Business, Management and Education

ISSN 2029-7491 / eISSN 2029-6169

2018 Volume 16 Issue 1: 81–93

https://doi.org/10.3846/bme.2018.2142

# THE INCREASING ROLE OF IT AUDITORS IN FINANCIAL AUDIT: RISKS AND INTELLIGENT ANSWERS

Gergő BARTA*

*Szent István University, Doctoral School of Management and Business Administration, Páter Károly str. 1., 2100 Gödöllő, Hungary*

Received 29 May 2018; accepted 09 June 2018

**Abstract.** Financial auditing cannot be imagined without the involvement of IT specialists since business processes are designed to be served by IT components such as ERP systems, online customer-facing applications, databases etc. Financial auditors therefore exposed to IT system and control reliance want to gain reasonable assurance that data and transactions stored in IT systems cannot be modified, access is controlled, and there is no suspicion of any fraud at business organizations. The paper tries to understand the current situation of IT audit involvement in financial auditing, interpret risks that parties face and provide some solutions by use of intelligent applications.

**Keywords:** financial audit, IT audit, IT controls, IT threats, risk management, machine learning.

**JEL Classification:** M42.

## Introduction

Financial auditors want to make sure that relevant IT systems in the scope containing sensitive financial information support their work, however, the increasing number of cybercrime activities and IT systems with lack of appropriate controls makes the audit process more difficult, emerging the question how much they can rely on the system. If the answer is no, then financial auditors must perform substantive testing and examine much more documents what results in ineffective audit work, and Chief level executives are initiating awkward discussions why the audit took more time and why it costs more.

As defined by IFAC (International Federation of Accountants "*the purpose of an audit (financial audit) is to enhance the degree of confidence of intended users in the financial statements.*" (IFAC, 2009). The role of financial auditors is, therefore, to perform procedures in alignment with predefined criteria to provide an opinion whether the financial statement of the audited organization is presented fairly. These predefined criteria are based on international accounting standards such as the IFRS (International Financial Reporting Standards),

*Corresponding author. E-mail: *barta.gergo@phd.uni-szie.hu*

US GAAP (the United States Generally Accepted Accounting Principles), HAS (Hungarian Accounting Standards) etc. Financial auditors, as a basis, express the audit opinion to obtain reasonable assurance, not an absolute assurance, which indicates that the goal is not to achieve total certainty, but a high-level confidence that financial statements are not materially misstated (ISACA, 2004). There are many reasons why absolute assurance cannot be provided. One of them is that it is impossible to detect each and every human error as it would require the financial auditors to inspect every transaction, invoice, bank statement, etc. That demands a huge amount of time and resources, thus raises the question of efficiency. Financial auditors use sampling techniques to select and observe audit evidence based on statistical and other criteria, hence there is a chance that there might be some errors that can go undetected. That is the reason why "materiality" is introduced into the world of financial auditing. Materiality is a concept indicating the significance of a transaction. Misstatements can be material if they could influence the economic decisions of users, taken on the basis of the financial statements (IFAC, 2009). The audit report issued by the audit firm expressing the opinion on financial statement has a high impact on the operation of an organization. The audit report can be used for the purpose of attracting external investors, obtaining credit, or it can affect the whole public appearance of the organization. As a consequence, auditors have a high responsibility to appropriately assess controls, procedures and perform testing to detect anomalies in business operation, therefore, detect the existence of material misstatements. To highlight the importance of the mentioned point, it is worth noting the most known case in history, the famous Enron scandal which eventually bankrupted and because of independence issues and the destruction of audit evidences, its audit firm, Arthur Andersen was found guilty and the audit license had been revoked making around 85.000 people unemployed (Li, 2010). In 2015, Tesco's profit had been overstated by £250 million leading to a loss of £2 billion in value for the company, which resulted in the change of Tesco's audit firm (The Guardian, 2014). As the examples show, financial auditors have an immense obligation to express a fair opinion on organizations' financial statements, however, with the increased digitalization techniques and complex information systems, other approaches should have been introduced in the process of financial auditing, as the spread of IT solutions not only caused convenience and automation of business processes but brought in many new risks into the life of organizations. To appropriately address these risks affecting the books and accounting, other experts are required to be involved in financial audits.

