doi: 10.15678/PG.2026.75.1.01

Journal of Public Governance
No. 1(75)/2026
ISSN 2956-6061 | e-ISSN 2956-6398

ACCEPTED MANUSCRIPT
Peer-reviewed and accepted for publication. Not yet copyedited, proofread or typeset.

Katarzyna Hady-Głowiak

Identification and Assessment of Risks in the Process of the Digitalization of Administrative Proceedings

Abstract:

Objective: The primary research objective of this publication is to conduct a managerial analysis focused on identifying the risks occurring in the process of electronization of administrative proceedings, as well as evaluating the functioning control mechanisms in this area.

Research Design & Methods: The study employs the dogmatic-legal method and literature analysis. This study integrates theoretical considerations with elements of empirical analysis based on the experiences of administrative practice.

Findings: Identifying and assessing risks in the process of digitising administrative proceedings constitutes an important element in ensuring their effectiveness, security and compliance with applicable legal provisions. This process enables the identification of threats in the legal, technological and social areas, which in turn allows for the implementation of control mechanisms individually tailored to a specific public administration unit. The development of digital tools, and consequently the improvement of management methods, means that unit managers should take actions to limit this risk to an acceptable level. As a result, effective risk management becomes an indispensable condition for the smooth functioning of modern public administration based on digital solutions. It is recommended that risk registers kept by individual public administration units should systematically include risks associated with the process of digitising administrative proceedings.

Implications/Recommendations: The research findings can be used to optimize administrative procedures. It is recommended to implement new risk control mechanisms.

Contribution/Value Added: This article addresses a distinct research gap in the field of risk management within the digitalization of administrative proceedings.

Article classification: theoretical article

Keywords: risk, administrative procedure, digitalization of public administration, control mechanisms, public administration.

JEL classification: H83

About this version: This is the accepted manuscript of an article peer-reviewed and accepted for publication in the Journal of Public Governance. It may differ from the final version of record in language, formatting and pagination. The version of record will replace it on the journal website; the DOI will remain unchanged.

Katarzyna Hady-Głowiak* – PhD, Institute of Economics and Security Studies, Witold Pilecki State University of Małopolska in Oświęcim, Poland; e-mail: kahadyglowiak@gmail.com; ORCID: 009-0006-3038-5476
* *corresponding author*

1. Introduction

The electronization of administrative proceedings constitutes one of the key directions in the modernization of public administration, aligning with the development of the information society. This process involves the use of information and communication technologies in order to increase the efficiency, transparency, and accessibility of the activities of public administration bodies. However, on the other hand, it is associated with certain risks, particularly in terms of the security of processed data and the protection of the privacy of participants in such proceedings. Additionally, ensuring the reliability of ICT systems remains a challenge, as does minimizing the risk of identification and technical errors that may affect the correctness of actions undertaken in the course of administrative proceedings. A key element of e-government is also the automation of administrative procedures, which enables services to be carried out without manual intervention. „ Automation can certainly accelerate the handling of administrative cases, improve decision-making processes by ensuring that all relevant details of a given case are taken into account, and also lead to savings in time, human resources, and financial costs" (Zimmermann, 2022, 72).

In this context, managerial control becomes particularly important. As a management system within public finance sector entities, it performs a coordinating and optimizing function for the course of administrative proceedings, ensuring their compliance with the law, efficiency, economy, and appropriate risk management, including risks arising from the ongoing digitalization of administrative procedures. In the Polish legal system, in accordance with Communication No. 23 of the Minister of Finance of 16 December 2009 on standards of management control for the public finance sector (Dz. Urz. MF z 2009 r. Nr 15, poz. 84) one of the management control standards concerns the area of risk management. The implementation of standards in the field of risk identification, analysis, and response is mandatory and forms the basis for ensuring the adequacy and effectiveness of the entire management control system in public finance sector entities. According to these standards, risk management is aimed at increasing the likelihood of achieving objectives and accomplishing tasks. Moreover, effective protection of an organization requires a thorough understanding of its resources; hence, the key role of risk analysis, which identifies defensive priorities. A detailed definition of the mission can contribute to establishing a hierarchy of objectives and tasks, and may also support the development of efficient and effective mechanisms that are helpful in risk management (Romaniuk 2012, 75). Management control is a continuous process and should also be tailored to the specific characteristics and needs of a given entity (Małecka-Łyszczek 2019).

