Securing Business Applications in the Age of Digitalization: Challenges and Strategies for Data Confidentiality

Claudia PARASCHIV
Bucharest University of Economic Studies, Bucharest
claudia.paraschiv@csie.ase.ro

This paper examines rapid and generated integration into business applications and highlights the transformational potential in areas such as content, acquisition assistance, and process automation is securing sensitive inputs/outputs, preventing model abuse, and ensuring transparency. The proposal is for a more multi-tiered approach involving data minimization, zero-travel architecture, and continuous model auditing. The rapid expansion of digital transformation and interconnected systems has intensified cyber risks, making cybersecurity audits essential for safeguarding organizational assets. This study reviews current literature, regulatory developments such as GDPR updates, and leading IT audit frameworks - including COBIT, ISO/IEC 27001, NIST CSF, and SOC reports - to highlight the growing need for integrated security strategies that combine technical controls with strong organizational processes. A conceptual solution is proposed through an iOS-based cybersecurity audit application designed to replace traditional manual methods. The application streamlines workflows, automates data handling, and provides real-time insights, improving audit efficiency, accuracy, and compliance. Findings emphasize that modern, technology-enabled audit tools are crucial for addressing evolving threats, increasing regulatory demands, and the security challenges introduced by AI, IoT, and cloud systems. Effective cybersecurity audits remain vital for organizational resilience, business continuity, and the protection of digital assets in the advancing digital landscape.

Keywords: *Generative AI, Data Confidentiality, Cybersecurity, Business Applications, AI Security, Risk Management, Audit*
DOI: 10.24818/issn14531305/29.4.2025.03

1 Introduction

In a time of widespread connectivity and swift digital transformation, enterprises must contend with a growing range of cyberthreats that compromise the security and integrity of their digital assets. This is an overview of the complex field of cybersecurity audit and emphasizes how important it is to protect organizational interests in the face of changing cyberthreats.

Moreover, the cybersecurity landscape has become more complex and challenging due to the rise of digital transformation projects and the proliferation of connected devices. Furthermore, cybersecurity audits cover organizational procedures and policies in addition to technical weaknesses. Research highlights the relationship between cybersecurity, digitization, and internal audit quality, highlighting the necessity of integrated organizational security strategies that include both procedural and technological components.

Cybersecurity audit is essential for promoting organizational resilience and continuity in the case of cyber incidents, in addition to risk identification and mitigation. These frameworks use cybersecurity audit insights to detect, respond to, and recover from cyber threats in an effective manner, strengthening organizational defenses and enhancing business operations continuity. [1]

Organizations can create proactive and effective cybersecurity audit strategies that support their overall business goals by combining these findings. By doing this, they can confidently traverse the dynamic and complicated cybersecurity landscape, protect their digital assets and maintain stakeholder trust in a world that is becoming more

interconnected by the day.

2 Background and literature review

In a world of increasing inter-connectivity and rapid digital enablement, enterprises are under constant attack from an ever-wider range of cyber-threat that puts in jeopardy the security and reliability of their digital assets. The necessity to adapt organizational regulation in the face of cyberthreats in a constant state of change was also highlighted. There are numerous academic studies on cybersecurity audit procedures that have already been implemented. The cybersecurity audit process has its ins and outs, benefits – in recognition & reduction of cyber risks/risks – and drawbacks. Today we see even more challenges in the cybersecurity landscape, as new digital transformation projects and connected devices are dramatically increasing it (Figure 1).