## 1. Digitalization and new threats

The automation of business processes is inevitable in order to stay in the competition. Digitalization can enhance productivity, reduce human error, and make the accounting process totally paperless. Based on a research work, performed in 2017 by one of the biggest audit firm, KPMG, about the digitalisation in accounting (KPMG, 2017), besides among others, data quality and data consistency have improved, and reporting speed and focus on processes has increased the most in recent years among the 146 companies the research has been conducted in Germany as shown in Figure 1.

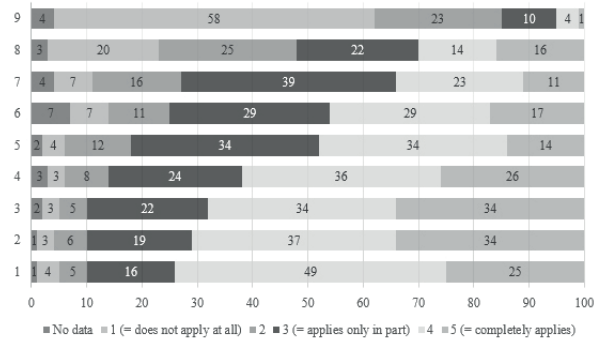


Figure 1. The influence of digitalization on accounting – status quo in Germany (source: KPMG, 2017)

The identifiers on the y-axis relate to the following items:

1. Data quality and data consistency have improved.
2. Reporting speed has increased.
3. The focus on processes has been increased.
4. The range of services has been expanded.
5. Employee qualifications have expanded in the direction of IT.
6. More tasks have been bundled internally.
7. Costs have been reduced.
8. There has been an overall reduction in accounting staff as a result of digitalisation.
9. More tasks have been outsourced to external service providers.

Important to notice that digitalisation also have an impact on the whole accounting profession, a great number of respondents agree that employees' qualification has moved towards the direction of IT which raises many questions beyond the subject of this article. How long will this profession be alive and how will it change the roles of financial auditors entirely? If the accounting process becomes totally automated, then IT professional involvement will be maximized, as the most of the focus will be on the reliability of IT services and IT controls. Financial auditors, then, should only understand the support business processes, but testing will maybe only required for the IT environment to obtain assurance that controls are designed, implemented and operating effectively to protect financial information. This reasoning serves as an evidence that IT experts' roles is a must, increased and expected to continuously increase in the years to come.

One of the biggest negative consequence of high-level automation is the extended exposure to cyber threats as systems are connected to large networks opening several doors to business-critical information in case appropriate controls are not implemented to protect business information assets. As new technologies are introduced by companies for development purposes every now and then, new threats and a new type of cyber attacks are appearing parallel to take advantage of not yet discovered vulnerabilities. Figure 2. shows the emerging trend of new malware specimen (in millions, where 2017 Q2-Q3-Q4 are forecasted) in the past few years where we can observe that the forecasted result for 2017 is almost 60 times

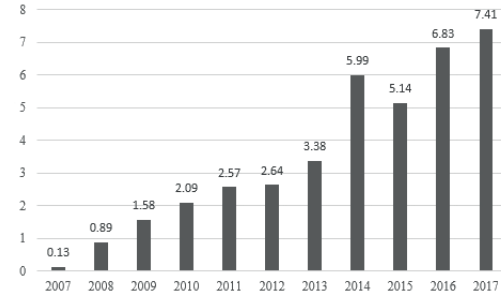


Figure 2. Viruses, Worms and Trojan Horses. Number of new malware specimen (in millions) (source: Statista, 2017a)

more new malware than in 2007 (Statista, 2017a). These malicious software programs can encrypt stored data and give the encryption key for a significant amount, steal business information committing data leakage selling the data and benefiting in the black market or totally stop the business causing reputation risk and induce disasters.