According to the view expressed in the subject literature, the solutions introduced by the Polish legislator are moving toward the digitalization of administrative procedures, which are intended to constitute an alternative to the traditional form used so far (Łuczak, 2014, 79). The risk management system within an entity is a key tool that the head of the entity can use to obtain information about the state of management control, thereby enabling them to make strategic decisions (Romaniuk 2012, 80).

The main research objective of this publication is to conduct a management-oriented analysis focused on identifying the risks occurring in the process of digitalizing administrative proceedings, as well as assessing the control mechanisms in place in this area.

In this study, the terms “electronization” and “digitalization” are used interchangeably; however, they are understood as referring to the same phenomenon, namely the implementation of digital solutions in administrative proceedings.

2. The Concept of the Electronization of Administrative Proceedings.

In terminological terms, the process of introducing information and communication technologies into public administration is referred to as e-administration (e-government), and it involves the use of modern IT and communication tools in order to provide public services efficiently (Adamus-Kowalska, 2018, 148).

Article 14 of the Code of Administrative Procedure (Journal of Laws 2025, item 1691, as amended) it establishes the principle of written form in administrative proceedings, indicating that cases should be conducted and resolved in writing, either in paper or electronic form. The provision specifies the formal requirements for signing documents, differentiating them depending on the form of the document. Nowadays, the principle of written form therefore means the obligation to both conduct proceedings and issue decisions in writing, with the possibility of recording documents either on paper or in electronic form (Przybysz 2026). Article 14 § 1a of the Code of Administrative Procedure leaves the public administration authority free to choose the form in which an action is recorded - either paper or electronic. This means that even where specific provisions require a written form, it may take either of these forms, provided that the specific regulations do not explicitly indicate only one of them (Wróbel 2025).

Article 14 § 1c of the Code of Administrative Procedure also allows for the use of automatically generated documents bearing the qualified electronic seal of a public administration body, exempting them from the requirement of being signed by an employee of the authority. The absence of detailed regulations in the Code of Administrative Procedure justifies treating

article 14 § 1c as „opening the procedure to the automation of administrative proceedings" (Krawczyk 2025, art. 14, 145).

Moreover, the possibility has been provided to handle cases using online services, following prior authentication of the participants in the proceedings in accordance with the regulations on the computerization of the activities of public entities (Journal of Laws 2025, item 1703, as amended). Online services constitute one of the manifestations of the principle of written form in administrative proceedings. Although this concept has not been statutorily defined, it refers to tools made available by public administration bodies (such as ePUAP or PUE ZUS), which can be used after prior authentication of the participant in the proceedings in accordance with article 20a section 1 or 2 of the aforementioned Act on the Computerization of the Activities of Public Entities (Krawczyk 2025, art. 14, 145). Practical examples of the use of electronic forms of communication in Poland also include ICT systems applied in public administration, such as mObywatel, e-Urząd Skarbowy, the Internet Patient Account (IKP), and the Social Insurance Institution Electronic Services Platform (PUE ZUS). These solutions employ user authentication mechanisms, such as the trusted profile (Profil Zaufany), electronic banking, the e-ID card, and confirmation of the moment a document is accessed or made available in the system. Within these platforms, users receive documents in their electronic inbox, while the system records the moment of their delivery or considers them delivered after a specified period of time, even if they have not been read. Thus, it becomes crucial not only to ensure that the user actually becomes acquainted with the content of the document, but also to guarantee the possibility of accessing it within the ICT system. The terms and conditions of these platforms regulate issues related to service of documents, user account obligations, and matters concerning document accessibility. The experience gained from the use of the above-mentioned platforms has a significant impact on the design and functioning of electronic service of documents within administrative proceedings.

