Journal scientific and applied research, vol. 29, 2025
International Journal

ISSN 1314-6289 (Print)
ISSN 2815-4622 (Online)

Original Contribution

CHALLENGES AND MEASURES FOR ADMINISTRATIVE SECURITY AT THE LOCAL LEVEL DURING THE INTRODUCTION OF THE EUROPEAN CURRENCY UNIT (EURO) IN BULGARIA

Iliana K. Simeonova

DEPARTMENT OF COMMUNICATION AND COMPUTER ENGINEERING AND SECURITY TECHNOLOGIES, FACULTY OF TECHNICAL SCIENCES, KONSTANTIN PRESLAVSKY UNIVERSITY OF SHUMEN, SHUMEN 9712, 115, UNIVERSITETSKA STR., E-MAIL: i.simeonova@shu.bg

ABSTRACT: *The topic of administrative security at the local level during the introduction of the euro in Bulgaria examines the main challenges and measures that local authorities need to undertake for the successful integration of the new currency in the country. With the transition to the euro, Bulgaria will need to ensure not only technical and logistical readiness but also efficient administrative processes that guarantee the security of the financial system. In this context, potential risks such as inflation, uncontrolled price increases, and public dissatisfaction, as well as social barriers related to the population's adaptation to the new currency, are analyzed. Undertaking serious measures for training public employees, adapting information technologies, and ensuring transparency in financial operations will be crucial to overcoming these challenges. Additionally, it is important for local authorities to coordinate their actions with the private sector and financial institutions to ensure a smooth transition to the euro. The strategies and practices implemented at the local level will determine the success of the overall process and strengthen the country's economic stability in the long term.*

KEY WORDS*: Administrative security, Eurozone, Cybersecurity, Information security, Sensitive data.*

1. Introduction

The introduction of the euro in the Republic of Bulgaria represents a strategic stage in the process of deepening integration into the euro area and strengthening the sustainability of the national economic and financial system.

Although the main focus is on macroeconomic parameters and reforms in the banking sector, the process also requires complex administrative preparation, especially at the local government level.

In this context, municipalities and mayor's offices are key institutional intermediaries between the central government and civil society – a role that gives rise to additional functional responsibilities as well as a number of managerial and institutional risks.

Administrative and corporate securities are key elements in ensuring an effective and sustainable transition to the euro.

They cover a wide range of activities, including ensuring cybersecurity, protecting sensitive data, enhancing institutional capacity through staff training, and preventing disinformation and abuse.

Administrative security is a key element for ensuring an effective and sustainable transition to the euro. It encompasses a wide range of activities – including ensuring cybersecurity, protecting sensitive data, enhancing institutional capacity through employee training, as well as preventing disinformation and abuse.

The aim of this article is to examine the main challenges related to the security of administrative structures at the local level and to formulate specific practical guidelines for mitigating the associated risks in the context of the upcoming currency transformation."

Changes brought about by the introduction of the euro

The introduction of the euro is a process that affects many administrative and technical aspects of local government work. The transition to the single European currency is not limited to economic and monetary integration. It implies significant transformations in the functioning of public administration at all levels, including changes with a direct impact on administrative security – understood as a set of organizational, legal, and technical mechanisms for protecting institutional capacity, information infrastructure, and trust in the public sector.

Some of the most significant changes include financial, legal, and regulatory changes conversion of local fees, taxes, and budgets from levs to euros; Updating of administrative acts, contracts, and regulations; Changes in accounting practices and reporting by municipal units.

Public institutions are required to bring their internal regulations, ordinances, contracts, and administrative procedures into line with the currency change: All public documents and administrative decisions related to financial parameters must be updated. This requires a detailed legal review and expert support to avoid legal loopholes or the invalidity of administrative actions.

Adaptation of information systems is updating the software platforms used by municipalities – for e-services, taxation, public procurement; Ensuring compatibility with the new requirements of the Bulgarian National Bank and European financial institutions.

The introduction of the euro requires a complete overhaul of administrative information systems:

• Integration of the euro into accounting, financial, and archiving systems;

• Migration of databases and unification of interfaces for working with dual currency accounting (during the transition period);

• Reassessment of vulnerabilities in electronic portals and systems for serving citizens and businesses.