Cybercriminals are threatening companies, individuals, other organizations by stealing data or making them unavailable causing business disruption that can have a high impact on the accuracy of source data feeding financial statements. If business services are not available e.g. as a result of a DDoS attack, background processes being responsible for automated accounting might not work in alignment with management intention and several items might go unbooked. Of course, this is just examined from the perspective of data integrity relevant to the financial statement, in worst case scenario, business organizations are not able to continue business for a longer period which can result in bad public appearance increasing reputational risk, finally resulting in bankruptcy. One of the biggest recent ransomware is Petya which demanded $300 for decrypting computers infected 2.000 devices causing disruption in the UK, US, France, Germany, and mostly in Ukraine where the list of victims included the Ukrainian Government, Interior Ministry and Ukrainian National Bank (The Telegraph, 2017). External threats, therefore, should be taken care of by implementing logical and physical measurements, for both preventing and monitoring its existence, and action must be taken when its presence is detected.

However, threats not only can come from externally, but internal fraud is also present and based on the research of Kroll (2015), internally committed frauds also show an emerging trend. In the study 768 senior executives were interviewed from worldwide, and 75% of companies were reporting internal fraud, which has increased 14% compared to the results obtained in 2012. Figure 3 illustrates the trend of types of fraud and declared vulnerabilities.

The identifiers on the y-axis relate to the following items:

1. Theft of physical assets
2. Vendor, supplier or procurement fraud
3. Information theft
4. Management conflict of interest
5. Regulatory or compliance breach

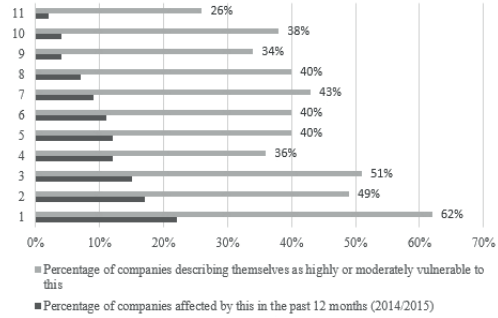


Figure 3. Companies affected by fraud and vulnerable to it (source: Kroll, 2015)

6. Corruption and bribery
7. Internal financial fraud
8. Misappropriation of company funds
9. Money laundering
10. IP theft
11. Market collusion

Number 1 internal fraud is the theft of physical assets that beyond decreasing the property of organizations, highly contributes to data leakage as employees or external parties stealing the device as well as the information stored on them. Fraud can be due to human error, careless, and also on purpose in order to benefit in some way from the lack of internal controls by the perpetrator. Internally committed fraud can be as well as dangerous as external attacks since employees have already access to highly restricted and business-critical information. Altering business information in order to show better business performance may seem attractive for management or other employees hoping for better year-end bonuses. Internal financial fraud was named in the referenced research as the 7$^{th}$ type of fraud that caused the biggest headache for companies which definitely have a great impact on the reliability of the financial statement. Thus, business data might be manipulated and the financial statement may present distorted data as a result. This type of fraud can be easily committed if controls are not in place. Access rights should be appropriately granted, continuously monitored and reviewed in order to prevent and detect unauthorized access (such as to modify financial data), adequate logging should be established so that organization could continuously monitor transactions and detect anomalies, and definitely the internal roles and responsibilities should be segregated so that one employee cannot be involved in one whole process (such as booking an invoice and then approving it).

As we can see here, financial auditors have to face many new challenges with the emerging trend of digitalization, however, financial auditors by themselves cannot cope with the mentioned problems, therefore, IT expert involvement is needed to give an opinion about the control environment of IT systems to adequately address the risk arising from the use and operation of technological solutions having an expanded impact on the completeness and accuracy of financial data.

