[1.]Tímea ANTAL, [2.]Róza SZÁMADÓ

A SNAPSHOT OF THE EMERGENCE OF COMPLIANCE AND ARTIFICIAL INTELLIGENCE – RESULTS OF AN ONLINE SURVEY OF HUNGARIAN COMPANIES

[1.]Óbuda University, Doctoral School on Safety and Security Sciences, HUNGARY
[2.]Óbuda University, Bánki Donát Faculty of Mechanical and Safety Engineering, HUNGARY

Abstract: The research focused on the issues related to compliance (Concept: compliance is a kind of conformity to standards within an organisation, be it legal or organisational ethical rules.') and the emergence of artificial intelligence (AI) in Hungarian businesses. The questionnaire survey sought answers from Hungarian businesses in three areas: 1 – Can compliance as a security factor be a priority? What concepts do businesses associate with the terms compliance and AI; 2 – Does the use of AI tools go hand in hand with ensuring compliance? ; 3 – Is the use of AI tools and the fact and emphasis on ensuring compliance related to security awareness? Based on the questions, three hypotheses were formulated: 1. compliance is a security factor; 2. the use of AI tools is associated with compliance assurance in Hungarian enterprises; 3. the fact and emphasis of compliance assurance in the use of AI tools is related to security awareness. The results of the online questionnaire survey confirmed the assumptions, but at the same time there are several intersections between the two areas, which highlight that both are new topics and concepts for Hungarian businesses. As a consequence, there is still much uncertainty about their practical application. Many research questions in this area still need to be answered in the future.
Keywords: compliance, artificial intelligence, security awareness, Hungarian companies

1. INTRODUCTION

The key social and economic trends for the third decade of the 21st century are sustainability and digital transformation. The primary resource of digitalisation is the ever–increasing amount of data, the measurement, management and use of which represents legal, technological, economic and even social challenges. A technological revolution is taking place in the form of digitalisation, automation and robotisation. As a consequence, all aspects of our life need to be transformed; complex problems require complex solutions. According to data of Statista [2] the estimated data traffic on the internet per minute in 2021 and in 2024 was:

Table 1. Estimated data traffic on the internet per minute 2021, 2024 (Source: own creation)

Data type	2021	2024
Youtube content uploaded	500 hours	no data
E–mails sent	197,6 million	251,1 million
Online shopping	1,6 million dollár	no data
Messenger/ Whatsapp messages 2021 Reels videos Facebook and Instagram 2024	69 million	138,9 million
TikTok downloads	5000 downloads	16000 downloads
LinkedIn new connections	9132 new connections	9000 new connections

The data shows that internet traffic has clearly increased between 2021 and 2024. Email sending has increased by more than 25%, TikTok downloads have tripled. Reality is constantly being digitally mapped and a virtual reality is gradually joining the physical world. In this process, the amount of data produced and stored is doubling.

It is a remarkable duality that sectors and organizations based on artificial intelligence have grown into tens of billions of dollars in industries over the past decade, yet to date there has been no significant growth in mitigating the risks associated with artificial intelligence. According to Statista [3] data, the artificial intelligence market will continue to grow until 2030. The value of nearly $100 billion in 2021 is expected to increase twenty–fold by 2030, to nearly $2 trillion.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

