European Research Studies Journal
Volume XXVI, Issue 3, 2023

pp. 750-763

The Impact of Digitalization and the COVID-19 Pandemic on Information Security Management in the Enterprise

Submitted 21/07/23, 1st revision 12/08/23, 2nd revision 18/09/23, accepted 30/09/23

Marek Ciekanowski[1], Sławomir Żurawski[2], Zbigniew Ciekanowski[3], Yury Pauliuchuk[4], Jan Boguski[5]

Abstract:

Purpose: *The aim of this article is to present the role of information security in the management process of modern enterprises.*
Design/Methodology/Approach: *The research question posed is: What impact did the COVID-19 pandemic have on the utilisation of information technologies in enterprises? To address these questions, qualitative methods were employed. A detailed analysis of statistical data, both at national and European Union levels, regarding the utilisation of information technologies in enterprises and the impact of the COVID-19 pandemic on their operations, was conducted. The research utilised literature analysis, online sources, and an in-depth examination of data from national sources such as the Central Statistical Office (GUS) and Eurostat.*
Findings: *The COVID-19 pandemic had a significant impact on the utilisation of information technologies in companies, affecting their functioning in the virtual space and planned activities. The development of the digital space expanded the capabilities of enterprises, introduced the possibility of remote work, and enabled communication through digital tools. Ensuring information security played a crucial role in the process of management, storage, and data transfer.*
Practical Implications: *The analysis of the collected material demonstrates that the integration of management systems plays an important role in contemporary enterprises. This is a complex process that requires information technology skills, knowledge, and competencies among employees and managerial staff. Therefore, it is important to focus on the needs of seeking and implementing increasingly advanced systems for data collection, transmission, and protection in organisations.*
Originality/Value: *The analysis of the gathered material shows that digitization has become a necessity and an essential source providing access to the latest information. The authors*

[1]*University of Social Sciences, Poland, ORCID: 0009-0009-1271-0652, marek@ciekanowki.pl;*
[2]*State School of Higher Education in Chełm, Poland, ORCID: 0000-0001-9527-3391, slawomir.zurawski@onet.pl;*
[3]*Faculty of Economics, John Paul II Univerrsity of Applied Sciences in Biała Podlaska, Poland , ORCID: 0000-0002-0549-894X, zbigniew@ciekanowski.pl;*
[4]*Siedlce University of Natural Sciences and Humanities, Poland, ORCID: 0000-0002-2077-5124, y.pauliuchuk@wp.pl;*
[5]*Warsaw Management University, Poland,, ORCID ID: 0000-0003-1556-8371, jan.boguski@mans.org.pl;*

present a multidimensional issue of information security in the process of enterprise management.

Keywords: *Safety, enterprise, system, organisation, information, management.*
JEL: *D89, M10, M15.*

Paper type: *Research article.*

1. Introduction

We live in an era of changes hitherto unrecorded in human history. These changes bring forth specific effects. Individual enterprises find themselves entangled in the labyrinth of unpredictability and numerous intricacies. Each new discovery necessitates further exploration. Questions posed by humans generate more questions (Knight, 2006, p. 17). All of this engenders complexity, in which an increasing array of problems and challenges emerges, confronting contemporary enterprises (Thalassinos and Berezkinova, 2013).

Making decisions in difficult conditions characterised by prevailing uncertainty is more arduous than making them under conditions of heightened risk (Tyszka, 2010). The years 2020-2021 were exceedingly challenging for both entrepreneurs and the entire economy.

Presently, we are witnessing the increasingly frequent emergence of hitherto unprecedented conditions of significant global uncertainty worldwide. One such situation is the COVID-19 pandemic (Wolniak, 2022, p. 22). Never before in Poland had a lockdown been imposed, encompassing so many sectors of the economy. This action was a consequence of the declaration by the World Health Organization (WHO) on March 11, 2020, of a COVID-19 pandemic state caused by the SARS-CoV-2 coronavirus. In Poland as well, a state of epidemic threat was declared. In the initial period, the focus was primarily on medical issues related to countering the threat.

Despite the awareness of the negative impact of the pandemic on the economy, analysts predicted the introduction of restrictions on the freedom of conducting economic activity, and even its prohibition. Entrepreneurs, apart from the formal-legal consequences, also experienced the negative financial effects of the pandemic. The development of the modern world is inseparably linked to information and communication technologies. They provide a reliable, flexible, fast, and effective means of disseminating information.

