TIKD: A Trusted Integrated Knowledge Dataspace For Sensitive Healthcare Data Sharing

Julio Hernandez
ADAPT Centre
Dublin City University
Dublin, Ireland
julio.hernandez@adaptcentre.ie

Lucy McKenna
ADAPT Centre
Dublin City University
Dublin, Ireland
lucy.mckenna@adaptcentre.ie

Rob Brennan
ADAPT Centre
Dublin City University
Dublin, Ireland
rob.brennan@adaptcentre.ie

***Abstract*—This paper presents the Trusted Integrated Knowledge Dataspace (TIKD), a new dataspace, based on linked data technologies and trusted data sharing, that supports integrated knowledge graphs for sensitive application environments such as healthcare. State-of-the-art shared dataspaces do not consider sensitive data and privacy-aware log records as part of their solutions, defining only how to access data. TIKD complements dataspace security approaches through trusted data sharing that considers personal data handling, data privileges, pseudonymization of user activity logging, and privacy-aware data interlinking services. TIKD was implemented on the Access Risk Knowledge (ARK) Platform, a socio-technical risk governance system, and deployed as part of the ARK-Virus Project which aims to govern the risk management of Personal Protection Equipment (PPE) across a group of collaborating healthcare institutions. The ARK Platform was evaluated, both before and after implementing the TIKD, using the ISO 27001 Gap Analysis Tool (GAT) which determines compliance with the information security standard. The results of the evaluation indicated that compliance with ISO 27001 increased from 50% to 85%. The evaluation also provided a set of recommended actions to meet the remaining requirements of the ISO 27001 standard. TIKD provides a collaborative environment, based on knowledge graph integration and GDPR-compliant personal data handling, as part of the data security infrastructure. As a result of this work, a new trusted data security methodology, based on personal data handling, data privileges, access control context specification, and privacy-aware data interlinking, was developed using a knowledge graph approach.**

***Index Terms*—Dataspace, Knowledge Graph, Trusted Data, Personal Data Handling**

I. Introduction

Sharing data between healthcare organizations can facilitate medical diagnosis and biomedical research. Healthcare data is sensitive and organizations understand the importance of securely sharing, storing, managing, and accessing medical data. Recent work in medical data sharing is based on cryptosystems and blockchain approaches [1]–[3]. These approaches were designed to facilitate the sharing of patient medical records between healthcare institutions but do not support collaborative data sharing environments for the purpose of research, for example, where sensitive data could be shared between partners to improve or support related works. This paper explores the use of dataspace, a data management framework capable of interrelating heterogeneous data, for the sharing of sensitive data in a collaborative environment, as well as the use of knowledge graphs (KGs) in constructing a trusted data sharing environment.

In recent years, KGs have become the base of many information systems which require access to structured knowledge. A KG provides semantically structured information which can be interpreted by computers, offering great promise for building more intelligent systems [4]. KGs have been applied in different domains such as recommendation systems, information retrieval, medicine, education, and cybersecurity among others [5]. For example, in the medical domain, KGs have being used to construct, integrate, and map healthcare information. In the security domain, KGs have being used to detect and predict dynamic attacks.

A dataspace follows a "pay-as-you-go" approach where the priority is to set up the most beneficial aspects of the dataspace functionality, and to improve the semantic cohesion of the dataspace over time [6], [7]. The services offered over the aggregated data do not lose their surrounding context, i.e., the data is still managed by the owner, prevailing autonomy needs [8].