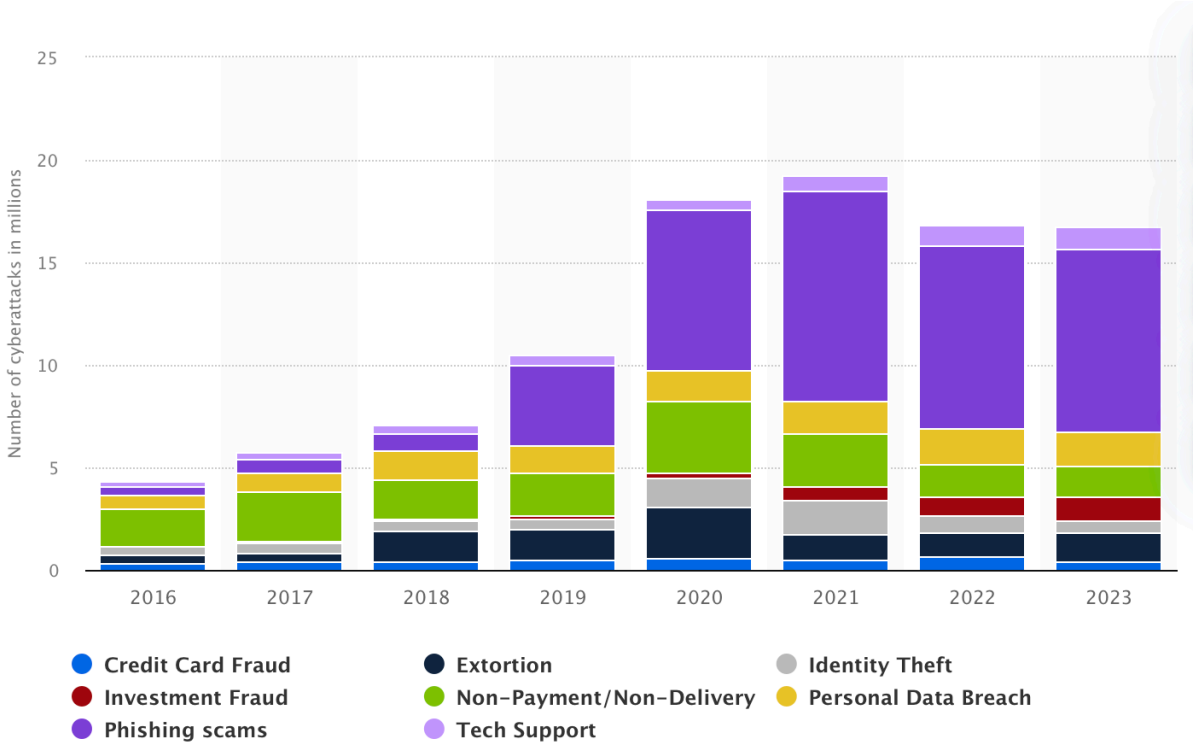

Fig. 1. Annual number of cyberattacks worldwide from 2016 to 2023, by type (in millions)

All of this means that there is also a rising number of procedures assessed, besides various weaknesses discovered during cyber security audits. This is of paramount importance as recent scholarly studies have demonstrated that this relation indicates the integration in corporate security practices and measures, which are a blend of procedural activities and elements –it shows businesses should implement solutions that offer suitable technical arrangements ran with the help of workers to achieve real results. In addition to risks identification and mitigation, cybersecurity audit is critical in promoting organizational resilience and business continuity during cyber incidents. By taking these necessary steps, individuals and organizations can safely navigate a constantly evolving cybersecurity landscape while safeguarding digital security assets that remain the property of others. Integrating Cybersecurity as part of risk aspect part of the above process includes performing cyber security audits to determine key risks the organization may be exposed to and reviewing existing policies/procedures/and controls that help keep those risks at tolerable levels. Overall, the cybersecurity audit is a method of