The advancement of technology introduces new possibilities that offer the potential for dynamic growth. Teleinformation technologies have become a catalyst for socio-economic changes and undeniably have created new perspectives, thereby initiating a new era for business activities in Poland and around the world. Information

technology significantly influences the shaping of security and the functioning of enterprises, regardless of their field of operation.

2. Management of the Enterprise

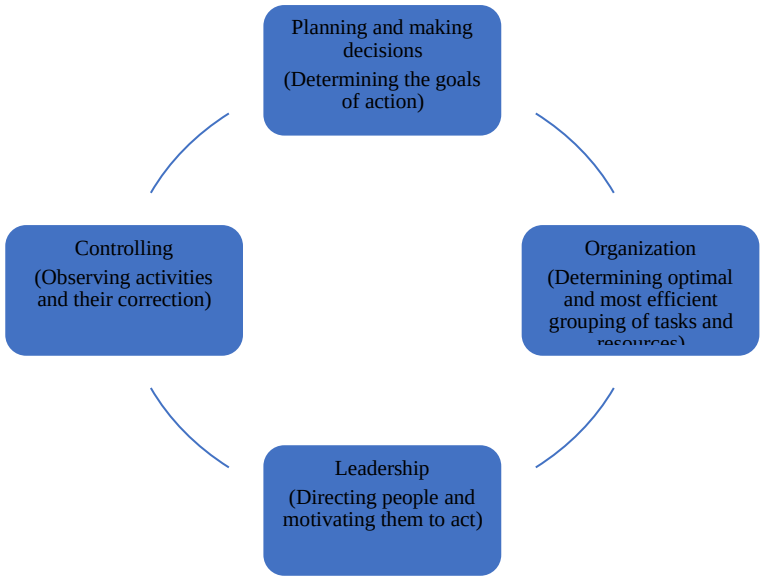
Global changes triggered by the pandemic imply the emergence of new existing risks in various areas of business functioning (Jedynak and Bąk, 2021). Organisation and management are considered a relatively new field of science (Ciekanowski, Majkowska, and Załoga, 2018, p. 46).

Managing a company is a process that operates in a loop, so to speak. The individual stages of this process repeat regularly. This allows for the introduction of minor but often significant and necessary adjustments and changes in each subsequent cycle, which impact various factors, including efficiency, the speed of company development, and its competitive advantage. Drucker defines "management" as a process that can be characterised by the following elements:

a) Management primarily relates to people. The key resource of any organisation is people, so managers should focus on maximising the potential inherent in employees;
b) Management is deeply rooted in culture. This is associated with the need to consider the values recognized by a given community, which create specific norms of behaviour;
c) Management demands clear and comprehensible values, goals, actions, and tasks that connect organisation participants. Although the role of organisational culture as a management tool is often underestimated, it can play a significant role in increasing the effectiveness of a company's actions;
d) Management should enable the organisation to have the ability to learn, and therefore, to adapt to changing environmental conditions;
e) Management requires the proper flow of information within the organisation as well as its exchange with the environment. Effective cultivation of relationships with the environment in which the organisation operates requires communication skills;
f) Management requires an extensive system of indicators that allow for the control, assessment, and improvement of effectiveness;
g) Management must be unequivocally oriented towards the fundamental and most important goal, which is a satisfied customer. In the current conditions of increasing competition, this is the only way to maintain and increase market share (Dołhasz, Fudaliński, Kosała, and Smutek, 2009, p. 46-47).

Contemporary methods of enterprise management encompass four key phases, which have been presented in Figure 1.

Figure 1. *Stages of the enterprise management process*



Source: *Own elaboration based on Griffin R.W., Podstawy zarządzania organizacjami, PWN Scientific Publishing House, 2004 Warsaw.*

Planning involves predicting future conditions, indicating the means through which set goals and tasks are to be achieved. Planning is an attempt to foresee the future and prepare for changes. As we move to lower levels, we increase the specificity and detail of planning while shortening its horizons (Dołhasz, Fudaliński, Kosała, and Smutek, 2009, p. 49).

Organising entails the selection of means and conditions of operation, as well as their arrangement in time. This function is referred to as the introduction of a specific order. Organizing aims to create a structure that allows for efficient and effective management of a particular organisation (Ibidem, p. 50).

Leading is a function that involves guiding and governing. The result of leadership is the action, thinking, or behaviour of subordinates in a specific manner (Michalski, 2013, p. 21).

