HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 3. szám 109–131.
DOI: 10.32567/hm.2022.3.8

Annamária Edegbeme-Beláz,[1] András Kerti[2]

A New Approach to Information Security Auditing in Public Administration

Due to the rapid pace of globalisation and digitalisation and the better usage of ICT technology, cybercrime is also rising. Hence, the secure operation of controlling and auditing information systems is fundamental in both the private and public sectors. It is generally accepted in the private sector that companies seek an independent third-party's assistance to carry out information security audits. However, how do information security audits work in public administration?

The article aims to characterise and assess information security auditing in public administration and define a new solution for conducting such audits. The article is considered a theoretical research paper. Theoretical research explains the basic terms related to auditing and defines conditions for efficient and effective information security auditing. Additionally, the research aims to answer whether the internal (bureaucratic, within the public administration organisational system) or external (third-party) audits prove more effective.

Keywords: **information systems security, auditing, public administration, audit principles, internal and external auditing**

1. Introduction

Public administration is an independent system with data and workflow, terminology, special procedures and rules. The primary mission of the public sector institutions is to realise public tasks within the internal and external domain; at the core of this mission stands nothing else but information. Therefore, information security management and auditing in public administration affect the efficiency, reliability

[1] PhD candidate, Óbuda University Doctoral School on Safety and Security Sciences, e-mail: belaz.annamaria@uni-obuda.hu
[2] Associate Professor, University of Public Service, e-mail: kerti.andras@uni-nke.hu

and quality of the realised public tasks. Information security audit is a complex process that requires good knowledge and understanding of the internal and external environment of public administration and its structure in systems and processes. Hence, information security management and auditing in public administration are often analysed in a way that separates it from the functioning of a public institution as an entirety.[3]

For the public administration system to remain operational in the long run, and the protection of data generated, stored, processed and transmitted in the systems to be ensured, the state has a significant task of organising, developing and maintaining an information security approach. To achieve this goal, information security tasks and programs must be orchestrated at both legal and strategic levels; moreover, risk analysis, evaluation processes and solutions, and predictive functions must form an integral part of them. Many countries and organisations acknowledge the need to develop efficient solutions that facilitate increased information security levels.[4]

The protection of the organisational system and infrastructure of the public administration is principally justified because public administration is responsible for the implementation of fundamental state tasks, so when we talk about administrative tasks and functions, we examine the underlying prevailing state interests behind these tasks.[5] The five primary domains of public administration (foreign affairs, law enforcement, military affairs, jurisdiction and financial administration) stem from the statehood of the state, scilicet, the exercise of public power. With the modernisation of the state and public administration, these five essential functions will not disappear but will be constantly extended and differentiated. It is indisputable that the protection of public administration and the infrastructure supporting it is a crucial area for all states.

For the subject of the present study, the question is inevitable: what do we mean by security? For most people, security is nothing more than a calm, threat-free state. At the same time, we must acknowledge that this definition is rather superficial, as there are many theories and different scientific approaches to the concept of security. After examining the definitions used to describe security, Máté Gábri [6] made the following statement:

[3] Ana-Maria Suduc et al.: Audit for Information Systems Security. *Informatica Economică,* 14, no. 1 (2010). 43–48; Kenneth J. Knapp et al.: Key Issues in Data Center Security: An Investigation of Government Audit Reports. *Government Information Quarterly,* 28, no. 4 (2011). 533–541; Dalibor Drljača – Branko Latinović: Audit in Public Administration's Information Systems – External or Internal? *IOP Conference Series: Materials Science and Engineering,* 200, no. 1 (2017). 1–7.

[4] Edyta Karolina Szczepaniuk et al.: Information Security Assessment in Public Administration. *Computers and Security,* 90 (2020). 1–11; Costel Mironeasa – Georgiana Gabriela Codină: A New Approach of Audit Functions and Principles. *Journal of Cleaner Production,* 43 (2013). 27–36.

[5] Annamária Beláz: A közigazgatás információbiztonsága: megjósolhatók az incidensek? *Hadtudomány,* 29, no. 3 (2019). 92–104.

[6] Máté Gábri: Biztonsági komplexumok az információs korban. *Hadmérnök,* 5, no. 4 (2010). 110–121.

"… in general, the concept of security is built around some kind of threat, which has a source and a subject. The definition of a threat can be objective or subjective. The former is characteristic of the traditional theory, while the latter is characteristic of novel thinking. In connection with a threat, security may mean the complete absence of a threat or the existence of assets that can be used to limit or reduce the threat."

Among security professionals, Ole Wæver is one of the novel thinkers. In his perspective, security is a state where threats exist, but we can take countermeasures.[7] We believe that this definition can be adequately applied in the present study, as information security threats from cyberspace are constantly present, i.e. they exist. However, the governments in the context of the performance of security tasks can defend against security incidents and develop existing capabilities. We will present a new solution for handling such threats by an innovative approach of information security auditing in the public administration sector.

The subject of the research is the public administration institutions in Hungary, in the context of the security of auditing information systems. The public administration constitutes a complex mega-system comprised of multiple subsystems. Functional and organisational complexity of public administration, regarding the security management of information systems, constitutes an interdisciplinary subject of research. The theoretical basis of the discussed issue originates in various academic fields, e.g. computer science, public administration science, management and quality sciences, security sciences and legal theory.

The main goal of the research is to propose a new public institution for information systems security auditing. Reaching the adopted goal required realisation of the following, theoretical in nature, detailed goals:

- defining information security auditing in the public sector
- demonstrating and identifying the challenges and risks of the two major audit types used currently
- explaining why there is a need for a new perspective and what possible advantages may the new approach bring

2. Overview of auditing

To understand the disparities between the bureaucratic internal and the suggested new independent information security auditing models in the public sector, we first need to understand the fundamental auditing concepts. In the following section, we will scrutinise: 1. the purpose of auditing; 2. the types of audits; 3. the function of audit; and 4. the audit process. Information security (IS) systems audit differs from auditing financial records, general operations, or business processes. Each of these disciplines share the common foundation of principles, standards, processes and

[7] Fen Osler Hampson: Review: Barry Buzan – Ole Wæver – Jaap de Wilde: Security: A New Framework for Analysis. *International Journal,* 53, no. 4 (1998). 798–799.

activities.[8] However, to distinguish from the more common financial connotation, it is important to highlight that in this research the focus is on IS auditing and not on the financial assessments.

2.1. Audit goals

In the literature, there are several definitions for auditing,[9] but all of them involve the following keywords: effective, efficient and economical use of resources; data integrity; compliance with national and international standards; collecting and evaluating evidence.

Based on these theories, auditing is a complex notion, and a management tool that evaluates an organisation's performance determines the implementation of the management principles and controls if the criteria for the activities are met. Through auditing, the status of the auditable institution and its enterprise capabilities can be measured. An audit always has a baseline, or standard of reference against which the auditee is compared. As a management tool, audit generates trust in: support and implementation of performance policy, the achievement of objectives and the creation of added value. Completing the audit process will provide relevant and representative conclusions on which directions for improvement can be established.[10]

Auditing purposes are not always alike, different areas can be audited for numerous purposes in an organisation.[11] Firstly, legally compulsory audits are conducted to inform external stakeholders about the company's operation, the supervision system and the functioning of certain restrictions and policies. The regulation of mandatory audits applicable to every organisation in the same domain, so in addition to reliability and supervision, audits impact the development of equal opportunities and fair competition.

