Journal of Research and Innovation for Sustainable Society (JRISS)
Volume 6, Issue 2, 2024
ISSN: 2668-0416
Thoth Publishing House

DOI: 10.33727/JRISS.2024.2.29:263-272

AGILE APPROACHES, FOR E-BUSINESS SOLUTIONS STRATEGY, AT THE GOVERNMENT LEVEL

Cristian Brancu [1], Oana Turcu[2], Marius Stefan[3] and Madalina Popp[4]

[1234] Bucharest University of Economic Studies, Romania

Email: cristibrancu2018@gmail.com; ardesbio@gmail.com; marius.stefan@mfe.gov.ro; madalinarusu13@yahoo.com

Abstract.
Modernity is characterized by major transformations and evolutions, which have penetrated into the depths of all levels of human existence, in all economic, political and social spheres, thus significantly increasing the quality of life. The Information Society is the model of society in which the main good is information itself. Although the accelerated development of information and communication technologies (ICT) is the process behind the evolution of the information society, the new model of society means much more than technological progress. In the technological age, action plans and policies are being developed to meet the challenges, the most important technology being ICT, which allows information to be processed and conveyed in a revolutionary way. The information society is the ICT-based knowledge society. Information society technologies will evolve in the direction of being at the fingertips of the knowledge process, by generating, storing, and transmitting knowledge. Knowledge is the result of the information management process, thus promoting innovation, economic development, and decision-making in an efficient and transparent way. Knowledge and scientific information are of enormous importance in the global information society, by: supporting innovation, promoting economic development, making decisions in an efficient and transparent way, at the governmental level and especially for the implementation and use of intelligent technologies in the development of the degree of digitization of public services through financing provided by European funds and the National Recovery and Resilience Plan. In order to move on to building the knowledge society, it is necessary to reduce the digital gap, which accentuates disparities in development, excluding groups and even countries, from the benefit of information and knowledge. The limiting factor in development will be related to the human capacity to assimilate and develop these technologies, to use them in new fields of activity, for new products and services

Keywords: *intelligent technologies; e-business; digital transformation; awareness, developmental state, economic development, growth, innovation..*

Introduction

E-business is the basis of the new economy, of an information society that catalyzes the future of an increasingly secure artificial intelligence for the development and use of new technologies of the future. The fracture between e-Services vs. e-Activities in the post-pandemic context is evidence of the

emerging strategy, which will generate various opportunities for the ever-changing business environment: e-Applications (e-learning, e-working, e-banking, e-Services, e-Activities, teleworking), basic services (e-mail, file transfer, Virtual Private Network), telecommunication networks (telephone lines, cable, radio, satellite, 4G, 5G, 6G), emerging technologies adoptable to the e-Business sector (IoT, EoT, Cloud, Fog).

The technological infrastructure of the new economy, in constant need of ensuring all the principles related to cyber security, generates new e-business models, from e-commerce to the desideratum of the e-Government implementation strategy, through digitalization and computerization of public administration in Romania.

Electronic applications made because of the efficient management of European funds are a national interest, to achieve the goal of the positive evolution of the national economy, with critical values for achieving the balance of the rule of law and national security.

The impact of eBusiness on natural resources and production factors draws attention to the efficient use of resources, which has become a business imperative and an essential component of Romania's national recovery and resilience plan. More efficient use of resources can be a major factor in economic growth. The field of European funds is constantly changing as well as the IT applications intended for their management, representing the first attempts at computerization and innovation in public administration. They are a new way of developing the national economy and e-business by promoting and pursuing European policies: distance learning (e-learning), remote work (e-working), electronic commerce (e-commerce), electronic banking services (e-banking), electronic government (e-government), electronic health services (e-health).

In an information society in which the quality of life, as well as the prospects for social change and economic development, depend to a greater extent on information and its exploitation, the institutional field of management of IT applications for European funds becomes a matter of national importance, with critical values for national security. Reinventing government can be achieved through digitalization and government computerization, which involves modernizing the current IT infrastructure through specific external funding sources such as European funds, doubled and secured by advanced cyber protection and defense capabilities against possible vulnerabilities or cyber attacks.