Controlling involves establishing results and assessing the progress of actions. Controlling is a systematic activity aimed at comparing actual measures with set standards. Control is the regulation of organisational activities aimed at achieving set goals (Dołhasz, Fudaliński, Kosała, and Smutek, 2009, p. 53).

When organising activities in a company, a manager typically has four groups of resources at their disposal:

a) Human resources consist of employees and collaborators of a given company. The efficiency of the entire organisation largely depends on their competence, knowledge, skills, and their contribution to the work;
b) Financial resources are the means available to the company in the form of cash, deposits or bank accounts, loans, and others. With these resources, the company can undertake investments without jeopardising its financial liquidity;
c) Physical resources encompass all buildings, equipment, production machinery, vehicles, and electronic equipment owned by the company, and which can be utilised in its operations;
d) Informational resources denote unique knowledge that is recorded and codified, as well as the knowledge possessed by employees, patents, copyrights, customer databases, and established service standards (Kozak, 2014).

Management is a conscious, systematic process. This process should be conducted in accordance with applicable legal regulations by individuals who have been granted appropriate authority and assigned specific tasks that constitute a series of complex actions aimed at ensuring the proper functioning of the organisation and the achievement of designated goals (Bąk and Kapusta, 2015, p. 11).

3. Information Security Management System

We live in an information society where the symbol is the individual of information (Homo informaticus). This individual stands out with abilities that are essential for using new technologies effectively. Through knowledge and skills, they can utilise these technologies for the purpose of better information processing (Wątroba, 2006, p. 441-449; Do *et al.*, 2022).

In today's world, there is a continuous need for acquiring information, and consequently, the utilisation of modern information technologies. This element constitutes one of the main factors influencing the functioning of organisations, including enterprises. With the emergence of this factor, a new field in science has arisen: information management. It encompasses areas such as data management, planning information systems, and the analysis of information flow and circulation processes within an enterprise.

Information management is typically regarded as one of the functions of management with high strategic significance, as evidenced by the nature of information and its role in management processes. The characteristic features of today's organisations include:

a) the development of the information services sector,
b) semantic growth in information diversity,

c) an increase in the intensity of information streams, all while experiencing dynamic development in the diversity of information processes (Dulbiński, 2005, p. 1).

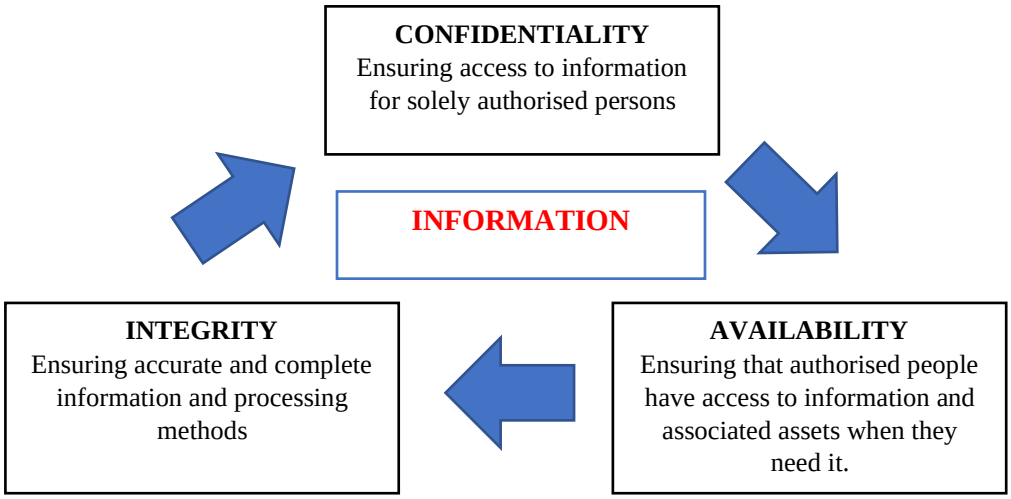
The primary task is to maintain a high level of security within the organisation (Żurawski, Załoga, and Ciekanowski, 2019, p. 318). The Information Security Management System (ISMS) is nothing more than an action strategy aimed at ensuring the appropriate protection of information. The goal of this strategy is to continuously improve the procedures and actions taken to minimise the risks associated with confidentiality breaches.

The information security system is intended to protect the organisation in such a way as to ensure:

a) the continuity of operations;
b) minimising losses;
c) maximisation of returns on investment and business-related activities.