---

[8] Stephen D. Gantz: Chapter 5. Types of Audits. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014c.

[9] Mironeasa–Codină (2013): op. cit.; Drljača–Latinović (2017): op. cit.; Andrea Kő – Balázs Molnár: *Az információrendszerek auditálása. Az informatika és az információrendszerek ellenőrzési és irányítási módszerei.* Budapest, Corvinno Technology Transfer Kft., 2009; Giorgia Mattei et al.: Exploring Past, Present and Future Trends in Public Sector Auditing Research: A Literature Review. *Meditari Accountancy Research,* 29, no. 7 (2021). 94–134; Bjørn Stensaker: *External Quality Auditing: Strengths and Shortcomings in the Audit Process*. *External Quality Audit: Has It Improved Quality Assurance in Universities?* Woodhead Publishing Limited, 2013.

[10] Costel Mironeasa – Silvia Mironeasa: The Process Approach and the Generated Value at the Process Level. *Metalurgia International,* 14, no. 6 (2009). 89–93; Mironeasa–Codină (2013): op. cit.; Ling Lei Lisic et al.: You Can't Get There from Here: The Influence of an Audit Partner's Prior Non-Public Accounting Experience on Audit Outcomes. *Accounting, Organizations and Society,* 100 (2021); Qiu Gaosong – Yuan Leping: Measurement of Internal Audit Effectiveness: Construction of Index System and Empirical Analysis. *Microprocessors and Microsystems,* (2021); Stephen D. Gantz: Chapter 1. IT Audit Fundamentals. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014a.

[11] Gantz (2014a): op. cit.

The condition is different in the second circle: voluntary audits. As its name suggests, the institutions are not obliged to conduct voluntary audits but carry out these evaluations to reach the highest possible self-control and development level. Moreover, these organisations collect more data on their operation by conducting audits, giving them broader control over their processes, and implementing management plans.

The third possible goal of auditing is to get certified. For a third-party audit, the audit baseline is usually defined in rules or legal or regulatory requirements related to the purpose or objective of the audit.[12] These assessments often result in a certificate stating that the organisation's management systems and processes conform with that baseline. The most popular quality management standard is ISO 9001, and the ISO/IEC 27001 is the leading international standard for information security management systems (ISMS).

There are unique objectives for information security audits,[13] which are the following:

- check the existence of security policy, standards, guidelines and procedures
- identify the inadequacies and examine the effectiveness of the prevailing policy, standards, guidelines and procedures
- identify and understand the actual vulnerabilities and risks
- review present security controls on operational, administrative and managerial issues, and ensure compliance to minimum security standards
- provide recommendations and corrective actions for enhancements

2.2. Types of audits

To understand the question of auditing, it is necessary to see the differences between the audit types. There are several classification methods of audits in the professional and academic literature, depending on the scholars' aspects and viewpoints.[14] In this article, we typified the audits by three features: 1. independence; 2. scope; and 3. application domain. The following table summarises our cataloguing.

[12] Gantz (2014a): op. cit.

[13] Suduc et al. (2010): op. cit.

[14] Drljača–Latinović (2017): op. cit.; Gantz (2014c): op. cit.; Gregory Michener et al.: Are Governments Complying with Transparency? Findings from 15 Years of Evaluation. *Government Information Quarterly,* 38, no. 2 (2021); Deniz A. Appelbaum et al.: Analytical Procedures in External Auditing: A Comprehensive Literature Survey and Framework for External Audit Analytics. *Journal of Accounting Literature,* 40 (2018). 83–101; Gary Giroux – Rowan Jones: Measuring Audit Quality of Local Governments in England and Wales. *Research in Accounting Regulation,* 23, no. 1 (2011). 60–66.

Table 1: Main types of audits

Category	Audit type	Description
Independence	Internal audit	The audit process is an integral part of the organisation. It means the continuous control of the systems' security status and reliability, the existence of security requirements; the implementation of the organisation's security policy; the compliance and application of internal regulations.
	External audit	Also known as third-party auditing, independently and impartially monitors the internal audit, the operation of the internal control and management system and the audited system's security status.
Scope	Organisational audit	The extent of this audit is the organisation as a whole, with all its functions, subsystems and processes.
	Specialised audit	This is a targeted audit; the examination's extent is limited to specific procedures, functions, or systems.
Application domain	Operational audit	Operating audit has the purpose of evaluating the structure of internal controls of a given process or work area. An example of this type of audit is the audit of application controls and logical security systems. This is a specific and targeted audit.
	Financial audit	The purpose of this audit is to evaluate the validity of financial reports. It relates to the integrity and reliability of financial information. This audit in public administration institutions is obligatory by law and usually performed by contracted auditing companies such as PricewaterhouseCoopers and Deloitte. It can also be done by an authorised independent and licensed auditor under the condition that there is no conflict of interest, and the auditor is not an employee of the institution auditing.
	Integral audit	The integral audit, in essence, is implemented to evaluate organisational goals related to the financial information, preserving of property, efficiency and harmonisation with the overall goals of the audited institution.
	Administrative	Aims to evaluate issues related to the efficiency of operative productivity within the organisation or institution. An administrative audit can be agreed even as part of more complex reviews and audits.
	Information security audit	IS auditing is an umbrella term, relates to the next sections: technical evaluation auditing management of IT control procedures auditing the processes of the IT department, software development and inspection of application systems compliance with international and national standards Its goal is to maintain the confidentiality, availability and integrity of the data stored and the system by collecting and evaluating evidences. This should assure achievement of business, organisational and control aims and that the unwanted events will be discovered, prevented and/or corrected.

Source: Compiled by the authors.

2.3. Audit functions

The ecosystem where an organisation activates affects its functions, system and processes; thus, one must consider the environment and the flow exchange between the system processes during the evaluation process.[15] As discussed earlier, the audit is a management tool, a process with its functions, which must be integrated into the organisation's management scheme.

Mironeasa and Codină (2013) argue that irrespective of the nature of the audit mission, application domain, or type, audit functions must be the same as follows:

- Function 1 – management tool – provides information for the decision-making process
- Function 2 – quality assurance vector – sets the performance level of the audited entity by assessing the effectiveness and efficiency
- Function 3 – intelligence provider – the participating persons develop additional well-defined competencies
- Function 4 – recognised authority – results are appreciated and put into practice
- Function 5 – mediator – the level of compliance is judged concerning the referential used
- Function 6 – means of influence – communicates management and stakeholders' expectations
- Function 7 – priority setting – establishes a hierarchy of the most important aspects (risks) that may affect functionality
- Function 8 – reliability provider – brings added value by relying on facts and real evidence
- Function 9 – impact creator – produces effects upon evidence

2.4. Audit process

Having in mind various aspects and points of interest for audit, the organisation's management must define the audit program (known as the Audit Charter), including the aim, type, scope and volume. Generally, the audit program falls into two phases: investigation and reporting. The auditor gathers the data, facts and evidence from the report's basis during the investigation phase. The report shall include the audit findings, whether the management complies with professional practice and regulations.[16]

Information security audits usually follow a risk-based approach, which results in a longer audit program consisting of the following phases:

1. *Planning* – determining and selecting effective and efficient methods for performing the audit and obtaining all necessary information. Since audits can last from just a few hours to several months, planning must include the audit schedule at least a year in advance.