Modern administrations have as priorities the development of services for citizens, the provision of quality information (consistent and current), in forms as accessible as possible to any citizen regardless of the level of education. At the same time, the aim is to create the necessary tools, the active participation of any citizen, in the administrative and political decisions that concern him. The act of governing should be seen as a business process, the main objective of which should be to diversify and improve the quality of services to citizens. For a reinvention of government in the information society, at least four defining concepts have emerged - e-democracy, e-citizen, e-politics, e-state:

- Electronic democracy - the internet can strengthen democratic participation in government.
- The citizen of the information society - the citizens of the new society / young people have training in modern technological fields being the key actors of the future governments.
- Politics in the digital age - attempts to manifest politics in digital form are becoming more visible through the significant increase in online election campaigns.
- The electronic state - the phenomenon of globalization fueled by the digital integration of markets, involves rethinking and redefining the concept of nation-state.

E-Business solutions strategy at the government level

The development of e-Business solutions, through financing with European funds, can be the main direction of restoring the economic balance, lost as a result of events such as the CO-VID pandemic, or the marked negative effects in all existing essential plans of the modern individual. shaping a 5th generation war, of an informational type specific to the knowledge society. Because the effects of using advanced technologies include negative aspects and threats even on national security. That is why any development of electronic tools that will generate evolution in the process of digitalization and automation, implies the provision of the cyber defense component.

Through the projects financed from European funds, starting with 2014, a national cyber defense network was developed, of the critical infrastructure type of national interest, comprising most of the key institutions of the state. The use of Emerging Technologies and the improvement of cyber threat prevention activities in MIPE, will result in the evolution in financial management and implicitly the operational efficiency.

In Romania, the evolution of cyber infrastructure for European funds is conditioned by inter-institutional cooperation, carried out in the form of strategies, harmonized with European legislation, and materialized through specific projects to ensure cyber security, as well as awareness of the importance of security at the entire state apparatus.

All state institutions will be included in this national system of prevention and protection against cyber-attacks. Desirable and achievable activities in the context of the transition to the Government Cloud and achieving interoperability, through the considerable contribution of cooperation with state institutions, specialized in ensuring cyber security, such as Cyber-int National Center - National Authority in Cyber - Intelligence.

Malfunctioning or inadequate parameters of applications for European funds, integrated in the related cyber infrastructure, will generate the state of vulnerability constituted by blockages of the mechanisms of registration and increase of the absorption of European funds.

The decrease in the absorption of European funds is and will be a real threat to Romania's national security, due to the implications: economic; financial; social; political; as well as because of Romania's obligations as a member of the European Union.

In any situation of blockage in this sensitive area of European funds, the information for national security will be dominated by the need to capitalize by immediately informing the Minister of European Investments and Projects, as well as by adopting the necessary measures to eliminate the deficiencies found. Thus, avoiding the threats of disengagement risks, through an efficient management of European funds, in the conditions of the desideratum of good management of this objective of national strategic interest.

Achieving the country's interests, as well as acts of destruction, degradation or rendering in disuse the structures necessary for the proper conduct of socio-economic life - can be a threat - even by generating a state of blocking the absorption of European funds, a situation that falls into the provisions of Chapter 3, related to the National Strategy for National Defense 2015-2019 and art. 3, letter f, Law 51/91.

Identifying and capitalizing on these possible risks is information for national security, which will be achieved gradually, due to a high degree of persistence, as well as the perpetual lack of sufficient and efficient resources, endowed with the necessary specialization in the correct management of the computer system. constantly evolving, with more emphasis on results and efficiency and the creation of public values, including at the level of critical infrastructure - national cybernetics, in this newly developed branch of the economy - the field of European funds.

