. Intelligent automation can have big impact on businesses as it enables the automation of entire workflows. An intelligent robot is capable of learning and performing human-perception demanding tasks. In addition to all the opportunities, intelligent automation brings new risks to companies' risk profiles. This study seeks to determine which of the risks caused by intelligent automation are perceived to be most significant in organizations, what kind of challenges they pose to internal audit and how is can internal audit rise to the challenge.

Internal audit’s changing role is relevant research subject as organizations are seeking for new ways to manage risks and meet compliance requirements. New kinds of risks force organizations to not only manage them differently, but to make organizational changes. One sign of this trend is that Institute of Internal Audit (IIA) is at the time of this research in process to review Three lines of defense -model (Nicholson 2019, 3-4). Three lines of defense -model

presents three lines of organization's risk management. The third line of defense in the model is internal audit.

Risks caused by new technologies are also relevant research topic as pace of technology adaption is becoming more rapid and business environment more competitive. Intelligent automation has not been studied lot, especially from risk perspective. As intelligent automation can be free from human intervention, it can process huge amounts of data, it has big effect on workforce and regulatory burden concerning intelligent technologies and data processing is increasing, more research of the topic especially from risk perspective is needed.

1.2 Definitions of the key concepts

Risk

There is no unified definition for risk. In common language, risk often means possible negative outcomes due to some uncertain event occurring and possibility of positive outcomes are left out from the definition (Krause 2006, 707). Especially in professional use, risk can also mean possible positive results. Especially business risks often concern both aspects. (Ilmonen 2013, 10-11) Nevertheless, definition of risk is objective and usually linked to specific contexts. For example, in insurance business risk is usually considered as unwanted event but in other businesses risks can also be seen as opportunities.

Hansson (2010) defines risk as realization of harmful occurrence of an event that is not certain or impossible (Koskinen 2018, 12, according to Hansson 2010). Kogan and Wallach determined kind of a scientific starting point to risk already in 1964 by stating that risk is twofold, it includes opportunity as well as possibility of danger. Thus, science often includes aspect of opportunity to the meaning of risk. (Juvonen et al. 2014, 9, according to Kogan & Wallach 1964) Risks are estimated based on their probability, their consequences and meaning. Every object has different meaning for each risk, which leads to risks being evaluated subjectively. (Ilmonen 2013, 12) Also," harmful events" in Hansson's definition can be subjectively evaluated.

Risk management

Risk management can be defined as actions to control uncertainty to achieve one's objectives. Modern attempt to manage risks is not only taking defensive actions. Many business decisions

are about using current resources for future uncertain results. This means that risk management and risk taking are part of a same process, not opposites. (Crouhy, Galai & Mark 2013, 1)

In organizational risk management, primary objective of risk management is to ensure continuity of business and especially securing investors' investments and reaching required return rates. Usually risk management also has important role in reaching different external requirements. (Ilmonen et al. 2013, 18-19, 30)

Enterprise risk management

Enterprise risk management (ERM) differs from traditional risk management perspective in a way that risk management is performed at organizational level and is considered in strategy planning. Main objective in ERM is to achieve organization's strategic objectives, by identifying potential events that may affect the entity, and manage them within determined risk appetite. (Fraser & Simkins 2010, 1)

Three lines of defense

The three lines of defense -model is commonly used in risk management. The three lines of defense clarify roles and duties of risk management. Model is designed to be appropriate for any organizations – regardless of their size and complexity. According to model, the three lines are necessary to ensure effective risk management and internal control. The first line of defense is management controls and internal control measures. The second line is formed by various risk control and compliance oversight functions, which are established by management. Independent assurance i.e. internal audit is the third line of defense. Every line has a distinct role in organization's governance framework. (IIA 2013a, 2)

Internal Audit

Internal audit is an independent support function of the board and senior management. Its mission is to provide an objective evaluation, assurance and consultation to support organization's development and objective achievement by evaluating and improving the effectiveness of risk management, control and governance processes. (www.iia.org.uk) The primary function of internal audit is to support the highest governing body of the organization (for example the Board of Directors) and the executive management by providing independent and objective insights into the organization and its activities and making recommendations for their improvement. Internal Audit is thus part of the corporate governance system, together with the board, senior management and auditors. (Niemi 2018, 13)

The Framework for Professional Practice in Internal Auditing

The Framework for Professional Practice in Internal Audit is a conceptual model, which defines guidelines for the IIA (The Institute of Internal Auditors) profession. The framework contains the mission of internal audit as well as mandatory and recommended guidelines. Mandatory guidelines include the definition of internal audit, standards and ethical rules. Recommended guidance includes application guidance and additional guidance. (Niemi 2018, 26-27)

Robotic process automation (RPA)

RPA is software programmed automation. RPA can imitate rules-based, repetitive tasks such as cut and paste, merging, button clicks etc. Simply, RPA is used to automate simple IT tasks with external software. (Christofferson et al. 2018, 25) RPA software works on user interface layer and can interpret existing applications. (IRPAAI.com)

Intelligent automation

To automate end-to-end processes that need cognitive skills, artificial intelligence capabilities need to be integrated to RPA. Simply, artificial intelligence means that machines can perform tasks that require human intelligence such as making predictions, learning from data and finding meanings from pictures and voice (Watson et.al 2019, 13) Artificial intelligence includes machine learning, deep learning, natural language processing and generation and computer vision (Bajenescu 2018, 48; Watson et.al 2019, 13). This combination of cognitive technologies integrated to RPA is called intelligent automation.

1.3 Research objectives and outlining

The purpose of this research is to combine empirical research with existing research to gain a clear understanding of the key risks that organizations perceive to be caused by intelligent automation and what challenges do these risks pose to internal audit and how can internal audit meet the risks and stay in a relevant role also when managing risks of intelligent automation.

There are three research problems and they are equally relevant. However, the first research problem serves as the basis for the other two research problems. The purpose is to refine the

risks of intelligent automation discussed in the theory section by identifying, which risks are most central, since the answers to the other two research problems are probably closely linked to which risks are the most important.

Research problems:

1. What are the key risks of intelligent automation?

2. What challenges internal audit faces due to risks of intelligent automation?

3. How can internal audit meet the challenges caused by risks of intelligent automation and stay relevant?

The second research problem seeks to find an answer to the challenges that risks of intelligent automation pose especially to internal audit function. The second research problem aims to investigate how internal audit can overcome the challenges, for example, with new tools or practices

The research is outlined to only concern intelligent automation, which means robotic process automation with cognitive qualities, not physical robots. What led to this outlining is that organizations from diverse industries are already using intelligent automation on their processes. Organizations, which use intelligent physical robots are quite limited. Intelligent software robotics in the other hand can be used to automate, for example, credit decisions, invoicing, order processing and different kinds of customer service operations. These are processes that can be found from all kinds of businesses from logistics to banking.

Other matter that is out of the scope of this research is, how internal audit can utilize intelligent automation on its own operations. Different cognitive and analytical tools are taken into consideration when researching changing practices of internal audit. However, objective of this research is not to find out, how internal audit can use cognitive tools in detail. The perspective of intelligent automation used in organizations that are subject of auditing was chosen because, first, both perspectives could not have been researched comprehensively enough in research of this scale, but also because like stated above, intelligent automation can be used in all kinds of organizations and their functions. Therefore, intelligent automation is used on larger scale in organizations that are subject of auditing than internal audit function, at least at the time of the research. Thus, this research does not concern new tools of internal audit, but rather how internal audit approaches audit areas and how it manages audit engagements.

1.4 Research Methods

This research is a mixed methods research, which means that both, qualitative and quantitative methods are used. By using a variety of methods, the research subject can produce versatile and comprehensive results. The different methods used in mixed methods research can be a combination of both qualitative and quantitative methods. (Jyväskylä University 2015) In this research, quantitative method was used to verify results from qualitative research.

Qualitative research provides a comprehensive overview of real-life depiction and exploration. The starting point for qualitative research is the complex and specific examination of the material. (Koskinen, Alasuutari & Peltonen 2005, 52) Because the research topic is very new in business as well as in research, qualitative research is suitable research method. But to add scalability of research results, it was seen functional to also approach the subject from quantitative perspective.

Qualitative material was collected through four expert interviews. First, different risk categories and risks concerning intelligent automation were identified from previous research and literature. These beforehand identified risks and categories were used in the interviews, but interviewees were encouraged to give their insight outside these categories as well. The interviewees were three chief audit executives from different organizations, which operate in different industries. The fourth interviewee was executive director of IIA (Institute of Internal Auditors) Finland.

The interview method was a semi-structured interview in which the interviewer has pre-defined questions, but the interviewee can answer them very freely and propose new questions (Koskinen, Alasuutari & Peltonen 2005, 104). Quantitative material was collected with a survey to members of IIA Finland. The survey was published on IIA's website and member newsletter. The survey was also published in Teams group for internal auditors in Deloitte Finland and to internal auditors in OP. The survey material was analyzed with Excel visualized with Microsoft Power BI.

1.5 Theoretical framework and previous research and literature

The objective of this thesis is to find out the key risks of intelligent automation and what challenges they pose to internal audit and how internal audit can meet the challenges. Intelligent automation was chosen as the research subject technology because of its special characteristics that can cause new risks to organizations, but which are complex to audit as well. What makes internal audits relation to managing risks of intelligent automation interesting research topic, is internal audit's unique role in the organization. Internal audit is an independent and objective function that evaluates and improves the effectiveness of risk management, control and governance processes. As an independent function, internal audit has unique perspective to organizations operations.

The theoretical framework starts with theory of enterprise risk management, which have been divided to three lines of defense in organization's risk management, according to Three lines of defense -framework, created by Institute of Internal Auditors (IIA). First line of defense contains functions that own the risks, the second line includes functions that oversee or specialize in risk management and are responsible of compliance. The third line is internal audit, that provides independent assurance. (Chartered Institute of Internal Auditors 2019)

The results of this research are interpreted against internal audit's mission and role in the three lines of defense of risk management and as a part of part of the corporate governance system, as well as IIA's Professional practices -framework and Competency framework, as they strongly guide mission, profession and operations of internal audit. The focus area of the research is marked with green color in the visualization of the theoretical framework.

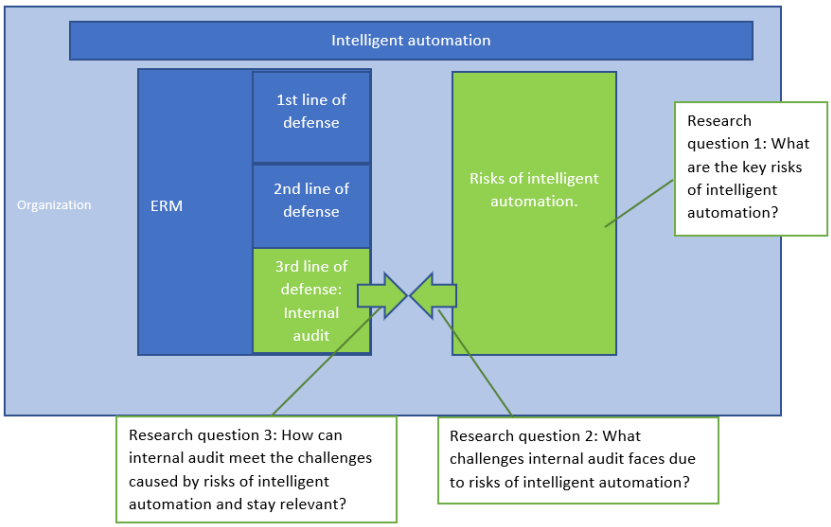

Figure 1 Theoretical framework

Traditionally internal audit's role has been considered as assurance provider. However, also advising and consultative role of internal audit has been identified in literature. Literature about internal audit used in this research is manly from Institute of Internal Auditors (IIA) and Niemi (2018) but also from companies that provide internal audit services. Deloitte has created own internal audit framework called Internal Audit 3.0. This framework also presents risk anticipating role of internal audit in addition to assurance and advise. Anticipating role was also included to interviews and survey conducted. Internal audit's role is actual topic at the time of this research, as IIA is in process to review three lines of defense -model.

There is lack of research of intelligent automation from risk perspective. However, some research has been made and the research objective was to confirm results of previous research as well as add new findings to previous research. Some previous research and literature used in this research are specifically about risks of intelligent automation or artificial intelligence, but also research and literature about digital risks in general has been used, as many digital risks apply to many kinds of technologies.

When speaking of intelligent automation or artificial intelligence in general, most research has been made about algorithms and data, which intelligent technologies are using. Risks of intelligent algorithms identified from previous literature mostly concern algorithm opacity, incorrect algorithm design or implementation and increasing reliance on algorithms. For example, Osoba and Wesler in their book An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence (2017) have identified risks related especially to algorithms and

reliance on them. Also, Lehto (2017) and Băjenescu (2018) discuss algorithm risks in their publications. Other publication used quite lot in theory of this thesis is paper about algorithm and bias in financial industry by Petrasic et al. 2017.

As cyber risks in general are very relevant topic in the field of risk management, there is lot of research about cyber risks. Most studies also concern special characteristics of artificial intelligence, like big amounts of data and lack of human intervention in data processing. Using personal or other ways confidential data also means more and constantly increasing regulatory requirements for organizations. These data and privacy related risks are discussed by, for example, Lehto (2017) and Lehto and Nettaanmäki (2015). The importance of data compliance and its challenges are also emphasized in ECIIA's Risk in focus reports (2018 & 2019), which study the most relevant topics for internal audit as well as in Gartner's Audit hot spots -report (2018).

The ECIIA's report and Gartner's report also emphasize how workforce planning is changing due to digitalization and automation adoption. Also, many companies providing professional services, for example the big four companies, have made research about digital risks and risks of intelligent automation. This research is used in the thesis but as confirming research to other sources.

1.6 Structure of the thesis

The first four chapters of the thesis form theory part of the research. First theory chapter, chapter two, deals with risks and risk management in general, as well as enterprise risk management. Internal audit and its relevant frameworks are discussed in chapter three. After that, risks of intelligent automation are discussed in the last theory chapter, chapter four.

Empirical part of the thesis is divided to two chapters. Chapter five discusses results from the interviews and survey conducted in terms of risk of intelligent automation. Second empirical chapter, chapter six, discusses challenges, which risks of intelligent automation pose to internal audit and, how internal audit can rise to the challenges. Conclusions of the research results are discussed in chapter seven.

The last chapter of the thesis is synopsis. In the beginning of synopsis, there is a summary where all three research questions are answered shortly, as conclusions are already discussed in chapter seven. Also, research is evaluated and ideas for further research discussed in synopsis.

2 RISK MANAGEMENT

2.1 Risk and risk management

There are many definitions of risk. Especially in common language, risk is usually used to describe possible events that can have negative impacts, but this is only one perspective. Especially in professional use, risk can also mean possible positive results. Especially business risks often concern both aspects. (Ilmonen 2013, 10-11) Nevertheless, definition of risk is objective and usually linked to specific contexts. For example, in insurance business risk is usually considered as unwanted event but in other businesses risks can also be seen as opportunities.

Hansson (2010) has determined minimal features of risks as follows:

1. Risk is related to unwanted events and
2. Occurrence of the event in question is not certain neither impossible

Whereupon, Hansson's definition of risk is realization of harmful occurrence. (Koskinen 2018, 12, according to Hansson 2010) Kogan and Wallach determined kind of a scientific starting point to risk already in 1964 by stating that risk is twofold, it includes opportunity as well as possibility of danger. Thus, science often includes aspect of opportunity to the meaning of risk. (Juvonen et al. 2014, 9, according to Kogan & Wallach 1964) In this research, risk is addressed as possibility of harmful events as well as opportunity. Benefits and opportunities of intelligent automation are discussed in the theory section of this thesis and discussion is based on findings from reviewed literature. Although, in the first research question, intention is to find out especially, what are the most meaningful harmful events that organizations face because of intelligent automation.

Risks are estimated based on their probability, their consequences and meaning. Every object has different meaning for each risk, which leads to risks being evaluated subjectively. (Ilmonen 2013, 12) Also," harmful events" in Hansson's definition can be subjectively evaluated.

Risks can be categorized with different approaches. Clear risk means risk that has only possibility for some harmful event to realize, and speculative risks are risks that include possibility of negative event and positive opportunity. Dynamic risks change along with economic cycles and circumstances. Static risks stay the same over time. Business risks are often both speculative and dynamic. Subjective risks are personal risks and objective risk is the relative volatility of the realized loss around expected loss. Unsystematic risks are risks that can be reduced by decentralizing risk portfolio. Systematic risks can't be reduced by decentralizing. (Koskinen 2018, 16)

Nevertheless, the baseline of risk is that uncertainty is linked to an event. According to ISO 31000 standard, risk is the uncertainty's effect on objectives. If consequences of an event are precisely known in advance, it is not a risk. Level of uncertainty can vary between risk quite lot as well as severity of consequences. (Juvonen et al. 2014, 8) Uncertainty of an event can be everything between total ignorance and between precise probability estimation, that is based on justifiable information base and calculation methods (Koskinen 2018, 11-12). Third factor of risk is meaning of risk, which can be very subjective. Meaning of risk indicates, how we experience the risk and its possible realization. (Juvonen et al. 2014, 8)

Opportunities and threats can be evaluated for example by experience, with case studies or mathematically. When measuring risks mathematically, subjective meaning of risks is usually not included, and evaluation is based on probability and severity of consequences. (Juvonen et al. 2014, 8-10) Commonly used definition of risk is:

RISK = PROBABILITY x SEVERITY OF CONSEQUENCES

Probability of risk can be evaluated with probability distribute. However, this method can be used only in case of typical risks. If risks are new and unusual or dynamic, probability can't be evaluated. As stated before, business risks are usually dynamic in nature. Severity of a risks depends on risk taker's risk appetite and risk-bearing capacity. (Juvonen et al. 2014, 8-10)

Evaluating risks and performing risk management depends on knowledge about risks' probability and effects. Ralph Gomory (1995) categorizes knowledge about uncertainty to three different categories: known uncertainty, unknown uncertainty and unknowable uncertainty.