[15] Alexandra Kanellou – Charalambos Spathis: Auditing in Enterprise System Environment: A Synthesis. *Journal of Enterprise Information Management,* 24, no. 6 (2011). 494–519; Michener et al. (2021): op. cit.

[16] Kő–Molnár (2009): op. cit.

2. *Data collection* – determining how much and what type of information to be captured and how to filter, store, access and review the audit data and logs.

To get the most out of the audit process, the auditor needs to gather intelligence. The volume and type of information and how to filter, store, access and review the audit data and logs are determined before the auditing in the planning phase. During the audit process, there can be several data sources. Figure 1 demonstrates the most common ways how auditors can collect data.

Figure 1: Data sources during an audit
Source: Compiled by the authors.

1. *Audit tests* – audit tests can be a compliance test (general review of existing security policies or standards and their compliance with the professional requirements) or substantive tests (detailed review of the existing security configurations and technical investigation).
2. *Reporting* – present the current security environment.

Report of findings should be promptly issued and present in the current security context. The audit report must be complete (contain all selected criteria), pertinent (stick to the audit scope) and accurate. It must contain appropriate conclusions and findings revealed during the audit, resulting in recommendations in line with the audit objectives, efficient, feasible and scheduled. The report is written in a language that is comprehensible to the management. The auditor's opinion expresses the interests concerned in applying the audit functions and is found in the audit results called audit findings. In this way, the opinion becomes a value that fits the organisation's culture.

Since vulnerabilities and threats evolve with time and the situation, security audits should be conducted periodically. This way, the fulfilment of security policy and the set of controls required to reduce risks to a satisfactory level can be ensured. Therefore, auditing should not be viewed as a one-way practice but a crucial part of the organisational life cycle.

3. Internal – bureaucratic – audits

As outlined in Table 1, we classify audits by different features; one is independence. Based on independence, we can talk about internal and external audits. With internal audits, the whole process is an integral part of the organisation. It means the continuous control of the systems' security status and reliability, the existence of security requirements; the implementation of the organisation's security policy; the compliance and application of internal regulations.

In practice as Figure 2 demonstrates, it implies that – depending on the size and structure of the organisation – at least one employee works as an auditor. He/she plans the audit, gathers the information, carries out the audit process and reports to the management. The auditor should be a competent person with sufficient skills and knowledge needed to implement the audit. The management should make all necessary efforts to make the internal auditing as independent as possible.

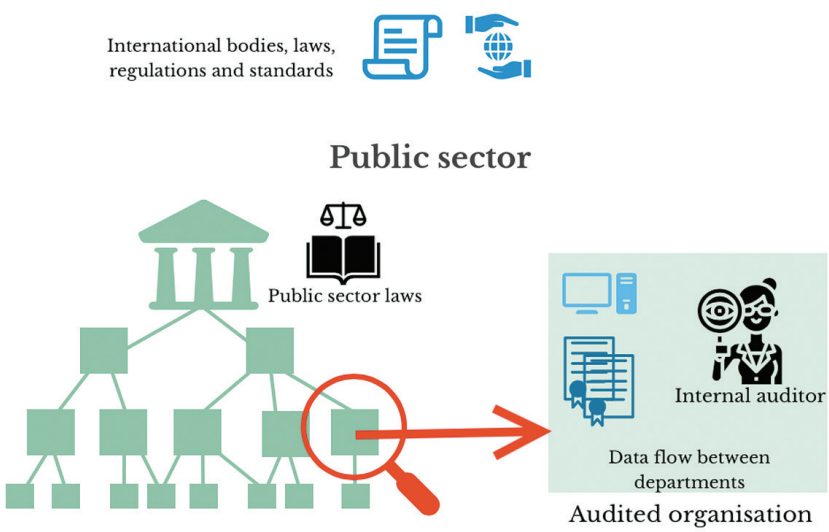

Figure 2: Internal auditing in the public sector
Source: Compiled by the authors.

Internal auditing is widely used in all sectors and every organisational level and it is especially popular in the public sector. Internal auditors are not just skilful professionals

but members of the organisation they are auditing; therefore, they can quickly evaluate the processes and procedures due to working experience and affiliation. The required information is easily reachable; there is no need for data transmission, which means the risk of data loss or leakage is extremely low. Moreover, as employees of the auditee, they strive to get the best outcome for their institution, are eager to pay attention to details, and focus on security aspects.

Despite the numerous advantages of internal auditing, there are many concerns regarding the efficiency and effectiveness of such audits. Unfortunately, to date, there is no settled term or usage in the scientific literature for the various descriptions of audit efficiency (so-called efficiency, value for money, comprehensive or performance auditing); therefore, when used in this article, we are referring to the broad area of efficiency meaning getting the most from the inputs and the expected results from the outputs.

What is the primary concern regarding the effectiveness of internal audits? Auditing has previously been the subject of extensive fieldwork and ethnographic analysis, regarding this Kanellou and Spathis (2011) notes: "Auditors' notions of 'effectiveness' were seen as key to the expression of auditing findings. Simply put, auditors said what they thought their audiences were ready to hear, both in terms of a willingness to act, in terms of political possibility, and in terms of an ability to act." Nevertheless, what happens when the auditors say what their audience is ready to hear? There must be a discrepancy between the audit findings and reality; consequently, auditing itself cannot fulfil its purpose. In his studies about a distortion of truth, Michael Taussig refers to such kind of discrepancy as 'public secret' that is generally known but cannot be articulated or spoken.[17] Later in his analysis amplifies this to things that are so 'publicly secret' that even the appearance of knowledge of the secret must be avoided: hence people "know they must not know".

Based on Taussig's public secret concept Vaughan S. Radcliffe presents that people may become wrapped up in the public secret to the extent that at times they deny its existence entirely, while others may recognise the importance of upholding the public secret in the functioning of society. He states that auditors recognise the role of public secrets in the auditing world, and hence to the ready adherence to the public secrets of modern society, government auditing may unintentionally tend towards an attendance to those in power. How so?