A beneficial approach would be, to adopt a risk prevention strategy at the governmental level. The malfunctioning of the gear behind the fundraising will damage both the national budget and the image of the European level, with interoperability being a basic principle of the Member States. Failure to comply with the obligations assumed as a Member State may cause economic disadvantages, the development of society and the increase in the quality of life depending on developments in the management of current financial resources, as well as future membership of the European Union and specific financial years.

These data of national interest have an impact in the current year, when cyber-attacks are characterized by frequency and persistence, it is vital that organizations are armed with the most effective security tools and knowledge to prevent, detect and respond. to cyber threats. Vulnerabilities will always escalate into possible future threats and risks to national security, with the most effective approach being awareness and prevention.

A large-scale computer application goes through several states, transforms and even reinvents itself, if necessary, while ensuring the principles of continuity, operation, efficiency but especially

cybersecurity, in the future characterized by the automation of as many processes now undertaken by human intervention.

Including the interoperability requirements in relation to the European Commission, dictates a clear focus on functional and reliable reporting processes, increasing processing of documents in electronic format, signed with digital certificates. Concentration of resources can only provide solutions in safe operating conditions, provided only by a state of cyber security.

Legislation, including harmonization with European provisions, may be a vulnerability in the proper functioning of the business, in the context of increasing EU interoperability requirements request for related services costly for current technology used - EIF, part of Communication (COM (2017) 134)).

The attack on a critical cyber infrastructure of national interest, such as that of European funds, may occur because of security risks, which are not properly treated, resulting in data leaks, exfiltration, or by causing syncope in operation due to unforeseen disruptions induced services, in particular on electricity and internet services.

Long-term trends are the main threats that should be monitored, especially malware attacks in a Government Institution such as the Ministry of European Investments and Projects, which is an area of real interest for cybercrime groups, for the purpose of cyber espionage or theft of strategic information, such as that of the state:

- Malware, in particular: ransomware, worms and trojans.
- Social Engineering, in particular: Identity theft, Fishing, Hacking.

Since 2016, the government area has been at the forefront of data leaks. The ways are diversified, from the sale of credentials in the case of data encryption to the specific AI techniques and the tendency to use in any field of new information technologies, which have allowed the increase in the complexity of hacking attacks.

A common case for public sector reasons, in terms of modernization strategies through public procurement, is that of equipment failure outside the support / warranty period, thus posing a threat to the network topology.

Expiration of security equipment support is a serious issue in the operation of the IT system parameters, as it leads to a serious breach in the security umbrella created by the specific equipment, continuously managed and which should contain the latest updates to be truly effective, in the cyber fight against increasingly complex and persistent attacks.

Poor technology, also manifested in uninteresting trends in continuous modernization, affects the limits of processing in the evolution of servers, especially in the case of increasing the need for balancing at the application level and / or saving and restoring data.

Although data generated and processed automatically is an important pillar of public sector activity, the focus on electronic data assurance policy still does not enjoy a high degree of importance in public institutions due to the perpetual intermediate stage, computerization of public administration.

Awareness of the importance of the Security area, especially among specialized personnel and intended for ICT activities, requires preparation for combating the risks that the public institution will face, starting from the software components maintained up to date in terms of security, and even avoiding in periods technological or governance changes, situations such as the loss or lack of management credentials / access to work environments created by electronic tools. Often the political changes of management in the institutional framework are also reflected in the specific activities of the technical departments, by slowing down the decision-making process, which is not a good institutional practice, especially in the case of ensuring cyber security.

Failure to comply with the procedures for access to and security of data and documents in the public institution, as well as the preservation of obsolete and morally worn equipment or technology, creates a favorable environment for the incidence of security risks, including at cyber level. To align with new trends in cybersecurity and harmonize Community legislation, standards such as information security management (ISO 27001) and business continuity management (ISO / IEC 27031: 2011, 22301: 2012) will be considered. as well as the latest directions drawn by NIS - EU Directive 1148/2016.