## 2. Relying on information systems

Since paper-based accounting is not anymore taking place in the life of organizations, financial auditors have to make sure that financial data stored in different information systems are complete and accurate. This requires to perform an investigation on the IT infrastructure and related applications, databased etc., therefore on selected IT elements affecting financial reporting. As we could see from the previous section, this has to be done, so far, because of the existence of external and internal threats. The audit of information systems can be divided into two major fields as explained by Palmas, E. (2011): IT application controls and IT general controls. Application controls are specific controls related to specific information systems. They can be e.g. input controls that regulate the format and range of data for a transaction needing input data, or an appropriate authorization in a system. For example, in the SAP ERP application, authorizations can be granted via profiles, roles, which can contain transaction codes, table authorization, or regulating which company code an employee can access (Manara & Cavalleri, 2011). The IT auditor should have specific knowledge on the system, the auditor should know which controls are relevant and have to test whether it is in alignment with industry standards and good practices as well as established internal policies and applicable regulations. IT general controls are non-specific processes, procedures and policies which apply to the whole IT environment ensuring that IT operation (including access management and development) is adequately functioning enforcing an error-free operation. For example, IT auditors have to address the risk arising from poor access management processes. If access rights are not controlled, there is no management approval, no user access review taking place etc. then there is no assurance that business users are not modifying data being beyond their daily responsibilities. It is not only a threat to confidentiality being compromised but that due to the lack of knowledge or purposely, an employee can modify financial data. Definitely, the arising risk from general IT controls are wide, and appropriate risk identification and management processes shall be conducted by the auditors to understand the nature and extent of organizations to determine the risk level necessary for obtaining assurance that financial auditors can rely on the audited information systems. Not only can the human error be imagined, but information systems can go wrong in case of failure in the supporting hardware and infrastructure. If a storage stops functioning, then data is no longer available, and the accounting process must stop if there is no backup plan, such as providing business continuity by utilizing a secondary redundant site reserved for such disaster situations. If accounting stops then a control should be established requiring that every automatic job retrospectively performs accounting, and accountants also manage to book everything after the disaster situation is over. As we can observe, this area is quite complex, and one of the conclusion to note here is that more automation and use of IT infrastructure are leading to more and more risks, therefore, the role of IT auditors is increasing. The International Standard on Auditing published by IFAC (2009) details the following control areas which have to be carefully investigated:

- Data center and network operation
- System software acquisition, change and maintenance
- Program change
- Access security

– Application system acquisition, development, and maintenance

The following section explains more details about the topic of program change, as it directly relates to the innovation of organizations that drives businesses into the direction of more intelligent solutions introducing several new risks that can have an impact on financial data, therefore the reliability of financial statements.

## 3. IT development to stay in competition

Research and development is one of the key attributes that can contribute to surpass competitors, or at least to stay in competition for business organizations. In the perspective of the scope, it means that systems have to be developed, new features have to be introduced, legacy systems have to be changed to approach the current level of innovation that helps the whole company develop making the communication easier between information systems, better attempting customers or exchanging information with administration on a faster way. At the same time, development of information systems can negatively affect financial data integrity. New feature development should be controlled via an effective change management process. This means that application development should be appropriately documented in order to address how the change in the system would affect financial data e.g. with data transformation, developments must be appropriately tested in order to detect any anomaly, human error and malicious code, roles of development and implementation into the production environment has to be segregated in order to prevent a developer implement malicious or not tested code into production, and new developments have to be monitored whether they operate as intended. The problem here is that not always possible to take care of the mentioned points because of the lack of human resource or sometimes a change is needed as quick as possible to solve an urgent business problem, therefore, controls are bypassed e.g. in case a transaction is stuck in the system, or quick resolution is needed at month-end closing. Untested programme code, therefore, means a significant risk to financial data. SAP has introduced a so-called debug function in the NetWeaver 7 in 2005, which can be used to find mistakes directly in the programme code even in the production environment (Mohapatra, 2015). The biggest problem with that is that it allows to bypass application level controls by changing source code which is responsible for the protection of business data. One not appropriately considered access right and the system can become easily vulnerable. Definitely, there is a solution to overcome this problem by only granting this access to users when it is really needed by continuously monitoring its use, and once the job is done, the access shall be revoked. As we can see here, to adequately protect the information stored in information systems a great number of staff is required, but where is the balance between the cost and security? New developments also contain new vulnerabilities. If a new platform is introduced, then appropriately tested and protected applications can become vulnerable by the threats not yet discovered for operating platforms. In the case an application contains its security setting in the operating system level, then no matter how secured the application is, it can be bypassed. Figure 4 shows the new vulnerabilities for Microsoft products in the last few years until the end of February, 2018, as Microsoft Windows is one of the most popular operating platform.