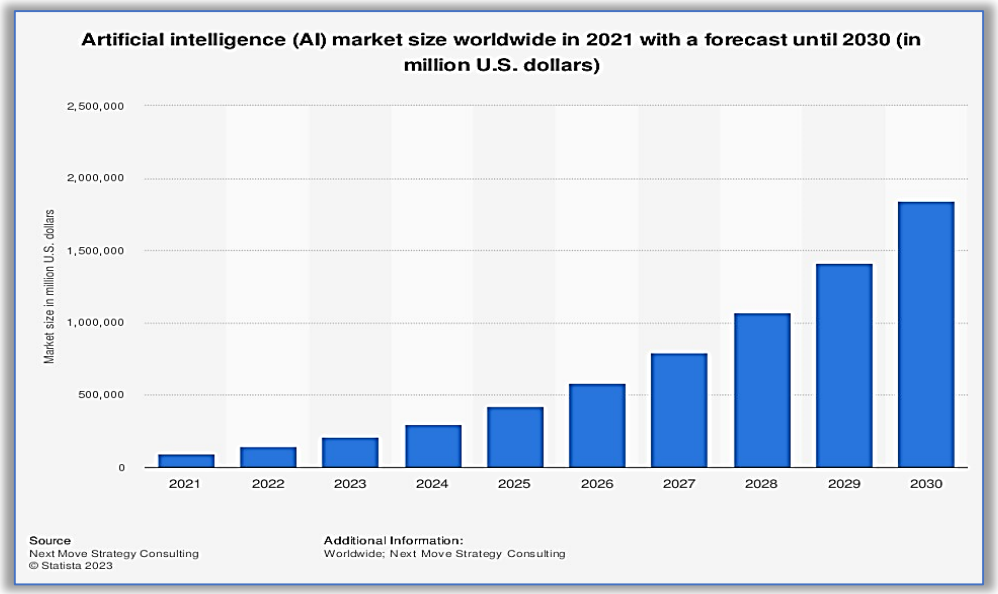

Figure 1. Artificial Intelligence Global Market Size Forecast 2021–2030 [4]

Artificial intelligence is present in many sectors, including finance, healthcare and transport, agriculture, logistics and commerce. Meanwhile, the concept of artificial intelligence is evolving organically, with ethical guidelines and legal regulation following the technology boom. Organizations and businesses are adopting risk management and auditing processes to ensure that their processes are up to the challenge and can remain resilient and competitive.

According to McKinsey's 2023 global research, only 21% of respondents say their organizations have developed policies that govern employees' use of artificial intelligence technologies in their work [5]. Between 2019 and 2023, McKinsey assessed risks related to artificial intelligence, among other things. In 2023, two new risk factors appeared among the most frequently mentioned risks: inaccuracy and intellectual property infringement. The second table shows the five most common risk aspects between 2019 and 2023. It can be seen that cybersecurity, regulatory compliance and explainability are the most significant risks between 2019 and 2023.

Table 2. According to McKinsey research, artificial intelligence risks 2019–2023 (Source: own creation)

Risk aspects	2023	2022	2021	2020	2019
Inaccuracy	56 %	no data	no data	no data	no data
Cybersecurity	53 %	51 %	57 %	62 %	62 %
Intellectual Property Infringement	46 %	no data	no data	no data	no data
Regulatory Compliance	45 %	36 %	50 %	48 %	50 %
Explainability	39 %	22 %	44 %	41 %	39 %

These trends impose significant and complex challenges, while data are constantly regenerated, providing ammunition for the further development of artificial intelligence, while the technology itself is in a constant development. Technology trends are far ahead of the regulatory environment. Citizens and organisations are increasingly demanding digital solutions, carrying them "in their pockets". Organisations are challenged to restructure their organisations in response to digital transformation.

I believe it is necessary to establish a strong link between AI and compliance. Both areas are "products" of the past 50 years. As a management tool, they can contribute to sustainable, resilient business operations, can create more efficient internal operations; and can increase service levels and resultorientation. There has been a lot of research into the definition of the terms. Their uniform legal regulation is immature. Standards play an important role. Moral – ethical considerations must be taken into account. Businesses still see them as a novelty. They require learning and knowledge application skills both at individual and organisational level. There is a need for openness and support from company management. Security and trust considerations are

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

essential in their use. In the short term, they require a greater financial investment, but can give businesses a competitive advantage in the long term. Good practices need to be identified and analysed. These are my underlying reasons why I started the survey of compliance and the emergence of artificial intelligence (AI) in Hungarian businesses.
The questionnaire survey sought answers from Hungarian businesses in three areas: 1 – Can compliance as a security factor be a priority? What concepts do businesses associate with the terms compliance and AI; 2 – Does the use of AI tools go hand in hand with ensuring compliance? ; 3 – Is the use of AI tools and the fact and emphasis on ensuring compliance related to security awareness?
Based on the questions, three hypotheses were formulated: 1. compliance is a security factor; 2. the use of AI tools is associated with compliance assurance in Hungarian enterprises; 3. the fact and emphasis of compliance assurance in the use of AI tools is related to security awareness.