seeing where the IT systems can be improved and then implementing fixes to make sure all cyber security efforts are enhanced. These audits look at a business's cybersecurity processes, as well as software and hardware to confirm their implementation is correct or to keep records of any inadequacies. Not every audit is the same. After a data breach or loss, advanced tools may be needed for more extensive investigations. A cybersecurity audit is an assessment of all the defenses and systems set up in any given region to protect against online attacks. The goal is to be certain the rules, plans and production all align with necessities and legal guidelines through thoroughly inspecting them. Businesses can also implement various quality practices to audit the efficiency and effectiveness of their cybersecurity policies, controls, and frameworks. A cybersecurity audit does that, comprehensively studying an organization's protection strategies and it should be part of an extensive threat control plan. The continuing virtual evolution brings with it new novel cyber risks, so companies want to make certain that their cybersecurity plans are flexible. On top of that ever-growing cyber-threat, the loss of an audit framework also exposes the employer to liability for violating jail and regulatory necessities. Regular reviews of cybersecurity allow the placement or openings within protective and defensive measures to be identified, enabling security teams to enforce the proper controls actively and prioritize danger management.[1] These fundamental pieces of a cybersecurity audit include: reviewing the rules and regulations around cybersecurity, ensuring that an integrated cyber strategy is enforced, evaluating employee-level of cyber competences as well as promoting threat-oriented auditing within the company. The report integrates cybersecurity, hazard management, and compliance guidelines into one, offering auditors with a complete understanding of an agency's basic cybersecurity fitness. Impact of industry specific audit approaches on outcome of the case would be explained in this section. It could cover creative versus conventional methods and how the two are more effective in different types of company settings. As technology continues to evolve, you might wonder how blockchain could ensure that audit trails were secure or if AI is sophisticated enough to predict and identify breaches before they occur. Ransom costs alone have been hitting the tens of millions for some businesses forced to pay escalating ransoms demanded by cyber criminals, and attackers targeting even family-owned small businesses have typically taken down these companies only to force ransom payments that often reach several tens of thousands at an absolute minimum. Moreover, the repercussions of poor cybersecurity can cause significant damage to an organization's corporate image.

The CIA triad stands for Confidentiality, Integrity, and Availability and it is the actual concept of information security. The elements of the triad encompass a vital component to maintaining data integrity so that it is secure, accurate and available. [2]

These are the three key pillars upon which all information security is built, with measures that meet these three principles. Organizations will be able to keep their data safe against unauthorized access, make it accurate, and ensure that when needed, it is available only for the authorized users. While there are many benefits to digitalization, the preservation of confidentiality, integrity and availability will be more critical than ever before as we strive to protect what remains sensitive in a highly interconnected operative context.

In 2024, several updates and enhancements have been made in the General Data Protection Regulation (GDPR) to deal with implementation problems and enforcement throughout the European Union as circumstances evolve.

Key Updates and Changes

Increased Fines and Enforcement Actions - By applying heavier fines based on a failure to comply with the regulation, flat enforcement is an appropriate type of increased variation in this way. A major social media platform was also fined €390 million for GDPR breaches linked to its use of targeted advertising in

January 2024. [3]

- Clarified Data Processing Rules - New guidelines have been issued by the European Data Protection Board (EDPB) on data processing, stressing the need for valid consent.
- Enhanced cross border cooperation - The one-stop-shop mechanism from GDPR has been improved so that controllers have to cooperate with only one lead supervisory authority (LSA) for cross-border processing cases. [4]
- Corrective measure regarding human error and insufficient practices - Based on the findings of supervisory authorities, it is required to implement additional necessary organizational and technical measures in respect of preventing the breach due to human error and inadequate practices These requirements include improved employee training, the use of encryption and secured channels for transmitting data.
- National Data Protection Laws - National data protections laws of individual countries such as France, Germany and Spain have to be updated accordingly in order to bring them in line with the GDPR. Apart from this, France has published its new requirements for biometric data processing and Germany keeps on emphasizing employee data privacy jurisdiction law. [3]
- After Schrems II - The European Commission adopted new Standard Contractual Clauses (SCCs) which offer a more comprehensive set of obligations and enhanced safeguards for transferring personal data out of the EU upon the ruling of the judgment. Negotiations are also underway about a new EU-US data transfer scheme that would serve as an appropriate replacement of the invalid Data Privacy Law Updates in Europe 2024: GDPR, ePrivacy and more. [5]
- AI and Data Privacy - EU just endorsed a novel AI Act that brings in first-ever rules concerning the safety of Artificial Intelligence systems as well as protections for consumers' fundamental rights. Going to close another gap between current AI governance and the principles of GDPR.