The term (ISMS - Information Security Management System) is recognized as the most optimal and effective solution for ensuring the confidentiality and availability of information, the protection of which is currently the primary objective of organizations and an inevitable requirement facing us in contemporary times. A schematic representation of the Information Security Management System, incorporating its key functions, is presented in Figure 2.

Figure 2. *A schema of the information management system*



Source: *Information management system, https://lexdigital.pl/system-zarzadzania-bezpieczenstwem-informacji*

Actions related to information security management are inherently linked to the trust of the business owner in all actions undertaken and executed by individuals. The value of the enterprise can be measured by the intellectual and competency contributions of each member or all strategic members (Nowicka and Ciekanowski, 2019, p. 89).

The breadth of Polish law and adopted European Union commitments necessitate a good understanding of incidents, actions, and appropriate practices for this system to function effectively, along with the ability to instil trust in the organisation being conducted. Currently, it is not permissible to entrust the security of the enterprise to untrained individuals lacking awareness of existing threats.

A significant issue is the failure of "leaders" in organisations, including businesses, to consider emerging threats or trivialise their significance. The inability to recognize various types of threats may even affect experienced leaders (Marjański, Starczewski, and Ciekanowski, 2017, p. 296). Often, organisations struggle to define the threats they face within their enterprises, and the absence of this element can have irreversible consequences, potentially leading to the destruction of the business.

In the turbulent environment of business leadership, one can only speculate with a high degree of probability that a unique event may suddenly emerge, altering the existing situation. However, it is impossible to plan for such an event. To be effective, one must ensure the widest possible access to local, national, and international information (Drucker, 1995, p. 15).

4. The Impact of the COVID-19 Pandemic on the Utilisation of Information Technologies in Enterprises

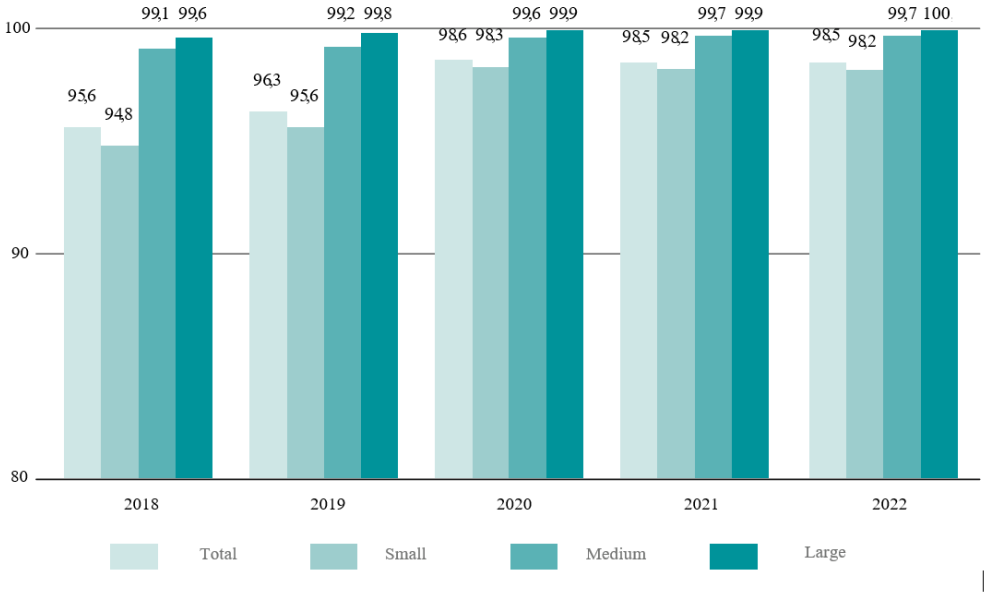
New technologies are employed in most, if not all, areas of enterprise operations and also have their role in various sectors of institutional activity. However, their implementation in many domains entails increased risks and various threats (Deloitte, 2020).

During the pandemic, due to the necessity of limiting direct human contact, new technologies played a crucial role in facilitating communication between enterprises and their business partners, customers, and especially among employees. Enterprises had to take on the risk associated with new ICT applications because it mitigated the more serious risk of coronavirus infection. In the event of infection, the level of effectiveness of employees working within the enterprise could significantly decrease and disrupt its operations to a significant extent.

Over the past few years, and especially in 2020, the importance of the Internet has significantly increased among individual users as well as among enterprises. There has been substantial progress both in Internet accessibility among corporate employees and in the possibilities for its utilisation.

