Victor Ababii
E-mail: ababii.victor@gmail.com
PhD student, Academy of Economic Studies of Moldova
Head of Division, Reporting and Statistics Department, National Bank of Moldova
Chișinău, Republic of Moldova
orcid.org/0009-0008-9573-0204

BANKING SUPERVISION THROUGH SUPTECH

Abstract: *The banking system requires continuous development to enhance stability and integrity of the financial sector by implementing the latest technological tools. Maintaining a sustainable financial system, resilient to the shocks generated by the digital age and able to adapt and prevent emerging cyber risks remains a priority for supervisory institutions, in response to financial supervision and risk management framework through leveraging state-of-the-art technology for better governance and control. SupTech's primary objective is to promote inclusion in the financial sector by focusing on governance management and digital financing. It`s goal is to support the development of an inclusive financial system built on a robust digital infrastructure that enhances efficiency, transparency, and resilience. As technological innovations advance, financial services have to evolve, requiring financial institutions to adapt their surveillance technologies (SupTech) to safeguard citizen interests. Establishing both normative and technical SupTech frameworks helps supervisory authorities to eliminate gaps in internal processes, streamline workflows, fortify risk management, protect consumers, and maintain financial system stability amid ongoing market changes. Implementing a SupTech framework involves several stages: diagnosing the institution's current state, defining the purpose, vision, and objectives of SupTech, identifying key drivers and adaptive capabilities, evaluating necessary actions, and detailing steps for successful implementation.*

A thorough diagnosis of the supervisory institution involves IT solutions that facilitate continuous bank monitoring and offsite supervision. This diagnostic analysis includes:
(1) Data products – identifying the position and trends to reach the level of AI-augment business intelligence tools;
(2) Analytics – aiming to implement analytics tools perspectives;
(3) Access controls - with the position on the agency - wide access;
(4) Storage – oriented towards the use target of big data tools;
(5) Validation and processing – aiming at the use of advanced data processing;
(6) Collection – using the latest AI-based collection trends or alternative data sources.
Configuring the SupTech framework involves transforming vulnerabilities into opportunities. For example, automating data flows can address deficiencies in manual data handling, risk assessment, and report generation. Implementing a data warehouse can solve challenges related to data consolidation, multiple analysis tools, system integration complexity, and data correlation.

SupTech aims to provide supervisory authorities with reliable, high-quality data, aligning with best practices in governance and data management. This ensures consistency in the

supervisory process and resilience to technological advancements. Digitizing surveillance processes is crucial for operational efficiency, with advanced analytics and business intelligence solutions enhancing surveillance information and decision-making.

Keywords: *SupTech, Fintech, Regtech, risks, data model.*

JEL classification: *G21*

ვიქტორ აბაბიი
E-mail: ababii.victor@gmail.com
დოქტორანტი, მოლდოვის ეკონომიკური კვლევების აკადემია.
მოლდოვის ეროვნული ბანკის სამმართველოს უფროსი,
ანგარიშგების და სტატისტიკის დეპარტამენტი
კიშინიოვი, მოლდოვის რესპუბლიკა
orcid.org/0009-0008-9573-0204