Known uncertainty refers to a situation where risk's probability distribution is known, for example, risk of death. Unknown uncertainty refers to a situation where possible events are identified but their probability is unknown. Unknowable uncertainty for one's part refers to a situation where possible occurring events are not known before hand at all. (Koskinen 2018, 16, according to Gomory 1995)

Risk-bearing capacity is usually determined as an answer to the question, how much financial losses can an organization bare in one year. This usually means the biggest possible negative impact to organization's revenue or another financial meter. Risk-bearing capacity can depend on many different factors. It can be linked, for example, to working capital or to liquid assets but also qualitative factors can affect organization's risk-bearing capacity. For example, the way how organization manages its risks and has arranged their internal audit, can affect risk-bearing capacity. (Ilmonen et al. 2013, 10-11)

Risk appetite means the amount of financial loss that organizations are willing to bare when seeking new business opportunities. In the end, risk appetite depends on owners and other stakeholders. When making business decisions management estimates, what are the possible benefits, for example, of a new investment and on the other hand, what are possible harmful consequences. (Ilmonen et al. 2013, 12-13)

As described above, organizations as well as individuals take actions to control uncertainty and achieve their objectives. Plainly, this is risk management. Modern attempt to manage risks is not only taking defensive actions. Many business decisions are about using current resources for future uncertain results. This means that risk management and risk taking are part of a same process, not opposites. (Crouhy, Galai & Mark 2013, 1)

Although, especially managing business risks can be executed in variety of ways, some ways to prepare for risk should be introduced. Firstly, risks can be transferred by insuring them. One can prevent risks by, for example, virus protection programs or designing buildings fire-proof. However, risks often can't be totally prevented. It is also possible to prepare for consequences. That means that one can try to minimize consequences when risk realizes, for example, with back-up stock. Preparing for risks, in the other hand, means that one can be financially prepared for risks with economic capital. Preparing for risks also concerns keeping part of the risk for one's self deliberately, for example, by having insurances with big deductibles. However, this can be quite challenging as financial consequences of a risk should be precisely enough evaluated. (Rantala & Kivisaari 2014, 92-94)

Primarily, objective of risk management is to ensure continuity of business and especially securing investors' investments and reaching required return rates. Usually risk management also has important role in reaching different external requirements. In general, requirements concerning risk management can be divided to external and internal requirements. External requirements come outside organization, for example, from legislators, risk management standards or generally accepted principles of society. External requirements can be very different between organizations, depending on what kind of environment organization operates in. For example, different fields can have different legislation about protecting environment and some entities have different requirements about executing internal audit. Internal requirements are agreed inside organization. Principles and goals on risk management are agreed in company's own vision, strategy, values and policies. (Ilmonen et al. 2013, 18-19, 30)

2.2 Enterprise risk management

Enterprise risk management (ERM) differs from traditional risk management perspective in a way that risk management is performed at organizational level and is taken to account in strategy planning. Traditional risk management has been called" silo risk management" as it is management separately in different parts of organization. Main objective in ERM is to achieve organization's strategic objectives, which also includes determining right risk appetite. (Fraser & Simkins 2010, 1)

Volumes and complexities of risks affecting an enterprise are increasing as well as expectations towards risk management. Rapid changes in information technologies, the explosion of globalization and outsourcing and increased competition make effectively overseeing the complex portfolio of risk more difficult and enterprise wide risk management more important. Like mentioned before, many business risks can be dynamic and untypical by nature, which makes predicting and measuring risks harder. Especially managing digital risks has special challenges that are discussed more precisely further on.

There are many ERM frameworks developed. Probably most famous of these frameworks are COSO (Committee of Sponsoring Organizations of the Treadway Commission) -model and ISO 31000 -framework.

2.2.1 COSO -framework

In 2004, COSO board commissioned and published *Enterprise Risk Management—Integrated Framework* that defined ERM as below:

"Enterprise risk management is a process, effected by the entity's board of directors, management, and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within the risk appetite, to provide reasonable assurance regarding the achievement of entity objectives."

In COSO -framework definition, it is emphasized that risk management should be a part of strategy planning and implementation. Risk management is value adding function, if it is performed by utilizing opportunities according to organization's determined risk appetite. Risk management may notice that organization is taking too much risk in some business area and not utilizing all opportunities in other area. Part of strategic risk management is to identify which risks can have collective effect on implementing organization's strategy. (Fraser & Simkins 2010, 1)

After the publication of the framework, risks have changed, new risks have emerged, and both boards and executives have enhanced their awareness and oversight of enterprise risk management. As the framework emphasizes meaning of strategic risk management and complexity, it was updated to meet the demands of an evolving business environment in 2017. The new publication is called *Enterprise Risk Management —Integrating with Strategy and Performance* and it highlights the importance of considering risk in both the strategy-setting process and in driving performance. (COSO 2017, 1-3)

Enterprise Risk Management—Integrating with Strategy and Performance clarifies the importance of enterprise risk management in strategic planning and embedding it throughout an organization. Risks are often reflected to already set strategies. Often starting point in risk management is to identify, which events can be risks to current strategy. New COSO -framework considers also two other aspects. Firstly, is the strategy aligning with organization's mission and values. Secondly, does strategy's risk profile align with organization's risk appetite. (COSO 2017, 5)

The framework itself is organized into five components that accommodate different viewpoints and operating structures. New framework connects ERM to increased stakeholder expectations more clearly, positions risk in the context of an organization's performance, and emphasizes

anticipating risks and that change creates opportunities, not only negative impacts. Five components presented in the framework are Governance and Culture, Strategy and Objective-Setting, Performance, Review and Revision and Information, Communication and Reporting. (COSO 2017, 6)

Governance's role in risk management is to set organization's tone. Tone reinforces risk management's importance and establishes responsibilities for enterprise risk management. Culture pertains to ethicality and desired behavior. COSO -framework emphasizes that ERM, strategy and objective-setting should work together. Risk appetite should be determined to cohere with strategy and business objectives should support implementing a strategy. (COSO 2017, 6)

Third component, performance, comprises risk identification and assessment. Risks are prioritized and assessed to cohere determined risk appetite. Performance should be reviewed to make sure that risk management components works as designed and if revisions are needed. Thus, the fourth component is review and revision. Fifth component is information, communication and reporting. Enterprise wide risk management requires communication flows throughout organization, from both, external and internal sources. (COSO 2017, 6)

These ERM components are supported by 20 principles that are categorized under the five components. The principles describe practices that can be applied in different ways to different kind of organizations. According to COSO, by implementing these principles, management and the board can expect that the organization understands and succeed to manage risks related to its business objectives and strategy. Examples of the principles are: exercises board risk oversight and defines desired culture under Governance and culture, defines risk appetite and formulates business objectives under Strategy and Objective-setting, identifies risk and implements risk responses under Performance, reviews risk and performance under Review & Revision and leverages information and technology under Information, communication and reporting. (COSO 2017, 7)

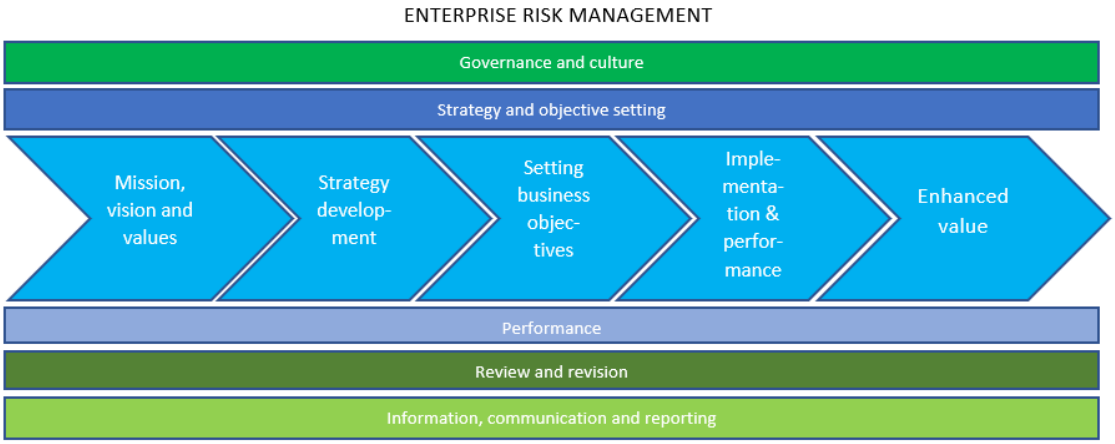

Figure 2 ERM after COSO -framework (2017)

2.2.2 ISO 31000 -standard

ISO 31000 is ERM standard developed by the International Organization for Standardization (ISO). The purpose of ISO 31000 is to give generic guidelines of establishing a risk management framework to support and develop risk management. Besides identifying and controlling risks, the standard is supposed to support organizations to achieve their objectives by helping them take risks consciously. (Niemi 2018, 332-333)

The standard was reviewed in 2018. New standard replaces ISO 31000:2009. In the revised Iso 31000, risk management is defined with principles, framework and risk management process. The biggest changes in the new standard are bigger emphasis in management involvement. The revised standard also recommends that risk management should be an integral part of the organization's structure, processes, objectives, strategy and operations. It considers value creation as an important part of risk management. It also describes other risk management principles, such as ongoing improvement, engaging stakeholders, organizational alignment and consideration of human and cultural factors in risk management. (SFS 2019, 5)

The standard is meant to be applicable for organizations of every size and type. As the standard is meant to fit all environments and manage all types of risk, the standard does not attempt to guide risk management with detailed specifics but rather to depict ideal risk management system.

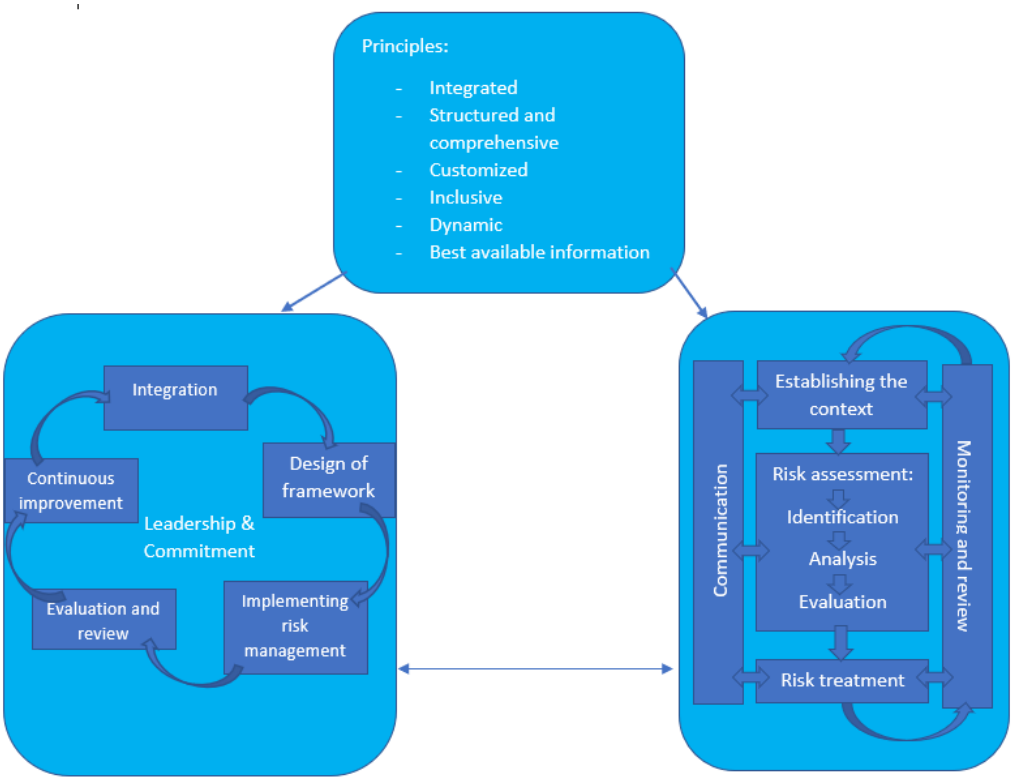

Figure 3 ERM after ISO31000 -standard (ISO 2018)

ISO 31000 -standard is visualized in figure 3. Management involvement, stakeholder engaging, organizational alignment, continuous improvement and other factors that ensure risk management being considered as integral part of organization's structure are presented in the framework of the standard.

The principles are requirements of effective risk management. There are eight principles and in the core of them is value creation and protection, as the main objective of risk management is to create and protect value. Principles around core area are the foundation of managing risk. Principles communicate the value and purpose of risk management. Therefore, they are required for effective risk management. Even if ISO 31000 is designed to fit all kinds of organizations, one of the principles, customizing, states that processes and framework must be customized and proportionate to organization's internal and external context and objectives. (committee.iso.org)

Third part of the standard is risk management process. The process states that risk management starts by defining organization's operational environment. According to the standard, the areas that need to be focused on when defining operational environment are business environment, organization it-self, risk management process and risk appetite. (Juvonen et. al 2014, 17)

After operational environment is defined, starts risk evaluation process, which includes risk identification, risk analyzing and determining the level of risk. After evaluation process, necessary control procedures are executed. According to the standard, risk management is a continuous process. Continuity is assured by reporting and recording, monitoring and communicating throughout risk management process.

2.3 The three lines of defense

The three lines of defense -model is commonly used in risk management. The three lines of defense clarifies roles and duties of risk management. Model is designed to be appropriate for any organizations – regardless of their size and complexity. According to model, the three lines are necessary to ensure effective risk management and internal control. (IIA 2013a, 2)

The lines are under the supervision of senior management. Top management is not included in the lines but plays an extremely important role in the operation of the model. It is a significant stakeholder in all policies, and it is responsible for overseeing the implementation of the model in all risk and control processes. (IIA 2013a, 2) The board gives direction to senior management by setting organization's risk appetite. Board also seeks to define principal risks facing the organization and assures that management is assessing these risks. Operating risk management is primary CEO's and senior management's responsibility and management should control organization's overall risk management activities in relation to agreed risk appetite. (Chartered Institute of Internal Auditors 2019)

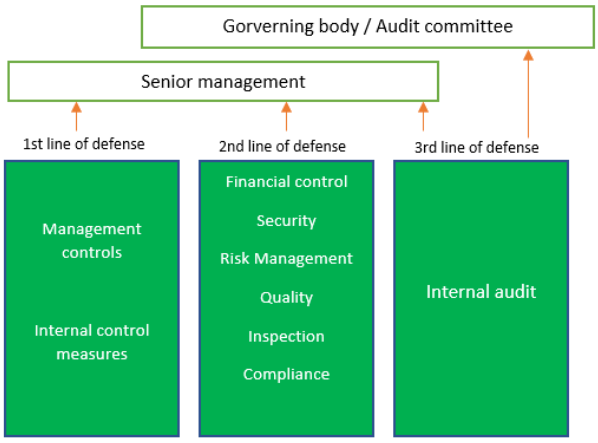

Figure 4 Roles of risk management after Three lines of defense - model (IIA 2013a)

The first line of defense is management controls and internal control measures. The second line is formed by various risk control and compliance oversight functions, which are established by management. Independent assurance i.e. internal audit is the third line of defense. Every line has a distinct role in organization's governance framework. (IIA 2013a, 2)

First line of defense, operational managers, own and manage risks. The first line is responsible of implementing actions to address process and control deficiencies. The first line is in responsible position in day-to-day risk management, including identifying, assessing and mitigating risks. Important part of first line's responsibilities is development and implementation of policies. Whereas, mid-level managers implement detailer procedures and supervises their execution. (IIA 2013a, 3)

To help building and monitoring controls established by the first line, there are second line's risk management and compliance functions in place. Naturally, specific functions and their agenda vary between different organizations. However, typical functions include risk management function, compliance function and controllership function. Risk management functions monitors the implementation of risk management and facilitates risk owners in defining the target exposure and adequate reporting throughout the organization. Compliance function monitors various specific risks, for example, noncompliance with regulation, whereas controllership function monitors financial risks and reporting. (IIA 2013a, 4)

As management functions, the functions of second line of defense can't give fully independent analyses to governing bodies. For this purpose, there is third line of defense. Internal audit is supposed to give comprehensive assurance. Internal audit has a unique role as it should be completely independent and objective. Internal audit gives assurance on how the first two lines

perform in achieving risk management and control objectives. Internal audit's mission to provide objective assurance covers all elements of an institution' risk management framework. (Chartered Institute of Internal Auditors 2019) More of internal audit's mission and role is discussed in separate Internal audit -chapter of the thesis.

3 INTERNAL AUDIT

Internal audit is an independent support function of the board and senior management. Its mission is to provide an objective evaluation, assurance and consultation to support organization's development and objective achievement by evaluating and improving the effectiveness of risk management, control and governance processes. (www.iia.org.uk)

The primary function of internal audit is to support the highest governing body of the organization (for example the Board of Directors) and the executive management by providing independent and objective insights into the organization and its activities and making recommendations for their improvement. Internal Audit is thus part of the corporate governance system, together with the board, senior management and auditors. (Niemi 2018, 13)

By choosing a board to take care of organization's governance, owners seek to assure that management considers their best interest. Governance system, and internal audit as a part of it, supports this objective. To best manage corporate governance, the Board must ensure that the information it receives for decision-making on the company's risk management, internal control and corporate governance is reliable and comprehensive. Internal Audit assists the Government by providing systematic risk-based, independent and objective assurance and consulting. (Niemi 2018, 14)

Internal audit as a third line of defense provide risk-based assurance to the organization's top management. Assurance should cover, how effectively organization assesses and manages its risk. Internal audit is an independent function but uniquely positioned within the organization. In addition to providing independent assurance, internal audit is also well-placed to be in an advisory role. Internal audit can advise organization from objective perspective, for example, in ways of improving processes and implementing recommended improvements.

Assuring and advising role of internal audit are traditionally presented in internal audit frameworks. However, risk anticipating role is also included in the most recent frameworks. Deloitte's Internal audit 3.0 -framework is supposed to illustrate internal audit as it should be after recent changes like technological innovations and updating internal audit professional standards in 2017. The framework presents three roles of internal audit: assure, advise and anticipate. According to the framework these three roles *"constitute the triad of value that Internal Audit stakeholders now want and need"* (Deloitte 2018, 4).