Since the outbreak of the COVID-19 pandemic and the implementation of guidelines based on physical distancing and other restrictions, the number of enterprises with broadband Internet access has increased significantly both in Poland and in Europe. Figure 3 illustrates enterprises with broadband Internet access categorised by size classes over the years 2018-2022.

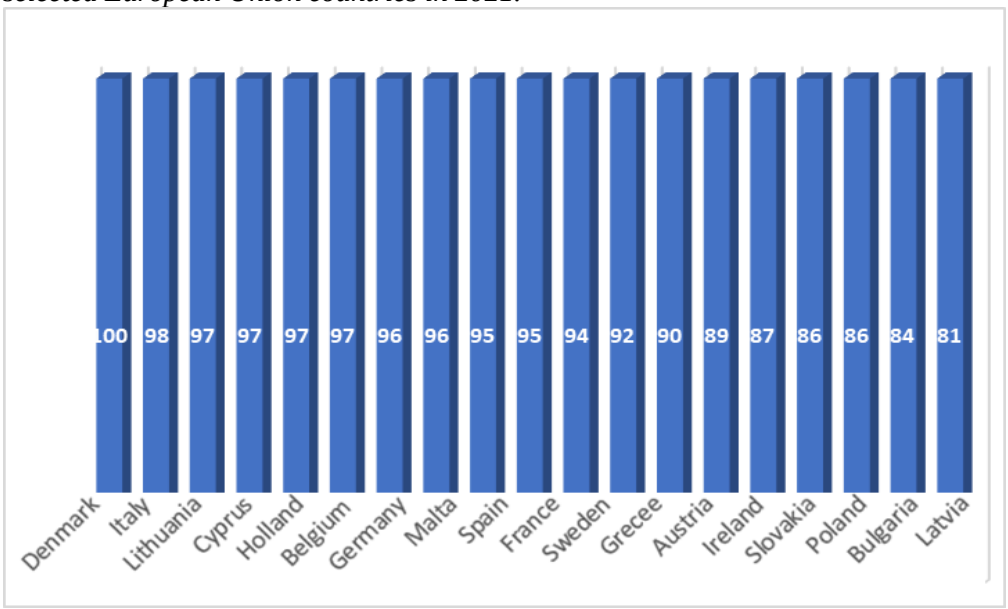
Figure 3. *Enterprises with Broadband Internet Access by Size Classes*



Source: *Informative society in Poland 2022, Central Statistical Office, https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/1/16/1/si_2022_003.pdf.*

In the years 2020-2022, the percentage of businesses with broadband internet access across the entire country exceeded 98%. This high level indicates the interest in the benefits of connecting to the global network. In 2022, in the majority of sections of the Polish Classification of Activities and Products (PKD), over 97% of businesses had access to the global network. Figure 4 shows businesses with access to the Internet via fixed broadband connections in selected European Union countries in 2021.

Figure 4. *Businesses with access to the Internet via fixed broadband connections in selected European Union countries in 2021.*



Source: *Informative society in Poland 2022, Central Statistical Office, https://stat.gov.pl/files/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/1/16/1/si_2022_003.pdf*

In 2022, the percentage of entities with broadband internet access exceeded 98%, with all surveyed large entities (employing 250 people or more) having it. The percentage of businesses equipping employees with portable devices for mobile internet access was 91.9%. More than two-thirds of businesses provided remote access to their resources for employees, and over one-third organised meetings via the Internet.

In 2021, in Poland, every second large business used open public data, with the most common data being related to the economy and finances (47.8%). The same group of entities most frequently used robots in 2022 (29.5%). In 2021, 15.1% of companies conducted online sales, with the majority of transactions being domestic.

In 2022, among businesses implementing ICT security measures, strong password authentication and data backup were the most commonly declared practices (82.0% and 68.3%, respectively). Businesses considering the environmental impact of ICT technology indicated that these issues were most important when choosing ICT hardware or services (64.1%) (Central Statistical Office, 2022).

Information and communication technologies are changing the modern world, and as a result, the way various organisations, including businesses, operate and function. They change how people communicate with each other, as well as with employers

and government agencies. The COVID-19 pandemic has brought significant changes to the functioning of businesses, with modern technologies playing a crucial role.

Faster communication and increased production efficiency have been achieved through the use of IT solutions. Table 1 presents data on businesses in which the utilisation of information and communication technologies increased in 2020 due to the COVID-19 pandemic.