საბანკო ზედამხედველობა SUPTECH-ის მეშვეობით

აბსტრაქტი: *საბანკო სისტემა მოითხოვს უწყვეტ განვითარებას ფინანსური სექტორის სტაბილურობისა და მთლიანობის გასაძლიერებლად უახლესი ტექნოლოგიური ინსტრუმენტების დანერგვით. მდგრადი ფინანსური სისტემის შენარჩუნება, რომელიც მდგრადია ციფრული ეპოქის შოკების მიმართ და შეუძლია ადაპტირდეს და თავიდან აიცილოს წარმოქმნილი კიბერ რისკები, რჩება პრიორიტეტად საზედამხედველო ინსტიტუტებისთვის, ფინანსური ზედამხედველობისა და რისკის მართვის ჩარჩოს საპასუხოდ, უახლესი ტექნოლოგიების გამოყენებით. SupTech-ის უპირველესი მიზანია ფინანსურ სექტორში ინკლუზიის ხელშეწყობა მმართველობის მართვასა და ციფრულ დაფინანსებაზე ფოკუსირებით. მისი მიზანია ხელი შეუწყოს ინკლუზიური ფინანსური სისტემის განვითარებას, რომელიც აგებულია მყარ ციფრულ ინფრასტრუქტურაზე, რომელიც ზრდის ეფექტურობას, გამჭვირვალობას და მდგრადობას. ტექნოლოგიური ინოვაციების წინსვლისას, ფინანსური სერვისები უნდა განვითარდეს, რაც მოითხოვს ფინანსურ ინსტიტუტებს მოახდინონ თავიანთი ზედამხედველობის ტექნოლოგიების (SupTech) ადაპტაცია მოქალაქეების ინტერესების დასაცავად. როგორც ნორმატიული, ასევე ტექნიკური SupTech ჩარჩოების ჩამოყალიბება ეხმარება საზედამხედველო ორგანოებს, აღმოფხვრას შიდა პროცესებში არსებული ხარვეზები, გაამარტივონ სამუშაო ნაკადები, გააძლიერონ რისკების მართვა, დაიცვან მომხმარებლები და შეინარჩუნონ ფინანსური სისტემის სტაბილურობა ბაზრის მიმდინარე ცვლილებების ფონზე. SupTech ჩარჩოს დანერგვა მოიცავს რამდენიმე ეტაპს: დაწესებულების ამჟამინდელი მდგომარეობის დიაგნოზს, SupTech-ის მიზნის, ხედვისა და ამოცანების განსაზღვრას, ძირითადი მამოძრავებლების და ადაპტაციური შესაძლებლობების იდენტიფიცირებას, საჭირო ქმედებების შეფასებას და წარმატებული განხორციელებისთვის ნაბიჯების დეტალურ აღწერას.*

საზედამხედველო დაწესებულების საფუძვლიანი დიაგნოსტიკა მოიცავს IT გადაწყვეტილებებს, რომლებიც ხელს უწყობს ბანკის მუდმივ მონიტორინგს და გარე ზედამხედველობას. ეს დიაგნოსტიკური ანალიზი მოიცავს:
(1) მონაცემთა პროდუქტები - პოზიციისა და ტენდენციების იდენტიფიცირება, რათა მივაღწიოთ AI-გაძლიერებული ბიზნეს დაზვერვის ინსტრუმენტების დონეს;
(2) ანალიტიკა – მიზნად ისახავს ანალიტიკური ინსტრუმენტების პერსპექტივების დანერგვას;
(3) დაშვების კონტროლი - სააგენტოს თანამდებობაზე - ფართო წვდომა;
(4) შენახვა – ორიენტირებული დიდი მონაცემთა ინსტრუმენტების გამოყენების სამიზნეზე;
(5) ვალიდაცია და დამუშავება – მიზნად ისახავს მონაცემთა გაფართოებული დამუშავების გამოყენებას;
(6) კოლექცია – AI-ზე დაფუძნებული უახლესი ტენდენციების ან მონაცემთა ალტერნატიული წყაროების გამოყენებით.

SupTech ჩარჩოს კონფიგურაცია გულისხმობს მოწყვლადობის შესაძლებლობად გარდაქმნას. მაგალითად, მონაცემთა ნაკადების ავტომატიზირებას შეუძლია აღმოფხვრას ხარვეზები მონაცემთა ხელით დამუშავებაში, რისკების შეფასებასა და ანგარიშების შემუშავებაში. მონაცემთა საწყობის დანერგვამ შეიძლება გადაჭრას გამოწვევები, რომლებიც დაკავშირებულია მონაცემთა კონსოლიდაციასთან, მრავალჯერადი ანალიზის ინსტრუმენტებთან, სისტემური ინტეგრაციის სირთულესთან და მონაცემთა კორელაციასთან.