According to article 39 § 1 of the Code of Administrative Procedure, a public administration authority delivers documents to an electronic delivery address, unless the delivery is made to an account in the authority's electronic system or at the authority's premises. Meeting the conditions set out in Article 39 § 1 of the Code of Administrative Procedure obliges the administrative authority to deliver documents in the form indicated by the party (Łuczak, 2014, 71). For an electronic address to be recognized as an address for electronic service within the meaning of article 39 of the Code of Administrative Procedure, it is necessary to use a public registered electronic delivery service, a public hybrid service, or a qualified registered electronic delivery service. These services must ensure the possibility of unequivocally

establishing the identity of both the sender and the recipient of the data transmitted through them (Krawczyk 2025, art. 39, 299. During administrative proceedings, difficulties may arise in correctly establishing the identity of the sender. This phenomenon creates a significant risk of violating personal data protection regulations, as well as the possibility of directing correspondence to the wrong recipient. Identification problems may result, among others, from difficulties in unequivocally determining the recipient of the correspondence - for example, in situations where a PESEL number is unavailable and persons with identical names and surnames reside at the same address. In such cases, a serious issue arises with regard to properly assigning correspondence to a specific individual.

The procedure provided for in article 39 § 2 of the Code of Administrative Procedure applies where delivery in the manner referred to in § 1 is not possible, and consists in serving the document against acknowledgment of receipt by the designated operator using a public hybrid service, or by the authority's own employees, or by other authorized persons or bodies. Pursuant to Article 46 of the Act on Electronic Delivery, (Journal of Laws 2026, item 3, as amended) when providing a public hybrid service, the designated operator converts an electronic document sent by a public entity from an electronic delivery address into a postal item for the purpose of delivering correspondence to the recipient. This conversion is carried out in an automated manner, ensuring the protection of postal secrecy at every stage of the service.

The regulation set out in article 39 § 3 of the Code of Administrative Procedure has a final character and applies only where delivery of documents cannot be effected by any of the previously indicated methods. In such a case, the authority effects service through a registered postal item within the meaning of article 3 point 23 of the Postal Law, or its own employees or other authorized persons or bodies.

The authority serves documents to an electronic delivery address, understood as the designation of an information system enabling communication by means of electronic communication, in particular electronic mail (article 2 point 1 of the Act on the Provision of Electronic Services; Journal of Laws 2024, item 1513, as amended). The obligation to possess such an address applies not only to public entities (article 8 of the Act on Electronic Delivery), but also to certain private entities, including professions of public trust (article 9 of the Act on Electronic Delivery). Documents recorded in electronic form are delivered to the electronic delivery address. In particular, electronic services make it possible to achieve key objectives of public administration, such as ensuring citizens access to information and public services regardless of place and time. E-offices enable the submission of applications, obtaining infor-

mation, and handling administrative matters online. Moreover, e-services contribute to increasing the efficiency of human and financial resource management through the automation of processes, including recruitment, training, and payroll administration. They also facilitate more effective cooperation between different administrative authorities thanks to improved exchange of information and data. It should be emphasized that e-services in public administration constitute a dynamically developing area which, together with technological progress, will play an increasingly important role in enhancing the efficiency and accessibility of public services (Słapczyński 2024, 343).

Modern technologies exert a significant influence on the functioning of public administration and on administrative law, both in terms of new opportunities and emerging risks. Public authorities are obliged to adapt to a dynamically changing reality and to make use of innovative solutions in order to improve operational efficiency and the quality of services provided. At the same time, administrative law should maintain an appropriate degree of flexibility and the capacity to respond to new challenges, particularly in areas related to data protection, information security, as well as ethical issues and liability (Słapczyński 2024, 343).

