This abstract was submitted to and presented at CCRC International Conference 2022.

A new approach to information security auditing in the public administration

Annamária Edegbeme-Beláz, Dr. habil. Andás Kerti; Óbuda University, Budapest, Hungary belaz.annamaria@uni-obuda.hu, National University of Public Service Budapest, Hungary

INTRODUCTION

Due to the rapid pace of globalization and digitalization and the better usage of ICT technology, cybercrime is also rising. Hence, controlling and auditing information systems' secure operation 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 (PA)?

PA is an independent system with data and workflow, terminology, special procedures, and rules. The primary mission of the public sector institutions is to realize 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 PA affect the realized public tasks' efficiency, reliability, and quality. Information security audit is a complex process that requires good knowledge and understanding of the public administration's internal and external environment and its structure in systems and processes. Hence, information security management and auditing in PA are often analyzed in a way that separates it from the functioning of a public institution as an entirety. (Drljača & Latinović, 2017; Knapp et al., 2011; Suduc, 2010) For the PA 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 organizing, 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 have to form an integral part of them. (Mironeasa & Codină, 2013; Szczepaniuk et al., 2020)

The protection of the organizational system and infrastructure of the PA is principally justified because the public administration is responsible for the implementation of fundamental state tasks. When we talk about administrative tasks and functions, we examine the underlying prevailing state interests behind these tasks. (Edegbeme-Beláz, 2019) The five primary domains of PA (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 modernization of the state and PA, these five essential functions will not disappear but will be constantly extended and differentiated. It is indisputable that the protection of PA and the infrastructure supporting it is a crucial area for all states.

METHODOLOGY

This research shows why and how auditing in the public sector needs a new perspective. We demonstrate what role does the concept of public secrecy play in auditing and how information plays a crucial role in the functioning of the PA as a system. First, we give an outline of auditing in general. Second compare the two main auditing models (internal and third-party) currently used for information security auditing in PA based on the following characteristics: Knowledge and reliability; Dependency-independency; Outcomes and customer satisfaction; Data safety and security. As a conclusion of our analysis, we provide a novel approach for conducting information security audits.

RESULTS AND DISCUSSION

Overview of auditing

In the literature, there are several definitions for auditing (Drljača & Latinović, 2017; Kő & Molnár, 2009; Mironeasa & Codină, 2013) but all of them involve the following keywords: effective, efficient, and economical use of resources; data integrity; compliance with standards; collecting and evaluating evidence. Auditing is a complex notion, and a management tool that evaluates an organization'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. 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.(Mironeasa and Mironeasa, 2009)

There are several classification methods of audits in the professional and academic literature, depending on the scholars' aspects and viewpoints. In this research, we typified the audits by three features (1) independence, (2) scope, and (3) application domain.

1. Table Main types of audits

Category	Audit type	Description
Independence	Internal	The process is an integral part of the organization. It means the continuous control of the systems' security status and reliability,

		the existence of security requirements; the implementation and compliance of the security policy.
	External	Known as third-party auditing, independently and impartially monitors the internal audit, operation of the internal control and management system, and the auditee security status.
Scope	Organizational	The extent of this audit is the organization as a whole, with all its functions, subsystems, and processes.
	Specialised	Limited to specific procedures, functions, or systems.
Application domain	Operational	Evaluates the structure of internal controls of a given process or work area. This is a specific and targeted audit.
	Integral	Evaluates organizational goals related to the financial information, efficiency, and harmonization with the goals.
	Administrative	Analyses issues related to the efficiency of operative productivity within the organization.
	Information security	Relates to the evaluation of: technical solutions, management of IT control procedures, software development and compliance with international and national standards

Internal – bureaucratic - audits

Based on independence, we can talk about internal and external audits. With internal audits, the whole process is an integral part of the organization. It means the continuous control of the systems' security status and reliability, the existence of security requirements; the implementation of the organization's security policy; the compliance and application of internal regulations. In practice it implies that - depending on the size and structure of the organization – at least one employee works as an auditor. S/he plans the audit, gathers the information, carries out the audit process, and reports to the management. Regarding the internal auditing Steinbart makes the following comment: „Certainly, self-monitoring is useful, and indeed, “line management ... provides assurance as a first line of defense over the risks and controls for which they are responsible. Yet, there is considerable evidence that people have great difficulty in identifying and in correcting errors in systems that they created themselves„.(Steinbart et al., 2018)

Third-party auditing

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. These audits can be organizational or specialized. Whenever a public entity wants a third-party auditor to scrutinize its workflow and security state, they have to hire a private sector company. Since public sector organizations are not obliged to work with the same auditor, each time a third party is introduced, the organization is required to trust the new entity. 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. As the recommendations are not obligatory, the organization has no legal responsibility to modify its system or workflow. The goal of these audits in the private sector is usually to prepare an organization for accreditation or certification; however, holding such certifications is not common in the public sector.