These changes create new risks related to potential security breaches, data loss, and non-compliance with regulatory standards for the protection of personal and sensitive information.

Management of human and institutional capacity and the role of the administration in society

Providing accurate, timely, and accessible information to citizens; Training employees to advise and serve citizens in the new financial context; Participating in public campaigns against misinformation.

Along with technical and legal transformation, human resources in public administration also need to be trained. Administrative staff should be trained to work in a dual currency environment and be more sensitive to errors and abuse. Untrained or poorly informed staff increases the risk of administrative violations, misinformation, and susceptibility to social manipulation.

Reputational and communication aspects of security

The introduction of a new currency also brings communication challenges related to trust in institutions. This is expressed in the following:

- Incorrect information provided to citizens or delays in key information can lead to panic, speculation, and loss of trust.

- Public institutions have a responsibility to ensure transparency, accessibility, and timeliness of information through official channels.

Key risks to administrative and corporate security

The introduction of the euro as the official currency in Bulgaria is a strategic and administrative priority of national importance.

Local government has a key role to play in this process, ensuring efficiency, transparency, and security in the transition to the new currency, but it faces a number of risks to administrative security.

The process of introducing the euro carries various risks, including cyberattacks, misinformation, administrative unpreparedness, and opportunities for fraud. Particularly sensitive are weaknesses in IT systems, lack of training for employees, and the danger of social tension. All these risks can jeopardize the effectiveness of the transition and public confidence. The main categories of

risks to administrative security associated with this transition, with a view to timely identification and adequate prevention measures, are:

Cyber risks and vulnerabilities in IT systems

The change of currency requires significant changes in administrative software systems. This leads to an increased risk of cyber-attacks [1,2] - during the transition to the euro, numerous information systems and databases are used, which may become the target of hacker attacks in the form of attempts to break into systems [1,2] that process sensitive financial and personal data. Malicious access to payment and document issuance modules. Inadequate database protection, especially in small and technically backward municipalities. Lack of preparedness for breaches due to a lack of contingency plans and incident protocols. Phishing and social engineering [1,2] – Malicious individuals may attempt to deceive employees through fraudulent emails or phone calls related to "technical support" or "updates" regarding the euro.

Table 1 Cyber risks

Risk	Description	Potential consequences
Cyberattacks	Increased vulnerability of information systems	Breach of confidentiality, loss of data
Phishing campaigns	Misleading employees through emails/phone calls	Password leaks, compromised access

Misinformation and social tension

The currency changeover period is vulnerable to the spread of: Fake news related to prices, exchange rates, and implementation deadlines. Panic among the population, especially among the elderly, caused by rumors or malicious campaigns. Manipulation with "dual prices," which may appear to be administrative arbitrariness if there is a lack of good communication and control.

Communication risks

Poorly informed citizens – If the administration does not conduct an effective information campaign, misunderstandings and tension among the population may arise. Spread of misinformation – During periods of transition, rumors often spread, which can cause public uncertainty.

Table 2 Risks related to the human factor

Risk	Description	Potential consequences
Insufficient communication with citizens	Lack of information about the change	Panic, distrust of the administration
Misinformation	Spreading rumors and speculation	Disturbing public order

Risks of fraud and corruption

The administration acts as an intermediary in the conversion of fees, assessments, fines, and other local payments, which gives rise to risks of: Deliberate overcharging or incorrect application of the exchange rate. Abuse of administrative influence in tenders, public procurement or concessions financed in euros. Interference by local economic interests that take advantage of weaknesses in control mechanisms.

Insufficient preparation of the administration, human error, and lack of training.

Many municipal structures suffer from: Insufficiently trained staff who do not fully understand the new requirements. Lack of clear internal guidelines on how to implement transitional procedures. Poor development of e-government, which increases the administrative burden and the risk of errors. Insufficient staff qualifications – If the administration does not provide adequate training, staff may make mistakes when entering or processing data related to the conversion. Sabotage or internal abuse – The currency change may be used by unscrupulous employees to commit fraud.