Progress in the development of new technologies will establish the desire to align with the new standards of the future, new solutions such as private or hybrid cloud will be adopted and at the governmental level, in terms of budget efficiency, but especially for specific reasons. cyber security. Clear and swift measures are used to address any cyber security breaches identified in the organization through the proper and responsible use of the vulnerability scanning IT component - with capabilities to propose corrective measures for ICT security. The analytical capitalization of information as evidence of virtual activity in the organization, is achieved through the management of technologies specific to the field of artificial intelligence, complementing the specific human cognition through additional learning methods generated by computing power.

The budget allocated to innovation in public administration will create and maintain the much-desired stability, especially in critical national areas, such as ensuring the absorption of European funds. In industry and the economy, the role of robotics and process automation will grow considerably, with technology-related changes bringing both benefits and vulnerabilities, particularly in cyber terms. A virtual parallel world will be created, in which the existence of the state, with all that it represents, must be protected, so that the environment is safe and secure, including for the individual. The consequences of competition in innovation produce major transformations including in society, simplifying the complex life of modern man, in the information society.

They will crystallize into a national interest for the Government Strategy, areas such as attracting European funds and ensuring cyber security, with the aim of modernizing, computerizing and digitizing the public administration in Romania. The inclusion of interoperability requirements in relation to the European Commission requires a clear focus on functional and reliable reporting processes, with results such as increased processing of documents in electronic format, signed with digital certificates. The concentration of resources can only provide solutions under safe operating conditions, ensured only by a state of cyber security

Literature review

Security is a priority, through specific European programs the capacity of operational cooperation is strengthened, with a desire for consensus on the values that underpin the EU's internal security. Mutual trust and the exchange of information will increase the preventive nature of the actions of the authorities, thus establishing the Standing Committee on Operational Cooperation in Internal Security, at national and EU level.

The system is a set of principles, rules, forces, which form an organized whole, which aims to put order in a field of theoretical thinking, regulating the classification of material in a field of science or making a practical activity work properly. the purpose pursued by complying with a set of rules and values. The state is outlined, as a way of ensuring the political existence, by the established order and the development of the community, the defense and guarantee of the territorial integrity as well as of its autonomy.

National security is that state of balance, legality, economic, social, and political stability which guarantees the existence and development of the sovereign, unitary, indivisible, independent state, through order, rights, and civil liberties. National security leads to the realization of constantly evolving values, guided by constitutional-democratic principles. The national interest becoming a fundamental thesis in the applied foreign policy. Security policy is represented in the long-term organization and ensuring security change and innovation. Security strategies, thus succeeding in adopting measures that counteract, threats that evade the state of security.

A strong nation is built on common norms and values, goals and aspirations, of paramount importance to individual interests. Citizen protection is a vision, an integral and important part of the National Strategy for National Defense. Information and communication technology have a complex impact not only on the economy and its efficiency but also on all aspects of people's lives. For a reinvention of governance in the information society, the following concepts have been identified that should be met:

- increase the state's capacity to absorb European funds using new technologies.
- increase the capacity of government administrations in public policy, both at national and European level.
- e-democracy - the internet can increase democratic participation in government, the citizen of the information society is active.
- the electronic citizen - the citizens of the new society / young people are attracted in the modern technological fields being the key actors of the future governments, the politics in the digital age is in continuous transformation.
- politics in electronic format - the manifestation of politics in digital form is becoming more visible through the significant increase of online election campaigns, the electronic state, and behavioral patterns.
- the electronic state - in the phenomenon of globalization fueled by the digital integration of the markets of the new economy, it will be desired to rethink and redefine the concept of nation-state.