Table 1. *Businesses in which the level of utilisation of information and communication technologies increased in 2020 due to the COVID-19 pandemic.*

Specification **a - number b - percentage**	**Total number of business enterprises**		**total**	Increase in percentage of employees with remote access to electronic mailbox of enterprise		Increase in the percentage of employees with remote access to application or systems of the enterprise different to electronic mail	
				Pandemic was the main reason for change	**Pandemic was not the reason for change**	**Pandemic was the main reason for change**	**Pandemic was not the reason for change**
Total	a	106537	35640	16338	2976	20196	1690
	b	100.0	33.5	15.3	2.8	19.0	1.6
Small	a	87066	22814	9787	2181	11433	1207
	b	100.0	26.2	11.2	2.5	13.1	1.4
Medium	a	15870	9597	4663	600	6267	394
	b	100.0	60.5	29.4	3.8	39.5	2.5
Large	a	3602	3224	1888	196	2499	90
	b	100.0	89.5	52.4	5.4	69.4	2.5

Source: *Own elaboration based on: Utilisation of information and communication technologies in enterprises in 2021, Central Statistical Office, https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-komunikacyjnych-w-jednostkach-administracji-publicznej-przedsiebiorstwach-i-gospodarstwach-domowych-w-2021-roku,3,20.html*

As the above statistics show, the number and percentage of employees with remote access to company email significantly increased, with the primary reason being the COVID-19 pandemic. The size of the company did not have an impact on this. Regardless of the number of employees, the growth of those with remote access to company email as well as those with remote access to applications or systems other than email also increased significantly. Table 2 illustrates the impact of Covid-19 on ICT utilization by business size class in the entire EU, as well as individual member countries, including Poland.

Table 2. *Influence of Covid-19 on the use of ICT according to the class of enterprise size*

	Increase in the percentage of employees with remote access to the business's electronic mail	No increase	Increase in the number of employees with remote access to applications or business systems other to that of electronic mail	No increase
The EU	32,8	54,9	32,7	54
The Euro zone	36,7	53,5	35,8	53,2
Belgium	39,7	44,9	43,5	40,1
Bulgaria	17,2	52,4	14,7	51,2
Denmark	18,6	65,4	23,2	61,7
Germany	41,7	45,7	38,7	46,9
Italy	30,8	67,9	32,6	65,9
Cyprus	35,7	53,6	33,1	54,6
Latvia	20,6	79,4	19,4	80,6
Lithuania	11,8	56,1	11,7	56,1
Luxemburg	33,4	43,5	31,7	41,7
Hungary	16,9	76,6	16,4	77,1
Malta	55,5	42	57,6	39,9
The Netherlands	42,2	57,8	42,4	57,6
Austria	38,2	43,4	37,5	44
Poland	18,1	58,2	20,6	54,3

Source: Eurostat, https://ec.europa.eu/eurostat/databrowser/view/isoc_e_cvd/default/table?lang=en

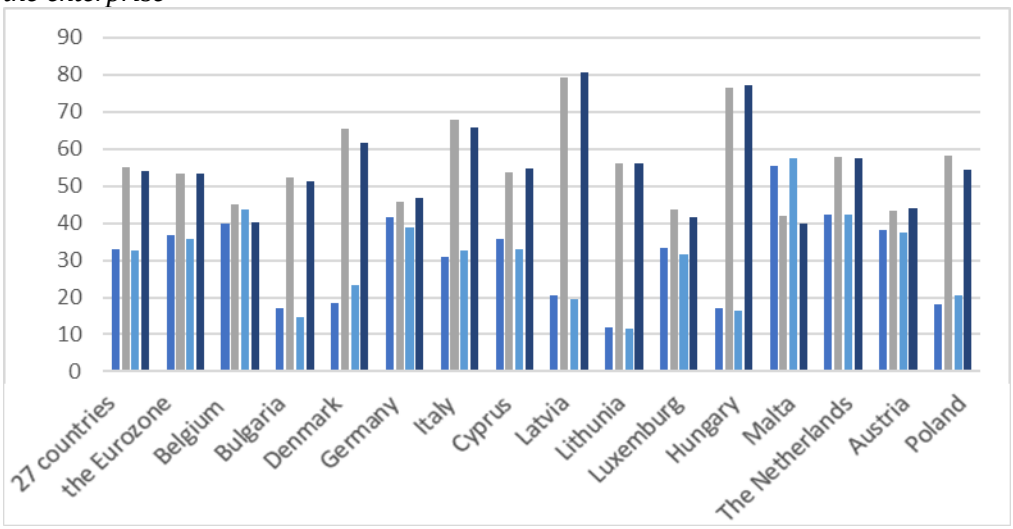
Data from Table 2 is presented in the Figure 5 below.