2. RESEARCH METHOD

The survey data were collected using an online, self–completion questionnaire between 07.11.2024 and 16.12.2024. The questionnaire was created using MS Forms. The questionnaire contained 35 questions, including both open and closed questions.
Statistical analyses were performed using SPSS 30.0 (SPSS Inc.,Chicago, Illions, USA) and MS Excel. For the closed questions, the response options “Don't know”, “No answer”, “Not concerned” were removed during analysis, no data imputation was performed.
Element numbers are marked for each test. The respondents, i.e. the sampling units, were representatives of firms in Hungary. Of the 140 respondents, 27 (19.3%) are company managers, 39 (27.9%) are company owners and 74 (52.9%) are other employees; while in terms of field, the largest number of respondents, 47 (33.6%), work in accounting, 42 (30.0%) in management, 27 (19.3%) in other, 13 (9.3%) in IT, 5 (3.6%) in marketing, 4 (2.9%) in administration and 2 (1.4%) in HR. Nearly 80% (79.3%) (111 firms) of the firms are micro or small, 9.3% (13 firms) are medium and 11.4% (16 firms) are large.

3. RESEARCH RESULTS

Compliance as a security factor

A research question was formulated as to whether compliance as a security factor can be given prominence and what concepts companies associate with the terms compliance and artificial intelligence. Due to the transformation and rapid evolution of the field, it is assumed that a paradigm shift is taking place in the application of compliance at the enterprise level with the advance of artificial intelligence (AI). To answer this question, we have reviewed the concept of compliance, assuming that in this case compliance as a security factor function may be more pronounced. The open–ended question “Q9: What are the first three things that come to mind when you hear the terms compliance and AI?” was processed by post–coding.
During the process, it was found that respondents did not separate their answers on compliance and AI (due to the fact that the question was not entirely clear to them), so the coding and statistical analysis was done for both concepts together. There were 139 assessable responses to the question, all of which could be classified into one or more of the 18 categories trained using the method of coding responses to the open–ended questions. The breakdown of the categories and the frequencies are shown in Table 3.
Among the responses that included a rating, the split between positive and negative reactions is 50/50, i.e. 53 rather positive and 51 rather negative ratings. The most frequent are security, risk, legal comments, responsibility, data linkage, and future and innovation. On this basis, it can be concluded that the perception is rather positive and the hypothesis can be considered validated, especially in view of the trends identified in this area.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

Table 3: Compliance – artificial intelligence determination

Category		Frequency of mention	
Category name	details, examples	people	%*
Security	security, data protection, data security	59	42%
Risk	risk/ risk management	44	32%
Development	innovation, development, improvement, future, opportunity	36	26%
Responsibility	responsibility	30	22%
Regulation	legal, legal compliance, law, regulatory/unregulated, transparency, standard	29	21%
Savings/Cost	time, money, administration, facilitation, speed, convenience, efficiency	16	12%
Ethics	ethical, ethical compliance, moral	9	6%
Risk	danger, misleading information, errors	9	6%
Reliability	audit/unverifiable, guarantee, reliability	8	6%
Assistance, support	assistance, support, satisfaction	8	6%
Data	information base, help to access information, mass of information, information trade, phishing	7	5%
Human capital replacement	automation, robot, loss of professions, unemployment	7	5%
Unknown, uncertain	unknown, alien, immature, uncertainty, distrust, caution	7	5%
Quality	professional quality, precision, accuracy	6	4%
Constraints	limits, boundaries, punishment, rigour	5	4%
Expenditure	learning, teaching, training, preparation, adjustment	5	4%
Requirement	compulsory, indispensable, compulsion	4	3%
Other	specific activities (e.g. translation, image generation) software (chat GPT), guidelines, standards (NIS2, ISO) and include mentions with a frequency below 2%	33	24%

Comment: * Out of 139 valid responses
Source: own creation

When asked "In which compliance area would you use AI?", only 48 respondents (34.3%) could specify an area. The remaining 92 respondents (65.5%) selected "My organisation does not use it". The distribution of the areas indicated is shown in the following figure. The highest proportion of respondents indicated process monitoring and reporting. At the same time, the responses also show that a significant growth in this area can be predicted in the future and that, as a consequence, an increase in the importance of issues related to use and regulation can be expected.