SupTech მიზნად ისახავს სამეთვალყურეო ორგანოებს მიაწოდოს სანდო, მაღალი ხარისხის მონაცემები, რომელიც შეესაბამება მართვისა და მონაცემთა მართვის საუკეთესო პრაქტიკას. ეს უზრუნველყოფს ზედამხედველობის პროცესის თანმიმდევრულობას და მდგრადობას ტექნოლოგიური მიღწევების მიმართ. სათვალთვალო პროცესების დიგიტალიზაცია გადამწყვეტია ოპერაციული ეფექტურობისთვის, მოწინავე ანალიტიკისა და ბიზნეს დაზვერვის გადაწყვეტილებებით, რომლებიც აძლიერებენ სათვალთვალო ინფორმაციას და გადაწყვეტილების მიღებას.

საკვანძო სიტყვები: *SupTech, Fintech, Regtech, რისკები, მონაცემთა მოდელი.*

JEL კლასიფიკაცია: *G21*

Introduction and review of literature

The banking system requires continuous development in enhancing the stability and integrity of the financial sector by implementing the latest technological tools. Maintaining a sustainable financial system, resilient to the shocks generated by the digital age and able to adapt to and prevent emerging cyber risks remains a priority for any institution with a supervisory mandate, in providing a financial supervision and risk management framework through leveraging state-of-the-art technology for better governance and control.

Prof. "Louis de Koker" - The future of financial supervision is bright, responsive, and innovative. Embracing technology to ensure an accountable, competitive, and modern market. One

way technology is employed to advance financial integrity effectively and efficiently in collaboration with responsible, regulated institutions and the industries.

The market globalization and digitization challenges imposed to supervisory institutions require the digitization of processes, the automation of administrative procedures and need for more efficient and proactive approaches to monitor risks and compliance at financial institutions and extract a much more accurate analysis from their data. Thus, for a better organization and ensuring the technology trend, institutions increasingly turn to Regtech, Fintech and Suptech.

Regtech comes to the aid of fintech companies and financial institutions by ensuring compliance with regulatory requirements. Regtech continuously monitors and secures the activities and flags potential compliance violations. Based on the assurance of the basic system for enterprises, it identifies and alerts in a timely manner any deficiencies of non-compliance that appear in the activity. (The Future of Regulation, Risk Management, and Compliance, 2023, Finextra)

Fintech focuses on the use of technology to drive innovation in the financial sector, while Regtech and Suptech focus on managing the regulatory and supervisory aspects of these innovations.

On the other hand, the Suptech empowers the supervisory units of the financial authorities to supervise the financial industry, ensuring it`s stability and integrity. Suptech increases surveillance capabilities by providing supervisors with data-driven insights. This empowers them to conduct comprehensive audits and to detect system-wide risks at an early stage. Suptech's capabilities extend to analyzing market trends, modeling economic scenarios and even anticipating potential risks to the financial system, such as money laundering. It works like a weather forecasting system, capable to provide early warnings of impending financial storms. (Payment aspects of financial inclusion in the fintech era, 2020, BIS)

Suptech refers to "surveillance technology" and implies the technology application and data analysis solutions in order to complete and enhance the financial market surveillance capabilities of a financial authority. Suptech applications are used by financial authorities to access more granular, diverse, timely and reliable data to improve operational efficiency and to generate previously unattainable insights, thereby improving decision-making. SupTech's main objective is to define and ensure inclusion in the financial sector, it focuses on governance management and digital financing for supporting the development of an inclusive financial sector, based on a robust digital infrastructure that increases efficiency, transparency and resilience. Along with technological innovations, the degree of development of financial services also increases, which requires increased attention by adapting the surveillance technologies (suptech) of the financial institution to ensure and protect the interests of citizens. Thus, the definition of both normative and technical framework of SupTech ensure the supervisory authority to eliminate the gaps in internal business processes, streamline work processes, strengthen the risk management framework, protect consumers of financial services, ensure the stability of the financial system, ensure adaptation and continuous maintenance of the market to the changes taking place. To effectively identify and address these inherent risks, the work of surveillance teams will increasingly look like data science and should therefore be empowered by equally powerful technology tools and best practices. Technological innovation provides new opportunities for supervisors and financial authorities,