Thus, increasing the chance of creativity and innovation, by profoundly transforming the behaviors and profiles of citizens, from the reactive to the proactive. In the current geopolitical conditions and considering the possible cyber effects generated by the informational component of the current global state of war, it is necessary to ensure the cyber security component by using emerging machine learning technologies, cloud scanning features and sandbox analyzer to detect malicious activity that evades traditional endpoint attack prevention mechanisms.
Threat visualization features enable focus on specific aspects of investigations, helping to understand complex detections, and identify the root cause of attacks, thus maximizing immediate response capability. The integrated central console provides automated alert prioritization with one-click remediation functions. It will thus achieve continuous analysis within the organization, using unique capabilities to identify risk based on hundreds of factors. Providing clear guidance for mitigating potential risks at the user, network and operating system levels.

Methodology

The research was carried out at the level of the Ministry of Investments and European Projects, with the main aim of creating scientific and technological excellence by analyzing the results obtained through the use of intelligent technologies at the central administration level, as well as obtaining advantages in the field of cyber security and resilience of systems, services and critical infrastructure of national importance, as well as increasing the degree of cyber security culture in the central public administration and among contractual users or civil servants.

The period included in the analysis activity is between the years 2013-2024, including two programming periods of non-refundable financing from European funds, facilitated by the European Commission, as well as the National Recovery and Resilience Plan.

The three projects carried out by the Cyber-int National Center, to ensure cyber security at the national level, constituting a security umbrella, over the critical infrastructure of national interest, which will be reinvented through the digital transformation generated with the help of emerging technologies, which have produced an evolution considerable in government digital transformation.

Emerging technologies and the integration of machine learning functionalities through artificial intelligence, at the level of the Ministry of Investments and European Projects, as a development measure through innovation, will produce positive effects including on the development of the national economy by increasing the absorption of European funds in a secure cyber environment.

Results and discussions

The decisive step in the use of emerging technologies through the integration of Machine Learning and Artificial Intelligence functionalities, at the level of the Ministry of Investments and European Projects, was made within the projects financed from non-reimbursable funds, as a measure of the development

through innovation, of a critical infrastructure of national interest, through -a cooperation agreement with the National Authority in the field of Cyber-intelligence - the National Cyberint Center - within the Romanian Information Service.

The result is potential threat prevention, deep visibility, accurate incident detection, and intelligent response to minimize infection exposure and stop unauthorized attacker access.As an integrated workstation protection package, the integrated device security management platform ensures a uniform level of security across MIPE's IT environment, so that attackers cannot find a weakly protected workstation to use as an entry point for dangerous actions against the organization. The security equipment used within the organization offers advanced management capabilities to prevent, detect and investigate cyber security incidents, by analyzing the risks generated by possible attacks, as well as timely automatic remediation of threats. Increasing awareness of the importance of ensuring cyber security will be achieved by informing users, making the first measure of protection against cyber-attacks within the organization. Human error can be avoided through e-learning and the implementation of the security assurance component starting from the individual level.

These aspects implemented in the organization will counter the attacks of hackers, by ensuring regular information activities regarding good practices through constantly sent emails, organization of courses and training, eliminating the possibility of subsequent, much more serious problems, especially regarding the information and data belonging to the central administration.

The public administration will evolve towards a different approach to the use of emerging technologies, translating into future strategies, the need to use solutions in cloud, on-premises or hybrid cloud environments, depending on budgets and available advantages or disadvantages, fulfilling a strategy of innovation and development of digitization processes by using the funds related to the National Recovery and Resilience Plan. Agile approaches can be used to develop E-business solutions at the government level by breaking the development process into smaller, manageable chunks, testing and continuously iterating the solution, involving stakeholders throughout the development process, and adapting to changing requirements.

To implement agile project management skills in a government organization, the following steps can be taken:

1. Educate organization management and stakeholders on agile methodologies and their benefits.
2. Identifying projects that can benefit from an agile approach and creating cross-functional teams to work together.
3. Develop an agile project management framework that aligns with the organization's goals and objectives.
4. Defining project goals and objectives and prioritizing work based on value and impact.
5. Using agile methods such as sprints, stand-up meetings and retrospectives to manage projects.
6. Fostering a culture of collaboration, feedback and continuous improvement.
7. Ensuring that the project management team has the necessary skills and training to effectively apply agile methodologies.
8. Monitor project progress and adapt approach as needed.