In Germany, the possibility of issuing decisions using algorithms has existed since 2017. The Federal Geo-Information Act (SR 510.62) It indicates that an administrative act may be carried out entirely by automated means, provided that this is permitted by law and that the authority does not have discretionary powers. In addition to an electronic decision, which is characterized by being embodied in an electronic document, a fully automated decision is distinguished by the fact that the decision-making process is entirely automated through appropriate software. An administrative decision is therefore issued without the processing of personal data (Staniszewska 2024, 54).

A comparative analysis leads to the conclusion that the solutions adopted in Germany may serve as an important reference point for the further development of Polish regulations, particularly in the area of institutionalizing digital risk management and strengthening its oversight mechanisms. In particular, the German model allowing for automated administrative decision-making, while limiting administrative discretion, demonstrates how digital efficiency can be combined with the preservation of legal safeguards for individuals.

Electronic means of completing procedures and formalities are essential for simplifying administrative procedures, as well as for the standardization of electronic processes in administrative proceedings (Kraska & Matuszewska-Maroń 2013, 74). It is also crucial for the elec-

tronization of administrative proceedings to define the conditions for storing electronic documentation, ensuring the confidentiality, integrity, completeness, and availability of data (Suchanowska 2026).

3. Categories of risks related to the digitization process.

Risk can be defined as an unwanted and uncertain event related to the possibility of an uncertain loss, which is most often a financial loss (Ostasiewicz (red.), Składki i ryzyko ubezpieczeniowe. Modelowanie stochastyczne (Ostasiewicz 2004, 11). Risk is the uncertainty associated with an event or action that may affect an organization's ability to achieve its objectives. It may manifest itself as a negative threat or a positive opportunity (Ministerstwo Finansów 2004, 6). Mechanisms should be introduced to ensure the continuity of operations of a public finance sector entity, making use, among others, of the results of the risk analysis carried out. According to the standard PN-EN ISO 22300:2018-07, business continuity management is a holistic management process that identifies potential threats to an organization and the impacts those threats may cause if they occur, providing a framework for building organizational resilience and enabling effective response in order to protect the interests of its key stakeholders, its reputation, brand, and value-creating activities (PN-EN ISO 2018).

International Standards for the Professional Practice of Internal Auditing (Official Journal of the Ministry of Development and Finance, 2016, item 28) The Standards define risk as the possibility that an event will occur which will affect the achievement of established objectives. Risk is measured in terms of impact (consequences) and likelihood of occurrence. According to the Standards, risk identification in relation to objectives and tasks should be carried out at least once a year. In the case of a government administration department or a local government unit, it should be taken into account that objectives and tasks are also accomplished by subordinate or supervised units. In the event of a material change in the conditions under which the entity operates, risk identification should be performed again. Subsequently, the Standards indicate that the identified risks should be analysed in order to determine the likelihood of occurrence of a given risk and its possible consequences. The acceptable level of risk should be specified. For each significant risk, the appropriate type of response (tolerance, transfer, withdrawal, or action) should be defined.

The digitisation of administrative procedures, by transferring them into cyberspace, creates threats of high significance. Consequently, in the area of data protection as well as cybersecurity, risk analysis enables the identification of threats, assessment of their likelihood and impact, and subsequently leads to the selection of adequate technical and organisational

measures. Risk analysis in these areas is a continuous process, requiring updates in response to emerging threats within a given public finance sector entity (Śliwiński & Watras 2026). The organisation is required to implement an appropriate risk identification programme and to develop adequate risk awareness. Risk identification should be integrated into the organisation's main operational and managerial processes, so that the organisation maintains a current and comprehensive view of its risks (Ministerstwo Finansów 2004, 21).