Both in Poland and in other EU countries, the impact of the COVID-19 pandemic on the use of information technologies in enterprises is significant. In 2020, 33% of EU enterprises increased the proportion of employees with remote access to the company's email system, and the same percentage (33%) increased the percentage of employees with remote access to other ICT systems.

Among EU member states that have available data (collected voluntarily, with participation from 19 member states), Malta recorded the highest percentages of enterprises that increased the percentage of employees with remote access to the company's email system (55%) or other teleinformatics systems (58%), followed by the Netherlands (42%), Germany (42% and 39% respectively), and Belgium (40% and 43% respectively). Conversely, the lowest percentage of enterprises that

increased remote access to their email (12%) or other teleinformatics systems (12%) was observed in Lithuania.

Figure 5. *Influence of Covid-19 on the use of ICT according to size classification of the enterprise*



Source: *Eurostat, https://ec.europa.eu/eurostat/databrowser/view/isoc_e_cvd/default/table?lang=en*

As demonstrated by the above analysis, mobility restrictions due to the COVID-19 pandemic compelled many enterprises to increase or even transition to digital technologies to sustain their operations (Eurostat, 2022). A substantial portion of enterprises experienced the long-term effects of the pandemic as a manifestation of materialising specific strategic risks (He and Harris, 2020).

In this regard, research was conducted by various institutions worldwide, including Harvard Business University, which conducted a study on a sample of 21,000 firms from around the world. The main findings from the research include a 12.9% increase in the number of online meetings and a 13.5% increase in the number of participants, with an average meeting duration shortened by 20.1%.

Additionally, the average daily user work hours extended by 8.2%, and there was an 8.3% increase in email intensity beyond regular working hours (DeFilippis, Impink, and Dago, 2021). Therefore, information security is a crucial element of organisational functioning, and an effective information security management system is the means to ensure it (Łuczak, 2009, p. 70).

5. Conclusions

The integration of management systems within an enterprise is a complex process that should be considered from various aspects. The diversity of areas within

management systems, including information security, should aim for synergy. It is difficult to imagine a modern enterprise functioning in a constantly changing environment without the use of cutting-edge technologies. The latest technologies serve as a means to achieve the company's development and gain a competitive edge.

With the advancement of new technologies, new threats related to information security also emerge rapidly in a positive sense. In today's organisations, every aspect relies on the flow of processed information. Unauthorised access to this information poses a significant threat to its operations.

Effective protection is one of the elements of a properly functioning and operating enterprise. The emergence of COVID-19 and its rapid global spread initiated and forced many organisations to change their structures and directions towards digitalization and increasing resilience to cyber threats. These changes led to new regulations introduced by decision-makers to combat the pandemic.

Therefore, it becomes necessary to ensure an appropriate level of security for both private and public organisations. Without taking appropriate measures to reduce the level of risk, disruptions in their operations can occur, resulting not only in decreased efficiency and temporary interruptions but even in the complete cessation of their activities. In response to the research problem posed, "What impact did the COVID-19 pandemic have on the utilisation of information technologies in enterprises?" It must be stated that the COVID-19 pandemic had a significant impact on the use of information technologies in enterprises, their functioning, and planned actions.

References:

Bąk, P., Kapusta, M. 2015. Rola bezpieczeństwa w zarządzaniu przedsiębiorstwem, nr 74, t. 2, 11-19. Zeszyty Naukowe Uniwersytety Szczecińskiego nr 855. Finanse, Rynki Finansowe, Ubezpieczenia.

Ciekanowski, Z., Majkowska, J., Załoga, W. 2018. Wpływ otoczenia na funkcjonowanie organizacji, Zeszyt 13, nr 4, 45-58. Nowoczesne Systemy Zarządzania.

DeFilippis, E., Impink, S., Dago, S. 2021. Collaborating During Coronavirus: The Impact of COVID-19 on the Nature of Work. Harvard Business School Organizational Behavior Unit, Working Paper No. 21-006.

Do, T.D., Pham, H.A.T., Thalassinos, E.I., Le, H.A. 2022. The impact of digital transformation on performance: Evidence from Vietnamese commercial banks. Journal of risk and financial management, 15(1), 21.

Dołhasz, M., Fudaliński, J., Kosała, M., Smutek, H. 2009. Podstawy Zarządzania. Wydawnictwo Naukowe PWN, Warszawa.