Table 3 Risks related to the human factor

Risk	Description	Potential consequences
Insufficient training	Lack of preparation for working with the new rules and systems	Errors in data entry, confusion among citizens
Internal abuse	Intentional actions by employees	Financial losses, damaged reputation

Inadequate protection of documents and information, which manifests itself in Leakage of sensitive information – Documents containing financial or personal data may be unlawfully disclosed or used. Reliability of paper and electronic archives – The transition may lead to loss or confusion of archived information if timely measures are not taken.

Table 4 Risks when working with documents and information

Risk	Description	Potential consequences
Leakage of information	Poor protection of documents and files	GDPR and privacy violations
Outdated archives	Lack of compatibility with the new currency	Confusion in inquiries and audits

Organizational and logistical risks

Insufficient coordination between departments – The lack of clear distribution of responsibilities and good control can lead to delays or chaos.

Outdated systems – The administration's software systems must be adapted to the new currency in a timely manner.

Table 5 Organizational and logistical risks

Risk	Description	Potential consequences
Poor coordination	Lack of clear task allocation	Delays in administrative activities
Non-adapted systems	Software not updated to the euro	Financial and reporting inaccuracies

The following recommendations can be made to local authorities:

- ✓ Conduct training for employees on working with the euro.
- ✓ Strengthen IT security and system monitoring.
- ✓ Conduct regular vulnerability tests.
- ✓ Transparent communication campaign for citizens.
- ✓ Create a crisis response plan for breaches or misinformation.

Necessary measures to ensure administrative is ensuring ensure a smooth and secure transition to the euro at the local level, a systematic approach with specific measures in several key areas is needed.

Recommended measures include strengthening cybersecurity through software updates and encryption. Auditing and updating the software used by local administrations to ensure compatibility with the new currency and data protection requirements. Implementing modern antivirus and intrusion detection systems and protection against malware [1,2]. Regularly backing up databases and introducing encrypted communication channels between municipal units. Developing incident response plans, including simulations of cyberattacks and emergencies.

Table 6 Strengthening cybersecurity in local government

№	Measure	Description
1	Software updates	All information systems must be updated to the latest versions with security patches.
2	Two-factor authentication (2FA)	An additional level of protection for access to systems and sensitive data.
3	Regular audit of IT systems	Conducting internal and external vulnerability audits.
4	Access control	Restricted access to systems based on position and role – "minimum access."
5	Cybersecurity training	Conducting training for employees on cyber threats and protection.
6	Appointment of an IT security officer	Specialist responsible for coordinating security and incident response.
7	Development of internal rules and procedures.	Established security protocols, incident response, and notification procedures.

№	Measure	Description
8	Informing employees.	Internal communication regarding current risks and preventive measures.
9	Restricting the use of personal devices	Policy of using only company devices with controlled protection.
10	Regular data	Automated and secure backup of important data with the option of recovery.
11	Detecting and blocking phishing emails	Filtering and automatically flagging suspicious messages.
12	Marking external emails	Adding a warning when receiving an email from an external sender.
13	Simulated phishing attacks	Conducting controlled tests to train employees.

Increasing staff capacity through includes training programs for administrative staff on new financial, legal, and technical procedures. Specialized training for local IT specialists on data protection and breach response. Creation of internal operational guidelines for staff working with the euro in public administration.

Table 7 Improving staff capacity

№	Measure	Description
1	Conducting thematic training courses and seminars	Organizing regular training courses on topics such as cybersecurity, working with sensitive data, financial control, and procedures for introducing the euro.
2	Preparation of internal manuals and instructions	Development and distribution of clear, concise guidelines for work during the transition period.
3	Knowledge tests	Conducting short tests after training to check the knowledge acquired and identify additional training needs.
4	Appointing internal security coordinators.	Designating key employees in each department/division to monitor compliance with procedures and train new colleagues.
5	Promoting a culture of security	Creating an organizational environment in which every employee is motivated to be vigilant and report any irregularities or risks they notice.
6	Simulated crisis situations	Conducting realistic exercises to respond to security breaches, information leaks, or cyberattacks.
7	Access to up-to-date information and resources	Providing employees with access to online platforms, newsletters, and training materials on current topics related to the euro and security.