In Deloitte's framework, assurance remains as a core role of internal audit. However, range of activities, issues and risks assured should be broader and more real-time. Considered internal audit's unique objective role and stakeholders' expectations, advising management on control effectiveness, change initiatives and enhancements to risk management fits well to internal audits' capabilities. Anticipative role of internal audit instead changes internal audit from backward-looking function to forward-looking function that is proactive rather than telling what went wrong in the past. (Deloitte 2018, 4)

Unlike auditing, there is no separate legislation for internal auditing in Finland. However, there are references in various laws and regulations to the internal audit function and its functions. The purpose and duties of internal auditing in the case of various organizations are set out, for example, in the Insurance Companies Act, the Act on Occupational Pension Insurance Companies and the Law on Credit Institutions. In general, the role of internal audit is defined in Financial Supervisory Authority Standard 4, 1: 6 Organization of internal control and risk management: "The function of internal audit is to effectively and comprehensively review the effectiveness of internal control and report directly to senior management." In addition to the law, any internal auditor should comply with professional internal audit guidelines. (Niemi 2018, 25-26) Because there is no strict regulation concerning conduction of internal audit, unlike auditing, ways of conducting internal audit can vary quite lot, especially because there are inhouse internal audit functions and companies that provide external internal audit services. However, all internal auditors must follow professional practices framework and professional standards.

3.1 Framework for International Professional Practices in Internal Audit

The Framework for Professional Practice in Internal Auditing is a conceptual model, which defines guidelines for the IIA (The Institute of Internal Auditors) profession. The framework contains the mission of internal audit as well as mandatory and recommended guidelines. Mandatory guidelines include the definition of internal audit, standards and ethical rules. Recommended guidance includes application guidance and additional guidance. (Niemi 2018, 26-27)

The mission of internal audit articulates, what internal audit should seek to accomplish in organization. In the framework, mission surrounds mandatory and recommended guidelines, which indicates, how internal auditors should utilize the whole framework when following the mission. IIA defines the mission of internal audit as follows: *To enhance and protect organizational value by providing risk-based and objective assurance, advice, and insight* (IIA Australia).

The definition of internal audit states the fundamental purpose and scope of internal audit. The official IIA definition of internal audit is "*Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes"* (IIA Australia). Especially objectivity, independency, systematic and value-adding are key words of internal audit and they should always be accomplished (Niemi 2018, 29)

To ensure that internal audit's mission is accomplished, and guidance is followed, the mandatory guidance includes also professional standards. The standards are not legally binding, but they should be followed regardless if internal auditor is a member of IIA. The standards were revised most recently in 2017. There are three types of standards: attribute standards, performance standards and implementation standards. (Niemi 2018, 30)

Attribute standards concern required attributes of internal auditors and organizations practicing internal audit. The attribute standards provide guidance on, for example, competence and accountability, objectivity and independence as well as continuous improvement and quality

assurance of the internal audit function. Performance standards set quality requirements for internal audit. Internal audit function's performance can be evaluated against these requirements. The performance standards provide guidance on, for example, planning, reporting, resourcing and quality assurance. (Niemi 2018, 31) Implementation Standards expand upon the Attribute and Performance Standards by providing the requirements applicable to assurance (IIA 2016, 1).

The core principles define the characteristics and procedures required for an internal auditor (Niemi 2018, 32). For internal audit to be considered effective, all principles should be present and operating effectively. Ways of achieving the principles, as well as internal audit function, can be quite different between organizations. Nevertheless, failing to achieve any of the principles probably means that an internal audit activity was not as effective as it could be. (IIA Australia) Core principles of internal audit are:

- *Demonstrates integrity.*
- *Demonstrates competence and due professional care.*
- *Is objective and free from undue influence (independent).*
- *Aligns with the strategies, objectives, and risks of the organization.*
- *Is appropriately positioned and adequately resourced.*
- *Demonstrates quality and continuous improvement.*
- *Communicates effectively.*
- *Provides risk-based assurance.*
- *Is insightful, proactive, and future-focused.*
- *Promotes organizational improvement.*

(IIA North America)

Principles of integrity, competence and independency are also part of IIA's Code of Ethics. In addition, the code of ethics includes also confidentiality as a main principle. Principles are relevant to internal audit function and profession. Principles are supplemented with Rules of Conduct. Rules of conducts describe behavior expected of internal auditors. The rules help interpreting the Principles and ethical conduct into practical applications. (IIA Australia) For example, rule 4.1 concerning competency states: "*Internal auditors shall engage only in those services for which they have the necessary knowledge, skills, and experience*" (IIA North America). Later in the thesis, changing requirements of internal auditors' competency due to

digital risks and especially intelligent automation are discussed and this rule of conduct's significance is discussed more.

Code of ethics, principles, definition and standards are mandatory guidance. In addition, The Framework for Professional Practice in Internal Auditing includes recommended guidance, which describes practices for effective implementation of mandatory guidance. The recommended elements of the IPPF are Implementation guidance and supplemental guidance. (IIA North America) Implementation guidance focuses on approaches, methods and aspects, but does not describe processes and procedures in detail. The guidelines include guidance, for example, on reporting to the senior management and board of directors, planning, implementing and communicating results of an audit. Supplemental guidance is a step-by-step guide on how to perform an internal audit. They include detailed processes and procedures such as tools and techniques, step-by-step procedures, and examples of their output. (Niemi 2018, 46)

3.2 Competency requirements of internal auditors

Global Internal Audit Competency Framework defines the competencies to meet the requirements of Professional Practices Framework (IPPF). The competency framework is also a created by Institute of Internal Auditors (IIA). The framework defines competency as *"ability of an individual to perform a job or task properly, being a set of defined knowledge, skills and behavior".* (IIA 2013b,1)

The framework guides identification, evaluation and development of required competencies in individual internal auditors. The framework includes ten core competencies, which are recommended to every level: staff, management and chief audit executive. Each core competency is supplemented with more detailed competencies. Even if competencies have been identified individually, they are all linked to each other. (IIA 2013b,1) The ten core competencies are listed below.

1. *Professional ethics: Promotes and applies professional ethics*
2. *Internal audit management: Develops and manages the internal audit function*
3. *IPPF: Applies the International Professional Practices Framework (IPPF)*

4. *Governance, risk and control: Applies a thorough understanding of governance, risk and control appropriate to the organization*
5. *Business acumen: Maintains expertise of the business environment, industry practices and specific organizational factors*
6. *Communication: Communicates with impact*
7. *Persuasion and collaboration: Persuade and motivates others through collaboration and cooperation*
8. *Critical thinking: Applies process analysis, business intelligence and problem-solving techniques*
9. *Internal audit delivery: Delivers internal audit engagements*
10. *Improvement and innovation: Embraces change and drives improvement and innovation* (IIA 2013b, 1-2)

All the ten core competencies are relevant regarding auditing intelligent automation. However, the most relevant ones are discussed in this chapter. The most relevant competencies have been selected based on interviews conducted in this research. They are Internal audit management, Governance, risk and control, Business acumen, Critical thinking and Improvement and innovation.

Internal audit management competence includes, for example, articulating expectations, setting goals and monitoring performance and staff workload. The most relevant parts of internal audit management competence regarding intelligent automation might be maintaining competencies to effectively deliver internal audit. Maintaining competencies concerns manager's own skills as well as developing plan to develop internal audit team's professional competency. Especially technical skills are important when speaking of auditing intelligent automation. (IIA 2013b, 7)

Governance competencies highlight especially giving comprehensive insight into organization's risk profile, contributing to the development of risk aware culture in organizations and monitors future risk changes to organization's risk profile. Thus, internal audit function should also contribute to identifying and assessing risks concerning intelligent automation, both current and possible future risks. To be able to deliver requirements of governance competences, internal auditor should also possess competencies listed in Business acumen -core competence. Many business acumen competencies concern maintaining knowledge about organization, its processes, its risks as well as microeconomic and

macroeconomic factors that might impact organization's performance. One business acumen competence is especially relevant if organizations are using intelligent automation: *"Assesses and takes account of how IT contributes to organizational objectives, risks associated with IT, and relevance to the audit engagements"* This means that internal audit function should have comprehensive knowledge about how intelligent automation works, what organization seeks to accomplish by using intelligent automation and how it could be assured that intelligent automation works as planned and helps organization to reach its objectives. The competency framework also states that internal auditor should take account organization's strategy as well as operative objectives. (IIA 2013b, 9-10) Therefore, intelligent automation should not be audited as separate feature, but as part of actions to reach organization's objectives.

According to the framework, part of critical thinking competencies, in addition to exercising professional skepticism is to apply appropriate tools to effective delivery. The framework mentions analytical tools as well as automated tools. Innovation competencies include both, contributing to innovation activities in organizations as well as innovative contributions inside internal audit function. According to the framework, internal audit should seek opportunities, practice continuous improvement as well as contribute to identifying change and innovation related risks and implementing change programs across audit function and audit team. (IIA 2013b, 15-16)

4 INTELLIGENT AUTOMATION

When speaking of automation, it is relevant to start by defining robotic process automation (later RPA). RPA is software programmed automation. RPA can imitate rules-based, repetitive tasks such as cut and paste, merging, button clicks etc. Simply, RPA is used to automate simple IT tasks with external software. (Christofferson et al. 2018, 25) RPA software works on user interface layer and can interpret existing applications, which is why initial investments to RPA are low and payback periods are short. Process automation can consistently carry out functions and it can be scaled up or down to meet organization's demands. (IRPAAI.com)

To automate end-to-end processes that need cognitive skills, artificial intelligence capabilities need to be integrated to RPA. Simply, artificial intelligence means that machines can perform tasks that require human intelligence such as making predictions, learning from data and finding meanings from pictures and voice (Watson et.al 2019, 13) Artificial intelligence includes machine learning, deep learning, natural language processing and generation and computer vision (Bajenescu 2018, 48; Watson et.al 2019, 13). This combination of cognitive technologies integrated to RPA is called intelligent automation.

Originally, algorithms, like algorithms that powered trading models in the 1990s were instructions-based programs, were created to follow detailed steps. Therefore, early algorithms were only able to act based on clearly defined data and variables. After development of big data, machine learning and artificial intelligence, algorithms that are not bound by the parameters of their operational code can be designed. Algorithms can now use thousands of variables and have become remarkably adept at independent decision-making. Especially need to exploit usable information from big data has pushed algorithm development forward. (Petrasic et al. 2017, 2) Artificial intelligence and automatics are hardly new technologies, but recent developments in technologies and computing power have helped to build new generation of software robots (Laurent, Chollet & Herzberg 2015, 2)

4.1 Benefits of intelligent automation

As mentioned before, with intelligent automation, it is possible to automate whole processes because artificial intelligence can perform tasks that need human consideration. RPA brings many benefits such as increasing productivity, cost reduction and improving employee experience. Integrating cognitive capabilities can take those benefits even further. Organization can especially improve their customer experience with intelligent automation (Watson et. al 2019, 6) Deloitte's intelligent automation survey (Watson et. al 2019) indagates that that the top three benefits that organizations expect from intelligent automation implementation are increase in productivity, cost reduction and increasing productivity. Also, better customer experience was important.

When intelligent systems are properly implemented, they increase processing speed, reduce human errors and lower labor costs and at the same time improve customer service experience. Organizations increasingly rely on algorithms when they want to make timely effective decisions that consider big amounts of data and human decision-maker would never be able to comprehensively understand. (Petrasic et al. 2017, 1) However, two issues must be noticed here; human behavior of the human employee, whom automation would replace and human behavior of customer, if automation works on client surface (Jaksic & Marinc 2019,7).

According to Laurent, Chollet and Herzberg (2015, 2) intelligent automation is starting to change ways business is done in almost every sector of the economy. Different intelligent automation applications vary from routine work to revolutionary, for example from collecting data to guiding vehicles. Accenture (Patel 2018) has listed eight key benefits of intelligent automation: accuracy, speed, service continuity, greater processing efficiency, ease of use, workforce agility, scalable infrastructure and strategic focus. Like mentioned before, intelligent automation reduces human errors in processes. Human errors can be, for example, wrong data inputs and missed steps. Intelligent automation can also reduce process cycle times significantly, especially in organizations that have lot of customer information processing. Also, service continuity can be enhanced by adopting intelligent automation, as intelligent software bots can perform same tasks as people but don't have the same limitations, like office hours. (Patel 2018, 7-8)

Intelligent automation can make processes more efficient and it is easier to implement and use than many other forms of automation, like physical robots. Also, capacity of intelligent

automation can be changed quickly, almost instantly. This means that organizations can react to demand peaks quickly, which improves customer satisfaction as well as workforce satisfaction. Also, when processes are automated, and costs saved, organizations can focus human resources to areas where they are needed. According to Accenture, the biggest advantage of intelligent automation adoption probably is turning strategic focus into cases and tasks that do need greater cognitive thinking and empathy than intelligent automation can perform, like big business decisions. (Patel 2018, 7-9) In addition to these benefits, Watson et al. (2019, 5) identify analytical capabilities as one benefit, as with smarter business decision can be made in some areas by using intelligent automation, which can sometimes take more factors comprehensively into account than humans.

4.2 Risks of intelligent automation

While gaining benefits from intelligent automation, organizations also face new challenges and risks. Many risks concern especially cognitive technologies, but many digital risks are relevant to all kinds of new technologies. New technology in general forces organizations to face new kinds of risks and therefore reconsider their risk management activities as well as internal audit planning and execution.

Risks in this chapter are divided to following categories: technology risks, regulatory risks, privacy risks, cyber risks, people related and organizational risks, ethical risks and financial risks. The categorization is made based on different categories identified from literature and previous research. However, all categories are linked to each other and in some cases, it is hard to define, which category risk belongs to. For example, many technology risks are caused by human so initially they are people related risks. However, all technology and data are designed and provided by people. Therefore, technology risks in this research include algorithm bias, incorrect implementation and incorrect data input. Matters concerning workforce capabilities and organizational issues are discussed in the chapter about people related risks. However, all risks which have been identified from previous research and literature are presented in this chapter of the thesis, but it was seen suitable to divide them to different categories to make the research constant and easier to follow. Regulatory and privacy risks are discussed in the same chapter, as big part of regulation concerning using intelligent automation is related to data compliance and privacy protection.

4.2.1 Technology risks

Organizations have begun to use cognitive technologies and solutions for different purposes, for example, financial services' processes and performing surveillance. However, often decision-making principles of artificial intelligence solutions are not transparent to organizations, so they produce results without explanations and monitoring inappropriate decisions may be difficult. Vulnerabilities like biased data, unsuitable modeling techniques, and incorrect algorithms might stay unnoticed. Therefore, artificial intelligence can produce biased results, which can have big effect on business operations. When new techniques, like intelligent automation, develop rapidly, methods for monitoring them lag technology adoption. It is important to seek transparency to intelligent automation decisions to manage its risks, also by internal audit. (Albinson, Thomas, Rohrig & Chu 2019, 6) It must be noticed that reliance in intelligent systems is increasing and excessive reliance on intelligent solutions can lead to additional risk taking and even raise system risk (Jaksic & Marinc 2019, 11).

Algorithm decision making is often opaque to organizations. Transparency of algorithms is an emerging research area. Transparency requirements are increasing, as organizations use large volumes of personal data and complex data analytics are used for decision-making. Algorithmic transparency is important for several reasons. Firstly, errors in algorithm decision-making are hard to identify if decision-making logic is not clear. If algorithms are transparent, organizations can notice, for example, discrimination introduced by algorithmic decision-making. Also, transparent decision-making enables to hold parties in the decision chain accountable, which can encourage organizations to adopt appropriate corrective measures, if incorrect or harmful decision patterns are identified. Secondly, transparency helps to identify errors in input data used by algorithm. Thirdly, if errors or adverse decisions are noticed, they can be prevented in the future. Decision-making logic can be corrected or features in input data changed to fit to purpose. (Datta, Sen & Zick 2016, 1)

In instructional algorithms, biases are relatively easy to identify, if developers are looking for them. What is different about smart algorithms, is that they are capable of functioning autonomously and how they collect data and process it is now always clear, even to developers. This opacity makes identifying and understanding biases more difficult. In algorithmic system, there are three main sources of bias: input, training and programming. (Petrasic et al. 2017,2)

Input biases occur when the source data is biased, for example, because it lacks some information, or it does not represent information that it was supposed to, or it reflects historical biases. (Petrasic et al. 2017,2) Data used by artificial intelligence applications is created by humans and can be imperfect. As artificial intelligence processes information and makes decisions based on fed data, flawless results can't always be expected. Recognizing this is the first step to manage technology risks. As AI does not understand tasks that it is performing and operates based on training data, overestimating AI's capabilities may have unwanted consequences. (Băjenescu 2018; 48, 51)

Intelligent robots operate based on given and taught algorithms. Algorithms model human thinking and decision-making process. Challenges in algorithm design are to design algorithm that manages different situations and conditions and can logical and analytical decision-making. Algorithms should be able to make decisions but operate based on limited solution options. (Lehto 2017, 9) Training bias can occur in either the categorization of the baseline data or the assessment of whether the output matches the desired result. (Petrasic et al. 2017, 2) If algorithms have errors, they might not perform as expected which leads to misleading results that can have variety of harmful consequences (Băjenescu 2018, 51)

What makes risk of "misbehaving algorithms" more severe is increasing uncritical reliance on algorithms. Algorithmic decisions are not reliable just by being results of complex and careful design. Even if automation decreases the opportunity of human biases, their consistency is not equivalent of objectivity. (Osoba et al. 2017, 2) Deodeo (2015, 1) states that "algorithms may be mathematically optimal but ethically problematic." Accountability is more complex, when speaking of biases done by artificial intelligence than speaking of human decisions. For example, it can be hard to define, if the party relying on algorithmic decisions or the party who designed the algorithm is accountable. Especially, relying on algorithms' correctness can be a big problem with intelligent automation, as it can be used to automate whole processes. Without any human intervention, the whole process could be working incorrectly long enough to have significant consequences.