Risk analysis is a multifaceted process, which means it requires time and the involvement of people who are familiar with the activities carried out within the organisation. In practice, owners of processes, IT team members and supplier personnel are engaged in identifying threats, safeguards and likelihoods. In the event of changes introduced to processes, personnel or tools, the risk analysis must be reviewed and appropriately updated (Szczytko-Sołtysiak 2024).

For the purposes of this publication, risks arising in the process of digitising administrative procedures have been divided into three main categories: legal, technical and social risks. This classification allows for a comprehensive consideration of threats resulting both from the normative aspects of public administration functioning and from technological and social conditions affecting the effectiveness of implemented digital solutions. The development of digital tools in public finance sector entities, including systems such as e-service of documents (e-doręczenia), gives rise to numerous significant legal risks. One of the key threats is the frequent changes in regulations and the introduction of transitional periods. Currently, the e-service of documents system operates in parallel with the ePUAP system. An important risk in administrative proceedings is also the breach of provisions affecting the effectiveness of service of documents, which may lead to the recognition of service as effective despite the lack of fulfilment of formal requirements. The consequence of such actions may be the violation of the rights of the parties to the proceedings, including the right to defence and the right to active participation in the proceedings. Systemic and organisational errors, such as the unavailability of the delivery mailbox, technical problems or incorrect assignment of a delivery to the wrong addressee, create significant risk. Major difficulties for staff of public administration units are posed by the verification of electronic signatures and situations where a signature has been improperly affixed. In this context, a risk of breaching the written-form principle can be identified.

Where different forms of service - paper and electronic - must be used for the same document addressed to various parties to the proceedings, the regulations applicable from 5 October 2021 must be taken into account. Under these rules, when a document is originally

created in electronic form in an information system of the public administration authority and bears a qualified electronic signature, a trusted signature, a personal signature, or an appropriate electronic seal, and is to be served in paper form, its printout must be prepared. This printout should faithfully reflect the content of the electronic document and be delivered to the addressee. At the same time, it must contain an appropriate statement indicating that the original document was created in electronic form and signed or sealed with the relevant electronic signature or electronic seal (Przybysz 2026). Electronic service supersedes traditional service, which means that simultaneous service of the same document in both paper and electronic form is not allowed (Postanowienie NSA z 4.06.2014 r., II GSK 1197/14, LEX nr 1467669).

Another significant threat consists of errors in addressing correspondence to the parties to the proceedings, since in electronic systems user identification is based on specific authentication mechanisms, which do not always guarantee complete certainty regarding the person's identity. It is also necessary to take into account risks related to the protection of personal data, such as sending correspondence to an incorrect recipient or using unsecured communication channels (e-mail without appropriate safeguards). In the case of technical risks associated with the functioning of information systems, their sources include infrastructural limitations, organisational factors and user errors. A key problem remains the risk of failures in information systems and limited availability of digital services. Interruptions in system operation, server overloads or planned technical works may lead to a temporary inability to perform administrative actions.

A significant risk area comprises cyber threats, including, among others, phishing attacks, ransomware and unauthorised access to data. Within administrative proceedings, personal data of the parties to the proceedings are processed (see: Hady-Głowiak & Hady-Głowiak, 2025), including personal data of a special category.

One of the most important categories of threats in administrative proceedings may consist of distortions of the content of electronic documents, resulting from errors in converting formats, compatibility problems with software or file damage. In the context of ongoing administrative proceedings, such irregularities may have serious legal consequences, including affecting the content of decisions or leading to their incorrect interpretation.

The process of digitising public administration also entails significant social implications. Among them, issues of equal access, citizens' level of trust in public institutions and society's ability to use digital tools are of particular importance. The digitisation of administrative procedures may also lead to digital exclusion of certain groups, such as older persons, residents

of areas with limited access to information and communication infrastructure, and individuals with lower digital skills, which may conflict with the principle of universal access to public services. Another problem is the low level of citizens' trust in the information systems used by public administration, which in turn slows down the process of digitization. According to J. Zimmerman, resistance to the computerisation of administration stems in part from social mentality and from the trust placed in the traditional paper-based form of administrative procedures (Zimmermann, 2022, 73). The issue of ensuring equal treatment of the parties to the proceedings gains particular significance, as parties with better access to technology may obtain an advantage in accessing information.