Autonomous Public Auditing Agency (APAA)

Governments face many challenges these days. In order to address rapidly developing technologies, they need a more profound knowledge of these technologies and evolving policies simultaneously. (Nyikes et al., 2016; Tonurist & Hanson, 2020) As The APAA is an auditing institution within the PA system established by the government. Its goal is to overview and strengthen the information system security of the public sector by conducting regular audits. There are several specifications of the APAA compared to the third-party audits. The most significant are: (1) The central government budget finances the APAA audit process; therefore, all public entities can participate in the audit programs irrespective of their financial status. (2) The personnel of the institution made up of public servants with the necessary regulatory and technical expertise. (3) 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.

Advantages of the Autonomous Public Auditing Agency

The following section will analyze the advantages of setting up the APAA 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: An auditor should be a technically competent person with sufficient skills and knowledge needed to implement an audit.(Steinbart et al., 2012) Information security audits require profound technical and legal knowledge. Based on the working experience and familiarity with the organization, internal auditor is skillful in evaluating the technology, processes, and procedures. A third-party external auditor may only follow the instructions from frameworks and standards and is not explicitly experienced in the field, and might lack the knowledge on legal aspects of the audit topic. The APAA auditor would be a professional equipped with the required technical knowledge and experience both in the PA systems' procedures and the best practices.

(2) Dependency: For auditing to reach its goal independence of the audit process is vital. In an internal audit a hint of subjectivity will always be present. Radcliff states in his discoveries on public secrets (Radcliffe, 2008, 2011) that the truth value of audit findings in such areas is profoundly doubtful. Third-party auditors are entirely independent, but they might lack the understanding of the bureaucratic processes and terminology. APAA professional equipped with the necessary knowledge but entirely independent.

(3) Outcomes and customer satisfaction: 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 external auditor's primary goal is customer satisfaction and reliability of processes.

(4) Safety and security: During internal auditing all information, data stay "in the house" – there is no need for transmission. Despite signed confidentiality agreements, third-party auditor is a potential point for data leakage. This 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 does not leave the PA 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.

CONCLUSIONS

This research established that information security management and auditing in public administration affect the realized public tasks' efficiency, reliability, and quality. Information security audit is a complex process that requires good knowledge and understanding of the public administration's internal and external environment 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 rationalizations 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 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 utilizing this new method would require further empirical research to adopt scientifically justified assessment criteria.

References

Drljača, D., & Latinović, B. (2017). Audit in public administration's information systems - External or internal? *IOP Conference Series: Materials Science and Engineering*, *200*(1). https://doi.org/10.1088/1757-899X/200/1/012026

Edegbeme-Beláz, A. (2019). A közigazgatás információbiztonsága: megjósolhatók az incidensek? *HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA*, *29*(3), 12–92. https://doi.org/10.17047/HADTUD.2019.29.3.92

Knapp, K. J., Denney, G. D., & Barner, M. E. (2011). Key issues in data center security: An investigation of government audit reports. *Government Information Quarterly*, *28*(4), 533–541. https://doi.org/10.1016/j.giq.2010.10.008

Kő, A., & Molnár, B. (2009). *Az Információrendszerek auditálása,: Az informatika és az információrendszerek ellenőrzési és irányítási módszerei*. Budapest: Corvinno Technology Transfer Kft. https://doi.org/978-963-06-7254-2

Mironeasa, C., & Codină, G. G. (2013). A new approach of audit functions and principles. *Journal of Cleaner Production*, *43*, 27–36. https://doi.org/10.1016/j.jclepro.2012.12.018

Mironeasa, C., & Mironeasa, S. (2009). The process approach and the generated value at the process level. *Metalurgia International*.

Nyikes, Z., Németh, Z., & Kerti, A. (2016). The electronic information security aspects of the administration system. *SACI 2016 - 11th IEEE International Symposium on Applied Computational Intelligence and Informatics, Proceedings*. https://doi.org/10.1109/SACI.2016.7507395

Radcliffe, V. S. (2008). Public secrecy in auditing: What government auditors cannot know. *Critical Perspectives on Accounting*, *19*(1), 99–126. https://doi.org/10.1016/j.cpa.2006.07.004

Radcliffe, V. S. (2011). Public secrecy in government auditing revisited. *Critical Perspectives on Accounting*. https://doi.org/10.1016/j.cpa.2011.01.014

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2012). The relationship between internal audit and information security: An exploratory investigation. *International Journal of Accounting Information Systems*, *13*(3), 228–243. https://doi.org/10.1016/j.accinf.2012.06.007

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15–29.

https://doi.org/10.1016/j.aos.2018.04.005

Suduc, A. (2010). Audit for Information Systems Security. *Informatica Economica*, *14*(1), 43–48.

Szczepaniuk, E. K., Szczepaniuk, H., Rokicki, T., & Klepacki, B. (2020). Information security assessment in public administration. *Computers and Security*, *90*. https://doi.org/10.1016/j.cose.2019.101709

Tonurist, P., & Hanson, A. (2020). Anticipatory Innovation Governance: Shaping the future through proactive policy making. In *OECD Working Papers on Public Governance* (Issue 44). https://doi.org/10.1787/cce14d80-en