The 2025 is landscape of data protection changing very first with the rapid pace of digitalization. The personal data boom fuelled by the integration of these technologies in everyday life has contributed toward a significant increase in the volume as well as variety of personal data processed. The rise in the use of digital tools and a corresponding increase in personal data during the crisis requires strong safeguards to protect peoples' privacy rights and maintain trust. The importance of data protection cannot be emphasized enough in an era where digitalization has spread across all sectors right from the heath industry to finance.

The method of data protection by using blockchain technology for secure data transactions is becoming more and more widespread. A decentralized nature of blockchain can improve data integrity and security, yet it also brings up concerns about data privacy or the right to be forgotten, because personal information saved on blockchain networks is theoretically impossible to alter.

Organizational conditions and best practices:

Regular audits and DPIAs (Data Protection Impact Assessments) - Regularly auditing the data processing activities being undertaken in your organisation, viewing this through the lens of a DPIA, to identify and endeavour to remedy compliance risks.

Employee Training - Make sure your employees are aware of data protection principles and practices to reduce the risk factor for human error.

Advanced Security Technologies – We have implemented cutting-edge encryption, access controls and intrusion detection systems to better secure customer personal data.

Transparent Policy - Always keep clear and transparent data privacy policies that should let the individuals be aware of their rights and how their information is being processed. [3]

An incident response plan: Organizations must create and maintain data breach-specific incident response plans so that they can respond to such incidents in a timely manner.

By 2025 data protection still continues to be of vital importance as digitalization advances at pace. Such regulatory frameworks are constantly updating, and the rise of legislation

such as GDPR highlights that vigilance on data protection is highly necessary. In order to protect personal data, organizations must keep up with changes in regulations, implement the best practices and take advantage of new technology. The road to complete data security will always remain a work in progress and we shall constantly need grow cooperatively with the increasing pace of digitalization. [4]

In 2025, the framework of IT auditing is reflected in such major standards that deliver total frameworks for reviewing the functionality, security, and compliance of IT systems. It is critical for organizations to follow these standards in order to verify that their IT practices adhere with legislature and other norms. There are some specific standards that we used in IT audit which I am mentioning over here for year 2025:

- COBIT (Control Objectives for Information and Related Technologies) - It provides a best practice framework for enterprise governance of IT. [6]
- ISO/IEC 27001 - Is the name of an international standard for information security management systems (ISMS). It is catalogued set of security controls based on international standards and guidelines to ensure information confidentiality, integrity, and availability. [7]
- NIST Cybersecurity Framework - Developed by The National Institute of Standards and Technology, provides a framework for improving the security and resilience of critical infrastructure. It's used in many industries to help organizations manage and mitigate cybersecurity risks. It is a framework consisting of five core functions: Identify, Protect, Detect, Respond and Recover. [8]
- ITIL (Information Technology Infrastructure Library) – Is a framework of best practice approaches intended to facilitate the delivery of high-quality information technology services. It's a practice for IT service management (ITSM) efforts that focus on aligning IT services with the needs of business. Although ITIL is not an "audit standard" in the traditional sense, it remains a useful framework for auditors to utilize when assessing whether IT service management processes are functioning effectively and efficiently. [9]
- SOC (Service Organization Control) Reports - Specifically SOC 1 and SOC 2, are auditing standards established by the American Institute of Certified Public Accountants (AICPA). It is vital for service organizations to have them in place as these enable their clients to assess control's effectiveness. SOC 1 provides information about controls that are relevant to financial reporting. SOC 2 covers controls relevant to security, availability, processing integrity, confidentiality and privacy. [10]
- Payment Card Industry Data Security Standard (PCI DSS) – Is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. It is mandated to be complied with by any merchant or issuer who accept or issue credit/debit cards, and vital for businesses involved in processing card-based transactions. [11]
- CMMI (Capability Maturity Model Integration) - An approach to improve organizational processes, which can be used as a guidebook for process improvement across the organization or project. It is a measuring tool for all the procedures of an organization to determine where they need further progression or development. [12]

3 Proposed solutions - A case study or Conceptual Framework/Application

The flow describing the cybersecurity audit (Figure 2) is a vital activity in the changing world of modern corporate operations, assuring the availability, integrity, and confidentiality of digital assets. The function and effectiveness of cybersecurity audit procedures in enhancing organizational resilience and reducing cyber threats are thoroughly examined in this paper. The abstract explains the changing nature of cybersecurity audit methods and their consequences for modern business contexts by drawing on a wide range of literature,

including empirical research, theoretical frameworks, and practical insights.