Thus the implementation of Kanban in Jira at the government level can be achieved for better project management. Agile approaches such as Kanban and Jira can be used to support the implementation of agile methodologies in emerging technology implementation and software development projects. Kanban is a visual tool that allows teams to manage their workflow by visualizing and optimizing their workflow. It provides a transparent and collaborative way to manage tasks, prioritize work and improve efficiency by identifying bottlenecks and reducing waste.

Jira, on the other hand, is a project management tool that supports agile methodologies like Scrum and Kanban. It provides a platform for managing tasks, tracking progress and collaborating with team members. Jira also provides features such as sprint planning, backlog management, and agile reporting that can facilitate the implementation of agile methodologies. By using Kanban and Jira in conjunction with agile methodologies, teams can improve productivity and increase transparency. By following

these steps, a government organization can successfully implement Kanban in Jira for better projects coordination. Agile project management focuses on continuous releases and incorporates customer feedback at each iteration. Software teams that adopt agile project management methodologies increase their development speed, expand collaboration, and promote the ability to better respond to market trends. Using such methods, agile project management practices will be perfected. Nowadays, Kanban has been defined as a complete flow management solution designed to help us visualize work, maximize efficiency and be agile.

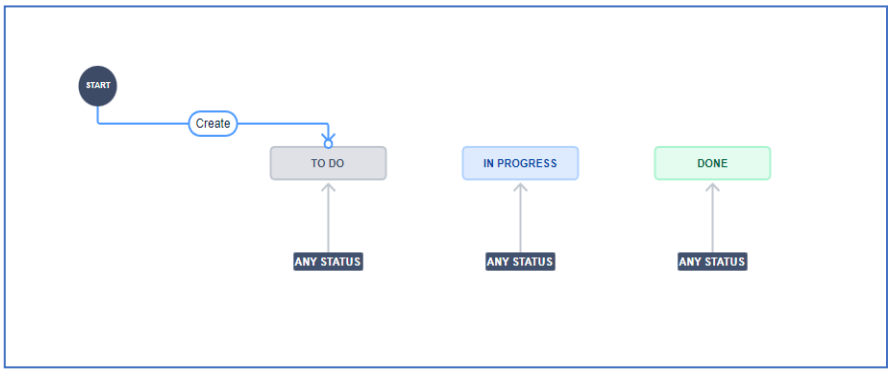
Kanban focuses on ensuring steady flow efficiency and getting things done continuously, rather than starting new work all the time. The basics of the method can be divided into two sets of Kanban principles and six practices. The integration of machine learning and artificial intelligence functionalities, at the level of the Ministry of Investments and European Projects, can be seen in Tables 1 below, while the Flow construction stages – JIRA Platform – Kanban Methodology can be seen in Figure 1 below.

Table 1. Integrating Machine Learning and Artificial Intelligence functionalities, at the level of the Ministry of European Investments and Projects

Implementation period	Protected workstations	Increasing the degree of cyber protection	Automate responses to detected and remedied cyber attacks	Fixed vulnerabilities	Possible security risks
2013-2017	250 to 450	200 Endpoints	About 50%	75%	25%
2020-2023	450 to 1700	1250 Endpoints	About 75%	90%	10%
2023-2027	1700 to 3400	3400 Endpoints	About 95%	95%	5%

Source: Author' own research

Figure 1. Flow construction stages – JIRA Platform – Kanban Methodology – Ministry of European Investments and Projects



Source: Ministry of European Investments and Projects

Conclusions

The unified and integrated technologies offer a measurable advantage in obtaining more efficient results, benefiting from unique management consoles and tools adapted to the level of expertise held in the organization, completed with the cyber security strategies built by the Cyber Security department of the Ministry of Investments and European Projects. The budget allocated to innovation in public administration, through specific European funding programs, will create and maintain the necessary stability, especially in critical areas of the national economy, such as the absorption of European funds.