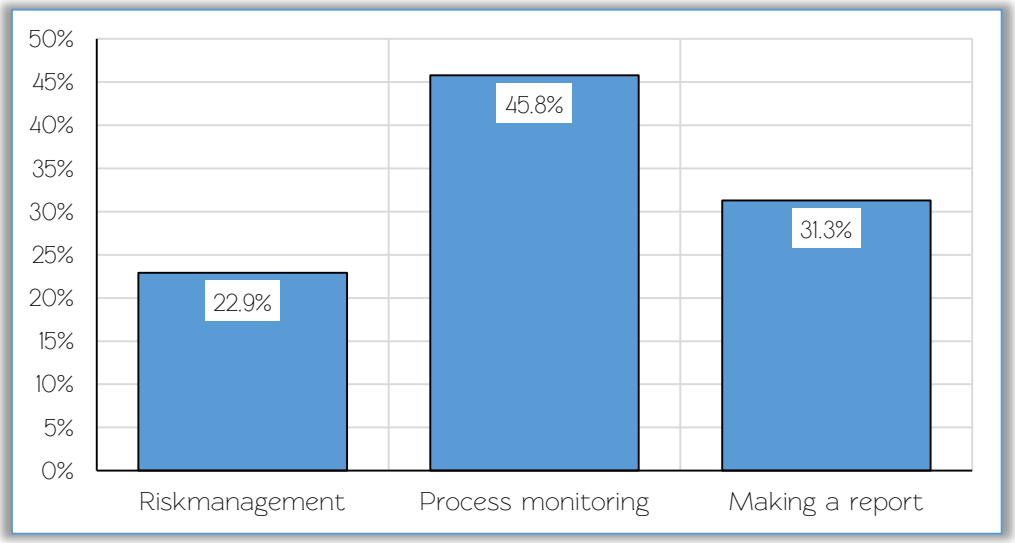

Figure 2: In what compliance area would you use AI? (N=48)
Source: own creation

Compliance can become a tool for effective strategic risk management and promote a higher level of security. Based on theoretical literature the concept of compliance can be defined in short: meeting legal requirement. The table below presents the approaches in parallel with a description of the content of compliance (what to comply with).

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

Table 4.: Compliance definitions, Source: own creation

Author	Compliance definition	Compliance with what?
Georg Gösswein	Operating in accordance with the law [6].[1]	Legislation.
Mónika Balogh	"Compliance with and operation in accordance with all applicable rules and requirements (legal and otherwise)." [7]	Legislation, other rules, requirements.
Dennis Bock	"In the most general sense, compliance is – from an organisational perspective – an umbrella term for measures to demonstrate compliance with the law, to achieve behaviour that is in accordance with legal requirements, internal rules or other recommendations to be followed." [8]	Legislation, internal rules, recommendations.
Thomas Rotsch	"Compliance (...) is defined as the operation of businesses in compliance with the law in force, which is a characteristic of areas where complex and complicated regulation requires the application of preventive measures by "experts" to demonstrate compliance." [9]	Legislation.
Dr. István Ambrus, Dr. Kitti Mezei, Dr. Erzsébet Molnár	"In other words, compliance is a kind of conformity to standards within an organisation, be it legal or organisational ethical rules." [10]	Legislation, internal rules ethical norms, international standards, standards.

We can find a connection between the definitions of compliance in practice and theory. Legislation, rules and ethical norms are common. The new aspect is security in practice.

The terms compliance and AI are rated with half and half positive and negative reactions respectively. The most frequently mentioned are security, risk, legal comments, liability, and data related. Based on this, it can be stated that compliance as a security factor function may be prominent. It can be concluded that the use of AI tools is significantly associated with ensuring compliance, i.e. companies that use AI tools are more likely to have compliance requirements than those that do not use AI. More than half of the respondents use some form of AI tool, and the preferred use of AI tools in the organisation's operations is in the areas of marketing, production, market research and management. Compliance rules are the most commonly used tool for monitoring organisational workflows, followed by training and certification requirements management. Internal communication is by far the most common method of information, but training and websites are also highlighted.