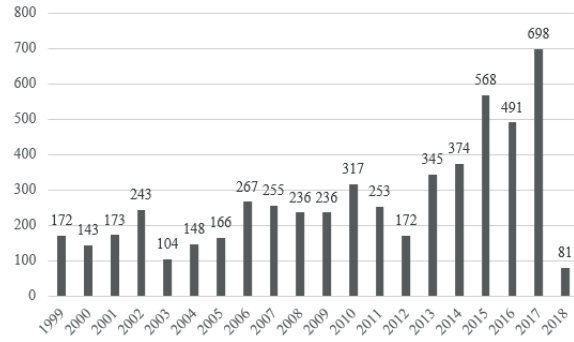


Figure 4. Microsoft vulnerability statistics (source: CVE Details, 2018)

The general trend is increasing that can be favourable for cybercriminals as well internal fraud commenters, since they can take the advantage of vulnerabilities if they are not addressed in time, or the patch management process (responsible business procedure for hardening servers and installing corrective program code) is not operating effectively. As a summary, automated processes create many new risks. Beside preventive controls, detective controls can help detect any anomaly if log files of information systems are appropriately monitored and secured from modifications e.g. by employees.

## 4. Monitoring transactions

Log monitoring cannot be effective if performed totally manually as because of human errors. Several mistakes, failures and behaviour being different from the standard operation can go undetected. What can be then the solution? How to answer for more and more business process automation? Is it even possible to detect each and every fraud and potential risks at all? Information systems can produce a tremendous amount of log files. Each user log-in, each data modification, each application process, each background job running, each automated process activity at several layers of information technology elements. On this increased number of files sometimes are impossible to go through manually, it would require many new employees endangering efficiency and creating more cost. So why not respond to the enhanced level of automated operations with the automated investigation? What do we need to prepare and have in order to apply automated analysis? In case of external threats, the network traffic can be monitored so as to detect anomalies in daily operation. This can be done by looking up for unusual behaviours. First, the normal operation should be analysed creating patterns what employees are using for the network, and then the task is to determine data flow which differs from these patterns. The same can be performed for internal transactions, just in this case not only the network and electronic channels to the IT infrastructure shall be monitored, but each and every access, data change and flow. A test period should be developed when data for the normal business operation is collected, appropriately analysed, and then patterns are created. Definitely, there are many things to be considered. First is, that it has to work on a time series basis i.e. an internal fraud may take for several months when the committee tries to build up the perfect crime in silence. Second, action

plans have to be in place once an anomaly is detected to answer for possible fraud or attack. The biggest question, is definitely, how is it even possible to carry out, and that is when the challenge starts from.

## 5. Artificial Intelligence as a possible solution

With the increased technology development, artificial intelligence has arisen. Based on recent researches, artificial intelligence seems to have tools to solve the above-mentioned problems. Artificial intelligence is a scientific area which aims to empower computers with human thinking and problem-solving. Haugeland (1985) defined artificial intelligence as a new experiment to make computers to think, and used the expression as "*conscious machine*". Nillson (1998) defined artificial intelligence as the scientific area of intelligent behaviours of objects. The very first idea and the basics of artificial intelligence was detailed by McCulloch and Pitts (1943), in their publication they investigated the human nervous system and concluded that machines could also work on the principles of the human brain, opening the door for recent machine learning systems with their publications, which is a subfield of artificial intelligence. Machine learning can be applied to teach algorithms based on historical data to recognize patterns, therefore, may appear to be useful to detect and prevent fraud. Machine learning has three major fields of research (Raschka, 2015):