The opacity of algorithms makes judging decision correctness, evaluating risks of artificial intelligence and assessing fairness more difficult. Problem might be small if algorithms work infallible. However, most algorithms do not have guarantee of infallibleness. And even if the algorithm it-self was bias-free, infallibleness also requires that they are applied appropriately and that data they use is correct. (Osoba & Wesler 2017, 3) Programming bias could

occur in the original design or when a smart algorithm can learn and modify itself through contacting with human users, the assimilation of existing data, or the introduction of new data. (Petrasic et al. 2017, 2) Validity of learning algorithm especially is a complex issue, as it is function of validity of its implementation and the correctness of its learned behavior. Learning algorithms might not consider new contexts and might be vulnerable to the characteristics of their training data. To work right in different contexts, learning algorithms need ability to adapt to changing inputs. Not being aware of this might result to harmful results of artificial intelligence implementation. (Osoba & Welser 2017, 7)

One example of this is Microsoft's artificial intelligence chatbot Tey, which was designed to discuss in compellingly human way with Twitter users. Tay wa successfully tested in controlled environments. The key feature of Tay was to learn and respond to users by ingesting user data. That learning feature enabled users to manipulate its behavior to make Tay answer offensively. Problem was, that Tay's experience or its training data did not take novelty in a new context into account. (Osoba & Welser 2017, 7; Lee 2016)

It is important to remember, that many technology risks are fundamentally caused by humans. Software development is not always bias free as all software are developed by humans. This can lead to software not working as they were supposed to work, or software has vulnerabilities which able cyber-attacks. Realized software risks can have massive impacts, especially artificial intelligence software because of their self-governing nature and big amounts of data that they are processing. (Lehto 2017, 8)

According to Watson et al. (2019, 2) organizations often lack the skills to develop support for intelligent automation, demand for third party vendors increases. Deloitte expects a shift from building in-house capabilities to buying automation as a service partly because talent shortages and cost pressures. Increasing use of third-party vendors increases traditional third-party risks like disruption risks. However, intelligent automation procured from external party creates new kinds of risks as well. The visibility to algorithm design and underlying training data is even more limited when using external vendors. (Albinson et al. 2019, 7)

4.2.2 Regulatory and privacy risks

There is little legislation governing artificial intelligence, but this is about to change, as legislation always reacts to new technologies with delay. Systems using large volumes of data must comply with privacy legislation. Especially EU's General Data Protection Regulation sets limitations for using consumer data. As artificial intelligence makes decisions on their own based on training data, new aspects of liability must be considered when using intelligent automation. (Băjenescu 2018, 54)

As regulation is evolving and increasing, companies must keep up with regulatory readiness, so they can react to regulatory expectations effectively. At the same time, companies must execute current requirements of compliance and expedite the implementation of the regulation's mandates, such as transparency, consent and breach reporting. With new technologies, companies must anticipate many aspects of regulation, for example, how strictly regulation is enforced, and which parts will regulators focus on.

Regulators are struggling to catch up as evolution of digital economy is faster than never and companies and countries are forced to implement new assets rapidly in very competitive environment. It is possible that organizations are establishing digital strategies and implementing new technology without knowledge about future regulatory environment. This creates risk of not being compliant with regulation or massive efforts to meet compliance requirements as well as having to shut down or slow down strategy execution or facing choice between executing a digital-first strategy and complying with all current and coming regulations. Wait-to-see strategy can also be dangerous choice, as competitors can be executing their digital strategies and therefore have significant competitive advantages. (Christofferson et al. 2018, 17, 27)

Especially personal information and consumer privacy is protected by legislation. In Finland, privacy is protected in Article 10 of the Constitution Law. Challenge is in applying regulation in digital world. Fast technology development has brought challenges to handling personal information. Organizations, both private companies and public organizations can use personal data extremely widely. (EU 2016/679, article 5) European Union's General Data Protection Regulation -directive (GDPR) regulates use of personal information. Directive took effect 2016. The directive includes lot of regulation about the use of personal information in general, but also specifically regulation about automatic information processing.

First time automatic information processing is mentioned in the directive is 15th article, which states: *"In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used. The protection of natural persons should apply to the processing of personal data by automated means, as well as to manual processing…"* Thus, personal information should be protected also when personal information is processed with automatic means. Naturally, automatic processing creates challenges to data protection as technology has to be more complex.

63rd article of the directive states that *"Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing"*. Firstly, this means that organizations should understand logic behind intelligent automation's processing and secondly, understand the consequences of automatic processing. Of course, this means that organizations must assure that logic and results of intelligent automation are what they were intended. This aspect poses a challenge to internal audit, because correctness of intelligent automation's logic must be audited as well as organizations understanding of it. The directive brings out two examples: automatic refusal of an online credit application and e-recruiting practices without human intervention.

It is also stated in the directive that decisions based on evaluating personal aspects relating to data subject and that are based only to automated processing and can have legal effects or similarly affecting consequences concerning the data subject should not be made against data subject's willingness. In other words, data subject should have right to not be a subject of such decision. not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. However, decision-making based on such processing should be allowed where expressly authorized by Union or Member State law. The directive also states other exceptions. For example, if *"…processing is necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent…"* (EU 2016/679, article 71)

Article 71 also states important information in internal audit's point of view: "*...the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organizational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimized, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject and that prevents, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or that result in measures having such an effect. Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions."*

Article above has lot of importance for internal audit. Article obligates organizations to assure that logic behind intelligent automation is correct, risks for errors are minimized, data is secured, and automation does not provide results that could be anyhow discriminatory. This sets lot of external requirements for organizations and also requirements for internal audit, as it should assure that organization fulfills its regulatory obligations.

Also, article 90 says, that if there is a high-risk facing individual's rights or freedom, the party using personal information should carry out data protection impact assessment before using the information. This should be applied especially, if organization uses big amounts of personal data or data is sensitive in nature. Impact assessment should also be made if organizations is making decisions concerning individuals by systematically and extensively profiling individuals based on personal information and characteristics. (EU 2016/679, article 90-91)

Assessing privacy risks and staying compliant with regulation is not easy as privacy can also be understood in variety of ways. Privacy risks do not only concern artificial intelligence or intelligent automation, but rather the whole digital society. Digital privacy is different in every layer of digital world. According to Sartonen, Huhtinen and Lehto (2016, 5-6) these layers are physical, syntactic, semantic, service layer and cognitive layer. Physical layer means people's physical devices like computers and smartphones. On syntactic level, users appear as IP-addresses, email-addresses and other user accounts which can be used to log in to different devices or services. Semantic layer contains personal information, which can be in picture, text or voice format. In service layer, people are part of different social media communities like Facebook or blog networks.

Privacy is associated with these identities and ascending from the physical floor the level of complexity increases. Due to complexity of digital identities, defining privacy in the digital world is not simple. Privacy includes different factors, for example, personal confidential information, right to control own information and protect it, intimacy, anonymity and freedom of action. (Lehto 2017, 10-11) These factors also apply in digital world, although their definition is more complex and multi-dimensional. Therefore, setting limit for privacy in digital world is difficult, which poses a challenge for regulators.

Anonymization of data is used to address privacy concerns when handling large amounts of personal data information. What comes to cognitive technologies, they can use a large digital footprint that people leave in the digital world. Therefore, anonymization does not necessarily prevent intelligent system from identifying identities. (Lehto 2012, 11)

4.2.3 Ethical risks

Ethical issues are often emphasized in media when speaking of artificial intelligence. It is troublesome to determine ethical principles based on which robots operate technologically but also because ethicality is subjective. Moral questions that usually determine human behavior also determine behavior of algorithms. Challenge is, that usually people are not unanimous about ethical issues and sometimes it can be hard to determine, what is acceptable according to society (Kananen & Puolitaival 2019, 220)

There are many perceptions even about, what is objective in developing artificial intelligence. Some might think that the objective is to strive as close as possible to human thinking and some that the objective is to accomplish ideal rationality. Opinions probably vary in between. (Ollila 2019, 29) If there is no mutual understanding of the purpose of artificial intelligence, how can there be mutual understanding about its ethicality? Also, it is important to separate developer's ethic from bot's ethic. Developer's ethic means thinking about what kind of algorithms are ethically right to develop. Bot's ethic means ethical perceptions been taught the artificial intelligence agent. (Ollila 2019, 247)

Ethicality can be measured by estimating consequences of each action. Problem is, that sometimes actions that are generally considered culpable might have best consequences. In practice, it can be hard to accomplish solutions that suit everyone and do not cause harm to anybody. (Lehto 2017, 10) Ethicality is determined by humans and there are endless

interpretations of ethical. Artificial intelligence's behavior is determined by these interpretations. Therefore, term "misbehaving" algorithms can be misleading if there is no error in the algorithm, but their behavior is determined ethically questionable. (Osoba & Welser)

Artificial intelligence has been criticized because it can be difficult to be certain, how it comes to conclusions. Again, algorithm opacity creates challenge to use intelligent automation, as it may be difficult to be certain that algorithm makes decisions and forecasts ethically. (Kananen & Puolitaival 2019, 221)

As new artificial intelligence capabilities improve, organizations will need to decide, if they want to use all these capabilities. Organizations must take ethical impacts of new capabilities into consideration. In Gartner's (Christofferson et al. 2018, 19) 2019 Audit Hot Spots survey, Fifty-nine percent of CIOs report facing ethical challenges related to digitalization. The complexity and lack of transparency of algorithmic decisions and propensity to learn create significant challenge. The ethical consequences are to increase dramatically, as fields such as medicine and law expand their use of data analytics and artificial intelligence. Inadequately managing ethical implications of digital advances can have many kinds of consequences, for example, legal consequences and reputational consequences. 85% percent of consumers say they would stop doing business with a company if they didn't trust its use of their personal data (PwC 2017, 3).

The ethical risk of intelligent automation has two sides. Firstly, intelligent automation can behave ethically questionable. Zuiderveen Borgesius (2018, 14-15) has listed some examples of discriminatory artificial intelligence applications. Firs example is from public sector. Correctional Offender Management Profiling for Alternative Sanctions (COMPAS) is used in some parts of United States to predict, if defendants will commit crimes again. COMPAS does not take racial origin or skin color into account. However, research by Angwin et al. (2016) found out that even if COMPAS correctly predicts recidivism with 61% accuracy, but african american people are almost twice as likely to be labelled a higher risk but not actually reoffend than whites. Zuiderveen Borgesius also mentions artificial intelligence application, which was used to select prospective students in UK and led to discrimination because of bias in training data. Other example mentioned is Amazon's artificial intelligence system for screening job applicants. The system was found out to be discriminatory against women.

The second side of the risks is that important business opportunities are not taken advantage of because ethicality of intelligent automation is too difficult to ensure. Ethical problems in

intelligent automation do not only lead to reputational loss and client satisfaction but can also have legal consequences. Article 14 of the European Convention on Human Rights states: *"The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status"* Both direct and indirect discrimination are prohibited by this article. Indirect discrimination means that some practice seems neutral at first but ends up discriminating against some people. (Zuiderveen Borgesius 2018, 18-19) Discriminatory artificial intelligence systems are usually these kinds of indirectly discriminative systems because discrimination by them is usually unintentional.

4.2.4 Cyber risks

According to Online Trust Alliance (2018, 2-3) Cyber incident are defined as unauthorized:

1. access to a system or device and its data,
2. extraction, deletion or damage to any form of data,
3. disruption of availability and/or integrity of any business operation,
4. activities causing financial or reputational harm

The same report also states that 93% of cyber incidents in 2017 could have been prevented. This means that adequate controls to prevent cyber incidents were not in place, but they could have been. As an assurer and enabler of sufficient control environment, internal audit can have a big effect on cyber security.

The growing complexity of organization's infrastructure and increasing usage of technology creates new access points to organizations. As companies digitalize and further embrace advanced technologies, they are also opening new endpoints and weak links. One hundred eleven billion lines of new software code are produced each year and by 2020, there will be 20.4 billion connected devices, up from 6.4 billion in 2016. (Christofferson et al. 2018, 11)

Benefits and opportunities brought by new technologies, like intelligent automation, can be significant to organizations. Therefore, they can overshadow security concerns. Problem concerns especially intelligent technologies, as they are often at some level unmonitored. Increased reliance on intelligent technologies also makes noticing security problems slower. (Christofferson et al. 2018, 11) As artificial intelligence systems can process huge amounts of

data, hackers who want to steal personal data or confidential information about a company are increasingly likely to target artificial intelligence systems. (Băjenescu 2018, 54) According to Deloitte's the Future of cyber -survey (Powers et al. 2019, 23) data management complexities was the most answered question when 500 C-level executives were asked, what is the most challenging aspect of cyber security management across their organization.

Cyber security is built on human activities, organizational processes, and information technology. Cyber security is important part of intelligent automation adoption, implementation and usage. If cybersecurity solutions are not executed in the best possible way, it can cause serious consequences to information technology infrastructure and data, which is important to business or to customers or employees. (Lehto 2017, 2, 12)

Identifying possible cyber threats from the beginning of adaption process is a prerequisite for the use of intelligent automation or new technology in general. However, identifying and assessing cyber threats should not stop to the adaption phase. Secure software design should continue throughout the system lifecycle. And correctly executed security solutions can also help managing, for example, risks related to ethical issues.

ECIIA (European Confederation of Institutes of Internal Audit) published Risk in focus 2020 - study in 2019. ECIIA got responses from 528 Chief Audit Executives (CAEs) across Europe. Study found that 78% of CAEs thinks 'Cybersecurity and data security' as one of the top five risks that their organizations face and 21% singled it out as the top risk, making it more widely referenced than any other risk area. 68% of CAEs also report that cyber and data security is one of the top five risks on which internal audit spends most of its time in organizations. (ECIIA 2019, 11) Cyber security risks are even more relevant topic after GDPR came into effect in 2018. Loss of reputation or malfunction of IT infrastructure can cause significant losses. In addition, also the regular consequences should be taken into consideration, as explained more thoroughly in Regulatory risks -chapter.

However, there is upside risk of cyber security as well. Cyber security should not only be about preventing possible incidents, but to be a competitive asset and value creator. Ability to keep data safe and quickly respond to cyber breaches is an opportunity to build trust with stakeholders. (ECIIA 2019, 16)

4.2.5 People related and organizational risks

Due to today's uncertain and complex environment, risk-aware culture throughout organizations is needed more than ever. As security threats grow, lack of coordination between security and risk management can lead to slow respond times and therefore to inefficient responses to risks caused by disruptive technologies. These coordination and planning issues are compounded by nearly half of organizations not having risk appetite or tolerance statements and 77% lacking formal cybersecurity incident response plans. Without organization-wide risk ownership, organizations diminish their ability to adequately identify and respond to risks and persevere in the current risk environment. (Christofferson et al. 2018, 21) Yet, according to ECIIA's risk in focus 2020 -survey, 58% of CAEs think Digitalization, disruptive technology and other innovations as a top five risk to their organization, but just over half (30%) of this proportion of CAEs say it is in the top five risk areas that are audited the most.

Automation is predicted to be one of the biggest disrupting factors in the coming years, yet many organizations struggle to understand how it will impact their organization's talent needs. While companies anticipate a digital business transformation within the next few years, it is uncertain, whether automation will create or change jobs or make eliminate them. Outcome will probably be mix, depending on field and company type. Some job descriptions are already becoming obsolete. In 2020, AI is projected to create 2.3 million jobs and eliminating 1.8 million jobs. The uncertainty surrounding the head counts and skills needed in the future to support digital business transformations makes it difficult for organizations to ensure they have the workforce they need and competences they need to achieve their goals. (Christofferson et al. 2018, 29)

Utilization of emerging technologies requires new skills for achieving objectives and protecting against increasing and more complex security threats (Christofferson et al. 2018, 29). According to Deloitte's executive survey (Watson et al. 2019, 2) organizations piloting intelligent automation see lack of vision and ambition as a key barrier. As organizations often lack the skills to develop support for intelligent automation, demand for third party vendors increases. Deloitte excpects a shift from building in-house capabilities to buying automation as a service partly because talent shortages and cost pressures.

In addition to shortage of management and strategic skills, according to Gartner's Audit Hot Spots 2019 -research (Christofferson et al. 2018, 29) one of the biggest issues facing organizations today is lack of technical skills. Positions related to artificial intelligence, big data

and data analytics are hard to recruit for, which causes risks of delays in technology adoption and disruptions in ongoing projects. Other concern is organization's capability to keep up with security threats. According to CSO (Morgan 2017) 3,6 million cybersecurity jobs will be unfilled by 2021. 52 % of IT security professionals doubt their ability to stay on top of security threats given the lack of employee skills (Cummins 2018). Gap between skills that organizations possess and speed of technology disruption forces organizations to face risks of not being able to firstly start intelligent automation planning, implement intelligent automation, carry out already started projects and protect themselves from security threats.

The challenge is not only in finding capable personnel but to train personnel and integrating workforce into technology adaption. Culture building is an important factor in any kind of digital transformation. And it does not only concern organization's own workforce but also rental workforce and vendors too. (Albinson et al. 2019, 20) After all, technology is designed and used by people. This applies especially when speaking of intelligent technologies, as they can work with, not just for, people and their behavior logic is determined by people. Cultural resistance can prevent organization to get anticipated technology from technology adoption. In the other hand, people in an organization should also understand, that artificial intelligence agents can't be blindly trusted.

4.2.6 Intelligent automation adoption and financial risks

If the intelligent automation adoption is successful or not and if risks realization can be prevented depends lot from, what are the objectives of using intelligent automation and how objectives align with intelligent automation strategy. Although intelligent automation has big potential benefits and opportunities, implementing intelligent technologies is more complex than implementing just robotic process automation. Therefore, to succeed in intelligent automation adoption, it is important to find the balance, where intelligent technologies should be applied to RPA or where processes should be performed manually. This is important part of maximizing return of investment while minimizing risks and unnecessary complexity. (Joseph 2018, 9) However, not only cost reduction should be considered when implementing intelligent automation. According to Albinson et al. (2019, 9) it can be difficult to realize full potential of intelligent automation if the focus is only in reducing costs. Other benefits like consistency, quality and accuracy.

What can go wrong with aligning intelligent automation objectives with organization's strategy is often related to lack of intelligent automation capabilities and vision in organizations, like discussed in the chapter about people related risks of intelligent automation. Therefore, commercial intelligent automation solutions become more common and external consulting is used in organizations. Like discussed in the chapter about people related risks, adopting holistic change management approach is one of the prerequisites for realize the complete advantages of intelligent automation (Albinson et al. 2019, 8)

Also, the whole control environment around the automated process must be redefined and outdated controls replaced. New controls need to be designed and old ones digitized through analytics or other technologies. Risk management and control design should be already part of objective setting and planning phases. (Albinson et al. 2019, 8)

According to Watson et al. (2019, 7) organizations seem to be quite slow with their intelligent automation adoption, given the benefits that could be gained. Deloitte conducted a survey about intelligent automation adoption and its impact to workforce planning in 2019. 523 executives answered and according to the survey, 50 % of companies piloting intelligent automation knew how they will capture value from intelligent automation projects. The number was 78 % with organizations that were already in scaling phase. (Albinson et al. 2019, 7) If it is not clear how to capture value with intelligent automation in the piloting phase, it might mean that also the objectives are not clear. Therefore, adopting intelligent automation does

All risks mentioned in this chapter about risks of intelligent automation can lead to financial consequences as they all can impact business in different ways. For example, by reputational loss, sanctions, high recruitment costs and malfunctioning IT-infrastructure. However, all these factors can affect investment's return of investment (ROI). Taken all these risks into account when planning intelligent automation is the first step to manage financial risk of intelligent automation adoption.