which improves market surveillance and policy development. Thus, firstly, we have to understand the technologies that private sector players use to develop these systems and the data science approaches they use to process the resulting data. (State of SupTech report, 2022, Cambridge Centre for Alternative Finance (CCAF), University of Cambridge)

Methodology

In order to achieve the goal and reach the objectives we have set, we aimed to develop a comprehensive research methodology, which includes the most varied methods, so that the phenomenon of surveillance analysis through Suptech is exposed as well as possible. Thus, the research will be oriented in two directions: theoretical and applied. The theoretical direction aims to examine the theories regarding the Suptech concept. The applied direction aims to diagnostic the supervisory institution and to determine the actions necessary for the development of Suptech through IT solutions used either to process structured reports for quantitative analysis, or to access unstructured reports or text documents for qualitative analysis that will increase the quality of the process of supervision in making the best decisions.

Results

The configuration of new business models, the digitization of new financial products and services introduced new risks for supervisors, those risks that overtake the old ones. The main challenges faced by supervisors is the volume of digital data produced and shared by Fintech. Digitized operators and financial consumers warns to leave supervisors with a lot of data, leaving them in insufficiency ofuseful information for qualitative analysis. Changes in financial technologies adopted by financial institutions, for example from rules-based software to dynamic algorithmic models such as machine learning, these changes mean that financial authorities have to diversify the way these technologies work, to recognize the inherent risks to which they are subject to and to identify approaches and tools to supervise them effectively.

As the rapid digitization of the private sector continues it`s march forward, the skills required for financial oversight increasingly resemble those of data science. Innovation leaders have to develop fundamental knowledge of the data lifecycle – including data collection, validation and processing, storage, governance and analysis. Thus, it's important to know the terminology and components of data science. Effective oversight means working with an interdisciplinary team to manage the development, implementation and maintenance of Suptech as data products and using of appropriate tools to assess the effectiveness and correctness of these solutions. Data science is, of course, a rapidly and continuously developing field that requires frequent and persistent discussions and knowledge sharing.

The implementation of a SupTech normative and technical framework is based on the completion of stages that define the components of the SupTech framework as follows: diagnosis the current situation of the institution; defining the purpose, vision and application of SupTech objectives; establishing key drivers for SupTech development and adaptive capabilities; evaluation of the necessary actions for the implementation of the SupTech framework; as well as the detailed steps in successfully implementing SupTech.

Any diagnosis of the supervisory institution uses a set of IT solutions that ensures the data collection process based on a supervisory process oriented towards the continuous banks monitoring and offsite supervision. Diagnostic analysis is focused on a set of IT solutions that

compile the data stack for prioritized surveillance processes (ie, continuous bank monitoring and offsite surveillance). All these IT solutions are used either to process structured reports for quantitative analysis or to access unstructured reports or text documents for qualitative analysis:

Table 1. Suptech Generations Framework

	0G MANUAL	1G MINIMAL TECH	2G DIGITALY TRANSFORMED	3G ADVANCED TECH	4G BIG DATA & AI
Data products	Minimal statistical summaries	Static report generation	Automated dashboards	Dynamic and interactive visualizations	AI-augmented business intelligence tools
Analytics	No additional analysis	Manual analysis only	Descriptive/ Diagnostic Analytics Tools	Predictive Analytics Tools	Prescriptive Analytics Tools
Access Controls	Individual access only	Team access only	Department access only	Limited agency-wide access	Agency-wide access
Storage	Physical media	Centralized file-based storage	On-Premise Relation Databases	Cloud computing database systems	Big Data tools
Validation + Processing	Manual or no validation after receipt of data	Automated validation integrated into data submission process	Statik Task Automation	Robotic Process Automation (RPA)	Advanced Data Processing
Collection	Manually Submitted	File server	Web portal	API	AI-based collection or alternative data sources