The economy and society will undergo transformations, the role of robotics in industry and the automation of repetitive processes in organizations will increase considerably. The revolution of emerging technologies brings both benefits and vulnerabilities, threats and risks, especially in cyberspace, regarding the need to ensure cyber defense. By reinventing governance and computerizing public administration, a parallel virtual world will be created, in which the existence of the state, with the balance of the necessary security state, must be protected, so that the cyber environment is safe and secure even for the citizens. The repercussions of competition in innovation produce major transformations through interoperability and synergy, including in society, simplifying the crowded life of modern man in the era of the information society.

Strategic areas such as the attraction and absorption of European funds, by ensuring cyber security, aiming at the modernization and computerization of the public administration in Romania, constituting a national interest for the government's evolution in innovation. Creating a global framework of security and trust in ICT, with an expansive trend towards automating repetitive processes, will generate the achievement of optimal efficiency. These strategic objectives aim at the creation of scientific and technological excellence, obtaining advantages in innovation through the security and resilience of systems, services and critical infrastructure of national importance, as well as increasing the degree of cyber security culture among officials in the central public administration.

An important stage will be achieved in the inter-institutional collaboration, for the achievement of the fundamental objectives of the country strategy, the field of funds becoming a critical infrastructure of national interest, through the inherent implications generated in the national economy, all important plans of the current modern society being affected, from the financial - up to economic, social-educational, even political, with all the necessary risks assumed through the decisions applied at the level of future strategies. The efficient management of the infrastructure and applications intended for the management of European funds, having a particular importance in the evolutionary process of increasing the quality of life, represents the first step towards knowledge, innovation and development of society in the information age.

REFERENCES

[1] European Commission (2022) Jobs and the economy during the COVID-19 pandemic https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/jobs-and-economy-during-coronavirus -pandemic.ro.

[2] European Information Society (2005) - Publisher: Foundation for European Studies.

[3] European Commission - Brussels, 3.3. (2021) One year since the outbreak of COVID-19: fiscal policy response
https://ec.europa.eu/info/files/one-year-outbreak-covid-19-fiscal-policy-response_en.

[4]Presidential Administration - Bucharest (2020) Romania - National Strategy for National Defense for the period 2020-2024.
https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf

[5]European Council - Council of the European Union - March (2010) - European Union Internal Security Strategy;
https://www.consilium.europa.eu/ro/documents-publications/publications/internal-security-strategy-european-union-towards-european-security-model/.

[6]Decision of the Official Gazette no. 677 (2020 - August 14) - on the approval of the National Program for the digitization of micro, small and medium enterprises, financed under the Operational Program Competitiveness 2014-2020.
http://legislatie.just.ro/Public/DetaliiDocument/229226 - OFFICIAL GAZETTE no. 756 of 19 August 2020.
[7]EU Directive 1148 / (2016) - Measures for a high level of security of networks and information systems in the Union.
https://cert.ro/pagini/ansrsi.
[8]Regulation (EU) (2016) / 679 - on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC (General Data Protection Regulation).
[9]The European Union Agency for Cybersecurity (ENISA), (2021) September 13 - Methodology for a Sectoral Cybersecurity Assessment
https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment.
[10]The European Union Agency for Cybersecurity (ENISA), (2020) April 15 - Advancing Software Security in the EU
https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework
[11]National Cybersecurity Directorate (DNSC) - (2021) September 30 - European Cybersecurity Month - ECSM
https://cert.ro/citeste/comunicat-luna-europeana-a-securitatii-cibernetice-2021
[12]Oracle Romania (2022) Emerging technologies: IoT, EoT, AI, Blockchain https://www.oracle.com/ro/emerging-technologies/.
[13]Cloud Computing, Events - October 6, (2021 at 11:19 am) - Cloud Conference brings new technologies to the forefront - (clubitc). https://www.clubitc.ro/2021/10/06/conferinta-de-cloud-aduce-in-prim-plan-noile-tehnologii/.