4. Control mechanisms

In the context of digitising administrative proceedings, control mechanisms are procedures and instruments whose purpose is to monitor, verify and limit risks in the activities of public finance sector units. These measures aim to ensure that actions taken within administrative proceedings are lawful, effective and secure in the era of digitalisation. A control mechanism functioning in public institutions should take into account, within its specific characteristics, the most important areas of risk, which, through appropriate control mechanisms, should facilitate their reduction or neutralisation (Romaniuk 2012, 76).

Risk arising within ongoing administrative proceedings constitutes an inherent element of their functioning, which cannot be completely eliminated. This implies the need to undertake systematic and multifaceted management actions aimed at its maximum minimisation and at limiting the consequences of its materialisation.

Table 1. Selected Risk Areas and Control Mechanisms

Risk area	Risk description	Control mechanisms
Legal risk	Risk of incorrect application of law, frequent changes in legislation and the introduction of transitional periods; risk of defective administrative actions; risk of breaches of regulations affecting the effectiveness of service of documents and leading to a danger of wrongfully recognising a service as effective; risk of an administrative decision being declared invalid.	Establishment of internal procedures, training of employees, cross-checking of actions by a second person or a supervisor, development of standard document templates, monitoring of changes in statutory provisions and case law.
Security of data of participants in administrative proceedings.	Risk of leakage, theft or loss of data of participants in administrative proceedings.	Securing data transmission and storage, encrypting data, controlling access to systems and data, security audits, and applying the principle of data minimisation (processing only data that are necessary for the purpose).

IT system failures	Lack of availability of electronic platforms, failures of information systems, and breach of the principle of timeliness in administrative proceedings[1].	Redundancy of systems, business continuity plans, maintaining backups, implementing backup procedures, and establishing alternative service channels.
Digital exclusion	Lack of access of selected groups of citizens to digital services.	Establishment of traditional service channels, digital support, and education.
Lack of interoperability	Difficulties with integration between the systems of public authorities.	Introduction of common data standards between authorities, and manual verification of atypical cases.
User errors	Risk of procedural errors committed by the parties and officials resulting from the ambiguity, constant changes and complexity of regulations governing digitisation.	Training of employees, data validation in the system, and technical support.

Source: Author's own analysis.

5. Conclusion

Identifying and assessing risks in the process of digitising administrative proceedings constitutes an important element in ensuring their effectiveness, security and compliance with applicable legal provisions. This process enables the identification of threats in the legal, technological and social areas, which in turn allows for the implementation of control mechanisms individually tailored to a specific public administration unit. The development of digital tools, and consequently the improvement of management methods, means that unit managers should take actions to limit this risk to an acceptable level. As a result, effective risk management becomes an indispensable condition for the smooth functioning of modern public administration based on digital solutions. A well-functioning control system, supported in its activities by an appropriate model for determining risk areas and, consequently, by an effective risk management mechanism, may reduce or even eliminate the negative consequences of adverse events occurring within the unit (Romaniuk 2012, 81). It is recommended that risk registers kept by individual public administration units should systematically include risks associated with the process of digitising administrative proceedings.