Source: Developed by the author based on State of SupTech report, 2022, Cambridge Centre for Alternative Finance (CCAF), University of Cambridge

Based on the Suptech Generations Framework, the entity applies the diagnosis and so identifies in which framework it is positioned with the main monitoring tools. Based on the diagnosis, weaknesses are identified, as well as challenges such as processes that require manual intervention, challenges related to the use of multiple IT solutions that are not integrated and systems that limit the ability to make proactive and responsive decisions. Any supervisory entity tends to the following:

(1) Data products – identifying the position and trends to reach the level of AI-augment business intelligence tools;
(2) Analytics – aiming to implement analytics tools perspectives;
(3) Access controls – with the position on the agency–wide access;
(4) Storage – oriented towards the target use of big data tools;
(5) Validation and processing – aiming at the use of advanced data processing;
(6) Collection – using the latest AI-based collection trends or alternative data sources.

The configuration of the SupTech framework takes place from the identification of vulnerabilities to their transformation into opportunities. For example, the deficiencies related to human interventions on uploading and extracting data, manual processing in risk assessment, as

well as manual creation of reports can be capitalized into the opportunity to streamline data flows derived from structured data. The use of several IT solutions that bring with them a more difficult data consolidation, the use of several analysis tools, complexity of integration between systems, as well as the lack of data correlation, bring the opportunity to implement a data warehouse at the institution level. The table below shows how we can get opportunities from some vulnerabilities:

Table 2. From pain points to opportunities

Pain points	Pain points category	Opportunities
1. Burdened Data Loading and Extraction that requires human intervention	1. Processes that require manual intervention	1. Streamlining data flows derived from structured data
2. Manual Risk Assessment process (other than credit monitoring)		
3. Manual Report Creation		
4. Consolidation Complexity and Inadequate Data Connectivity	2. Challenges related to the use of multiple IT solutions	2. Implementing an agency-wide data warehouse
5. Use of Multiple Analytics Tools		
6. Cross-System Integration		
7. Lack of Data Correlation		
8. CRR Sequential Data Processing	3. Systems that limit the ability of making proactive and responsive decisions	3. Developing an integrated reporting scheme
9. Lack of Early Warning System and Monitoring Systems		

Source: Developed by the author

The SupTech comes to the supervisory authority to ensure reliable and qualitative data, to respond to the best practices of governance and data management, which as a result will ensure the consistency of the supervisory process and resistance to technological progress. Digitization of surveillance processes remains the key to success in operational efficiency and automation of surveillance processes, advanced analytical methodologies, business intelligence solutions will only improve surveillance and decision-making information. The purpose of this continuous assessment is firtstly to monitor and assess the financial health, risk profiles and compliance of financial institutions with regulatory frameworks. Second, it serves as a preventive measure, allowing the timely identification and mitigation of potential risks, thus saving the stability and resilience of the banking sector.

For a better understanding of diagnosis and identification of SupTech solutions, it will be presented the activity through which we will examine recent cases of digital financial services (DFS) related to money laundering, terrorist financing and financial proliferation in the jurisdiction of the Republic of Moldova. We will analyze the trends, vulnerabilities and strengths of the regulatory framework and consider recommendations for improvement.

Looking at these cases, it's clear that Moldova is trying to handle money laundering and financial crimes, but the way we enforce our rules isn't strong enough. Sometimes, it seems like even with all these rules and tech, we're just going through the motions to look good for the outside world, rather than making real changes that protect our financial system and people. This could

make some people wonder if we're more focused on filling out forms and checking boxes than actually stopping crime.