Big financial consequences can occur if the adoption of intelligent automation can't be delivered. In this case, ROI is negative and capital for other investments is wasted. Especially these kinds of risks, that could be fatal to the implementation must be carefully assessed in the beginning of intelligent automation objective setting and adaptation planning. For example, changing legislation or large-scale cyber-attack could stop the adaption or move it forward. This is one reason, why risk management should be part of planning phase. If internal audit

should also be part of the process from the beginning or not, is discussed when answering to the research questions in chapter 5.

5 MOST IMPORTANT RISKS OF INTELLIGENT AUTOMATION AND CHALLENGES TO INTERNAL AUDIT

5.1 Research material

Empirical part of the thesis consists of interviews and survey. Interviews were conducted during March 2020. Interviewees are listed below.

- Kaarina Sinersalo, CEO, Institute of Internal Auditors Finland (IIA)
- Tapio Tierala, Head of risk management and internal audit, Aalto University
- Sirkku Holmström, Head of Internal Audit, Finavia Corporation
- Sakari Lehtinen, Chief Audit Executive, OP Financial Group

Interview material was acquired from companies presenting different industries to get comprehensive picture about the subject matter, as research does not concentrate in specific industry or organizations. Interviews were in-depth and semi-structured interviews. In semi-structured interviews, the interviewer has prepared topics, issues and questions to discuss, but still has possibility to vary the wording and order of questions. In-depth interviews, researcher interviews subjects in tailored and detailer manner and interviewees can answer freely to the questions. Questions in in-depth interviews tend to be open-ended and therefore allowing unique answers. (Walle 2015, 18)

In semi-structured interview, it is also possible to ask additional questions, if those rise during the interview or the interviewee can also propose new questions. The advantage of semi-structured interview is that, the interview and collected research material are somewhat systematic but interview is conversational and informal. (Erikson & Kovalainen 2008, 20-21) The interviews were successful, and lot of insight was provided from each of the interviewees. Results of the interviews are not discussed in individual level and answers can't be linked to individual interviewee.

Some observations about possible research results were already made after the interviews, as all the four interviewees had some same answers and thoughts. To get more confirmation to these findings identified already in the interview phase, several statements were included to the survey conducted and participants were asked, if they agree or disagree with the statements. In mixed-methods research, interviews can be useful supplement and add depth to other approaches, for example if there is need to conduct some in-depth insight before designing a survey (Adams 2015, 494)

The survey was conducted with Google Forms. The survey was published in IIA Finland's member newsletter, IIA Finland's website and LinkedIn-page, in a Teams-group for internal auditors in Deloitte Finland and to internal auditors in OP Financial Group. Answering to the survey was anonymous. The survey had 30 responses. Survey was selected to be the other research method as it is easy and fast way to get lot of responses to complement deeper answers acquired in the interviews. The survey included multiple-choice questions and open questions. Because the research topic is quite new to organizations, it was seen suitable to ask also open questions in the survey, as professional insight can be difficult to provide with only multiple-choice answers.

More answers to the survey would have given more reliable results, but considering the novelty and quite limited target group, 30 answers with four in-depth interviews can be considered to give quite comprehensive picture about the research topic. Some background information was also asked from the survey participants. Firstly, the participants were asked how long they have been working with internal audit. The distribution of answers is seen in figure 5. About 43% of participants have been working with internal audit under five years. However, over half of the participants have been working with internal audit over five years.

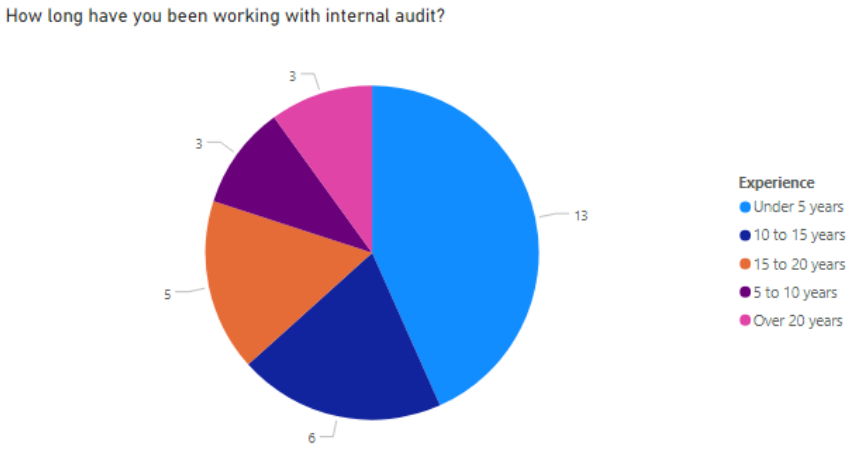

Figure 5 Distribution of answers to question 1

The participants were also asked, if intelligent automation was used in their organizations or in organization they are auditing. The participants include in-house auditors as well as auditors from companies providing external internal audit services. Therefore, questions were formatted to include both. The answers were divided to half. 50% answered that intelligent automation is used in their organization or organization they are auditing and 50% answered no. Although, it would have been ideal to get answers only from internal auditors who have experience of intelligent automation, it was not expected because novelty of the technology. However, internal auditors probably have views on how intelligent automation can impact internal audit, even if they don't have experience from it.

5.2 Technology risks

As discussed in chapter 4, technology risks of intelligent automation include incorrect data, malfunctioning algorithms because of their biased design, malfunctioning algorithms because of their incorrect implementation and malfunctioning technology. Opacity of intelligent algorithms makes implementation and noticing biases more difficult to organizations. Opacity of algorithms was also brought up in all interviews and it is strongly linked to all risks caused by intelligent automation, especially to risk of lack of competent workforce.

All interviewees thought that opacity of intelligent algorithms makes noticing biases in intelligent automation difficult. Increasing reliance on intelligent systems makes the issue more severe. According to one of the interviewees, if organization is not certain of how the algorithm in intelligent automation operates, its possible that organization is not fully aware, what data automation is using and if something relevant that could affect automation's decision-making is left out.

There is no certainty that algorithm design is made correctly, especially when technology is provided from external vendor. Two of the interviewees also brought up that even if automation is designed correctly, it might not work as it was supposed to in new context and implementation. Correct implementation is key requirement for automation to work correctly. All the interviewees also thought that it is important to plan control environment and assure that it is adequate already when planning the implementation of intelligent automation. Interviewees also emphasized the importance of taking legal and ethical requirements to account when designing controls to automation. If the automation generates biased results, it

can have several consequences, for example, to customer satisfaction, organizations reputation and inefficiencies to business activities.

With all technology, there is also a risk of automation not working and giving incorrect results or just shutting down because of overload or other reasons. The problem with intelligent automation is that whole processes can be automated with it. Automation not working can lead to conducting the process impossible. This can lead to bad customer satisfaction rates and financial losses. Human errors can be prevented by using automation. However, it must be noticed that errors in automation are probably systematic and therefore probably have more severe consequences that human errors (Haight & Caringi 2007, 710).

According to the survey conducted, organizations acknowledge technology risks of intelligent automation quite well. In question 5, which was only answered by internal auditors, whose organization or organization they are auditing has intelligent automation in use, 14 out of 15 participants answered that their organization has considered intelligent automation related technology risks. Question 6 in the survey was an open question, where participants were asked which intelligent automation related risks are the most relevant for their organizations. Five open answers were related to technology risks. One participant answered: *"The most relevant risk is probably possibility that intelligent automation doesn't provide results that is supposed to because its decision-making logic is difficult to monitor".* Another participant already took to account internal audits point of view: *"Technology risks are the biggest, because there are many factors to audit: input data, decision-making logic and if the automation is correctly implemented".*

In question 8, participants were asked to rate importance of each risk category from 1 to 5, 1 being not important and 5 extremely important. In technology risks, all participants answered value between 3 to 5. When participants were asked to choose the most important category in question 9, technology risks were ranked as the most important category, with seven participants out of 30.

The biggest challenge to internal audit seems to be skills of internal auditors, which will be discussed in chapter 6.1. However, opacity of intelligent systems sets big challenge to internal auditors, the same way it does to the management and employees working with automation. If biases due to opacity are difficult to notice by organization, it is also difficult for internal audit. All the interviewees brought up this aspect and how it requires more understanding about intelligent automation and technical skills from internal audit. For example, one of the

interviewees stated that "*Possibility of understanding artificial intelligence decision-making incorrectly is bigger than, for example, with data-analytics, because processing is more abstract. Does the organization really understand how artificial intelligence processes information? Risk is that people working with intelligent automation do not understand what data is uses and if something relevant that could affect the outcome has been ignored. And does internal audit understand how automation processes information to notice if something important has been left out or automation generates incorrect results?"*

Based on the interviews and previous research, eight challenges regarding intelligent automation from internal audit's perspective were identified. In question 13 of the survey, participants were asked, which of the challenges is the biggest one or if the biggest challenge is something else. There were three challenges to get most answers and opacity of intelligent systems was one of them. Thus, the participants of the survey also saw opacity as a big challenge for internal audit.

5.3 People-related risks and organizational risks

According to the interviews conducted, one of the biggest challenges for organizations is competent workforce. Competency is needed in strategy planning, implementation, using and monitoring intelligent automation. It was brought up in the interviews, that planning intelligent automation needs insight and understanding about the benefits and risks of intelligent automation, but also about how intelligent automation aligns with organization's strategy. Strategy setting and utilizing intelligent automation potential where suitable is discussed more in the next chapter.

All interviewees brought up the problem of reliance on intelligent systems if it is no clear in the organization how it operates. One of the interviewees stated: *"People in the organization need to be trained to understand, what intelligent automation does, what it does not do, and what is people's role as partners to automation. Organization can't just trust that automation does everything correctly and ethically"*. Other interviewee discussed the topic: *"In addition to people designing the automation, also management and people that are part of the process, in which intelligent automation is implemented, need to understand how it works. Training needs to be provided. Current labor markets have more demand for technically skilled workforce than*

there is supply". Thus, the challenge is in educating current workforce as well as recruiting capable workforce.

However, not only technical skills are required when adopting intelligent automation to organizations processes, but also special knowledge about legal and ethical requirements when using intelligent systems. Ethical and regulatory risks are discussed in more detail later in this main chapter. Especially now, when data integrity and corporate responsibility are very important even for organizations that don't have intelligent systems in place, skilled workforce from these areas is important.

"To get as much as possible benefits from intelligent automation and in the other hand manage its risks, organizations should build culture that emphasizes benefits of using intelligent automation, ethical usage of data and importance of not blindly relying on intelligent systems" was stated in one of the interviews. Like discussed in one of the interviews, people should be partners of intelligent automation. If automation is seen as threat or if people rely on it too much in the organizations, there is a risk that full potential is not reached. Like all reforms, also intelligent automation implementation should be accompanied with change management.

One of the interviewees also brought up that different parts of organizations, including internal audit, should work together to identify inefficiencies in processes that could be fixed with automation and to identify possible risks throughout the organizations. All the interviewees were asked question if three lines of defense might change or combine somehow when speaking of managing risks of intelligent automation. This matter is discussed in more detailed manner chapter 6, but all interviewees shared mutual understanding that three lines of defense should be in cooperation that expertise from all lines is used. However, the roles of the three lines should be clear in cooperation.

One of the interviewees brought up the challenge of auditing culture. Culture is abstract and very different in all organizations. Also, all interviewees brought up the challenge of auditing people's competencies and skills. If one of the biggest risks of intelligent automation is that organizations don't fully understand how it works and therefore it stays unnoticed if intelligent automation gives incorrect or, for example, discriminatory results, internal audit should assure that there is enough understanding about the data, working logic and what are the objectives that are trying to be achieved with intelligent automation. To really evaluate someone's knowledge about technology, internal auditor should possess enough knowledge about the subject as well, was stated in one of the interviewees.

In the survey, seven of 15 participants to question 5 answered that their organization or organization which they are auditing has considered people related risks regarding intelligent automation. When participants were asked to rank risk categories according their relevance from 1 to 5, people related risks got average of 3,7. When asked, what is the most important risk, four out of 30 participants answered people related risks. However, one of the three biggest challenges to organizations from internal audit's perspective was "Short of competent workforce". This seems to mean that also participants of the survey recognize challenge to audit people's competencies. Also, internal audit team's skills were answered to be the biggest challenge for internal audit, but this matter will be discussed in a separate chapter.

5.4 Planning intelligent automation adoption and exploiting opportunities

In the survey, four out of 15 participants answered that their organization has considered risks related to strategy, planning and implementation of internal audit. When participants were asked to rank risk categories according to their importance, risks related to strategy, planning and implementation got average of 3,7. Four Participants did rank these risks to be the most relevant risks of intelligent automation.

In all the four interviews, it was discussed that strategy and planning also require understanding on how intelligent automation works. One of the interviewees stated: *"Organizations have to understand how intelligent automation works and what it does not do, when deciding, where to implement it and how it serves organization's operations. Organizations need to have adequate understanding of the technology it self to strategically plan intelligent automation adoption. Management needs the understand the whole picture and risks need to be considered already in the planning phase."*

Challenges are not only in planning to adopt intelligent automation, but also in seeing the opportunities. One of the interviewees thought that the biggest risk regarding intelligent automation probably is missing the opportunities that intelligent automation could bring. All other interviewees also brought up the risk that organizations do not understand the opportunities that intelligent automation could bring and therefore do not exploit them. One interviewee stated that *"Finding new ways of continuous improvement should be a part of organization's strategy. There is a risk that organization does not identify inefficiencies*

because they are not constantly looking for them and do not understand opportunities of new technologies. And if internal audit does not keep up with new technologies, inefficiencies can stay unnoticed by internal audit as well". Therefore, internal audit's skills and competences play important part in noticing opportunities to make processes and business activities more efficient. One interviewee stated that *"to stay relevant, internal audit has to keep up with its technological skill to help organizations identify possibilities that adopting new technologies could bring".* Skill requirements of internal auditors are discussed more in chapter 6.1.

Financial risks of intelligent automation can be consequences from realization of all other risks, for example, cyber risks or regulatory risks. But the risk that intelligent automation investment does not provide the desired return of interest is often caused by mistakes in the planning phase, for example, risks are not considered in the planning phase or intelligent automation adoption does not align with organization's strategy. Financial risks were not seen as one of the most relevant risk categories in the survey but is overlapping with all the other categories. Only one participant thought that financial risks is the most relevant category.

5.5 Regulatory risks

All the interviewees thought that increasing regulation sets big challenge to organizations in assuring that data used and intelligent automation processing comply with regulation as well as ethical standards. Possibilities to use, for example, personal data are so multiple with intelligent systems, that many examples of unethical or illegitimate use of data have occurred. Below are listed some quotations from all four interviews conducted.

- *Possibilities to use data and profiling in business are very wide, but organizations have figure out, what is legally and ethically possible*
- *If logic behind artificial intelligence is not clear to the organizations, it can cause the organization to face challenges with compliance requirements*
- *Regulation is very important, because if regulatory requirements are not considered already in the planning phase, it can cause barriers to technology adoption and unnecessary implementation costs. Organizations must be proactive with possible future regulatory requirements as well.*

- *Correctness of intelligent automation decision-making logic must be very thoroughly assured especially when it uses data which is highly regulated.*

As it can be concluded from the answers, it is important to ensure that the data that intelligent automation is using is legitimate, intelligent automation uses it according to legislation and this requires knowledge about current legislation, proactive approach to be prepared for future legislation and adequate understanding about the technology. Like discussed in the chapter 4, regulation, for example, EU's General Data Protection Regulation (GDPR) requires that organizations can explain the logic behind automatic decision-making and profiling and prove that it is legally compliant.

11 out of 15 participants answered that their organization has considered regulatory risks and when asked to rank risk categories according to their relevance from 1 to 5, regulatory risks got average of 3,63. Three of the participants considered regulatory risks as the most relevant risks. Only two of the participants considered increasing regulatory requirements concerning data protection and automated decision-making as the biggest challenge for internal audit in question 13.

Naturally, increasing regulatory requirements set new skill requirements to internal auditors as well, as it is harder to keep up with regulation. When it comes to intelligent automation, internal auditors should know, for example, all requirements of using profiling and personal data. The challenge is even bigger, because internal auditors must consider ethical aspects outside legislation as well.

5.6 Ethical risks

In addition to considering regulatory requirements when implementing and using intelligent automation, organizations must make sure that use of data and artificial intelligence is ethical. As discussed in chapter 4, ethicality is subjective. Therefore, it can be difficult to determine ethical principles that are not included in regulation. And even if the use of data is ethical and algorithms designed not to, for example, be discriminatory towards any group, in-direct and unintentional discrimination of the algorithm is still possible, like in the examples of discriminatory biases of intelligent systems in chapter 4.