Transparency and communication with the public through information campaigns

Local information campaigns to explain the process of introducing the euro, including through leaflets, meetings, and online resources. Establishment

of citizen information centers to receive reports of fraud or irregularities. Publication of clear tariffs, fees, and sample bills in euros to avoid manipulation and speculation.

Table 8 Transparency and communication with the public through information campaigns

№	Measure	Description
1	Creating an information campaign	Developing a clear and accessible campaign for citizens – through brochures, websites, social media, and local media.
2	Opening of specialized information points	Establishment of physical and online points for providing information, references, and accepting questions from citizens.
3	Regular public announcements and briefings	Presentation of information on the stages of euro introduction and security measures through press conferences and local channels.
4	Preparation of frequently asked questions (FAQ)	Creation of a document or online section with answers to the most common questions related to the transition.
5	Bilingual communication (if necessary)	Providing information in other languages (e.g., Romani, Turkish, English) if the population of a given municipality requires it.
6	Feedback mechanism	Creating an easy way for citizens to report problems, suspected fraud, or misconduct by employees.
7	Training employees in communication with citizens	Conducting training in customer service during a sensitive transition period and working with vulnerable groups.

Cooperation with national and international institutions

Close coordination with national authorities – the Ministry of Interior, the Bulgarian National Bank, the National Revenue Agency, and the State Agency for National Security – for information exchange and joint action. Municipal protocols for interaction with the police and the prosecutor's office in cases of suspected fraud. Establishment of crisis teams at the local level when a rapid response is needed (e.g., in the event of a large-scale fake campaign).

Table 9 Cooperation with national and international institutions

№	Measure	Description
1	Establishment of a coordination mechanism	Establishment of working groups and coordination councils with representatives of central and local government and law enforcement agencies.
2	Cooperation agreements	Signing of cooperation protocols between institutions with a clear division of responsibilities in the event of incidents.

№	Measure	Description
3	Real-time information exchange	Creation of secure channels for rapid information exchange in the event of reports of fraud, counterfeiting, or security breaches.
4	Joint exercises and simulations	Conducting regular exercises with employees from different institutions to respond to critical situations.
5	Participation of the Ministry of Interior, the State Agency for National Security, the Bulgarian National Bank, and other key structures	Involvement of all national authorities relevant to financial and information security in the process of introducing the euro.
6	Harmonization of internal procedures	Harmonization of security rules and protocols between institutions working on the issue.
7	Centralized information platform	Development of a common electronic platform for coordination, reporting, and exchange of good practices between institutions.

Good practices from Croatia and Slovakia, conclusions for Bulgaria

The transition to the euro has already been successfully implemented in several Central and Eastern European countries, including Croatia (2023) and Slovakia (2009). Their experience can serve as a useful reference for Bulgaria, especially regarding administrative security at the local level.

- Croatia uses mobile applications for citizen control and centralized communication:

Centralized approach to communication: Croatian local authorities received standardized information materials and training modules distributed by central institutions. This limited the spread of misinformation and helped ensure uniform implementation of the measures.

Electronic tools for citizens: A mobile application for checking prices in kuna and euros was introduced, allowing consumers to monitor actual prices and report irregularities.

Focus on fraud prevention

Rapid response teams were set up at local level to check reports from citizens and investigate cases of exchange rate abuse.

- Slovakia organized training and used bilingual systems during the transition period:

Advance training for the administration

A year before the introduction of the euro in Slovakia, national and regional seminars were organized for the local administration with a practical focus, including simulations of real cases.

Bilingual administrative systems

For the period before and after the introduction, administrative forms and software were available in both Slovak and euro formats to avoid confusion and technical breakdowns.

Cooperation with local businesses

The municipality acted as an intermediary between small traders and the central government to ensure the correct application of the exchange rate, which strengthened public confidence.

From these examples, the following conclusions can be drawn for Bulgaria: the success of the introduction of the euro at the local level depends on:

- ✓ Early preparation and standardization of administrative processes;
- ✓ A strong and well-coordinated information campaign;
- ✓ Digital tools and platforms for transparency;
- ✓ Active involvement of the local community and civil society.