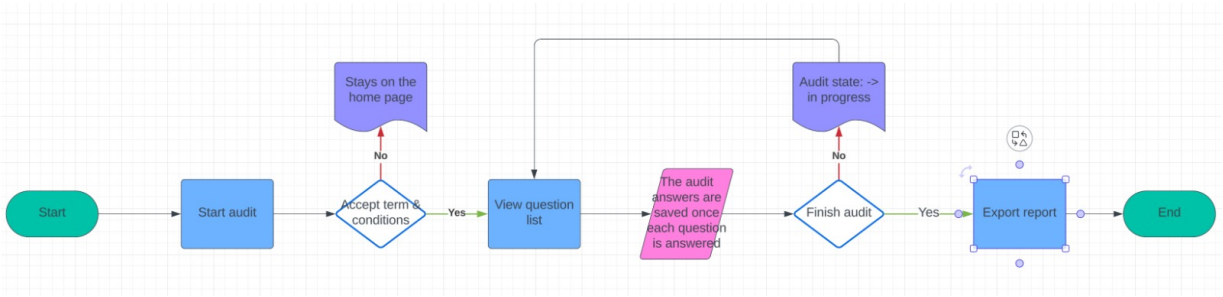

Fig. 2 Flow chart of the cybersecurity audit

The flow chart provided describes the flow process on how to audit an audit in an application. The process starts from Start to End with various decision-making gates that enable actions and decision-making processes. [13] At the Start, the audit is started, followed by an accept action where the user is presented with the terms and conditions to continue the audit. If the terms are not accepted, the flow will require the user to **"**Stay in Homepage," which stops, and returns the activity to square one, ensuring that the user first complies before continuing the audit process. From the accept, the user is allowed to view the question list, which is followed by data entry, suggesting a continuous saving of data on every audit progress, hence the user can stop and return to the audit without losing the information. After, the audit can be finalized, or continued if there has been new data entry, which is a decision-making point related to the audit statement. If the finalization is selected, it flows to exporting the audit report, which is the end gate that stops the entire process. The whole activity describes a process structurally and securely processed, ensuring an audit starting and ending at every stage of data entry and user decision.

In the era of speed, of digitization of all processes, from paying bills to making a restaurant reservation, of all smart devices that make our daily lives easier, the audit field is no exception.

The proposed solution for the problems mentioned in the previous chapter is a cybersecurity audit application, with iOS operating system, which will completely replace the classic Excel file with numerous spreadsheets.

Such an iOS application is based on dynamic style, speed, efficiency and effectiveness. Eliminating redundant and repetitive tasks that have existed until now in the general audit process. This application simplifies the entire process and the steps followed in carrying out the cybersecurity audit. It offers numerous tools and functions that automate this flow.

The basic functionalities of the application proposed as a solution to the existing and inefficient procedure at this time, have already been developed within the dissertation work.

The application aims to solve many current problems in security audits, such as the typical challenges faced by companies implementing these types of in-depth audits, such as lack of resources, the position of stakeholders or the complexity of incorporating new technologies.

The Figure 3 below describes the use case diagram of the proposed solution.

Recommendations can be provided immediately, having an overview of the company's situation, in real time. While currently it is necessary to wait for the testing of all controls and a long process of receiving evidence that duplicates the processes presented.

Also, the importance of GDPR is a globally discussed issue, which reinforces the idea of the need for security layers and their periodic verification through security audits.