The auditing language is itself defining and facilitating; therefore, an internal auditor in the public sector may define political problems as business problems, thus transferring political debate of potentially threatening matters. The auditing's ability to redesign what might otherwise be political only requires proper management and language techniques; consequently, an auditor only includes 'strategically wise' findings in the audit report. This practice decreases auditing efficiency because it cannot fulfil its function as an intelligence and reliability provider. In order to understand the real problems, the management has to critique the audit report from within, comparing audit findings with the public secrets – the things that are known but cannot be said

[17] Beryl Bellman: Defacement: Public Secrecy and the Labor of the Negative. *American Anthropologist,* 103, no. 3 (2001). 878–879.

or cannot be seen to be known. As Radcliffe summarises,[18] the truth value of audit findings in areas marked by public secrecy is highly questionable.

Besides the truth content of the audit reports, another area of apprehension towards internal auditing in the public sector concerns the auditors themselves regarding how they understand their work, position and function. Senior auditors who have several years of experience upholding public secrets might think that knowing what not to say or what not to know is essential in writing a successful and efficient audit report. "If the only positive outcomes seen from audit work are those cases in which recommendations are enacted then there is the potential for an inherently conservative and unambitious taint to enter audit inquiry. Auditors must deal with this as they manage their presentation of self, both to others and […] as a matter of identity."[19] In many organisations, the relationships among the various functional groups involved in information security are less than ideal. Internal auditors often experience conflict and even adversarial relationships with other organisational functions.[20] Thus, it is not surprising that the relationship between the internal audit and information security functions is sometimes characterised by conflict and distrust.[21] Auditors must deal with this as they manage their presentation of self, both to others and in representing and making sense of their work internally as a matter of identity.[22]

The two characteristics mentioned above – truth content and auditor profession – can apply to all application domains of internal auditing. However, when designing information security audits, four more areas should be analysed. These are: 1. knowledge and reliability; 2. dependency; 3. outcome and customer satisfaction; 4. information safety and security. The following heading will discuss these areas and how internal auditing works compared to the suggested independent auditing model.

4. New approach: independent auditing

4.1. Concept

As outlined in the introduction within source literature, the issue of information security management and auditing in public administration is often analysed in a manner that separates it from the functioning of a public institution as an entirety. Public administration is an independent system with its data- and workflow, terminology,

[18] Vaughan S. Radcliffe: Public Secrecy in Auditing: What Government Auditors Cannot Know. *Critical Perspectives on Accounting,* 19, no. 1 (2008). 99–126.

[19] Radcliffe (2008): op. cit. 115.

[20] Zaini Ahmad – Dennis Taylor: Commitment to Independence by Internal Auditors: The Effects of Role Ambiguity and Role Conflict. *Managerial Auditing Journal,* 24, no. 9 (2009). 899–925; Mortimer A. Dittenhofer et al.: *Behavioral Dimensions of Internal Auditing. A Practical Guide to Professional Relationships in Internal Auditing.* Altamonte Springs, Florida, The Institute of Internal Auditors Research Foundation (IIARF), 2010.

[21] Paul John Steinbart et al.: The Relationship between Internal Audit and Information Security: An Exploratory Investigation. *International Journal of Accounting Information Systems,* 13, no. 3 (2012). 228–243.

[22] António Samagaio – Teresa Felício: The Influence of the Auditor's Personality in Audit Quality. *Journal of Business Research,* 141 (2022). 794–807.

special procedures and rules; therefore, a systemic approach must be applied when interpreting security. When perceiving public administration as a system, it is reasonable to interpret security from systemic research. System security is understood as a property of an object, defined as the ability to protect an object's internal values (resources) against the occurrence of dangerous situations (threats).[23] If we accept this definition, the term security should be considered concerning possible threats and the risk of those. Information security secures legally protected information against unauthorised interference (disclosure, modification, erasing) in line with these statements.

During the examination we must keep in mind that the core mission of the public sector institutions is to realise public tasks within the internal (providing services for citizens) and external domain (cooperation of public administration units or with private sector institutions). According to Herbert A. Simon, public administration institutions carry out their tasks by finding the best decisions based on available information.[24] Decision-making in an institution is realised by processing input information into output information. In public administration, an institution is a set of cooperating elements that gather and process data (input data), emit and deliver feedback to achieve an adopted goal (output data). An example of the process described is the issuance of an administrative decision, e.g. license card, where the input data are the documents – such as certificate of driver's education course, certificate of the successful driving test, proof of residency and proof of age – delivered by the citizen, and the output data is the issued driving license.

We can boldly state that the functioning of public administration is based on gathering, processing, transmitting, storing and sharing information; therefore, information is one of the fundamental assets, and it is considered a protected value. Since information is a crucial element of public administration, a security incident can significantly lower the quality of administrative service. In extreme cases the disruption of these processes can lead to a complete breakdown of service delivery.

Both realisation and quality of provided services simultaneously must be taken into consideration as attributes of information security. Szczepaniuk et al. (2020) suggest defining information security in public administration as a state and a process in which:

- information security is achieved and sustained on a predetermined level of confidentiality, integrity and accessibility
- security of provided services is achieved and sustained on a predetermined level of reliability, accessibility and integrity of services
- authentication and accountability of entities, related to authentication of users utilising specific information and services are provided
- elements which constitute the public administration system are characterised with the ability to protect against current and future disruptions (threats) for

[23] Szczepaniuk et al. (2020): op. cit.

[24] Herbert A. Simon: Decision-Making and Administrative Organization. *Public Administration Review,* 4, no. 1 (1944). 16–30.

functioning or loss of specific values – the system is resistant toward threats (internal, external, accidental, purposeful)
- information and service users and recipients are aware of threats and are invulnerable to them
- perpetuators of security incidents have restricted possibilities to use cyber-space for the purpose of generating threats by utilising vulnerabilities and gaps within the security system

Since information itself and information security play a crucial part in the functioning of the public administration system, information security auditing has to play a vital role. Considering the above-mentioned internal auditing is not sufficient for public sector information security. However, a question is arising: Is third-party auditing considered the core mission of the public sector, or is there a demand for renewal?

We have to briefly revise how third-party auditing works and why it is used mainly in public administration to answer that question. From the dependency viewpoint, third-party auditing independently and impartially monitors the internal audit, the operation of the internal control and management system, and the audited system's security status. Regarding the scope, these audits can be organisational or specialised.

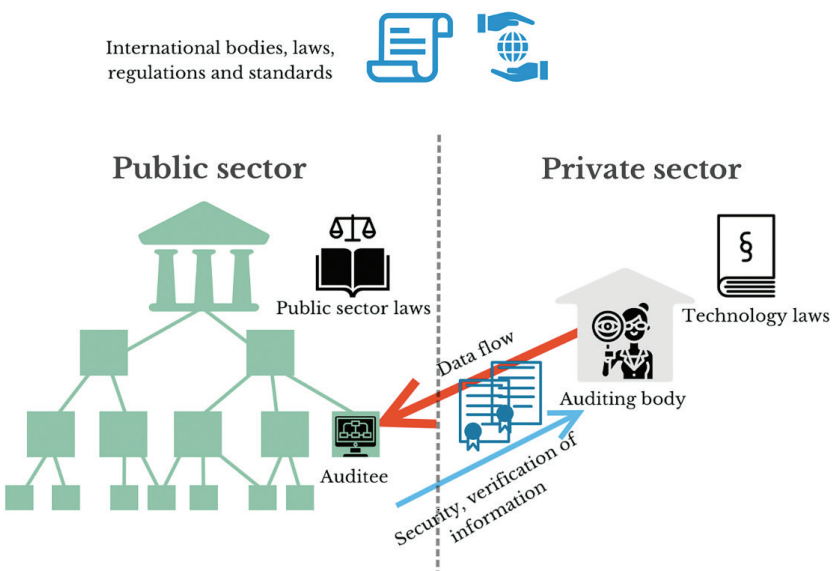

Figure 3: Third-party auditing of a public sector institution
Source: Compiled by the authors.