Conclusion

The introduction of the euro in Bulgaria is a process of great strategic importance that goes beyond purely economic transformation. Especially at the local level, the transition requires careful planning, good coordination, and a high level of administrative certainty. Local authorities are not simply executors of central policies – they are the first and most accessible institutions for citizens and businesses.

Adequate preparation, transparency, and commitment on the part of institutions will be crucial to the success of this process. The use of international experience and technological solutions will further ensure the sustainability of the administrative transformation.

This article has shown that the risks – from cyber threats to disinformation and administrative unpreparedness – are real and can compromise the entire process if not addressed in time. On the other hand, clearly defined measures—technical, organizational, and communicational—can significantly limit these threats and turn the transition into an example of effective change management. Key success factors include:

- Strengthening cybersecurity and protecting information systems; Preparing and training administrative staff;
- Active and transparent communication with the public;
- Cooperation between local and national levels, as well as with the private sector;
- Utilizing international experience and best practices from countries that have gone down the same path.

Bulgaria has the opportunity not only to introduce a new currency, but also to establish good governance practices that will increase citizens' trust in institutions. However, this requires timely, targeted, and sustained action now.

Acknowledgments

This article is supported by internal research project RD-08-109/05.02.2025 "Design and build a scalable research platform for Edge AI/HPS analytics", Konstantin Preslavsky University of Shumen, Faculty of Technical Sciences, Department of Communication and Computer Engineering and Security Technologies.

References:

[1] Boyanov, P., Implementation of TCP SYN flood cyber attack in the computer network and systems. A refereed Journal Scientific and Applied Research, Konstantin Preslavsky University Press, 2019, 17, 36-42, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), DOI: https://doi.org/10.46687/jsar.v17i1.270.

[2] Boyanov, P., Basic network penetration testing with the network tool Netcat in Linux-based operating systems. A refereed Journal Scientific and Applied Research, Konstantin Preslavsky University Press, Vol. 25, Shumen, 2023, ISSN 1314-6289 (Print), ISSN 2815-4622 (Online), pp. 15-30, DOI: https://doi.org/10.46687/jsar.v25i1.377.

[3] Croatian National Bank. (2023). Croatia's experience in transitioning to the euro.

[4] Decree No. 168 of the Council of Ministers of July 3, 2015.

[5] Dimanova, D., Kuzmanov, Z. Development of an Integrated Security and Communication System, International Scientific Referenced Online Journal, issue 63, November 2019, ISSN: 2367-5721, www.sociobrains.com. pp. 83-91.

[6] Dimanova, D., Kuzmanov, Z. Risk Measurement and Assessment. SocioBrains, international scientific online journal, publisher: www.SocioBrains.com, ISSN 2367-5721, pp. 63–69, issue 32, April 2017.

[7] European Central Bank. (2022). Handbook for the introduction of the euro.

[8] Information platform, evro.egov.bg

[9] Kuzmanov, Z., Cyberterrorism – definition and forms. SocioBrains, www.sociobrains.com, Published by: Veselina Nikolaeva Ilieva, Bulgaria, issue 76, December 2020, p. 151, ISSN 2367-5721, (online) – (Bulgarian language).

[10] Law on the Introduction of the Euro in the Republic of Bulgaria, published in State Gazette No. 65 of 08.08.2025.
[11] Law on the Bulgarian National Bank, Council Regulation (EC) No. 974/98 of May 13, 1998.
[12] Metodieva, Ts., "National and Corporate Security," NK with international participation "MATTEX 2018," Shumen University "Bishop Konstantin Preslavski," October 25-27, 2018, Shumen, ISSN: 1314-3921, vol. 2, 2018
[13] Metodieva, Ts., "Corporate Security and Its Components." Yearbook of Shumen University "Bishop Konstantin Preslavsky", pp. 338-341, ISSN 1311-834X, 2020 (Bulgarian language).
[14] Ministry of Finance of the Republic of Bulgaria. (2024). National plan for the introduction of the euro.
[15] National Plan for the Introduction of the Euro in the Republic of Bulgaria, Adopted by Council of Ministers Decision No. 665/25.09.2025.