Table 3. Risk threats vulnerabilities case study analysis

	Bank fraud case	Shell companies case	Investment scheme fraud case
Summary of case	The case involved a network of individuals using false identities to establish bank accounts, through which large sums of illicitly obtained money were transacted.	This case focused on the use of fictitious companies registered to conduct non-existent business activities, utilized primarily for laundering money through complex financial transactions.	This case involves an organized group that created fraudulent investment schemes promising high returns. They attracted significant funds from investors, which were then laundered through various channels, including real estate transactions.
How and where was case reported Provide a link	This case was detailed in the MONEYVAL follow-up report on Moldova, highlighting systemic vulnerabilities in bank monitoring systems. MONEYVAL Follow-Up Report on Moldova 2022	Reported in the MONEYVAL follow-up report, it underscored weaknesses in the regulatory framework overseeing company registration and financial reporting. MONEYVAL Follow-Up Report on Moldova 2022	This case was detailed in the MONEYVAL follow-up report, highlighting vulnerabilities in monitoring and regulating investment activities. MONEYVAL Follow-Up Report on Moldova 2022
Identify and explain demonstrated threat	The primary threat demonstrated by this case is the exploitation of lax identity verification processes within banks in order to facilitate money laundering.	The use of shell companies to obscure the origin of illicit funds, making it difficult for authorities to trace and recover assets.	The primary threat demonstrated by this case is the exploitation of financial systems to facilitate and conceal the proceeds from fraudulent schemes.
Summarize risk trends	A broader risk trend where criminal networks exploit weak spots in financial systems to launder money through seemingly legitimate banking channels.	The prevalence of shell companies in money laundering schemes reflects a broader risk trend where criminals exploit legal business structures to facilitate their illicit activities.	A broader risk trend where fraudulent financial schemes are used as a vehicle for large-scale money laundering.
Regulatory Framework vulnerabilities	Inadequate identity verification processes that fail to detect false documents. Insufficient transaction monitoring systems that do not flag unusual transaction patterns.	Loopholes in company registration processes that allow the establishment of entities without proper due diligence. Lack of effective cross-checks between financial and corporate regulatory bodies.	Inadequate oversight and regulation of non-traditional investment products and services. Insufficient investor education on the risks associated with high-yield investments.
Regulatory Framework strengths	Existing laws that clearly define the criteria for identity verification. Established channels for reporting suspicious activities, although they need strengthening.	Legal requirements for company registration do exist but need better enforcement. Some capability to audit and investigate registered companies, though it requires enhancements.	Existing regulations that govern financial products and their marketing, though enforcement needs strengthening. Frameworks for reporting suspicious activities are in place but require more proactive enforcement.

Supervisory approach / method / activity to address, guide and rectify the vulnerabilities	Introducing stricter identity verification requirements and enhancing real-time transaction monitoring capabilities.	Enhancing inter-agency cooperation and integrating more rigorous auditing processes for company registrations and operations.	Introduce stricter regulatory requirements for new investment products, enhance investor education programs, and strengthen enforcement of existing laws.
SupTech solution example addressing AML/CFTCPF risk identification or trend analysis	Deployment of advanced analytics and machine learning algorithms to identify and flag unusual transaction patterns automatically, enhancing AML/CFT/CPF risk identification and trend analysis.	Implementation of a blockchain-based registry for real-time tracking of company formations and transactions to improve transparency and reduce the risk of misuse of corporate structures in laundering schemes.	Utilizing AI and machine learning tools to monitor and analyze investment trends and behaviors to quickly identify and respond to potential fraudulent schemes.

Source: Developed by the author based on analysis of the financial services market in the Republic of Moldova

For the vulnerability risk analysis below I will come with a description of the technology solutions used in the early detection and prevention of the risks to which the financial activity related to money laundering, terrorist financing and financial proliferation is subject. Thus, for the better risk management, the following actions must be taken:

(1) Creation of an ICT Reporting and Incident Management Portal.