Third-party or external audits are performed by an auditing firm, entity outside the subject organisation. Depending by the size and the complexity of the IS audit,

the assessment is performed by a single auditor or a team.[25] As shown in Figure 3, whenever a public entity wants a third-party auditor to scrutinise its workflow and security state, they have to hire a private sector company. Though these companies must be accredited by the state to conduct audits (usually these corporations are registered or licensed with oversight bodies, such as the Committee of European Auditing Oversight Bodies [CEAOB]), undoubtedly, several risks arise when working with them.

Since public sector organisations are not obliged to work with the same auditor, each time a third party is introduced, the organisation is required to trust the new entity. Moreover, as discussed earlier, an audit ends with the issuance of the audit report, which contains appropriate conclusions and findings revealed during the audit, resulting in recommendations in line with the audit objectives. Since the recommendations are not obligatory, the organisation has no legal responsibility to modify its system or workflow. As the research by Stensaker (2013) shows "an external audit panel may be reluctant to reach and make explicit its conclusions and recommendations during the visit". This may imply that the opportunity of improvement for the client is lost, hence the impact of the audit process is extremely limited.

Regarding the internal auditing, Steinbart makes the following comment: "Certainly, self-monitoring is useful […]. Yet, there is considerable evidence that people have great difficulty in identifying and in correcting errors in systems that they created themselves."[26] In our opinion, this statement is true to third-party audits particularly in the public sector. The goal of these audits in the private sector is usually to prepare an organisation for accreditation or certification; however, holding such certifications is not shared in the public sector. Moreover, if we see public administration as a system, auditing should be considered an integral part of it. But how?

The solution is the adoption of a new approach by the establishment of the Autonomous Public Auditing Agency (APAA). Thanks to technological change, multi-causality, ad hoc approaches and short-termism, governments face many challenges these days. To address rapidly developing technologies, they need a more profound knowledge of these technologies and evolving policies simultaneously.[27] Instead of letting the control over their bodies, the governments should institute an auditing entity.[28]

[25] Stephen D. Gantz: Chapter 4. External Auditing. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014b.

[26] Paul John Steinbart et al.: The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes. *Accounting, Organizations and Society,* 71 (2018). 15–29.

[27] Piret Tõnurist – Angela Hanson: Anticipatory Innovation Governance: Shaping the Future through Proactive Policy Making. *OECD Working Papers on Public Governance,* no. 44 (2020).

[28] Zoltán Nyikes – András Kerti: Proposals for Amending the Regulation of the Administrative System. *Journal of Emerging Research and Solutions in ICT,* 1, no. 1 (2016). 68–74.

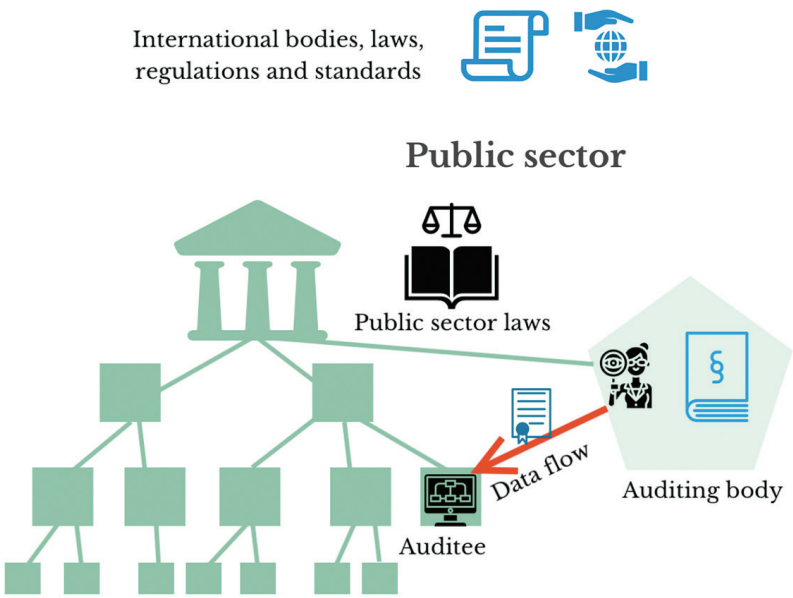

Figure 4: Autonomous Public Auditing Agency (APAA)
Source: Compiled by the authors.

As Figure 4 shows, the APAA is an auditing institution within the public administration system established by the government. Its goal is to overview and strengthen the information system security of the public sector by conducting regular audits. In the practice of analysis of information threats, various risk assessment methods are used, such as:

- OCTAVE – Operationally Critical Threat, Asset and Vulnerability Evaluation
- CRAMM – CCTA Risk Analysis and Management Method
- MEHARI – Method of Risk Analysis
- FMEA – Failure Mode and Effect Analysis
- ISRAM – Information Security Risk Analysis Method

Moreover, compliance with risk management methods within norms, standards and good practice would be required, such as: ISO/IEC 27001 norm and related norms (ISO/IEC 27001; ISO 27005), COBIT methodology, or NIST 800–37.

There are several specifications of the APAA compared to the third-party audits. The most significant are:

- the central government budget finances the APAA audit process; therefore, all public entities can participate in the audit programs irrespective of their financial status
- the personnel of the institution is made up of public servants with the necessary regulatory and technical expertise
- the audit report contains the analysis of non-compliance and errors accompanied by the set of controls required to reduce risks to a satisfactory level until the

next audit date. The failure to implement the necessary controls can conclude in receiving a fine. Since the feedback is not only in writing, but a detailed and executable action plan, there are no possibilities for misinterpreting it, finding in 'between the lines' information.[29]

The following section will analyse the advantages of setting up the Autonomous Public Auditing Agency for information security auditing and broader general audits for the public sector compared to internal and third-party auditing based on four characteristics. 1. knowledge and reliability; 2. dependency–independency; 3. outcomes; 4. data safety and security.