The goal is to plan strategies and rules to deal with possible cyber-attacks, as well as to strengthen cybersecurity defenses, based on the detailed audit strategies generated by the

assessment itself.

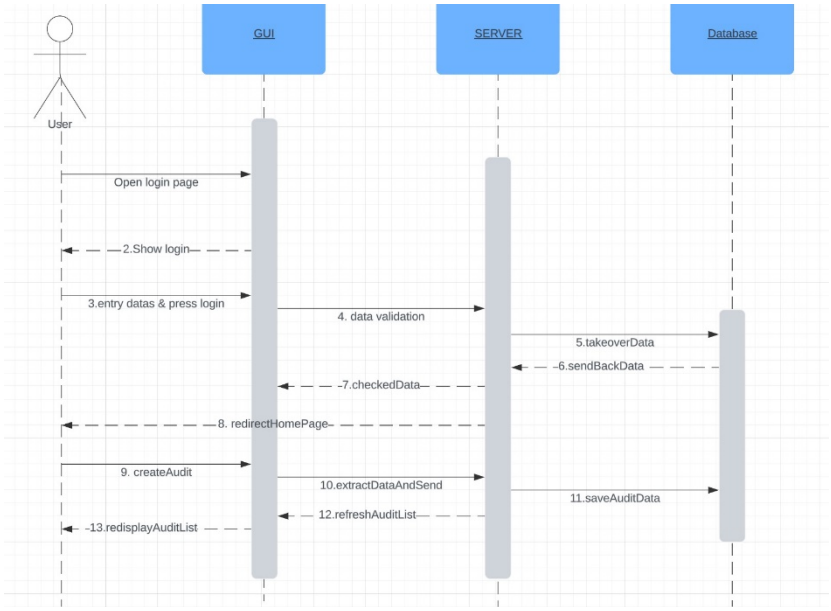

Fig. 3. Use case diagram of the system

All these features make the app a must-have for the future that awaits us in the digital age, a vital tool for companies that have understood the importance of cybersecurity and that bad publicity is not always bad publicity. A single security breach can jeopardize the trust of the entire company.

4 Conclusion

Overall, the iOS application created for the purpose of developing and managing audit forms is a powerful tool that significantly optimizes the process of auditing. Combining the audit forms with clients 'databases, form-building tools, audits previews, and highly detailed and nuanced forms enables the creation of audits that are valuable, accurate, and comply with relevant standards. The application could become an essential tool for any agency or organization that needs to maintain compliance with specific standards to ensure excellence and improve efficiency and effectiveness.

Developing an iOS application to manage a form for audit using MVVM-C and Swift ensures that developers are working in a highly modular, testable, and structured codebase. The components in the MVVM-C architecture ensure that each of them serves a well-defined role and responsibility, making single responsibility and separation of concerns. Swift's language also goes a long way in advancing this architecture, creating a solid foundation for developing complex, effective, and ultimate user mobile applications. Finally, the above-mentioned audit form application emphasizes how the usage of these tools and frameworks created applications developed to satisfy the complex business requirements and offer a good integration system, which can be easily amended to fit the new requirements.

The literal meaning of digitalizing everything has brought a drastic change in globalization nowadays because everything is dependent on technology and its wonders these days. All of those transformations have in turn resulted in tremendous efficiency, improvements to customer experiences, and novel business models. Yet, it also brings along huge risks especially in the context of data privacy and security.

The diversity of Internet of Things (IoT) devices, artificial intelligence (AI), together with the big data analytics provide an unmatched capability for collecting and processing increasing amounts of data. For example, small IoT devices that exist in smart homes or wearables & industrial equipment constantly generate huge volumes of personal

and confidential data. AI systems process this data to provide personalized services, and in many cases need access to large databases that contain private information.

In 2025 these same standards will already serve to create strong IT auditing practices for organizations which aim at guaranteeing the security and compliance of its IT systems as well with business needs. By following the standards, businesses can achieve better risk management, safeguard their sensitive information and assure stakeholders of their compliance.