Drucker, F.P. 1995. Zarządzanie w czasach burzliwych, Nowoczesność. Akademia Ekonomiczna w Krakowie, Kraków.

Dulbiński, A. 2005. Zarządzanie bezpieczeństwem informacji w przedsiębiorstwie. Wydawnictwa Naukowo – Techniczne, Warszawa.

Griffin, R.W. 2004. Podstawy zarządzania organizacjami. Wydawnictwo Naukowe PWN, Warszawa.

He, H., Harris, L. 2020. The impact of COVID-19 pandemic on corporate social responsibility and marketing philosophy. Journal of Business Research 116, 176-182.

Jedynak, P., Bąk, S. 2021. Risk Management in Crisis: Winners and Losers during the COVID- 19 Pandemic. Routledge, London, New York.

Łuczak, J. 2009. Metody szacowania ryzyka – kluczowy element systemu zarządzania bezpieczeństwem informacji ISO/IEC 27001, 19(91), 63-70. Zeszyty Naukowe Akademia Morska w Szczecinie.

Kasprzak, A. 2022. System zarządzania bezpieczeństwem informacji. https://lexdigital.pl/system-zarzadzania-bezpieczenstwem-informacji.

Knight, S. 2006. NLP w biznesie. Techniki skutecznego przekonywania. Wydawnictwo Helion, Gliwice.

Kozak, P. 2014. Jak skutecznie zarządzać przedsiębiorstwem. https://edufin.pl/jak-skutecznie-zarzadzac-przedsiebiorstwem.

Marjański, A., Starczewski, J., Ciekanowski, Z. 2017. Planowanie i organizacja działań przedsiębiorstwa w sytuacjach kryzysowych, T. XIII, Z. 5, Cz. III, 291-313. Przedsiębiorczość i zarządzanie, Wydawnictwo SAN.

Michalski, E. 2013. Zarządzanie przedsiębiorstwem. Wydawnictwo Naukowe PWN, Warszawa.

Nowicka, J., Ciekanowski, M. 2019. Kapitał ludzki we współczesnej organizacji. Zeszyt 14, nr 1, 79-90. Nowoczesne Systemy Zarządzania.

Ograniczenia związane z COVID zwiększyły wykorzystanie ICT w przedsiębiorstwach, Eurostat. https://ec.europa.eu/eurostat/en/web/products-eurostat-news/-/ddn-20220329-1.

Thalassinos, E., Berezkinova, L. 2013. Innovation Management and Controlling in SMEs. European Research Studies Journal, 16(4), 57-70.

Tyszka, T. 2010. Decyzje. Perspektywa psychologiczna i ekonomiczna. Scholar, Warszawa.

Wątroba, W. 2006. Homo informaticus w globalnym supermarkecie. In: Społeczeństwo informacyjne: aspekty funkcjonalne i dysfunkcjonalne, red. L.H. Haber, M. Niezgoda, Wyd. Uniwersytetu Jagiellońskiego, Kraków, 441-449. Cytuję za: A. Dąbrowska, M.Janoś-Kresło, A.Wódkowski, E-usługi a społeczeństwo informacyjne, Difin, Warszawa.

Wolniak, R. 2022. Wpływ pandemii COVID-19 na zarządzanie. 1(18)/2022, 21-32, Zeszyty Naukowe Wyższej Szkoły Zarządzania Ochroną Pracy w Katowicach.

Wykorzystywanie technologii informacyjno-komunikacyjnych w przedsiębiorstwach w 2021 r., Główny Urząd Statystyczny. https://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/spoleczenstwo-informacyjne/wykorzystanie-technologii-informacyjno-komunikacyjnych-w-jednostkach-administracji-publicznej-przedsiebiorstwach-i-gospodarstwach-domowych-w-2021-roku,3,20.html.

Wpływ cyfryzacji i pandemii COVID-19 na bezpieczeństwo cybernetyczne w instytucjach finansowych. 2020. https://www2.deloitte.com/pl/pl/pages/financial-services/articles/wplyw-cyfryzacji-bezpieczenstwo-cybernetyczne-instytucje-finansowe-covid-pandemia.html.

Żurawski, S., Załoga, W., Ciekanowski, Z. 2019. Wpływ sytuacji kryzysowej na zarządzanie bezpieczeństwem w organizacji. Rok XII, 2(43), 53-67. Przegląd naukowo-metodyczny. Edukacja dla bezpieczeństwa.