4.2. Advantages of the Autonomous Public Auditing Agency

The following table summarises the four areas of discussion:

- knowledge and reliability
- dependency–independency
- outcomes
- data safety and security

Table 3: Comparison between internal, third-party and APAA auditing methods

	Internal	**Third-party**	**Autonomous Public Auditing Agency (APAA)**
Knowledge and reliability	Skilful to evaluate the status of the technology, processes and procedures due to working experience and affiliation.	May only follow the instructions from frameworks and standards and not specifically experienced in the field.	Experienced both in the public administration system procedures and the best worldwide practices, standards and regulations.
Dependency	Public servant, member of the auditee organisation, complete objectivity is unapproachable.	Completely independent from the auditee organisation and the public sector as a whole.	Member of the public administration system, but fully independent from the evaluated organisation.
Outcomes and customer satisfaction	Pays less attention to the achievement of customer satisfaction; focuses more on security aspects.	Customer satisfaction is essential; focuses on overall functioning, especially in communication and information flow.	Main goal is the compliance with national and international regulations, achieving the 3 "E" management.
Safety and security	Narrowly defined "in-house" – no data transmission.	Potential point for "leaking of information"; may cause false interpretation of the collected data and mistrust.	Broadly defined "in house" – regulated methods of data storage and transmission within the public administration system.

Source: Compiled by the authors.

[29] Stensaker (2013): op. cit.

4.2.1. Knowledge and reliability

An auditor should be a technically competent person with sufficient skills and knowledge needed to implement an audit. "Auditing internal IT controls requires broad IT knowledge, skills, abilities and expertise in general and IT-specific audit principles, practices and processes."[30] Information security audits require more profound technical knowledge in a large and fast-changing field of ICT and the broad area of the information system component. "It is likely that when auditors possess technical knowledge, they can ask the kinds of important questions that cause information security professionals to see the potential value of further interaction."[31] Moreover, the auditor must understand the legal framework (legal aspects related solely to the audit of information systems and legal aspects of the audit topic, which is more specific) and the international standards and best practices on auditing. However, it is also necessary to know the legal framework for business operations in the company or the institution.

On the one hand, based on the working experience and familiarity with the organisation, the internal auditor is skilful in evaluating the IS technology, processes and bureaucratic procedures.[32] On the other hand, a third-party external auditor may demonstrate adequate IS knowledge and expertise supported by professional certifications. However, since public administration certificates and knowledge is not a prerequisite by law from external auditors to carry out assessments, it is possible that an auditor who has no work experience with public institutions may only follow the instructions from frameworks and standards and might lack the knowledge on legal aspects of the audit topic. Not having directly experienced counterparts' perspectives can leave auditors vulnerable to their pre-existing motivations.

Organisations need to either develop or acquire personnel with the specialised understanding of control objectives and experience in IT operations necessary to effectively conduct IS audits. The auditor of the APAA would be a professional equipped with the required technical knowledge and experience both in the procedures of public administration systems and the IS industry best practices, standards and regulations. When auditors possess detailed expertise about public administration and information security, they can develop deeper relationships with the information systems security function. Moreover, based on the experimental research conducted by Lisic et al. (2021) combined public sector and industry experience enhances the auditors' understanding of managers' motivations, and pressures, as well as their understanding of business processes and risk, thereby enabling them to more effectively evaluate and address risks leading to better audit judgments and higher audit quality.

[30] Gantz (2014a): op. cit.
[31] Steinbart et al. (2018): op. cit.
[32] Karim Hegazy – Anne Stafford: Internal and External Auditors Responsibilities and Relationships with Audit Committees in Two English Public Sector Settings. *Corporate Ownership and Control,* 18, no. 3 special issue (2021). 395–409.

4.2.2. Dependency

For auditing to reach its goal, as discussed earlier, the independence of the audit process is vital. If implemented as an internal audit, the management should make all necessary efforts to make this audit as independent as possible. However, a hint of subjectivity will always be present in these processes. At the core of information security audit is the evaluation of related risks. Even the most objective persons from the institution or organisation can be biased in evaluating the information systems and their functionalities.

Moreover, internal auditors are public servants and members of the auditee organisation; they are responsible to the top management of the public administration agency. The aims of the internal audit should be aligned with the mission and vision of the organisation, and the audit findings should support that vision. The notion of bureaucracy and the organisational hierarchy put auditors under the management. Their suggestions and recommendations therefore are subjected to the approval of the management, which is likely to ignore them in a situation where the findings of the internal auditors are adverse.[33] If we remember Radcliffe's discoveries on public secrets, the truth value of audit findings in areas marked by public secrecy is profoundly doubtful. Therefore, the accuracy of the internal audit findings will always be disputed. Significant amount of research was carried out to highlight the level of independence of internal auditors, and many came to the same conclusion as Dwamena and Ofori stating that internal auditors lack independence from management since they are mostly working under the direction and control of the management.[34]

In the context of external auditing such independence is often not just required, but legally enforced.[35] Nevertheless, since the third-party auditors are entirely independent of the auditee organisation and the public sector, they will lack the understanding of the bureaucratic public administration bodies' processes, terminology and organisational structure, which could unintentionally support public secrets.

An APAA professional is a member of the public administration system, equipped with the necessary knowledge but entirely independent from the evaluated organisation. The auditor would have no benefit from upholding a public secret but would understand the mechanism of public secrecy; therefore, the audit findings would be reliable and objective. Moreover, when an auditor "perceives its role to be more of an advisor instead of a policeman, mutual trust between the audit and information systems security functions is more likely to develop. In turn, as mutual trust between the two functions increases, so too does cooperation".[36]

[33] Richard Ofosu Dwamena – Nicholas Yaw Ofori: The Roles and Status of Internal Auditors in Public Sector Organizations. *Finance and Management Engineering Journal of Africa,* 3, no. 9 (2021). 1–22.

[34] Richard Ofosu Dwamena: Investigating the Relationship Exist Between Internal Auditors and Management. *Finance and Management Engineering Journal of Africa,* 3, no. 9 (2021). 23–35; Masruddin Jamaluddin et al.: Role Ambiguity, Role Conflict, Auditor Competence on Audit Quality: The Mediating Effects of Auditing Planning and Independence. *Universal Journal of Accounting and Finance,* 9, no. 6 (2021). 1551–1557.

[35] Gantz (2014b): op. cit.

[36] Steinbart et al. (2018): op. cit.

4.2.3. Outcomes and customer satisfaction

Client satisfaction is a related construct to audit quality.[37] Since the clients hire and pay the auditors to discover gaps and non-compliance in their processes, client satisfaction should be an important goal to most auditors. As the result of continuous digitalisation, many organisations process thousands of terabytes of internal and even more external data. Over time it is foreseeable that the audited institutions will expect deeper insights from the auditors (possibly through the usage of big data analytics) to maximise the benefits of their investments.[38] For this need, the APAA would be a suitable solution since it could act as a hub of IS information for the public sector. Given that the financial resources are provided by the state budget, the Agency would be able to invest in complex data mining and processing systems. With the advantage of data processing speed, these systems will help to improve the quality and efficiency of the audit, meet the requirements, and increase the trust level of clients.[39]

An audit can potentially add value in many ways because the feedback from audit can identify opportunities to improve the effectiveness of all types of information systems controls. The results target is the compliance of organisations with their own policies, moreover the coherence with national and international regulations, and it can identify the extent of corrective actions. Thus, the APAA auditor can achieve the "triple E" management (economy, efficiency and effectiveness).