All the interviewees brought up opacity of intelligent systems also when talking about ethical issues. Usually, it is not intention to use data or profile people in unethical manner, but if biases are not noticed, algorithm can produce ethically biased results for a long time. All the interviewees thought that organization needs understanding of the technology as well as knowledge about corporate responsibility and ethicality, to tackle ethical risks of intelligent automation. Concerning knowledge about corporate responsibility one interviewee stated that *"Managing ethical risks of artificial intelligence requires knowledge about corporate responsibility in addition to technical skills"* and other that *"Organizations need to keep up with responsibility and ethical questions and so must internal audit to provide added value to the organization".*

One interviewee thought about the subjective nature of ethical questions as follows: *"Someone has to make decisions about ethicality for the bots, so whose responsibility it is to decide what is right and what is wrong. Therefore, organization needs people with experience from this field as well as technical skills."* When subjectivity of ethical questions is challenge to the rest of the organizations, it is that also to internal audit. Internal audit has to struggle with the same problem and also require skills or educate themselves about ethical questions. If there is no some sort of framework or best practice defined to solve ethical issues that are not part of regulation, it is challenging for internal audit to determine, if actions of the organization are ethically right. One interviewee stated that *"Internal audit can assure that ethical principles have been defined and organization is following them. However, setting limits on what is ethical and what is not is difficult. Therefore, internal audit as well needs to keep up with ethical issues to stay relevant".*

According to the survey conducted, 5 participants out of 15 answered that their organization or organization which they are auditing has considered ethical risks. When participants were asked to rank risk categories according their relevance, ethical risks got average 3,4. Only one participant out of 30 answered that ethical risks are the most relevant ones of intelligent automation. However, when asked about very relevant specific risks from the risk categories, one participant answered that *"Ethical risks are not considered as part of the design and implementation of the intelligent automation"* and other participant "*Ethical risks like fraud risks".*

5.7 Cyber-risks

All interviewees thought that cyber-risks are very current topic and emphasized in all organization's internal audit planning too. Intelligent systems can process very big amounts of data continuously and therefore interviewees though that cyber threats are even more relevant subject when talking about intelligent automation. Interviewees also brought up that intelligent automation can often process sensitive information, like personal financial information for credit decision-making or payroll information, why consequences of cyber breaches would be severe. One of the interviewees stated, that "*Cyber risks are very relevant subject right now, especially with this kind of technology, where human intervention is minimized".* As whole processes can be automated with intelligent automation, automation processes data without human control and cyber breaches could disable the whole process. One interviewee stated: "Of course when data is used systematically, cyber breaches are more likely to be targeted to these kinds of systems and consequences would be more severe". One interviewee also brought up the possibility of programming intelligent systems functioning incorrectly.

According to the interviews, internal audit plays important role in assuring that used technology is secured. However, internal audit does not have the primary responsibility but assures according to its risk-based plan that controls are adequate and compliance requirement are met. The required controls depend on, how sensitive information automation is processing and if the information is under regulation. Challenge to internal audit is again capabilities of auditors about cyber security and tools, since all interviewees thought that analytical tools should be used to assure that intelligent automation is working from input data to results.

According to the survey conducted, 10 out of 15 participants whose organization or organization which they are auditing has adopted intelligent automation answered that organization has considered cyber risks related to intelligent automation in question five. When participants were asked to rank risk categories according their importance from 1 to 5 in question eight, 17 participants answered 5. Cyber risks got average of 4,4. When asked, which of the risk categories is the most relevant one in question nine, 5 participants answered cyber risks.

6 INTERNAL AUDIT'S RESPONSE TO THE CHALLENGES CAUSED BY INTELLIGENT AUTOMATION

Challenges for internal audit concerning each risk category were discussed in the previous chapter alongside each risk categories that organizations face. However, four factors, that make auditing risks of intelligent automation challenging and are common to all the risk categories were identified in the research. Firstly, internal audit competencies were seen as the biggest challenge for internal audit when auditing intelligent automation by both, interviewees and participants in the survey. Secondly, the position of internal audit within the organization and if internal audit is involved early in the intelligent automation was seen as a big challenge but also as a big advantage, if internal audit is involved early. However, internal audit's independent role needs to be ensured when conducting consultative activities. It was also concluded that opacity of intelligent systems as well as ways of monitoring them face challenge to internal audit.

Four main ways to tackle these challenges and stay relevant were identified from the interviews and the survey. Naturally, competences can be improved and maintained by training and if it is not possible or reasonable, competence gaps can be covered with different resourcing models. As said earlier, internal audits position and role can be challenge as well as advantage so responding to this challenge can be made by effecting internal audit's position as well as keeping up with competence requirements and practices to stay relevant to the organization. Use of data-analytics was found to be very relevant when talking of auditing intelligent systems. With data-analytics, internal audit can reach comprehensive conclusions and comprehensively evaluate intelligent automation despite of opacity of algorithms.

Keeping up with the competence requirements and being involved in the planning and implementation process are discussed in chapters 6.1 and 6.2. Resourcing models are discussed in chapter 6.3 and data-analytics in chapter 6.4. Conclusions are discussed in chapter 7.

6.1 Increasing competence requirements

Internal auditor's skill level and need to constantly update skills, whether they concern regulation, corporate responsibility, strategic planning, cyber security or technical skills was challenge common to all risk categories. Lack of transparency of algorithms, which was identified as a challenge from previous research and was also brought up by all the interviewees, demands quite high-level and specific technical skills from internal auditors. Challenges in keeping up with skill requirements was discussed with all interviewees and based on that observation, participants of the survey were also asked, what is the biggest challenge for internal audit in question 18. Options were competences, tools, resources and other. 27 of 30 participants answered competences. One participant answered tools and one answered resources. One participant answered option "other" and explained that he/she thought that lack of courage to audit new areas would be the biggest challenge. This answer can at least partly be linked to internal auditors' competences as well, as one's own skills usually play big part in taking on new challenges.

As discussed in chapter 3.2, in The IIA Global Internal Audit Competency Framework (IIA 2013b) internal auditors should continuously take or of their professional development and maintain up-to-date competencies required for effective internal audit delivery. There are many requirements to internal audit management to make sure that members of internal audit function have chances of professional development and possess needed competencies for effective audit delivery. If audit team does not possess needed competencies, it is more likely to audit risks to realize. Audit risks contains both, possibility that internal audit reaches to invalid or insufficient conclusions and gives faulty or insufficient advice to organization. As one interviewee stated: *"My view is that internal audit must have understanding and competencies in the audit subject, which poses a challenge especially in this intelligent automation, as it requires quite specific knowledge. However, internal audit planning should not be based on internal audit's competency limitations."*

One participant in the survey answered the biggest challenge for internal audit in auditing intelligent automation to be lack of courage to audit new areas. All the interviewees also thought that it is not appropriate that internal audit's only audits areas that they have the competencies to audit. One of the interviewees stated that *"Internal audit planning should be risk-based and not limited only to things that internal audit has competences to audit. Therefore, internal audit*

should acquire required competences to ensure risk-based approach in internal audit planning". Other interviewee was on the common ground and stated *"For internal audit to stay relevant, it should have enough understanding and technical skills. Basically, nothing should be off-limits as audit subject. Internal audit planning can't be based on function's competencies or it's purpose as value-adding function does not actualize".* Thus, if internal audit's scope is limited to things that it has competencies to audit, areas that should be audited considering its risks can be excluded from audit plan. However, because more complex business environment caused by new technologies, regulation, increasing competition and responsibility questions, skill requirements are impossible for one person to reach. One of the interviewees opened, how skill requirements have changed over time:

"I have been working with internal audit for 20 years and during that time, I have seen big change in internal auditors' competence requirements. 20 years ago, general knowledge and competences were expected from internal auditors on the principle, that skilled internal auditor can audit anything. Nowadays, so specific competencies are required that, for example, in this organization, internal audit has been divided to different groups that have specific competences within there area of responsibility. However, internal audit functions in Finland mostly consist one or two auditors and they can be experts in artificial intelligence or data-analytics only up to certain limit, as they must be able to audit everything else within the organization as well. Therefore, I think that they must constantly evaluate if new resourcing models are needed, especially to audit these new technologies."

Resourcing of internal audit will be discussed more in chapter 6.3. When interviewees were asked, what kind of new skills internal auditor needs when organization is adopting intelligent automation all interviewees answered that in addition to understanding, how intelligent automation works, internal audit should be competent in using data-analytics tools and keep up with cyber security, regulation and ethical discussion. However, technical skills and understanding of intelligent automation were seen biggest barriers. One interviewee talked about importance of technical skills as follows:

"Internal audit can probably find criteria which against it can evaluate for example responsibility matters. But if internal audit cannot truly understand what an intelligent system does, there is a risk that it will not get to the point where it can assess, what information is used and what it does and know how to assess its accuracy."

Especially auditing implementation of intelligent automation was seen challenging amongst the interviewees, because to fully understand the implementation process and help internal audit to understand how intelligent automation works and serves the process it is implemented in, internal audit should be involved in planning and implementation phase as well, still ensuring function's independency. Positioning of internal audit and its role is discussed more in the next chapter.

6.2 Internal audit's positioning in organizations and involvement in intelligent automation adoption

All the interviewees thought that internal audit's position in the organization and role in intelligent automation adoption process can be both, challenge and advantage. All interviewees thought that internal audit should be involved early, already in the planning phase when adopting intelligent automation or any other new technology, but internal audit's independency should be ensured. One interviewee stated: *"In addition to competences, internal audit's positioning in the organization can be big challenge to internal audit, when organization is adopting new technologies. If internal audit is seen only as back end assurance function and is not in concluded in the early stages of adoption, it can be difficult for internal audit to be relevant."*

Internal audit's positioning in the organization can vary between organizations. However, according to the interviews, early involvement would benefit organization to succeed in intelligent automation adoption and help internal audit do to assure that automation is implemented correctly and give more understanding to internal audit to assure that automation is working how it was supposed to. One interviewee brought up this perspective by saying that *"Internal audit can advise, from internal audit's point of view, from the start in a way that does not risk internal audit's independency. It can be relevant for internal audit's own understanding to be involved early so that internal audit's role is not just auditing the design but rather auditing the implementation as well."*

All the interviewees though that early involvement is important also because if internal audit is proactively part of the planning and implementation discussion, it can give its recommendations before implementation. If implementation is already done and internal audit's role is to assure

that it is implemented correctly and working as it was supposed to, it can be too late to make corrections that internal audit might recommend. One interviewee stated, that *"The earlier internal audit can be involved, the better. It is less reasonable to evaluate implementation afterwards when everything has already been done. Of course, it is a cultural question about how the organization is used to function. But absolutely internal audit should be involved at an early stage"*. However, it is important to take a notice that interviewees thought that internal audit's early involvement is important with all big IT-projects, not just with intelligent automation.

When participants of the survey were asked if they agree with statement "Internal audit should be involved earlier, even in designing phase, when organization is implementing intelligent automation" 27 out of 30 participants answered "agree" (4) or "strongly agree" (5) and only three participants answered, "don't agree or disagree" (3). Answers got average of 4,3 out of five, so also the survey results indicate that internal audit's early involvement is important when adopting intelligent automation.

Main objective in ERM is to achieve organization's strategic objectives, which also includes determining right risk appetite. (Fraser & Simkins 2010, 1) Managing intelligent automation is no different, and objectives and risk appetite need to be determined and clear from the beginning. Without clear understanding of objectives and risk appetite and tolerance, it is difficult to effectively to identify, evaluate, monitor and manage risks. Also controls must be designed as lack of adequate controls in automation might prevent organization to meet security, compliance and privacy requirements. (Goldman 2017) Planning adequate control environment was seen as an area where internal audit could be helpful in a consultative role by the interviewees.

The participants were also asked, what is the most relevant role of internal audit considering risks of intelligent automation. Options were assure, advise, anticipate and other. 18 answered assure, nine advise and three anticipate. Amongst the survey participants, maybe the most traditional role of internal audit, assure, is the most relevant one also when auditing intelligent automation. Three of the interviewees couldn't raise one role to be more important than another and one interviewee thought that assuring role is the most important one. However, all interviewees agreed, that advising role and anticipating role are especially important amongst assurance when organization is adopting new technology. Below are some quotations about internal audit's advising or anticipating roles from the interviews:

- *The involvement of internal audit is always an interesting question in the sense that the consulting role of internal audit is important in all IT projects. It is good for internal audit to play an independent consulting role in key development projects and also in artificial intelligence projects. Intelligent automation is no different.*
- *Intelligent automation is new area in organizations. Therefore, it would be ideal if internal audit could play a consultative role in implementation project already. However, all three roles are needed at some point.*
- *Whatever the new kind of investment or project is, the role of anticipating risks is important, as you need to know how to look ahead. You need to be able to look for potential new risks and not just look at what went wrong in the past. So, there is need to look further ahead. The consultative role is also important. For example, building a control environment is an area where consulting can be provided by internal audit. Anticipating and consultative roles will stand out more, when talking of new technologies.*
- *Proactive mindset helps identifying risks and I consider it very important. Consultative role and anticipatory role help internal audit add value to the organization.*

Based on the answers, it can be reasoned that traditional assurance role is still very relevant when auditing intelligent automation. However, when organizations are adopting new technologies, advising and anticipating roles stand out. All three roles are needed, and the earlier internal audit can be part of the technology adoption process, the better.

Like it is stated in the IIA's Professional Practices Framework and IIA's official definition, internal audit is independent and objective assurance and consulting activity. This means, that even if internal audit is involved in the planning and implementation in advising role, it should not be the one to make decisions. Internal audit should not be auditing their own work, or independency is not secured. One interviewee talked about independency: *"Internal audit should always consider what it can and can't do. It depends also on the area of which internal audit is consulting in. For example, control environment and compliance can be consulted. In principle, making recommendations is also consulting. After all, internal audit is not deciding, but recommending. However, internal audit must be careful not to be auditing their own work. Auditors must be able to draw the line and say no."*

When interviewees were asked about the Three lines of defense -model, which is being reviewed by IIA, all interviewees thought that it is important that roles of each line of defense are clear. All interviewees thought that especially with new technology projects, all three lines

of defense should understand the technology and possess technical skills, but also increase cooperation between lines. One interviewee brought up example of IT-department and internal audit figuring out together, how can the technology be audited. All the interviewees hoped that different lines would not work in silos but would add cooperation and centralize competences, especially when organization is adopting new technology or starting some other big projects. One interviewee wanted to emphasize the importance of still acknowledging the different roles and keeping them separate. Also, according to IIA's exposure document about three lines of defense (Carawan et al. 2019), one of the main criticisms towards the model is that "It suggests rigid structures and creates a tendency toward operational silos, which can be less efficient and effective".

However, it should be still ensured that roles are clear and internal audit's independency is ensured. One of the interviewees thought that *"Even if there are some development needs in how three lines of defense operate, I think it is important from governance point of view, that roles are still clear. If internal audit takes role where it is part of decision-making or approves activities, there is risk of independency being compromised. Another risk is that internal audit gets the role of developer and approver and responsibility taking in the first line reduces and decision-making responsibility is pushed to the third line. Independency should not be compromised, and conflicts of interest emerge. Internal audit should not audit its own work. The model of three lines of defense has offered back to internal audit's position. Changes are coming but they have to be made carefully".*

The survey also had open question: "Do you think that roles of three lines of defense change in managing the risks of intelligent automation or digital risks in general?" 16 participants answered to the question. Four participants answered that roles of the lines are not changing. Two participants answered blank and other had opinions on how roles change:

- *I think all the 3 lines must work seamlessly together in order to manage digital risks. The borders will blur between the roles of lines as technology will make more decisions on its own, for example.*
- *The third line is involved in the early stages to assure that risks are considered in the planning phase. So, boarders of the lines blur.*
- *Consultative role of internal audit is important so in a way third line will be involved in first and second lines' "tasks".*

These three answers are linked to need for more cooperation of the lines, which was identified from the interviews as well. There were also other views. One participant thought that advise and anticipate roles will increase in second and third line and continuous monitoring utilizing RPA or other intelligent solutions increases especially within second line of defense. Other participant thought that "*somehow intelligent automation will replace the first line of defense, and the controlling role of the second line will be more important"*. One participant answered that the lines must adapt to the changing environment. One answer brought quite unique perspective compared to other answers: *"1LoD has business incentives and don't actually care about controls. Need to deliver uber-cool things faster and faster. 2LoD is lagging more and more behind as they don't typically have enough resources. 3LoD can shelter themselves by auditing non-existence of controls and strategy etc."*

Three answers confirmed findings from the interviews but there were also many individual views. Therefore, there is no adequate reasoning to make conclusions about the answers that were not related to increasing cooperation. Although most of the participants who answered to the question thought that there is change occurring when managing risks of intelligent automation or digital risks in general, it might be that participants who did not answer the question thought that the roles are not changing.

6.3 Changing resourcing models

As discussed in chapter 6.1 about changing competence requirements of internal auditors, all interviewees thought that planning internal audit should be risk-based and basically nothing should be off limits as an audit area due to internal audit's competence limitations. However, interviewees also thought that internal audit should have adequate competences around the audit subject to reach valid conclusions and provide sufficient and valid recommendations. Interviewees brought up that in Finland internal audit function often consists one or two persons. One interviewee explained: *"In Finland, most of the internal audit organizations consist one or two persons and they only have possibility to be data-analytics experts or artificial intelligence experts up to certain limit, as they have to be able to audit everything else too in the organization. Therefore, using different resourcing models, like guest auditors, co-*

sourcing and outsourcing will increase. Also, larger internal audit organizations constantly have to consider if they need external help with something."

All interviewees agreed that especially small internal audit organizations can't keep up with all new competence requirements that new technologies set. And its not only technical skills but also new kind of knowledge about regulation and responsibility, for example. One interviewee thought that *"In general, I believe that maintaining competence is difficult, especially in small internal audit organizations. Expertise in special areas is required and internal audit has to partner up. Gaining insight from within the organization or elsewhere will become more common. Different resourcing models are sure to vary as more and more different skill combinations are needed"*

One interviewee explained more about challenges with maintaining competence. First, it is impossible to have profound knowledge about every area or technology in the organization, even if there was no time or other resource limitations. But if organization has two internal auditors, who also must follow the audit plan and make sure that all audits are conducted carefully, it can be difficult to find time to training. For example, profound understanding of artificial intelligence is not gained with one training session. In addition to time limitations, there are also budget limitations.

Guest auditing means allowing personnel from inside the organization to assist in audit as a subject matter resource. Guest auditors usually are used in the short term, for example, to assist with one project. (Ernst & Young 2013,11) All interviewees thought that insight from within the organization can be very useful and cost efficient. However, two interviewees also brought up that there are some aspects to consider before using guest auditors from within the organization, as independency can not be compromised. If guest auditor is too close to the subject, it might not be reasonable to use guest auditors or internal auditor should monitor the work very closely. One interviewee brought up that personnel inside the organization could provide insight to internal audit as a consultative resource as well.