A shared dataspace involving sensitive data requires personal data handling alongside data security methods. Biomedical data sharing [9] is an example of a collaborative dataspace where sensitive data could be shared as part of a research project. Medical data sharing approaches [1]–[3] use cryptosystems to share patients' medical records between health institutions, thus relying on cloud services to manage data. According to Curry et al. [10], a trusted data sharing dataspace should consider personal data handling and data security, such as access control and usage control, in a clear legal framework. As such, this work explores the following research question: to what extent will the development of an integrated sharing dataspace, based on linked data technologies, personal data handling, data privileges, and data interlinking, contribute to building a trusted sharing dataspace in a collaborative

This research has received funding from the ADAPT Centre for Digital Content Technology, funded under the SFI Research Centres Programme (Grant 13/RC/2106_P2), co-funded by the European Regional Development Fund and the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No. 713567. For the purpose of Open Access, the author has applied a CC BY public copyright licence to any Author Accepted Manuscript version arising from this submission'.

environment? In response, this paper proposes the Trusted Integrated Knowledge Dataspace (TIKD) - an approach to the problem of secure data sharing in collaborative dataspaces. The contributions of this research are:

1) A new trusted dataspace, based on knowledge graph integration and information security management, for collaborative, high risk environments such as healthcare.
2) An information security management system based on personal data handling, data privileges, pseudonymization of user logs, and privacy-aware data interlinking.

The structure of the remainder of this paper is as follows: the Use Case section defines the requirements of the ARK-Virus project. The Related Work section presents the state-of-the-art in shared dataspace approaches. The Description of the TIKD details the services of the dataspace. The Evaluation section presents the results from the ISO 27001 GAT. Finally, the Conclusion section presents a summary of this research and its future directions.

II. Use Case - ARK-Virus Data sharing

The ARK-Virus Project aims to provide a collaborative space for Personal Protection Equipment (PPE) risk management across diverse healthcare and public service organizations [11]. The ARK Platform uses Semantic Web technologies to model, integrate, and classify PPE risk data, from both qualitative and quantitative sources, into a unified knowledge graph. This model is expressed using the ARK Cube Ontology[1] and the ARK Platform Vocabulary[2] [11], [12]. The Cube ontology is used in the overall architecture of the ARK Platform by supporting data analysis through the Cube methodology - an established methodology used for analyzing socio-technical systems and for managing associated risks [13], [14]. The Platform vocabulary allows for the modeling of platform users, access controls, user permissions and data classifications.

Through the ARK-Virus Project a set of security requirements for the ARK Platform were defined (see Table I). These requirements include data interlinking, data accessibility (privacy-aware evidence distillation), and secure evidence publication (as Linked Open Data), as priority security aspects. The state-of-the-art in shared dataspaces does not consider data access level and data sharing level selection mechanisms. The ARK platform implements the TIKD model to cope with these requirements (see Table I) and to provide secure management of personal data, pseudonymized data (for GDPR-compliance), and security logs (for history records).

III. Related work

Shared dataspace approaches are concerned with security aspects, such as access control [9], [10], [15], [16] and usage control [17], [18], in order to provide services based on the dataspace philosophy of 'pay-as-you-go'. Shared dataspaces are primarily associated with the Internet of Things (IoT) [10], [15], [16], [18], where data integration from heterogeneous devices and access control are the main objective. In the field of trusted data sharing, data management approaches focus on cryptography techniques and blockchain methods in order to share data between agents (users/institutions) [1]–[3]. Blockchain is an internet database technology characterized by decentralization, transparency, and data integrity [19]. On the other hand, access control is based on public and private key cryptography. Table II provides a comparison of the state-of-the-art works and TIKD in relation to the requirements of the ARK-Virus Project.

Shared dataspace approaches cope with data fusion [16], usage control between multiple organizations [17], real-time data sharing [10], and privacy protection [15]. However, these approaches do not provide mechanisms for personal data handling in compliance with GDPR, defined levels of data access, or privacy-protected interlinking with external resources. TIKD is based on a set of Linked Data vocabularies that support these aspects.

IV. Description of the TIKD

The Trusted Integrated Knowledge Dataspace (TIKD) was designed in accordance with the ARK-Virus Project security requirements (see Section II). The TIKD services (Figure 1) define data permissions (knowledge graph integration, subgraph generation, and data interlinking), user access grants (security control), and external resource integration (data interlinking) to provide a trusted environment. The next subsections explain each of these services.