The internal auditor will pay less attention to customer satisfaction and pay more to the security aspects of the information systems. In contrast, the external auditor can focus instantly on the overall functioning of the information systems independently, especially when dealing with communication and information flow. The primary goal of the external auditor is customer satisfaction and reliability of processes. As shown in the results of the empirical study conducted by Giroux and Jones (2021), it indicates that private sector auditors provide higher quality audits on lower fees than in-house auditors. Other research proved that although an auditor's expertise in public sector auditing increased satisfaction and quality, yet the Big 4 external auditors did not provide either higher client quality or increased satisfaction.[40]

Many studies found[41] that job pressure of internal auditors and auditors at third-party auditing firms (time management and volume of audits) can lead to dysfunctional behaviours and those may directly affect the audit report. This will culminate in shortened audits, (signing off audit report before completion), lack of research on standards, superficial reviews of the auditees' documents and accepting weak explanations. Similarly, stress reduces the likelihood of detecting material misstatements.

---

37 Giroux–Jones (2021): op. cit.

38 Appelbaum et al. (2018): op. cit.

39 Thi Tam Le et al.: Risk-Based Approach and Quality of Independent Audit Using Structure Equation Modeling – Evidence from Vietnam. *European Research on Management and Business Economics,* 28, no. 3 (2022).

40 Donald Samelson et al.: The Determinants of Perceived Audit Quality and Auditee Satisfaction in Local Government. *Journal of Public Budgeting, Accounting and Financial Management,* 18, no. 2 (2006). 139–166; Mattei et al. (2021): op. cit.

41 Le et al. (2022): op. cit.; Mattei et al. (2021): op. cit.; Gaosong–Leping (2021): op. cit.

4.2.4. Safety and security

As previously stated, the auditor needs to gather intelligence to get the most out of the audit process. The volume and type of information and how to filter, store, access and review the audit data and logs are determined before the auditing in the planning phase. During the data collection phase, the auditor examines the data sources such as documents, testing, interviews.

From a safety aspect, the internal auditor is the most desirable choice since all the knowledge and data stay "in the house" – there is no need for data transmission and storage outside the organisation. Despite signed confidentiality agreements, the external third-party auditor may be perceived as a potential point for data leakage and a security problem. This perception might lead to not providing quality access to data; therefore, the auditor might misinterpret it, culminating in mistrust from both sides.

During APAA auditing, the data must be transmitted to another agency from the auditee organisation for processing purposes. Since the data does not leave the public administration system, the predefined data storage, transmission methods and laws apply, the transmission could be viewed as broadly defined in-house data exchange. Moreover, the management can trust the auditor on its skills and independent views.

5. Conclusions and recommendations

Governments are generally known to be risk-averse and rule-driven, based on stable structures and predictable decision-making. Avoiding risks is often justified for political reasons. However, by design, governments do not tend to act when confronted with new challenges. From the position of 'wait and see', governments are pushed to act when hazards materialise.[42] This approach is sometimes easier than intervention: it frees authorities from having to justify risky or interventionist policies but is insufficient in response to information security since adverse outcomes have already arrived.

This article established that information security management and auditing in public administration affect the realised efficiency, reliability and quality of public tasks. Information security audit is a complex process that requires good knowledge and understanding of the internal and external environment of public administration and its structure in systems and processes. We presented a new solution for handling threats by an innovative approach of information security auditing in the public administration sector called Autonomous Public Auditing Agency. This approach could help governments provide more efficient, effective and economical answers to information security threats. We believe that establishing the APAA approach and making rationalisations in the information security auditing might solve the problems concealed through public secrecy. There is ultimately pressure that means that auditors want to believe that some positive outcomes can come from their work.

Limitations: The theoretical foundations of the APAA model are aimed at indicating the fundamental problem in auditing of information systems security, which

[42] Tõnurist–Hanson (2020): op. cit.

is the lack of a systemic approach that would include the institution's mission and its aspect of providing proper quality of delivered services. However, evaluating the audit process of information systems security utilising this new method would require further empirical research to adopt scientifically justified assessment criteria.

References

Ahmad, Zaini – Dennis Taylor: Commitment to Independence by Internal Auditors: The Effects of Role Ambiguity and Role Conflict. *Managerial Auditing Journal,* 24, no. 9 (2009). 899–925. Online: https://doi.org/10.1108/02686900910994827

Appelbaum, Deniz A. – Alex Kogan – Miklos A. Vasarhelyi: Analytical Procedures in External Auditing: A Comprehensive Literature Survey and Framework for External Audit Analytics. *Journal of Accounting Literature,* 40 (2018). 83–101. Online: https://doi.org/10.1016/j.acclit.2018.01.001

Beláz, Annamária: A közigazgatás információbiztonsága: megjósolhatók az incidensek? *Hadtudomány,* 29, no. 3 (2019). 92–104. Online: https://doi.org/10.17047/HADTUD.2019.29.3.92

Bellman, Beryl: Defacement: Public Secrecy and the Labor of the Negative. *American Anthropologist,* 103, no. 3 (2001). 878–879. Online: https://doi.org/10.1525/aa.2001.103.3.878

Dittenhofer, Mortimer A. – R. Luke Evans – Sridhar Ramamoorti – Douglas E. Ziegenfuss: *Behavioral Dimensions of Internal Auditing. A Practical Guide to Professional Relationships in Internal Auditing.* Altamonte Springs, Florida, The Institute of Internal Auditors Research Foundation (IIARF), 2010.

Drljača, Dalibor – Branko Latinović: Audit in Public Administration's Information Systems – External or Internal? *IOP Conference Series: Materials Science and Engineering,* 200, no. 1 (2017). 1–7. Online: https://doi.org/10.1088/1757-899X/200/1/012026

Dwamena, Richard Ofosu: Investigating the Relationship Exist Between Internal Auditors and Management. *Finance and Management Engineering Journal of Africa,* 3, no. 9 (2021). 23–35. Online: https://doi.org/10.15557/FMEJA/2021/VOL3/ISS9/SEPT002

Dwamena, Richard Ofosu – Nicholas Yaw Ofori: The Roles and Status of Internal Auditors in Public Sector Organizations. *Finance and Management Engineering Journal of Africa,* 3, no. 9 (2021). 1–22. Online: https://doi.org/10.15557/FMEJA/2021/VOL3/ISS9/SEPT001

Gábri, Máté: Biztonsági komplexumok az információs korban. *Hadmérnök,* 5, no. 4 (2010). 110–121.