Interviewees thought that with new technologies requiring quite specific competences and because businesses are changing rapidly, internal audit needs to be flexible to adapt to new situation and constantly evaluate, if help outside the internal audit is needed, in-house or external. This can lead to resourcing models varying lot between different projects. Three of the interviewees brought up that with intelligent systems, some sort of co-sourcing models are probably best solution if internal audit does not have required expertise in the internal audit

organization. In this way, internal audit can utilize in-house insight about processes and culture and get more specific expertise of the technology or for example artificial intelligence ethics from outside the organization.

The survey participants were asked if the agree or disagree with statement "Outsourcing internal audit will increase when auditing intelligent automation". Answers were quite evenly divided to each option. Participants were asked to rank their agreement level from 1 (strongly disagree) to 5 (strongly agree) and answers got average of 3,03, so any conclusions about this statement according to the survey can not be made. To get better confirmation to the interview results, participants should had been asked what they think about increasing of co-sourcing or guest auditing, as participants could have understood the statement about outsourcing as outsourcing the whole internal audit.

6.4 Increasing use of data-analytics

Data analytics is process containing collecting, cleaning, transforming and analyzing data using data mining and statistical modeling (Batarseh & Gonzales 2018, 52, according to Richmond 2006). With data-analytics internal audit can use data mining techniques and procedures to reveal relationships, trends, or patterns by analyzing data. Internal audit can process information that would be much more difficult to discern by reading documentation and process presentations. By conducting analyses, internal audit can determine probabilities, for example, probability of fraud and further investigate irregularities. Big fundamental change is that internal audit could test even 100% of activities, rather than using sampling. Naturally, this means greater probability to identify errors, inefficiencies and noncompliance than sample testing. (Tang, Norman & Vendrzyk 2017, 1126-1128)

All the interviewees thought that data-analytics could be helpful, or even necessary, for internal audit to comprehensively audit intelligent automation. When asked, how internal audit can assure that intelligent automation is working from the input data to results, one interviewee answered, that *"With data-analytics, it is possible to go through the whole data in a different way. If you think about the speed at which artificial intelligence produces data, then analytics has the power to process it and find possible deviations".* Other interviewee answered: "*By*

going into the data and utilizing tools to study the functionality of the model and the output data. Analytics must be utilized; the implementation must be tested in practice. Has the automation produced comprehensive and correct results and how is the information described, i.e. is there sufficient transparency and documentation?"

One interviewee thought that important benefit of data-analytics is that larger entities can be tested. Because intelligent systems produce and use data so rapidly, adequately assuring that data does not have errors and artificial intelligence operates how it was supposed to, number of samples tested should be very big and resource consuming and still would not provide results near as trustworthy and comprehensive than data-analytics.

One of the interviewees told, that data-analytics are a focus-area in their internal audit organization and auditors' analytics competences are maintained by regular trainings. One of the interviewees thought that especially in small internal audit organizations, it is important to keep up with trends and maintain one's competences by networking, exchanging thoughts and participating in trainings provided by IIA.

Also survey participants were asked if they agree or disagree with statement "To assure that intelligent automation works from source data to results, internal audit has to use data-analytics". 26 of 30 participants answered that they strongly agree (5) or agree (4). Four participants answered that they don't agree or disagree (3). Scale was from 1 to 5 and this statement got average of 4,4. Conclusion that survey participants agreed with interviewees on that analytical tools should be in use when auditing intelligent automation can be made based on this result.

Survey participants were also asked, how do they see internal audit practices changing when auditing intelligent automation. 22 participants answered to the open question. 11 answers were related to increasing use of data-analytics, three answers said that practices are not changing, and rest of the answers concerned increasing competence requirements, especially technical skills and strategy planning, and increasing importance of consultative role of internal audit, giving support to the earlier findings made in the thesis about competence challenges and internal audit's position and role.

7 CONCLUSIONS

Conclusions of the results are presented in this chapter of the thesis. Firstly, conclusions are presented and then discussed in more detail answering to the research questions. The research questions were:

1. What are the key risks of intelligent automation?

2. What challenges internal audit faces due to risks of intelligent automation?

3. How can internal audit meet the challenges caused by risks of intelligent automation and stay relevant?

The key risks of intelligent automation identified from the research material are technology risks, cyber risks, risks related to design and implementation, risks related to strategy and people related risks. There were no specific number of risks defined in the research question, but these 5 risk categories were distinctly the most relevant ones based on the collected research material.

The biggest challenge for internal audit is lack of competences. Difficulties to keep up with competence requirements were identified especially with technical skills, regulation and cooperate responsibility issues. Second challenge identified is internal audit's position and role in intelligent automation adoption. If intelligent automation is not involved in the early phases of adoption process, making sufficient conclusions and giving valid recommendations is challenging. Third challenge is lack of transparency of intelligent systems. Fourth challenge is that ways of monitoring intelligent automation lack behind technology adoption, which is partly caused by lack of competences as well but also by lack of applicable tools.

Five ways to response to the challenges were identified. Internal audit should fill its competence gaps by training and constantly evaluating the most suitable resourcing options. Using variety of resourcing models is likely to increase especially in small internal audit organizations. Internal audit should also try to reach a position, where it can be in consultative role from the beginning of intelligent automation adoption process, but still remain its independency. In addition, internal audit should enhance its data-analytics capabilities and use them when auditing intelligent automation. The key findings are presented in Figure 6.

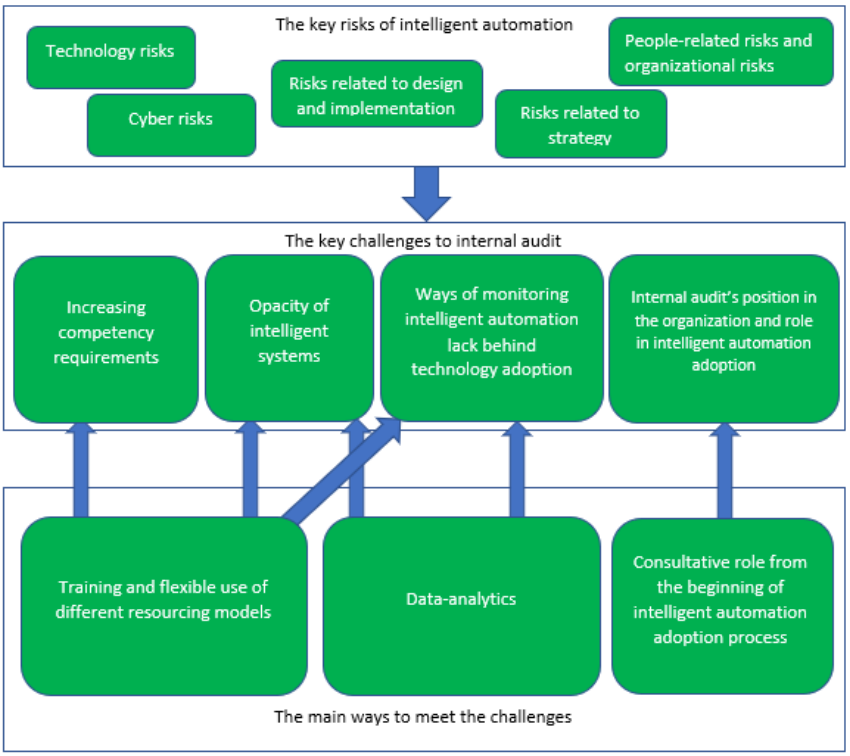

Figure 6 The key findings

7.1 The most relevant risks of intelligent automation

According to the interviews and survey conducted, all risk categories that were identified from previous research are relevant. When survey participants were asked to rank risk categories relevance from 1 to 5, all categories got average over three. However, based on interviewee statements and questions about risks' relevance in the survey, five most relevant risk categories were identified and individual risks within each category. Below is illustrated how answers were divided in each category in question eight. Risks are sorted from the biggest average to the lowest.

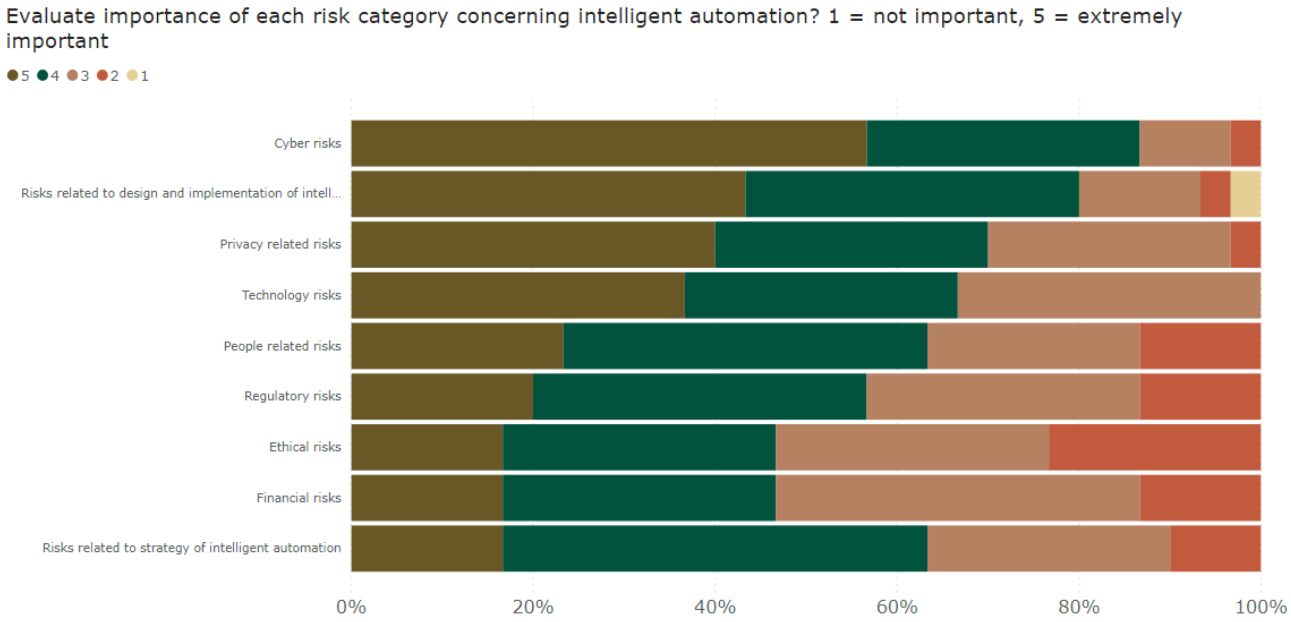

Figure 7 Answers to question 8

As can be seen from the graph, all risk categories were ranked quite high and only one category "risks related to design and implementation of intelligent automation got one answer with the lowest ranking. Each average is shown in table 1.

Table 1 Relevance averages of risk categories

Risks	Average
Cyber risks	4,40
Risks related to design and implementation of intelligent automation	4,13
Privacy related risks	4,06
Technology risks	4,03
People related risks	3,73
Risks related to strategy of intelligent automation	3,70
Regulatory risks	3,63
Financial risks	3,50
Ethical risks	3,40

Based on this question, the most relevant categories are cyber risks, risks related to design and implementation of intelligent automation, privacy related risks and technology risks, which all got average over 4. In question nine, where participants were asked to choose only one category, which they thought was the most relevant one. The most answers were given to technology risks and second was cyber risks. In third place were people related risks, risks related to design and implementation and risks related to strategy and of intelligent automation.

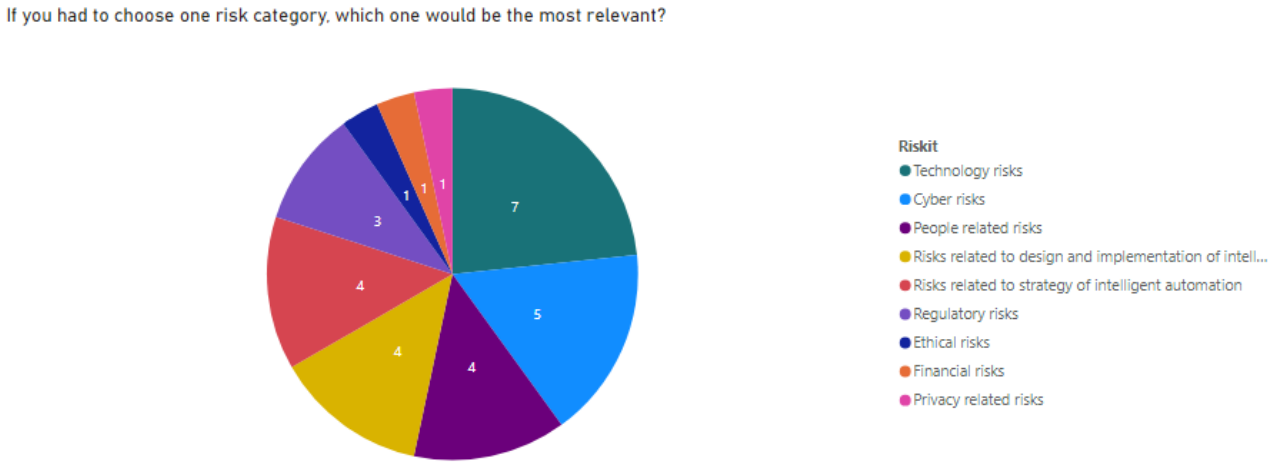

Figure 8 Distribution of answers to question 9

Results from question eight differ a bit from question nine, where participants were asked to evaluate relevance of each category, as privacy related risks was answered only by one participant. However, privacy related risks overlap in many ways with cyber risks. Risks related to strategy of intelligent automation got as many answers as ones related to design and implementation of intelligent automation and people related risks.

Interviewees considered all categories relevant, but some categories were more emphasized and individual important risks brought up from technology risks, cyber risks, people related risks and risks related to strategy and implementation. As discussed in previous chapters of this main chapter, interviewees brought up especially lack of transparency of intelligent automation decision-making, lack of competences, both using the technology and planning and implementing it, reliance on algorithms and more severe and probable cyber threats as intelligent automation can process very big amounts of data. Lack of competence and difficulties to find competent workforce can be categorized as people related risks and risks related to strategic planning and implementation. Also, if results from survey questions are converted to comparative figures where average from question eight are added to amount of answers in question 9, technology risks, cyber risks, risks related to design and implementation, risks related to strategy and people related risks have distinctly higher comparative figure than other risks.

Table 2 Comparative figures of risk categories according to relevance

Risks	Comparative figure
Technology risks	11,03
Cyber risks	9,13
Risks related to design and implementation of intelligent automation	8,13
People related risks	7,73
Risks related to strategy of intelligent automation	7,70
Privacy related risks	5,06
Regulatory risks	4,63
Financial risks	4,50
Ethical risks	4,40

7.2 Challenges to internal audit caused by intelligent automation

The second research problem was to find out, what kind of challenges is internal audit facing due to risks that intelligent automation causes to organizations. Challenges in auditing intelligent automation can lead to audit risks, which means that internal audit could not make valid and adequate conclusions and give valid recommendations to organizations. Four main challenges were identified based on research material: difficulties in keeping up with competence requirements, opacity of intelligent systems, methods for monitoring intelligent automation lack behind technology adoption and internal audit's position and role in intelligent automation adoption.

Interviewees and survey results indicate that the biggest challenge for internal audit is keeping up with competences, which are required when organization is using intelligent automation. Interviewees brought up technical skills, understanding about technology and how it serves the organization and knowledge about regulation and responsibility. Interviewees thought that complexity and opacity of algorithmic decision-making make understanding intelligent automation more difficult and therefore quite specific competence is required.

Challenges posed by competence requirements and lack of transparency in algorithmic decision-making was confirmed in the survey. In question 17, 90% of the participants thought that competence is the biggest challenge for internal audit when auditing intelligent automation. In question 13, participants were asked to choose one challenge that is the most relevant one in their opinion. Distribution of the answers can be seen from figure 8. Options were identified from the interviews conducted and previous research and participants were also able to suggest other options. The three options that got most answers were opacity of

intelligent systems, short of competent workforce and methods for monitoring intelligent automation lack behind technology adoption. Opacity of intelligent systems and methods for monitoring intelligent automation are partly linked to competence requirements but also to tools that are available for internal audit, like data-analytics.

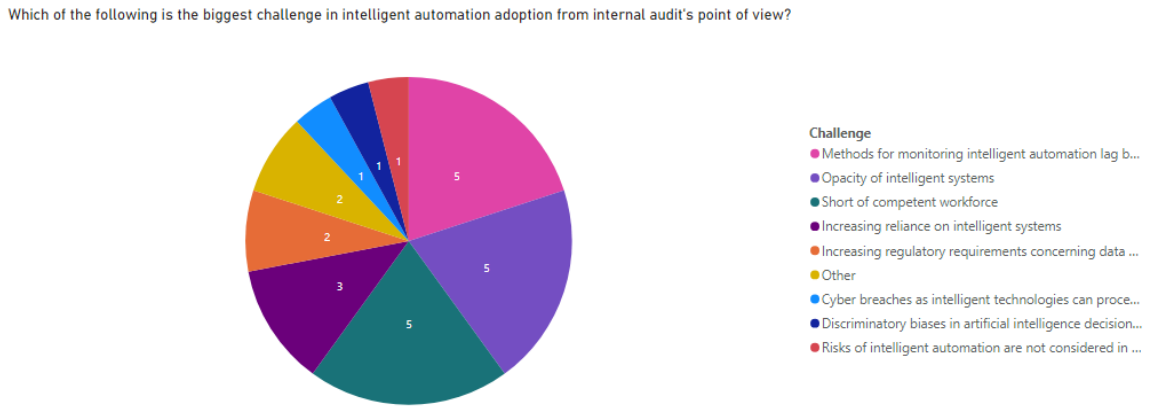

Figure 9 Distribution of answers to question 13

In addition to the biggest challenges identified from the survey, interviewees thought that internal audits position and role can also be a challenge. Interviewees thought that consulting and anticipating role of internal audit are important when organization is adopting new technology. If internal audit is not involved in planning and implementation process, internal audit's perspective can be external causing difficulties in auditing technology implementation. Therefore, internal audit's involvement makes internal audit's work more efficient in addition of helping the organization. Internal audit's early involvement gives internal audit change to give recommendations before technology is implemented, which is much more efficient than giving recommendations after all the work is done.

7.3 Internal audit's response to the challenges

The third research question was "Firstly, training and education is important to meet competence requirements and maintaining competence. Two of the interviewees also brought up that internal auditors should also constantly find ways for professional development also independently by networking and attending trainings and seminars outside their organization.