1.1.1. The use of AI tools goes hand in hand with ensuring compliance.

The use of AI tools by companies

The second issue – the use of AI tools by companies. For this research question, the following questions were asked in the questionnaire:

- Q10: Does your company use any AI–based tools? (Yes/No),
- Q11: If your answer to the previous question was "Yes", which are they? (You can tick more than one answer at the same time: Dall–E/ ChatGPT/ DeepL/ Brickabrack AI/ Gemini/ Claude/ Midjourney/ Character.AI/ QuillBot/ Microsoft Copilot/ TensorFlow/ SAP/ Bard/ Novel AI/ CapCut/ Janitor AI/ Civitai),
- Q12: In which areas have you seen your business using AI–based applications/tools? (You can select more than one answer at a time: My organisation does not use them/ Accounting/ HR / Customer service and support/ Administration/ Marketing/ Management/ Sales),

From this, the fact of asset use is measured by question Q10. And the extent of asset use is measured by the variable K12_K (summing up the number of areas marked), created from question Q12.

The compliance assessment was based on the following questions:

- Q33: Does the company have a compliance policy? (Yes/No),
- Q34: How often does the company review its compliance policy? (3: Annually/ 2: Periodically/ 1: When a new risk factor arises/ 0: Never),

[1] Gösswein, Georg: Mediation als Weg aus dem Compiance-Dilemma, Die Mediation 2017/2, A mediation als a compliance dilemmas aus dem Compiance-Dilemmas aus dem Compiance-Dilemmas (translated by Erika Csemáné Váradi - Judit Jacsó), AKV European Review, 2017/1, pp. 122–127

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

- Q35: What does your organisation currently use compliance rules for? (You can tick more than one answer: To monitor changes in legislation/ To manage training and certification requirements/ For reputational purposes/ To monitor and manage requirements and approvals),
- Q36: How is your organisation informing employees, contractors and other responsible persons about the company's compliance mechanisms? (You may tick more than one answer: by training/ by internal policies (e.g. Code of Conduct or Guidelines for the use of AI tools)/ by internal communication/ by using an internal company website/ by organising awareness–raising events).

Following the questions, variables were developed to reflect the fact and the emphasis on ensuring compliance. The fact of ensuring compliance is measured by variable K33, while the emphasis is measured by variable K34_2, which was created by combining the possible answers 1–3 of questionnaire question K34, as follows.

A cross–tabulation analysis was used to examine the co–occurrence of the use of the tool and the fact of ensuring compliance. The cross–tabulation created from the variables K10 and K33 is shown in Table 5.

Table 5.: Relationship between asset use and compliance assurance (cross–tab analysis)

		Q10: Does the company use any AI–based tools?		Total
		No	Yes	
Q33: Does the company have compliance rules and regulations?	None	56	30	86
	Have	7	30	37
Total		63	60	123

Source: own creation

The chi–squared test performed confirmed the association between the fact of using the tool and the fact of ensuring compliance (chi2=22.098, df=1, p<.001). The association is of medium strength (V=0.424, p<.001) according to the Cramer V coefficient.

The figure below shows that in the sample, firms that do not ensure compliance have a lower percentage of AI–based tool use (34.9%), while those that do ensure compliance have a higher percentage (81.1%).