1. Supervised learning
2. Unsupervised learning
3. Reinforcement learning

Supervised learning is used to teach algorithms with historical data to predict an outcome for unseen data. (Norvig & Russell, 2005) This outcome can be a category whether a transaction appears to be fraud or not. In addition, with supervised learning, the probability of a transaction being fraud can also be estimated. Unsupervised learning is used for recognizing pattern in existing data, however, no previous training is needed. It can group transactions which behaves similarly, thus, it can be used to initially determine what kind of business behaviours an organization can divide its transactions. Clustering algorithms belong to unsupervised learning. Reinforcement learning attempts to maximize a reward for a software agent in an environment. For the problems in scope, supervised learning can give promising results. One of the greatest machine learning algorithm which is widely used and most of the research focuses on is deep learning (Gartner, 2017a). Deep learning serves as a state of the art technology for autonomous vehicle driving, natural language processing, image and speech recognition etc. Deep learning is an extended version of neural networks, such as the principles were introduced by previously referenced McCulloch and Pitts (1943). Neural networks aim to copy the process of human decision making (Szatmári et al., 2013) The neurons collect data from the input, transport them to other layers of neurons, activating the data via an activation function, and finally providing data for the output neurons. With the application of neural networks, both regression and classification problems can be solved. Investigating transactions whether they are fraudulent or not is a binary classification problem and by feeding a neural network with historical data, it can predict the existence of fraud. The conclusion, and recommendation here is that adequate preventive controls should

be in place first to prevent any fraud either its coming from external or internal sources. However, preventive controls are not always enough as they can be bypassed because of not appropriate implementation or because of the problems of operating effectiveness. Therefore, detective measures should also be implemented, and the one which should be considered is to monitor the log files and each and every user activity. As information systems produces a large amount of log files, it cannot always be done manually because of the limit of human resource, but automated solutions should be developed such as with the help of machine learning which, with a great care and attention, can help organizations to detect in time any anomaly observed.

## 6. Auditing with artificial intelligence

Big Four public accounting firms have also recognized that artificial intelligence can be a useful supporting tool in financial audit and started adapting their solutions and made agreements with tech giants purchasing their intelligence products. Big Four companies are Deloitte, PwC, KPMG and EY, the four largest auditors in the world (Statista, 2017b). As summarized by Issa, Ting, and Vasarhelyi (2017) Deloitte are introducing a contract analysis system which aims to help auditors analyse complex and long documentation provided by the audited company as audit evidence. It can be performed by text mining and natural language processing saving precious time since auditors don't necessarily have to go through each and every contract, statement and policy, the system is capable to extract the necessary information which can then be used for further investigation. EY uses a software which can model human behaviour (EY, 2016), PwC applies artificial intelligence to optimize its internal processes (MIT, 2016), KPMG works with IBM's Wattson to detect audit exceptions based on loan grading (KPMG, 2016).

## 7. Challenges of artificial intelligence

Artificial intelligence can provide a wide variety of solutions which can help protect the integrity and confidentiality of financial data. If so, how is it possible that not each and every organization using it already? Gartner (2017b) has performed a research on the challenges of artificial intelligence where 83 companies were asked for an interview. The results of current artificial intelligence challenges shown on Figure 5.

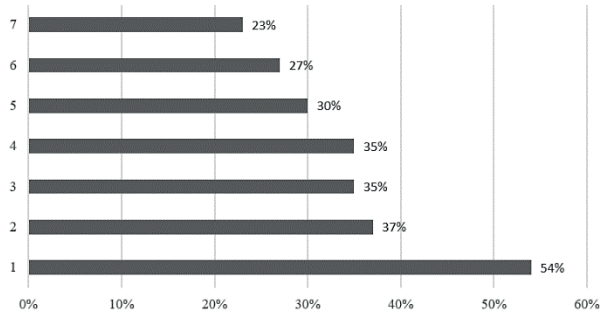


Figure 5. Biggest challenges of artificial intelligence (source: Gartner, 2017b)

The identifiers on the y-axis relate to the following items:

1. Lack of necessary staff skills
2. Defining our AI strategy
3. Identifying use cases for AI
4. Funding for AI initiatives
5. Security or privacy concerns
6. The complexity of integrating AI with our existing infrastructure
7. Determining how to measure value from using AI