Challenges and considerations to take into account:

- Ensure that data remains secure and private in accordance with the law;
- Explain how and why the data is used and who can see it;
- Make sure the assessment tools are fair and don't favor one over the other;
- Help smaller institutions that may struggle with new technology;
- Make sure all rules are applied the same way for everyone;
- Always have clear consent from institutions on how their data is used.

(2) Analysis of deviations through SWIFT monitoring

Challenges and considerations to take into account:

- Secure and protect personal and sensitive data;
- Ensuring transparency in the data use and access;
- Maintain fairness in data analysis to prevent bias;
- Ensure that all entities, regardless of size, can comply with data collection requirements;
- Supports the uniform application of the rules in all entities;
- Obtain explicit consent from entities to use data in compliance monitoring.

(3) Real-time fraud detection and SLA monitoring

Challenges and considerations to take into account:

- Protect the confidentiality and security of transaction data;
- Clarify how transaction data is monitored and used;

- Ensure fair monitoring, without bias towards any participant;
- Support smaller participants in meeting technology requirements;
- Consistently enforce compliance for all payment system participants;
- Securing informed consent for monitoring practices.

(4) Automated data collection and analysis system for MTPL

Challenges and considerations to take into account:

- Ensure robust data protection to prevent breaches;
- Maintain transparency in data processing and storage;
- Prevent any bias in automated data analysis;
- Provide technical support to all insurance entities for system integration;
- Apply the rules uniformly to all insurance providers;
- Clearly communicate data use and consent requirements to all parties.

(5) Automated OCR Licensing Process

Challenges and considerations to take into account:

- Secure sensitive information processed by AI OCR systems;
- Ensuring transparency in the automated decision-making process;
- Reduce the biases that AI systems might introduce during data processing;
- Help smaller entities to adapt to the automated submission requirements;
- Maintain consistent application of licensing rules;
- Obtain clear consent for the use of AI in the processing of personal and institutional data.

The goals and objectives of SupTech are achieved by configuring the final requirements for each essential level, in order to achieve the strategic goal, which are the key factors for the development of SupTech.

Development of Suptech is closely and directly correlated with *cyber security*, which is the starting point for ensuring operational resilience and building public confidence in the financial sector. Each Suptech solution must incorporate security measures that protect sensitive information from unauthorized access, breaches or misuse. Last but not least, an important role in ensuring cyber security is played by the personnel involved, where the application of the best cyber security practices are strictly respected and promoted, the rapid action against cyber-attacks and the application of the following cyber security principles:

(a) data protection - encryption, data masking and access controls, are crucial to improve data protection as Suptech operates with sensitive financial and surveillance data that must be protected against unauthorized access;

(b) data reliability - data integrity checks and audit trails help maintain the reliability of collected data, ensuring accurate and reliable data for effective surveillance. Any incident in ensuring data integrity will lead to incorrect conclusions and decisions;

(c) operational resilience and business continuity – the clear establishment of cyber security measures that will ensure the restoration and optimal functioning of the surveillance process by minimizing the impact and facilitating rapid recovery after security incidents;

(d) secure network architecture - implementing firewalls, intrusion detection and prevention systems, and secure remote access with virtual private networks helps prevent malicious actors

from manipulating surveillance systems or engaging in activities fraudulent that could undermine confidence in the market;

(e) regulatory compliance - compliance with relevant cyber security regulations and standards applicable at national and regional level;

(f) third-party risk management – collaboration with third parties implies compliance with cyber security regulations equally for all involved.

The *data framework* is another key factor in the development of the Suptech solution, by ensuring that the data is qualitative, secure and accessible, which allows qualitative analysis and making the most correct decisions. The data framework can be classified into three broad components: data governance, data model and data catalog, each of which must provide a structured approach to organizing, storing and accessing data in a way that supports strategic goals and objectives of Suptech.