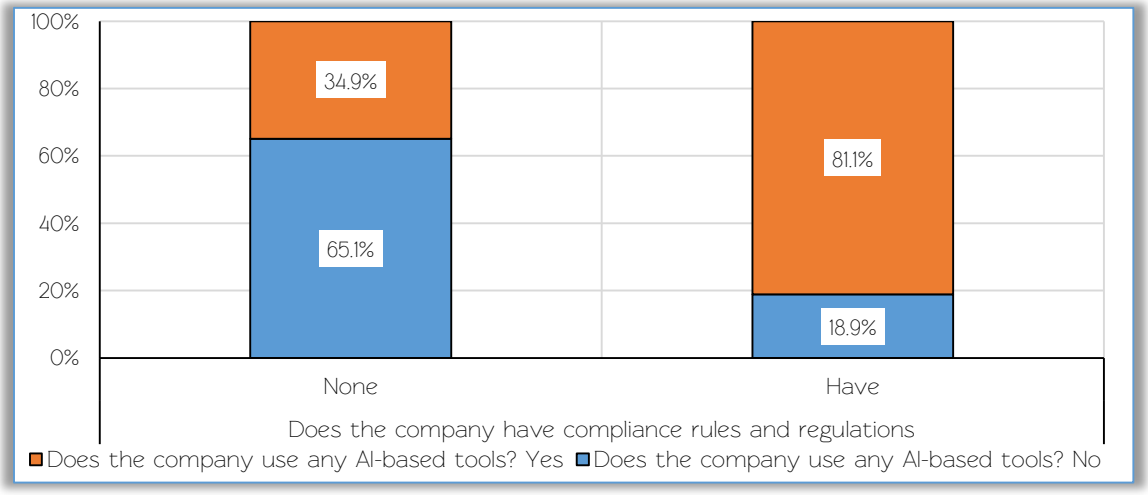

Figure 3.: AI tool use in relation to compliance assurance (N=123)

Source: own creation

It can therefore be concluded that the use of AI tools is significantly associated with compliance, i.e. firms that use AI tools are more likely to have compliance requirements than those that do not use AI.

The fact and emphasis on ensuring compliance in the use of AI tools is linked to security awareness. Ensuring compliance standards and policies and regularly reviewing them can increase the security awareness of employees.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

- The fact and emphasis on ensuring compliance in the use of AI tools is linked to the awareness of security.

An important hypothesis formulated in the study is that the fact and emphasis on ensuring compliance in the use of AI tools is related to the perception of safety. In testing this hypothesis, the use of AI tools and ensuring compliance is related to firms, while the perception of the benefits and risks of AI and the sense of security/uncertainty is related to respondents as units of analysis.
In relation to AI tool use, the correlation between the fact of ensuring compliance (K33) and emphasis on ensuring compliance (K34) and sense of security (K30) was examined using Spearman's rank correlation coefficient (rho) and significance testing. Both the fact of ensuring compliance (rhó=.482; p<.001) and the emphasis on ensuring compliance (rhó=.902; p<.001), have a significant positive effect on employees' safety perception. It can therefore be concluded that ensuring compliance and regular review of compliance standards and policies can increase workers' security awareness (Figure 4).

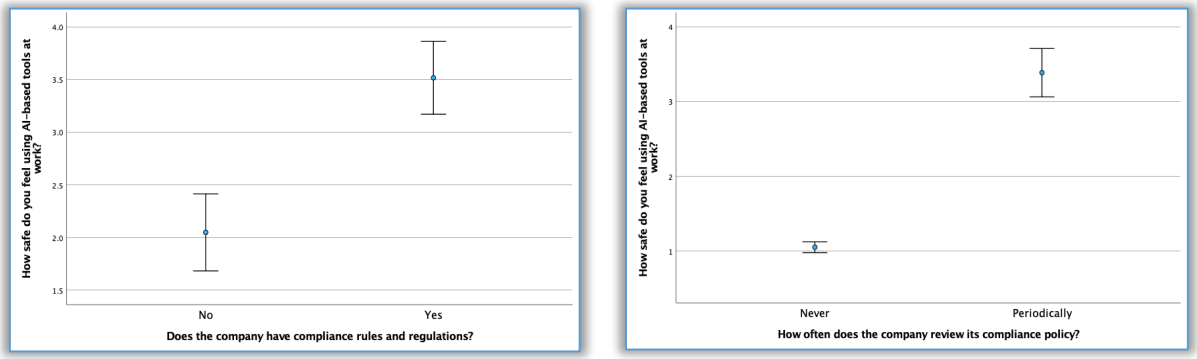

Figure 4.: The fact of ensuring compliance, the emphasis on ensuring compliance and the link between security awareness (average and 95%CI)
Source: own creation