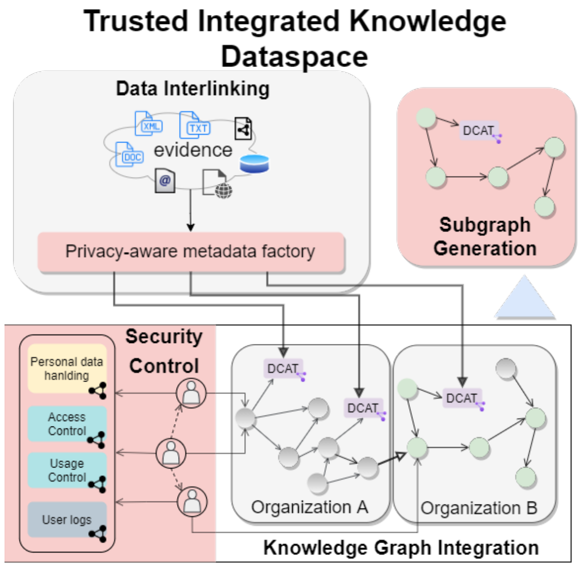

Fig. 1. The Trusted Integrated Knowledge Dataspace Services.

A. *Knowledge Graph Integration*

The knowledge graph integration service (Figure 1, Knowledge Graph Integration) is a central component of the TIKD. This service defines a dataspace where: i) multiple users can

[1] Available at https://openark.adaptcentre.ie/Ontologies/ARKCube

[2] Available at https://openark.adaptcentre.ie/Ontologies/ARKPlatform

TABLE I
ARK-Virus project requirements, description, and the solution proposed with the TIKD model.

#	Requirement	Description	Solution proposed with TIKD
1	Data encryption	Data stored on the ARK Platform will be encrypted and stored securely in line with the ISO 27001 information security standards.	The TIKD model will be deployed in an encrypted system based on a Linux Unified Key Setup (LUKS). Information security management will consider the ISO 27001 Gap Analysis Tool as a base reference.
2	Privacy-Aware Evidence Distillation	Users will be able to manually classify the information they enter into the platform as Public, Internal, Confidential or Restricted. Data will be securely stored in an evidence base and only accessible to users with the appropriate level of clearance.	The TIKD model defines a usage control to set access grants over data, determining who can collaborate (write access) on a project and who can read it (read-only access).
3	Data Interlinking	An interlinking function will allow users of the ARK-Virus platform to interlink risk management data with evidence stored within the platform and, in future iterations, related data held in external authoritative databases.	The TIKD model integrates an interlinking service to provide anonymous evidence integration. The evidence is integrated by means of data catalogues (DCAT) records describing the evidence metadata.
4	Evidence Publication as Linked Open Data (LOD)	Data stored in the ARK-Virus Platform database that has been classified as ‘Public’ will be made available as LOD via an open data portal.	The usage control service defines how data could be accessed based on their classification level. The data classified as public could be searched and collected for open publication purposes.

work on a KG within an organization, ii) multiple organizations can create KGs, iii) linking to datasets by means of the Data Catalog Vocabulary[3] (DCAT), instead of graphs/data, is supported, iv) fine-grained record linkage via DCAT records is supported, and v) where evidence and KG integration/linking is supported. DCAT is used to describe a set of resources associated with an specific organization but different authors. Each KG is defined based on the ARK-Platform and the ARK-Cube ontologies.

B. Security Control

The Security Control service (Figure 1, Security Control) is the main service of the TIKD. This service makes use of Linked Data vocabularies to handle personal data, access control context specification, usage control, and user logs. Personal data is described using the DPV, which was proposed by the W3C's Data Privacy Vocabularies and Controls Community Group (DPVCG). The DPV defines a set of classes and properties that can be used to describe and represent information about personal data handling for the purpose of GDPR compliance.