Data governance – establishes how data is managed, stored and accessed within the entity, ensuring a high level of security and consistency throughout its lifecycle. The core components used as part of data governance within Suptech are the following:

(a) data policies - cover issues such as data privacy, security, use and sharing, ensuring alignment with data laws and regulations and Suptech's strategic objectives;

(b) data governance structure – represented by standards covering data quality, formats, naming conventions and metadata management, facilitating accurate and reliable data analysis;

(c) data quality management - implementation of data quality monitoring and continuous improvement processes. Best practices involve periodic data audits and implementing corrective actions for identified issues;

(d) data lifecycle management - data must be managed effectively, preventing unnecessary duplication and ensuring that resources are used optimally and kept only as long as required by regulatory requirements.

The *data model* – another key factor for the development of Suptech is the way in which data is structured, organized, facilitating the analysis and visualization of surveillance data. The implementation of the data model occurs by including the following: defining data requirements (data quality, increasing the granularity of surveillance information); adopting an OLAP-centric approach; integration of data sources; standardization of data formats; ensuring flexibility and adaptation to the latest model supervision requirements. The final data model must provide a solid foundation for data-driven oversight and decision-making, enabling the entity to effectively analyze trends, identify risks, and make informed strategic decisions.

Data catalog – helps identify data, provides better access and governance of the information held. The data catalog can be defined as a centralized repository consisting of metadata and the main lines of their use. Creating and maintaining a data catalog has the effect of developing Suptech through the following steps:

(a) inventorying key metadata, such as data descriptions, sources, formats and usage instructions;

(b) creating a data catalog platform and integration with existing data systems and user-friendly interfaces for data exploration and discovery;

(c) metadata standardization;

(d) integration with data governance;
(e) ensuring consistency and compliance.

Conclusions

The rapid evolution of technologies and directly new datasets implies the need to streamline and automate more supervisory processes to respond to the assessment and regulatory compliance of supervised entities. Emerging technologies introduce new data sets into processes and provide predictive insights into potential deviations, facilitating effective data-driven oversight. Suptech helps improve every level of the surveillance process. Thus we can identify the combination of an unlimited set of applied tools in defining a SupTech-based surveillance from the processing of unstructured data such as LLM, OCR, NLP to the constitution of DWH and the application of AI tools.

REFERENCES

[1] Machine Learning Explainability & Fairness: Insights from Consumer Lending, FinRegLab's (2022) Retrieved from Working Paper: https://finreglab.org/research/machine-learning-explainability-fairness-insights-from-consumer-lending/

[2] Payment aspects of financial inclusion in the fintech era (2020), Retrieved from BIS: https://www.bis.org/cpmi/publ/d191.htm

[3] Questioning the AI: Informing Design Practices for Explainable AI User Experiences (2021) Retrieved from IBM Research's publication: https://arxiv.org/pdf/2001.02478

[4] State of SupTech report (2022), Cambridge Centre for Alternative Finance (CCAF), Retrieved from University of Cambridge: http://www.cambridgesuptechlab.org/SOS

[5] Suptech tools for prudential supervisionand their use during the pandemic, FSI Insights on policy implementation No 3 (2021), Retrieved from BIS: https://www.bis.org/fsi/publ/insights37.pdf

[6] The DataStack: A Data and Tech Blueprint for Financial Supervision, Innovation, and the Data Commons, (2020) Retrieved from BFA Global: *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3595344*

[7] The Future of Regulation, Risk Management, and Compliance (2023), Retrieved from Finextra: https://www.finextra.com/researcharticle/272/the-future-of-regulation-risk-management-and-compliance-2023

[8] The Next Wave of Suptech Innovation, Suptech Solutions for Market Conduct Supervision (2021), Retrieved from International Bank for Reconstruction and Development / The World Bank: https://documents1.worldbank.org/curated/en/735871616428497205/pdf/The-Next-Wave-of-Suptech-Innovation-Suptech-Solutions-for-Market-Conduct-Supervision.pdf