The ability of companies to influence employees' security awareness through IT security training was also investigated. A linear regression model was constructed in order to measure the impact of training by filtering out the effects of the aforementioned factors of ensuring compliance and emphasis on ensuring compliance. In the model, safety awareness (K30) is included as a dependent variable, and the frequency and usefulness of training, as well as the fact of ensuring compliance and the emphasis on ensuring compliance, are included as dichotomous (dummy) variables. The dummy variables are constructed from the corresponding original variables by category pooling. The results of the regressions show that, in addition to the fact of ensuring compliance and the emphasis on ensuring compliance, the usefulness of the training has a significant effect on the employees' perception of safety, but the frequency of the training has not been found to be a significant predictor.
Therefore, the analysis suggests that the firm can influence the security awareness of employees by ensuring compliance, periodic review of compliance policies and by providing training that is relevant and useful to employees. Of these, the strongest predictor is the usefulness of the training, but not the frequency of the training.
Compliance and artificial intelligence are emerging in practice in domestic businesses, but there is still much uncertainty and a strong focus on security in their application. In my view, the focus needs to be on information sharing and awareness raising, with the development of regulatory guidance, more training and internal communication.

4. FINDINGS – CONCLUSIONS IN A NUTSHELL

The results of the research clearly show that the three hypotheses were clearly confirmed by the analysis of the data collected. At the same time, the answers to the questions in the questionnaire also clearly confirm that compliance and AI are new areas for Hungarian businesses.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665

Based on the research, it is justified to enforce the following compliance–related operating principles tailored to the organization, i.e. taking into account the business operation, size, activities, legal and regulatory conditions, goals, processes, and other specificities of the enterprise. The research supports the necessity of the requirements specified in the framework.

The purpose of the guide is to legally ensure corporate adaptation to the dynamically developing digital environment. The development, application, maintenance and continuous development of the compliance management system are the responsibility of management. Compliance obligations arise from the activities, products and services of the organization and have an impact on operations.

The introduction, operation, measurement and continuous development of compliance–oriented security processes (Plan–Do–Check–Act – PDCA) ensures a consistent approach to the prevention and management of security risks. If, based on the contents of the documented processes, all participants are well aware of their role in the processes and know the assigned process steps, then the organization can respond more effectively to security risks, can handle security incidents faster, and can also minimize the consequences of incidents.

The next step should be to compile the compliance guide.

References

[1] Dr. AMBRUS István, Dr. MEZEI Kitti, Dr. MOLNÁR Erzsébet: Explanation of compliance legislation I., General and criminal compliance , Wolters Kluwer, 2021, p. 22.

[2] Clara JENIK: A Minute on the Internet in 2021: https://www.statista.com/chart/25443/estimated–amount–of–data–created–on–the–internet–in–one–minute/, downloaded: 30/11/2024., https://www.statista.com/statistics/195140/new–user–generated–content–uploaded–by–users–per–minute/ , downloaded:13/04/2025.

[3] https://www.statista.com/statistics/1365145/artificial–intelligence–market–size/ , downloaded: 14/09/2023.

[4] https://www.statista.com/statistics/1365145/artificial–intelligence–market–size/ , downloaded: 14/09/2023.

[5] McKinsey (2023): The state of AI in 2023: Generative AI's breakout year, https://www.mckinsey.com/capabilities/quantumblack/our–insights/the–state–of–ai–in–2023–generative–ais–breakout–year , dowloaded: 2023. 09. 04.

[6] GÖSSWEIN, Georg: Mediation als Weg aus dem Compiance–Dilemma, Die Mediation 2017/2, A mediation als a compliance dilemmas aus dem Compiance–Dilemmas aus dem Compiance–Dilemmas (translated by Erika Csemáné Váradi – Judit Jacsó), AKV European Review, 2017/1, p. 122–127.

[7] Mónika BALOGH: A labor compliance audit, Wolters Kluwer, Budapest, 2015, p. 15.

[8] BOCK, Dennis: Criminal Law Aspects of the Compliance Discussion – § 130 OWiG as a Central Norm of Criminal Compliance, ZIS 2009/2, p. 293.

[9] ROTSCH, Thomas: 4th Compliance, in: Achenbach, Hans/Ransiek, Andreas: Handbuch Wirtschaftsstrafrecht, 3rd edition, C.F. Müller, Heidelberg, 2012, p. 47.

[10] Dr. AMBRUS István, Dr. MEZEI Kitti, Dr. MOLNÁR Erzsébet: Explanation of compliance legislation I., General and criminal compliance, Wolters Kluwer, 2021, p. 22.

ISSN 1584 – 2665 (printed version); ISSN 2601 – 2332 (online); ISSN-L 1584 – 2665