Gantz, Stephen D.: Chapter 1. IT Audit Fundamentals. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014a. Online: https://doi.org/10.1016/B978-0-12-417159-6.00001-8

Gantz, Stephen D.: Chapter 4. External Auditing. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014b. 63–82. Online: https://doi.org/10.1016/B978-0-12-417159-6.00004-3

Gantz, Stephen D.: Chapter 5. Types of Audits. In Stephen D. Gantz (ed.): *The Basics of IT Audit.* Boston, Syngress, 2014c. 83–104. Online https://doi.org/10.1016/B978-0-12-417159-6.00005-5

Gaosong, Qiu – Yuan Leping: Measurement of Internal Audit Effectiveness: Construction of Index System and Empirical Analysis. *Microprocessors and Microsystems,* (2021). Online: https://doi.org/10.1016/j.micpro.2021.104046

Giroux, Gary – Rowan Jones: Measuring Audit Quality of Local Governments in England and Wales. *Research in Accounting Regulation,* 23, no. 1 (2011). 60–66. Online: https://doi.org/10.1016/j.racreg.2011.03.002

Hampson, Fen Osler: Review: Barry Buzan – Ole Waever – Jaap de Wilde: Security: A New Framework for Analysis. *International Journal,* 53, no. 4 (1998). 798–799. Online: https://doi.org/10.2307/40203739

Hegazy, Karim – Anne Stafford: Internal and External Auditors Responsibilities and Relationships with Audit Committees in Two English Public Sector Settings. *Corporate Ownership and Control,* 18, no. 3 special issue (2021). 395–409. Online: https://doi.org/10.22495/cocv18i3siart13

Jamaluddin, Masruddin – Indra Basir – Rahma Masdar – Lucyani Meldawati: Role Ambiguity, Role Conflict, Auditor Competence on Audit Quality: The Mediating Effects of Auditing Planning and Independence. *Universal Journal of Accounting and Finance,* 9, no. 6 (2021). 1551–1557. Online: https://doi.org/10.13189/ujaf.2021.090632 ; DOI: https://doi.org/10.13189/ujaf.2021.090632

Kanellou, Alexandra – Charalambos Spathis: Auditing in Enterprise System Environment: A Synthesis. *Journal of Enterprise Information Management,* 24, no. 6 (2011). 494–519. Online: https://doi.org/10.1108/17410391111166549

Knapp, Kenneth J. – Gary D. Denney – Mark E. Barner: Key Issues in Data Center Security: An Investigation of Government Audit Reports. *Government Information Quarterly,* 28, no. 4 (2011). 533–541. Online: https://doi.org/10.1016/j.giq.2010.10.008

Kő, Andrea – Balázs Molnár: *Az információrendszerek auditálása. Az informatika és az információrendszerek ellenőrzési és irányítási módszerei.* Budapest, Corvinno Technology Transfer Kft., 2009. Online: https://doi.org/978-963-06-7254-2

Le, Thi Tam – Thi Mai Anh Nguyen – Van Quang Do – Thi Hai Chau Ngo: Risk-Based Approach and Quality of Independent Audit Using Structure Equation Modeling – Evidence from Vietnam. *European Research on Management and Business Economics,* 28, no. 3 (2022). Online: https://doi.org/10.1016/j.iedeen.2022.100196

Lisic, Ling Lei – Jeffrey Pittman – Timothy A. Seidel – Aleksandra B. Zimmerman: You Can't Get There from Here: The Influence of an Audit Partner's Prior Non-Public Accounting Experience on Audit Outcomes. *Accounting, Organizations and Society,* 100 (2021). Online: https://doi.org/10.1016/j.aos.2021.101331

Mattei, Giorgia – Giuseppe Grossi – James Guthrie A.M: Exploring Past, Present and Future Trends in Public Sector Auditing Research: A Literature Review. *Meditari Accountancy Research,* 29, no. 7 (2021). 94–134. Online: https://doi.org/10.1108/MEDAR-09-2020-1008

Michener, Gregory – Jonas Coelho – Davi Moreira: Are Governments Complying with Transparency? Findings from 15 Years of Evaluation. *Government Information Quarterly,* 38, no. 2 (2021). Online: https://doi.org/10.1016/j.giq.2021.101565

Mironeasa, Costel – Georgiana Gabriela Codină: A New Approach of Audit Functions and Principles. *Journal of Cleaner Production,* 43 (2013). 27–36. Online: https://doi.org/10.1016/j.jclepro.2012.12.018

Mironeasa, Costel – Silvia Mironeasa: The Process Approach and the Generated Value at the Process Level. *Metalurgia International,* 14, no. 6 (2009). 89–93.

Nyikes, Zoltán – András Kerti: Proposals for Amending the Regulation of the Administrative System. *Journal of Emerging Research and Solutions in ICT,* 1, no. 1 (2016). 68–74. Online: https://doi.org/10.20544/ERSICT.01.16.P07

Radcliffe, Vaughan S.: Public Secrecy in Auditing: What Government Auditors Cannot Know. *Critical Perspectives on Accounting,* 19, no. 1 (2008). 99–126. Online: https://doi.org/10.1016/j.cpa.2006.07.004

Samagaio, António – Teresa Felício: The Influence of the Auditor's Personality in Audit Quality. *Journal of Business Research,* 141 (2022). 794–807. Online: https://doi.org/10.1016/j.jbusres.2021.11.082

Samelson, Donald – Suzanne Lowensohn – Laurence E. Johnson: The Determinants of Perceived Audit Quality and Auditee Satisfaction in Local Government. *Journal of Public Budgeting, Accounting and Financial Management,* 18, no. 2 (2006). 139–166. Online: https://doi.org/10.1108/JPBAFM-18-02-2006-B001

Simon, Herbert A.: Decision-Making and Administrative Organization. *Public Administration Review,* 4, no. 1 (1944). 16–30. Online: https://doi.org/10.2307/972435

Steinbart, Paul John – Robyn L. Raschke – Graham Gal – William N. Dilla: The Influence of a Good Relationship between the Internal Audit and Information Security Functions on Information Security Outcomes. *Accounting, Organizations and Society,* 71 (2018). 15–29. Online: https://doi.org/10.1016/j.aos.2018.04.005

Steinbart, Paul John – Robyn L. Raschke – Graham Gal – William N. Dilla: The Relationship between Internal Audit and Information Security: An Exploratory Investigation. *International Journal of Accounting Information Systems,* 13, no. 3 (2012). 228–243. Online: https://doi.org/10.1016/j.accinf.2012.06.007

Stensaker, Bjørn: *External Quality Auditing: Strengths and Shortcomings in the Audit Process*. *External Quality Audit: Has It Improved Quality Assurance in Universities?* Woodhead Publishing Limited, 2013. Online: https://doi.org/10.1016/B978-1-84334-676-0.50013-3

Suduc, Ana-Maria – Mihai Bîzoi – Florin Gheorghe Filip: Audit for Information Systems Security. *Informatica Economică,* 14, no. 1 (2010). 43–48.

Szczepaniuk, Edyta Karolina – Hubert Szczepaniuk – Tomasz Rokicki – Bogdan Klepacki: Information Security Assessment in Public Administration. *Computers and Security,* 90 (2020). 1–11. Online: https://doi.org/10.1016/j.cose.2019.101709

Tõnurist, Piret – Angela Hanson: Anticipatory Innovation Governance: Shaping the Future through Proactive Policy Making. *OECD Working Papers on Public Governance,* no. 44 (2020). Online: https://doi.org/10.1787/cce14d80-en