Technical developments in software applications have seen a significant change in the types of vulnerabilities and their associated complexity. The implementation of cloud architecture and modern SaaS applications has increased exposure to public APIs, external integration, and inadequate identity management in distributed environments. The introduction of traditional artificial intelligence into business applications (such as recommendations and unusual risk recognition systems) decisions, such as decisions that are not sensitive to data. With the integration of generative artificial intelligence (GENA) into mobile and enterprise applications, privacy is more complicated and less predictable. They are no longer connected only to the application code, but are the way in which data is processed, understood, and enforced by generative models that can be affected, manipulated, or exploited, algorithm transparency and compliance with new standards such as RMF and ISO/IEC 2001.

References

[1] M. Popa, S. Capisizu, "Using Quantitative Methods as Support for Audit of the Distributed Informatics Systems " Informatica Economica, vol. 14, no. 1, pp. 103-112, 2010.

[2] C. Hashemi-Pour, "CIA triad (confidentiality, integrity and availability)" [Online]. Available at: Available: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA. [Accessed 27 December 2024].

[3] Stephenson Harwood, "Data Protection update - December 2023/ January 2024" 6 February 2024. [Online]. Available at: https://www.shlegal.com/insights/data-protection-update---december-2023-january-2024. [Accessed 8 March 2025].

[4] Stephenson Harwood, "Data Protection update - May 2024" 31 May 2024. [Online]. Available at: https://www.shlegal.com/insights/data-protection-update---may-2024. [Accessed 2 June 2025].

[5] O. Kagan, "German State's Data Processing Authority Offers Strict Guidance on Post-Schrems II Data Transfers" 25 August 2020. [Online]. Available at: https://www.foxrothschild.com/publications/german-states-data-processing-authority-offers-strict-guidance-on-post-schrems-ii-data-transfers. [Accessed 17 October 2024].

[6] K. T. Hanna. [Online]. Available at: https://www.techtarget.com/searchsecurity/definition/COBIT. [Accessed 8 March 2025].

[7] Gowsika, "ISO 27001 Controls: A Guide to Implementing Annex A Controls" 15 February 2024. [Online]. Available at: https://sprinto.com/blog/iso-27001-controls/. [Accessed 8 March 2024].

[8] NIST, "Cybersecurity Framework" [Online]. Available at: https://www.nist.gov/cyberframework. [Accessed 25 October 2023].

[9] IBM, "What is ITIL?" [Online]. Available: https://www.ibm.com/topics/it-infrastructure-library. [Accessed 5 February 2024].

[10] A. Fitzgerald, "SOC Audit: What It Is, How it Works & How to Prepare Your Service Organization" 22 May 2024. [Online]. Available at: https://secureframe.com/blog/soc-audit. [Accessed 30 May 2024].

[11] A. Malone, "PCI DSS v4.0.1" 11 June 2024. [Online]. Available at: https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1. [Accessed 13 June 2025].

[12] ISACA, "What is CMMI?" [Online]. Available at: https://www.isaca.org/enterprise/cmmi-performance-solutions? [Accessed March 2025].

[13] I. Ivan, C. Brândaș, A. Zamfiroiu, " Audit Validation Using Ontologies," Informatica Economica, vol. 19, no. 2, pp. 25-33, 2015.

Claudia-Iuliana PARASCHIV holds a degree from the Faculty of Cybernetics, Statistics and Economic Informatics of the Bucharest University of Economic Studies, where she also completed a master's programme in IT&C Security. Additionally, she obtained a master's degree in European Law. She is currently a second-year doctoral student in Economic Informatics at the same institution. She has eight years of experience across cybersecurity, IT operations, and IT audit, developed through roles in major international companies. Her work span's identity and access management, security governance, enterprise applications, cloud and infrastructure monitoring, and large-scale audit coordination, combining technical expertise with risk-focused insight. In parallel with her doctoral studies, she serves as an instructor in the Department of Economic Informatics and Cybernetics at the Bucharest University of Economic Studies, where she teaches Android development. Her professional and academic interests encompass cybersecurity, digitalisation, law, business, and leadership.