Number 1, responded by more than half of the organizations is that they lack of appropriate experts who could be capable of building up the artificial intelligence infrastructure meaning that relevant business needs exist, but the education does not follow the technology trend that is an obstacle for further development. Number 2 challenge is that defining artificial intelligence strategy is problematic. Business strategy is the main source, each and every policy, procedure and strategy should be derived from ensuring that different functional areas also understand the business needs and other development initiatives in alignment with the business goals of organizations. If business strategy and IT strategy are not harmonized, then business and IT might follow their self-interest causing harm to achieve business objectives. Artificial intelligence strategy, therefore, should also follow business strategy, but if business strategy is not well defined, or does not even exist, then the strategy of artificial intelligence will not be a success story, more like unnecessary waste of money and resources. Number 3 challenges are identifying use cases for artificial intelligence and the funding problem of it. Finding appropriate business case can be hard due to a lack of knowledge or organization culture. Funding the initiatives is always a problem, as the quantitative value of artificial intelligence cannot always be measured, therefore, chief executives cannot be convinced the necessity of artificial intelligence. It can be seen as a plus cost, not the added value to the business operation. Number 4 challenge is the security and privacy concerns for applying artificial intelligence. As information systems are vulnerable against internal and external threats, artificial intelligence applications are not exceptions either. In addition, artificial intelligence can introduce new threats. Not properly trained intelligent applications can have serious consequences endangering not only financial data, but the whole operation of a company. Intelligent solutions can be used for automated decisions, chief level executes might rely on the outcome of such systems, therefore, if they are not appropriately tested or fine-tuned for current business needs, it may lead to false conclusions resulting in incorrect decisions. Also important to mention, since intelligent solutions can automate whole business processes, the production of malware is also possible meaning that machines by themselves empowered by artificial intelligent can be capable of producing more and more malware software flooding the internet with no human intervention meaning that with the trend of automation cybercriminals also have the tools build up intelligent blackmailing or malicious robots that cause significant harm for organizations and for the whole society. Number 6 challenge is the problem of integrating artificial intelligence with the current IT infrastructure. Still many organizations use legacy applications that operates well for long years, but these systems do not have the capability for further intelligent development because of the limits of obsolete

technology or programming standards. Number 7 challenge is the problem of measuring the real value from artificial intelligence monetarizing the added value, quantify and estimate exactly the reduction in costs, or benefits. This may be hard as for determining the value, key performance and financial indicators shall be measured historically, evaluated and then compared. But the lack of appropriate measurements might result in the fact, that certain solutions may not be comparable, therefore, the value cannot be estimated.

## Conclusion

Based on the analysis of relevant literature and statistics presented in this article, the conclusion can be drawn that with the increased use of automated solutions to reduce human error and optimize business processes, a couple of new risks are introduced into the life of business organizations that have to be taken care of. To protect information relevant to financial reporting, effective controls must be implemented that cannot be bypassed, but the lack of human resource and not appropriate design can leave information systems vulnerable. Financial auditors, in the era of digitalization, cannot perform an effective audit without the involvement of IT auditors. As the trend is increasing, IT experts are more needed to test IT environments in order to obtain assurance that financial data is appropriately protected, and there is no suspicion of internal fraud via the exploitation of vulnerabilities. Artificial intelligence can provide solutions as an answer to the risks introduced by digitalization, however, many challenges exist as of now that can pull back its high-level spread.

## References

CVE Details. (2018). *Microsoft: vulnerability statistics*. Retrieved from https://www.cvedetails.com/vendor/26/Microsoft.html

EY. (2016). *Insights-Driven digital innovation*. Retrieved from http://www.ey.com/Publication/vwLUAssets/EY-insightsdriven-digital-innovation/$FILE/EY-insights-driven-digital-innovation.pdf

Gartner. (2017a). *Hype cycle for artificial intelligence, 2017*. Retrieved from https://www.gartner.com/document/3770467?ref=solrAll&refval=193456093&qid=063144043355fa4bde62ca5985043d81#

Gartner. (2017b). *Predicts 2018: artificial intelligence*. Retrieved from https://www.gartner.com/document/3827163/meter/charge

Haugeland, J. (1985). *Artificial intelligence: the very idea*. MIT Press, Cambridge, Massachusetts.