In this context, attention should also be drawn to another issue. The development of public administration management and operations based on solutions using artificial intelligence will

[1] Risks in the context of ongoing administrative proceedings should be analysed with regard to the functioning of specific procedural institutions, such as, inter alia, the institution of reinstatement of a time limit. According to the judgment of the Voivodeship Administrative Court in Gliwice, circumstances related to a failure of the ePUAP system may constitute grounds for the reinstatement of a time limit, provided that they are made plausible. Technical problems with the operation of the ePUAP platform justifying the approval of such a request may also concern individual users and do not necessarily have to take the form of a critical system failure. However, making an individual ePUAP system failure plausible must be preceded by an attempt to establish whether the inability to effect service could indeed have occurred (Judgment of the Voivodeship Administrative Court in Gliwice of 21 December 2023, I SA/Gl 279/23, LEX No. 3653320).

be associated not only with the streamlining of administrative processes, but also with the emergence of new categories of legal, organisational and technological risks. In the literature, it has been pointed out that, in order to implement artificial intelligence systems, internal digitisation and AI-use strategies should be developed and adopted, specifying at least standards for the responsible use of technology, standards for transparency and oversight, and requirements regarding officials' competences. Moreover, training for officials is crucial and should cover the principles of AI-based systems, the assessment of the risks and consequences of AI-supported decisions, as well as the basics of personal data protection law and cybersecurity (Martyniuk-Placha & Miszczuk 2025).

Internal audit covers the assessment of the process of issuing administrative decisions, with particular regard to their digitisation, which constitutes an important element of the modernisation of public administration and affects the efficiency, transparency and compliance of authorities' activities with applicable legal regulations. Internal audit plays a key role in the electronification of administrative procedures, ensuring that the implemented digital solutions comply with legal provisions as well as with security and quality standards. It also enables the identification of risks and the improvement of processes, thereby increasing the efficiency and credibility of public administration.

The advantages of digitising administrative proceedings may include increased efficiency of public administration bodies through streamlining document flows and shortening case-handling times. The aim of the digitisation of administrative proceedings is to enhance the availability of public services for citizens. On the other hand, the disadvantages of digitisation should not be overlooked. This process may be associated with risks to data security and cyber threats, which can affect the proper functioning of public administration. The ongoing digitalization may lead to the digital exclusion of some citizens who do not possess the necessary skills or access to information and communication technologies. The lack of direct contact with an official may significantly hinder the proper explanation of complex and non-standard cases that require in-depth analysis and an individual approach, taking into account the specific circumstances of a given administrative matter. A further threat associated with the digitisation of administrative procedures may be the potential marginalisation of the role of some officials participating in the proceedings; however, it should be borne in mind that the human factor, in particular in the area of administrative discretion and judgment, cannot be fully replaced by digital solutions.

Therefore, the following de lege ferenda conclusions should be formulated. It may be important to introduce detailed regulations concerning risk management in administrative proceedings. It would be advisable to postulate the establishment of a statutory obligation for public administration bodies to maintain a digital risk register. It also appears necessary to require these bodies to periodically assess technological risks, in particular in the areas of cybersecurity and business continuity. Furthermore, it is essential to enhance the transparency of digital processes by ensuring access to information on how systems that influence case decisions operate.

Sources of law and case law

The Act on Electronic Delivery (Journal of Laws, 2026, item 3).

The Code of Administrative Procedure (Journal of Laws, 2025, item 1691).

The Act on the Computerization of the Activities of Public Entities (Journal of Laws, 2025, item 1703, as amended).

The Federal Geo-Information Act (Geoinformationsgesetz, GeolG) of 5 October 2007 (SR 510.62).

The Act on the Provision of Electronic Services (Journal of Laws, 2024, item 1513, as amended).

The Communication of the Minister of Development and Finance of 12 December 2016 on Internal Audit Standards for Public Finance Sector Entities (Official Journal of the Ministry of Development and Finance, 2016, item 28).

Communication No. 23 of the Minister of Finance of 16 December 2009 on Management Control Standards for the Public Finance Sector (Official Journal of the Ministry of Finance, 2009, No. 15, item 84).

Order of the Supreme Administrative Court of 4 June 2014, II GSK 1197/14 (LEX No. 1467669).

References

Adamus-Kowalska, J. (2018). Wdrażanie systemu elektronicznego zarządzania dokumentacją w administracji publicznej w kontekście informatyzacji i zarządzania zmianą [Implementing an electronic documentation management system in public administration within the context of computerisation and change management]. *Archeion, 119*.