If internal audit organization is small, for example, consisting one or two auditors, it is difficult to be experts in intelligent automation and data-analytics in addition to all other skills that are required from internal auditors in that organization. Then organizations need to find the best resourcing solution. Interviewees thought that organizations should be flexible to find solutions and constantly estimate, what would be the best option. Interviewees thought that organizations will use larger scale of variations, as new technologies can require quite specific skills. Especially guest auditor activities and co-sourcing were found as good options by the interviewees.

All the interviewees thought that using data-analytics to assure that intelligent automation is working from input data to results, is at least very useful if not necessary. Participants of the survey agreed with the interviewees as 27 of 30 participants answered that they agree or strongly agree with statement "To assure that intelligent automation works from source data to results, internal audit has to use analytical tools". The left three participants did not agree or disagree with the statements. Auditing with data-analytics is more efficient and it enables to process the whole data, which makes finding irregularities and errors more efficient than, for example, sampling.

Interviewees thought that to sufficiently understand intelligent automation and audit its implementation, internal audit should be involved early in the adoption process. If internal audit is only in a role of back end assurer, providing added value to the organization is harder than if internal audit would have been involved from the beginning. Interviewees thought that internal audit should be involved early in consultative role, but decision-making responsibilities should not be pushed to the third line, to ensure internal audit's independency. Survey participants agreed, as 27 of 30 participants answered to agree or strongly agree with statement "Internal audit should be involved earlier, even in the planning phase, when organization is adopting intelligent automation".

7.4 Evaluating the research

The research can be considered as successful. Answers to all research questions were found. Reasoning behind all answers is comprehensive and strongly based to the research material. Mixed-methods research was suitable research method for this research to have deep qualitative insight to the research matter but also quantitative confirmation.

The interviews were successful, as all interviewees had long experience from internal audit and had lot to say about the subject. The interviewees had very similar answers to the interview questions and brought up lot of similar thoughts outside the research questions. Therefore, credible results were gained from the interviews. It must be noticed that results can not be generalized to all organizations as only three organizations and IIA were presented. However, all interviewees have had long careers and had insight from industries that they are not currently working in as well.

Quantitative confirmation was gained from the survey, as well as deeper insight, as participants answered to the open questions quite comprehensively. However, the survey had 30 participants, which is not enough to make any statistical conclusions. More participants would have added reliability and weight to the results. However, the target group is not that big and research subject very fresh, so the final amount of answers was satisfactory. With research material of this size, the results of the survey can be considered as directional. Although, more confirmation to the results can be found from previous research. Attention must be paid also to the fact that 13 of 30 participants in the survey had worked with internal audit five years or less.

7.5 Ideas for further research

Objective of this research was to find out, what are the key risks of intelligent automation and how they affect internal audit. As the third research questions was “How can internal audit meet the challenges caused by risks of intelligent automation and stay relevant” data-analytics were discussed in a general level. Objective was not to find out specific methods of data-analytics, which internal audit could use. This could be subject for further research, to research on a deeper level, how internal audit can use data-analytics when auditing intelligent automation or artificial intelligence in general. There is already lot of research about data-analytics in internal audit, but not much about auditing intelligent systems using data-analytics. Other possible research subject could be, how internal audit can use intelligent automation or artificial intelligence in their own operations.

REFERENCES

Scientific sources:

Adams, William. 2015. Conducting semi-structured interviews. In: Newcomer, Kathryn, Hatry, Harry & Wholey, Jospeh. Handbook of practical program evaluation. Fourth edition. New York: John Wiley and Sons Inc.

Bailey, James. 2010. The IIA's Global Internal Audit Survey: Core Competencies for Today's Internal Auditor. Report II. Institute of Internal Auditors (IIA)

Băjenescu, Titu-Marius I. 2018. The risks of artificial intelligence. In Journal of Engineering Science (Chişinău) XXV.4 (2018): 47-56.

Batarseh, Feras & Gonzales, Avelino. 2018. Predicting failures in agile software development through data analytics. In Software Quality Journal. Volume 26, issue 1. Pages 49-66

Christofferson, Scott, Murray Michael, Kaiser, Emily, McKnight Leslee & Go, Rafael. 2018. 2019 Audit Plan Hotspots. Gartner.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 2017. Enterprise Risk Management- Integrating with Strategy and Performance Executive Summary.

Crouhy, Michel, Galai, Dan, & Mark, Robert. 2013. The Essentials of Risk Management. 2nd ed. McGraw Hill.

Datta, Anupam, Sen, Shayak & Zick, Yair. 2016. Algorithmic Transparency via Quantitative Input Influence: Theory and Experiments with Learning Systems. Carnegie Mellon University, Pittsburgh, USA.

Dedeo, Simon. 2015. Wrong Side of the Tracks: Big Data and Protected Categories, Ithaca, N.Y.: Cornell University Library.

Erikson, Päivi & Kovalainen, Anne. 2011. Qualitative research materials. London: SAGE Publications Ltd

Fraser, John & Simkins, Betty. 2010. Enterprise Risk Management. 1st edition. Wiley.

Garawan, Mark, Grocholski, John, Jenitha, Greg, Sorlie, Trygve, Urban, Shannon, Wong, Beili & Wright, Charlie. IIA Exposure document – Three Lines of Defense. The Institute of internal auditors (IIA).

Gomory, Ralph. 1995. The Known, the Unknown and the Unknowable. Scientific American

Haight, Joel & Caringi, Ralph. 2007. Automation vs. human intervention: What is the best mix for optimum system performance? A case study. In International Journal of Risk Assessment and Management. 7:5, 708-721.

Hansson, Sven. 2010. Risk: objective or subjective, facts or values. In: Journal of Risk Research. 13:2, 231–238.

Ilmonen, Ilkka. 2013. Johda riskejä: Käytännön opas yrityksen riskienhallintaan. Helsinki: Finanssi- ja vakuutuskustannus Finva.

Institute of Internal Auditors (IIA). 2016. International standards for the professional practice of internal auditing.

Institute of Internal Auditors (IIA). 2013a. The three lines of defense in effective risk management and control.

Institute of Internal Auditors (IIA). 2013b. he IIA Global Internal Audit Competency Framework.

ISO. 2018. ISO 31000:2018 Risk management — Guidelines. The International Organization for Standardization (ISO).

Jaksic, Marko & Marinc, Matej. 2019. Relationship banking and information technology: the role of artificial intelligence and FinTech. In Risk Management -journal. Vol 21, 1-18. Macmillan Publishers Ltd.

Juvonen, Marko, Koskensyrjä, Mikko, Kuhanen, Leena, Ojala, Virva, Pentti, Anne, Porvari, Paavo & Talala Tero. 2014. Yrityksen Riskienhallinta. Helsinki: Finanssi ja vakuutuskustannus FINVA.

Kananen, Heidi & Puolitaival, Harri. 2019. Tekoäly: bisneksen uudet työkalut. Helsinki: Alma Talent Oy

Kogan, Nathan., & Wallach, Michael. 1964. Risk taking: A study in cognition and personality. Holt, Rinehart & Winston.

Laurent, Patrick, Chollet Thibault & Herzberg Elsa. 2015. Intelligent automation entering the business world.

Lehto, Martti. 2017. Tekoäly ja kyberturvallisuus. In: Futura 36 : 2, 6-14.

Nicholson, F. 2019. Three lines of defense: report on the public exposure findings June-September 2019. Institute of Internal Auditors (IIA).

Niemi, Paula. 2018. Sisäinen tarkastus käytännössä. Helsinki: Alma Talent.

Ollila, Maija-Riitta. 2019. Tekoälyn etiikkaa. Otava.

Online Trust Alliance (OTA). 2018. Cyber Incident & Breach Trends Report - Review and analysis of 2017 cyber incidents, trends and key issues to address. The Internet Society (ISOC).

Osoba, Osonde & Welser, William. 2017. An Intelligence in Our Image: The Risks of Bias and Errors in Artificial Intelligence. Rand Corporation.

Parnas, David. 2017. The Real Risks of Artificial Intelligence. Communications of the ACM. 60:10, 27–31.

Petrasic, Kevin, Saul, Benjamin, Bomfreund, Matthew & Katherine Lamberth. 2017. Algorithms and bias: What lenders need to know. White & Case LLP.

Rantala, Jukka & Kivisaari, Esko. 2014. Vakuutusoppi. Turenki: Finva.

Richmond, Brian. 2006. Introduction to data analytics handbook . Migrant and Seasonal Head Start Technical Assistance Center, Academy for Educational Development.

Sandvig, Christian, Kevin Hamilton, Karrie Karahalios, and Cedric Langbort. 2014. Auditing Algorithms: Research Methods for Detecting Discrimination on Internet Platforms. Paper presented to the Data and Discrimination: Converting Critical Concerns into Productive Inquiry preconference of the 64th Annual Meeting of the International Communication Association, Seattle, Wash.

Sartonen Miika, Huhtinen Aki-Mauri, Lehto Martti. 2016. Rhizomatic Target Audiences of the Cyber Domain. The Journal of Information Warfare, Vol 15, Issue 4, Fall 2016.

Schubert, Renate. 2006. Managerial Finance. In: Krause Andreas (editor). Risk Management. 31:9, 706-715.

SFS. 2019. Riskit hallintaan –SFS-ISO 31000. Helsinki: Suomen Standardisoimisliitto SFS ry.

Tang, Fengchun, Norman Strand, Carolyn & Vendrzyk, Valaria. 2017. Exploring perceptions of data analytics in the internal audit function. In Behaviour and Information Technology - journal. 36:11, 1125-1136

Walle, Alf H. 2015. Qualitative research in business: A practical overview. Newcastle upon Tyne: Cambridge Scholars Publishing.

Zuiderveen Borgesius, Frederik. 2018. Discrimination, artificial intelligence, and algorithmic decision-making. Strasbourg: Council of Europe, Directorate General of Democracy.

Professional sources:

Albinson, Nancy, Thomas, Cherian, Rohrig, Michael & Chu, Yang. 2019. Future of risk in the digital era. Deloitte.

Ernst & Young. 2013. Matching Internal Audit talent to organizational needs – Key Findings from the Global Internal Audit Survey 2013. Ernst & Young.

Hatherell, Terry. 2018. Foreword. In Forging Internal Audit's path to greater impact and influence - Deloitte's 2018 Global Chief Audit Executive research survey. Deloitte.

Joseph, Adrian. 2018. Robotics and intelligent automation - Combining the power of human and machine. Ernst & Young.

Patel, Paresh P. 2018. Compelling Benefits, Common Misconceptions – Putting intelligent automation to work for federal. Accenture Federal Services.

Powers, Ed, Saif, Ifran, Mossburg, Emily, Amjad, Adnan, Norton, Kieran, Katyal, Vic, Morrison, Andrew, Kunchala, Vikram & Wyatt, Mike. 2019. The future of cyber survey 2019. Deloitte

Watson, Justin, Hatfield, Steven, Wright, David, Howard, Matthew, Witherick, Dupe, Coe, Lauren & Horton, Richard. 2018. Automation with intelligence - Reimagining the organization in the 'Age of With'. Deloitte Insights.

Web-sources:

Angwin, Julia, Larson, Jeff, Mattu, Surya & Kirchner, Lauren. 2018. Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica. Viewed 30.3.2020
https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Chartered Institute of Internal Auditors. 2019. Governance of risk: Three lines of defence.
https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/

Goldman, Sharon. 2017. The Role of Risk Management and Governance in Intelligent Automation. CIO form IDG. Viewed 9.4.2020.
https://www.cio.com/article/3242246/the-role-of-risk-management-and-governance-in-intelligent-automation.html

IRPAAI. 2018. What is robotic process automation? Viewed 22.1.2020.
https://irpaai.com/what-is-robotic-process-automation/

IIA. What is Internal audit?. Viewed 29.1.2020.
https://www.iia.org.uk/about-us/what-is-internal-audit/

IIA North America. Standards & Guidance — International Professional Practices Framework (IPPF). Viewed 28.1.2020.
https://na.theiia.org/standards-guidance/Pages/Standards-and-Guidance-IPPF.aspx

IIA Australia. Professional Guidance. Viewed 5.2.2020
https://www.iia.org.au/technical-resources/professionalGuidance/introduction

ISO. ISO 31000:2018 Risk management – Principles and Guidelines Viewed 5.2.2020.
https://committee.iso.org/sites/tc262/home/projects/published/iso-31000-2018-risk-management.html

Jyväskylä University. 2015. Monimenetelmäisyys. Viewed 7.2.2020.
https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/moni menetelmaisyys

Lee, Peter. 2016. Learning from Tay's introduction. Blog, Microsoft website. Viewed 19.3.2020.
https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/#sm.0001v8vtz3qddejwq702cv2annzcz

Morgan, Steve. 2017. Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021. CSO, Cybersecurity business report. Viewed 29.3.2020.

https://www.csoonline.com/article/3200024/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html

Legislative sources

European Convention on Human Rights. Council of Europe. 1950.

Regulation of the European Parliament and of the Council. (EU) 2016/679.

ATTACHMENT 1 LISTS OF FIGURES AND CHARTS

Figures

Tables

ATTACHMENT 2 INTERVIEW QUESTIONS

1. What risks of intelligent automation has your organization identified?
2. Are risks of intelligent automation considered sufficiently as a part of risk identification process?
3. Are risks of intelligent automation taken to account in internal audit planning?
4. Have your organization identified risks from the following categories? Do any relevant individual risks of intelligent automation come to your mind?
   - Technology
   - Cyber
   - Ethical
   - Privacy
   - Regulation
   - People and organization
   - Risks related to strategy of intelligent automation
   - Risks related to planning and implementation of intelligent automation
5. What kind of risks are most relevant ones from internal audit's point of view? Why?
6. How do you see internal audit's role or position change because organization is adopting intelligent automation from the following perspectives?
   - Traditionally, it has been thought that internal audit can have many roles, the most traditional one being assurance, the other advisory role and the most recent frameworks also include a risk anticipating role. How do you see these roles changing when auditing intelligent automation?
   - How do you see the role of internal audit in the strategy, design and implementation of intelligent automation?
   - Do you think that the roles of different lines of defense are changing when managing risks of intelligent automation or digital risks in general?
7. How do you see the internal audit practices changing when auditing intelligent automation?
   - How would the use of analytics could support the auditing intelligent automation in particular?
   - How can internal audit assure the functionality of automation from input data to decision making?

- How does internal audit ensure that the system is susceptible to interference, i.e. not all information entered it is assumed to be correct?

8. What concrete internal audit is planned to do in your organization this year regarding intelligent automation?
9. What are the biggest challenges for internal audit in auditing intelligent automation?

ATTACHMENT 3 SURVEY QUESTIONS

Part 1

1. How long have you been working with internal audit?

1) Under 5 years
2) 10 to 15 years
3) 15 to 20 years
4) over 20 years

2. Is intelligent automation used in your organization or in organization which you are auditing?

1) Yes
2) No

If answer is “Yes” participant continues to part 2. If answer is “No” participant continues to part 3.

Part 2

3. Have risks of intelligent automation been addressed as part of the risk identification process in your organization or in organization which you are auditing?

1) Yes
2) No

4. Are the risks of intelligent automation considered in internal audit planning in your organization or in organization which you are auditing?

1) Yes
2) No

5. Have your organization or organization which you are auditing considered intelligent automation related risks from which of these categories?

- Technology risks
- People related risks
- Cyber risks
- Ethical risks
- Regulatory risks
- Financial risks
- Risk related to strategy of intelligent automation
- Risks related to design and implementation of intelligent automation
- Privacy related risks

6. What intelligent automation related risks are the most relevant to your organization or organization which you are auditing?
7. What concrete internal audit has planned to do in your organization or organization which you are auditing this year in relation to intelligent automation?

Part 3

8. Evaluate importance of each risk category concerning intelligent automation? 1 = not important, 5 = extremely important.

- Technology risks
- People related risks
- Cyber risks
- Ethical risks
- Regulatory risks
- Financial risks
- Risk related to strategy of intelligent automation
- Risks related to design and implementation of intelligent automation
- Privacy related risks

9. If you had to choose one category, which would be the most relevant?

1) Technology risks
2) People related risks
3) Cyber risks

4) Ethical risks
5) Regulatory risks
6) Financial risks
7) Risk related to strategy of intelligent automation
8) Risks related to design and implementation of intelligent automation
9) Privacy related risks

10. Do you consider some specific risks from previous categories or other areas very relevant? What are them?
11. Do you think that previous categories cover all risks of intelligent automation or is some category missing?
    1) Yes
    2) No
12. If you answered "no" to previous question, what category is missing?
13. Which of the following is the biggest challenge in intelligent automation adoption from internal audit's point of view?
    1) Increasing reliance on intelligent systems
    2) Short of competent workforce
    3) Methods for monitoring intelligent automation lag behind technology adoption
    4) Opacity of intelligent systems
    5) Cyber breaches as intelligent technologies can process significant amounts of data and create new access points
    6) Risks of intelligent automation are not considered in designing phase
    7) Discriminatory biases in artificial intelligence decision-making
    8) Other
14. If you answered "other" to the previous question, what is the biggest challenge in intelligent automation adoption from internal audit's point of view?
15. Which of following roles of internal audit is the most relevant considering risks of intelligent automation?
    1) Assure
    2) Advise
    3) Anticipate
16. If you answered "other" to the previous question, what is another relevant role?

17. How much do you agree with following statements, 1=strongly disagree, 2=disagree, 3=don't agree or disagree, 4=agree 5=strongly agree?
    - Consulting role of internal audit will be more important when auditing intelligent automation
    - Internal audit should be involved earlier, even in the planning phase, when organization is adopting intelligent automation
    - Internal audit's relevance decreases when organization is adopting intelligent automation
    - To assure that intelligent automation works from source data to results, internal audit must use analytical tools
    - Outsourcing internal audit will increase because organizations are adopting intelligent automation
18. What is the biggest challenge for internal audit when auditing intelligent automation?
19. If you answered "other" to previous question, what is the biggest challenge for internal audit when auditing intelligent automation?
20. Three lines of defense: Do you think that the roles of three lines of defense change in managing the risks of intelligent automation or digital risks in general? How?
21. How do you see internal audit practices changing when auditing intelligent automation?
22. How can internal audit ensure that automation works from source data to results?