IFAC. (2009). *International Standard on Auditing 200. Overall objectives of the independent auditor and the conduct of an audit in accordance with internation standards on auditing*. Retrieved from http://www.ifac.org/system/files/downloads/a008-2010-iaasb-handbook-isa-200.pdf

ISACA. (2004). *IT control objectives for Sarbanes-Oxley. The importance of IT in the design, implementation and sustainability of internal control over disclosure and financial reporting*. Retrieved from http://www.isaca.org/knowledge-center/research/documents/sox-appendix_res_eng_0504.doc

Issa, H., Ting, S., & Vasarhelyi, A. M. (2017). Research ideas for artifical intelligence in auditing. The formalization of audit and workforce supplementation. *Journal of Emerging Technologies in Accounting, 13*(2), 1-20.

KPMG. (2017). *Digitalisation in accounting*. Study of the Status Quo in German Companies. Retrieved from https://home.kpmg.com/content/dam/kpmg/de/pdf/Themen/2017/digitalisation-in-accounting-en-2017-KPMG.pdf

KPMG. (2016). *The impact of cognitive technology on business and financial reporting*. Retrieved from https://assets.kpmg.com/content/dam/kpmg/pdf/2016/05/game-changer-impact-of-cognitive-technology.pdf

Kroll. (2015). *Global Fraud Report. Vulnerabilities on the Rise*. Annual Edition 2015/16. Retrieved from http://anticorruzione.eu/wp-content/uploads/2015/09/Kroll_Global_Fraud_Report_2015low-copia.pdf

Li, Y. (2010). The case analysis of the scandal of Enron. *International Journal of Business and Management, 5*(10), 37-41. https://doi.org/10.5539/ijbm.v5n10p37

Manara, M., & Cavalleri, A. (2011). *100 Things You Should Know About Authorizations in SAP*. Galielo Press Inc., Boston.

McCulloch, W. S., & Pitts, W. (1943). A logical calculus of the ideas immanent in nervous activity. *The bulletin of mathematical biophysics, 5*(4), 115-133. https://doi.org/10.1007/BF02478259

MIT. (2016). *AI drives better business decisions*. Retrieved from https://www.technologyreview.com/s/601732/aidrives-better-business-decisions/

Mohapatra, R. P. (2015). *Debugging for functional consultants*. Retrieved from https://blogs.sap.com/2015/05/26/debugging-for-functional-consultants/

Nillson, N. J. (1998). *Artificial intelligence: a new synthesis*. Morgan Kaufmann, San Mateo, California.

Norvig, P., & Russell, S. J. (2005). *Mesterséges Intelligencia Modern Megközelítésben, Második, átdolgozott, bővített kiadás*. Panem Kiadó, Budapest.

Palmas, E. (2011). IT General and Application Controls: The Model of Internalization. *ISACA Journal, 5,* 1-4.

Raschka, S. (2015). *Python machine learning*. Packt Publishing, Birmingham.

Statista. (2017a). *Ransomware makes up small share of growing malware threat*. Retrieved from https://www.statista.com/chart/10045/new-malware-specimen-and-share-of-windows-based-malware/

Statista. (2017b*). Revenue of the Big Four accounting / audit firms worldwide in 2017 (in billion U.S. dollars)*. Retrieved from https://www.statista.com/statistics/250479/big-four-accounting-firms-global-revenue/

Szatmári, J., Mucsi, L., Nagyváradi, L., Szabó, Sz., Barta, K., Bugya, T., Czigány, Sz., Pirkhoffer, E., Rábay, A., Tobak, Z., Boudewijn, L., Bartus, M., & Szatmári, J. (2013). *Modellek a geoinformatikában*. TÁMOP-4.1.2.A/1- 11/1 MSc Tananyagfejlesztés.

The Guardian. (2014). *Tesco loses £2bn in value as investigation of profit overstatement begins*. Retrieved from https://www.theguardian.com/business/2014/sep/22/tesco-loses-2bn-value-250m-profit-overstatement-investigation

The Telegraph. (2017). *Petya cyber attack: everything to know about the global ransomware outbreak*. Retrieved from https://www.telegraph.co.uk/technology/2017/06/27/petya-cyber-attack-everything-know-global-ransomware-outbreak/