Hady-Głowiak, S., & Hady-Głowiak, K. (2025). Bezpieczeństwo danych osobowych uczestników postępowania administracyjnego [Security of personal data of participants in administrative proceedings]. In E. Żuchowska-Kotlarz & A. Wołoszyn-Cichocka (Eds.), *Zarządzanie bezpieczeństwem i równością w systemach prawnych i społecznych współczesnej Europy* [Management of security and equality in legal and social systems of contemporary Europe].

Kraska, M., & Matuszewska-Maroń, M. (2013). Nowy wymiar standaryzacji dokumentów w e-administracji [New dimension of standardization of documents in e-administration]. *Przegląd Prawa Publicznego*, (4).

Krawczyk, A. (2025). Article 14. In W. Chróścielewski (Ed.), *Kodeks postępowania administracyjnego. Komentarz* [Code of Administrative Procedure: Commentary]. LEX/el.

Łuczak, L. (2014). Problematyka prawna doręczeń elektronicznych w procedurze administracyjnej ze szczególnym uwzględnieniem skutków prawnych e-doręczeń oraz oceny propozycji zmian ustawowych [Legal issues of electronic service in administrative proceedings, with particular emphasis on the legal consequences of e-delivery and the evaluation of proposed legislative amendments]. *Przegląd Prawa Publicznego*, (5).

Małecka-Łyszczek, M. (2019). Standardy kontroli zarządczej – monitorowanie i ocena [Management control standards – monitoring and evaluation]. LEX/el. Retrieved May 18, 2026.

Martyniuk-Placha, J., & Miszczuk, R. (2025). Sztuczna inteligencja w administracji samorządowej [Artificial intelligence in local government administration]. LEX/el. Retrieved May 18, 2026.

Ministerstwo Finansów. (2004). *Zarządzanie ryzykiem w sektorze publicznym. Podręcznik wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce* [Risk management in the public sector: A handbook for implementing a risk management system in public administration in Poland].

Ostasiewicz, W. (Ed.). (2004). *Składki i ryzyko ubezpieczeniowe. Modelowanie stochastyczne* [Insurance premiums and risk: Stochastic modelling].

Polski Komitet Normalizacyjny. (2018). *PN-EN ISO 22300:2018-07. Bezpieczeństwo i odporność – Terminologia* [Security and resilience – Terminology].

Przybysz, P. M. (2026). Article 14. In *Kodeks postępowania administracyjnego. Komentarz aktualizowany* [Code of Administrative Procedure: Updated commentary]. LEX/el. Retrieved May 23, 2026.

Romaniuk, P. (2012). Zarządzanie ryzykiem w kontroli zarządczej jako czynnik wspierający prawidłowe funkcjonowanie jednostek samorządu terytorialnego [Risk management in managerial control as a factor supporting the proper functioning of local government units]. *Samorząd Terytorialny*, (7–8).

Słapczyński, T. (2024). Administracja publiczna w realiach nowoczesności [Public administration in the context of modernity]. In J. Korczak (Ed.), *Administracja publiczna wobec nowych technologii. W kierunku neutralności klimatycznej* [Public administration in the face of new technologies: Towards climate neutrality].

Staniszewska, L. (2024). Postępujący proces elektronizacji administracji publicznej na przykładzie Szwajcarii

Funding
This research received no external funding.
Research Ethics Committee
Not applicable.
Conflicts of Interest
The author declares no conflicts of interest.
Copyright and License
This article is published under the terms of the Creative Commons Attribution 4.0 License. Published by Małopolska School of Public Administration – Krakow University of Economics, Krakow, Poland.
Data Availability Statement
The data supporting the findings of this study are available from the corresponding author upon reasonable request.
AI Declaration Statement
The author declares that no AI tools were used in the preparation of this manuscript.