The Access Control service mediates every request to the resources and data stored on the ARK Platform, determining whether the request should be granted or denied. TIKD defines a discretionary access control (DAC), based on context specification, where data owners can authorize and control data access. The Access Control service defines a user through the User[4] class from the ARK-Platform ontology. The User class was extended with the properties username, password, and email. The user's role determines their privileges over a KG - here the highest role is owner, the medium role is collaborator, and the lowest role is read-only. The Usage Control and Access Control services were designed to meet the Privacy-Aware Evidence Distillation requirement. The Usage Control service defines what users can, or can not, do on the ARK platform based on their role. In the context of TIKD, the Usage Control service ensures that a user has the appropriate role to access the KG as well as the corresponding data permissions (read/write). According to user's role, data owners and collaborators can read and write in the KG, whereas read-only users can only visualize the information in the KG. The Usage Control service is implemented based on the ARK-Platform ontology through the User class and the following properties:

- isOwnerOf[5]: relates an owner with a KG. The owner user can read and write.
- isCollaboratorOf[6]: relates a collaborator with a KG. The collaborator user can read and write.
- isReadOnlyUserOf[7]: relates a read-only user with a KG. The read-only user can visualize the project.

Finally, the User Log service will record the actions performed by users during their sessions on the ARK platform. User information is pseudonymized in the log data, using the Secure Hash Algorithm 3 (SHA-3), by combining the username, email, and registration date parameters. The user logs will record user activities on the platform and the results retrieved by the system (failure, success, warning, etc.) during a session, e.g., if the user tries to modify the KG but their role is read-only, the user log process will record this activity as well as the failure response from the system. The PROV

[3] https://www.w3.org/TR/vocab-dcat-2/

[4] https://openark.adaptcentre.ie/Ontologies/ARKPlatform#User

[5] https://openark.adaptcentre.ie/Ontologies/ARKPlatform#isOwnerOf

[6] https://openark.adaptcentre.ie/Ontologies/ARKPlatform#isCollaboratorOf

[7] https://openark.adaptcentre.ie/Ontologies/ARKPlatform#isReadOnlyUserOf

TABLE II
COMPARISON OF SHARING DATA IN DATASPACE AND TIKD TRUSTED DATA SHARING APPROACHES.

Title	Year	Data Encryption (Req #1)	Privacy-Aware Evidence Dest. (Req #2)	Data Interlinking (Req #3)	Evidence publication as LOD (Req. #4)
A risk-based framework for biomedical data sharing [9]	2017	–	Security levels	–	–
MedBlock: Efficient and Secure Medical Data Sharing Via Blockchain [3]	2018	Private and public keys	Blockchain	–	–
A Method and Application for Constructing a Authentic Data Space [16]	2019	–	Business rules and security levels	–	–
An Architecture for Providing Data Usage and Access Control in Data Sharing Ecosystems [17]	2019	–	Policies	–	–
A real-time linked dataspace for the internet of things: Enabling ”Pay-as-you-go” Data Management in Smart Environments [10]	2019	–	Roles	–	–
International Data Spaces [18]	2019	–	Roles	–	–
A Blockchain-Based Medical Data Sharing and Protection Scheme [2]	2019	Private and public keys	Blockchain	–	–
An IoT data sharing privacy preserving scheme [15]	2020	–	Policies	–	–
Medical Data Sharing Scheme Based on Attribute Cryptosystem and Blockchain Technology [1]	2020	Private and public keys	Blockchain	–	–
A Trusted Integrated Knowledge Dataspace (TIKD)	2021	Linux Unified Key Setup and ISO 27001 GAT	Roles and security levels	Data catalogs (DCAT)	Data classification

ontology[8] is used to implement the user logs, following an agent-centered perspective (i.e. focusing on the people or organizations involved in the data generation or manipulation process).

C. Data Interlinking

By means of an interlinking service, TIKD supports the integration of KGs and also provides special support for the integration of potentially sensitive external resources (a data interlinking requirement of the ARK-Virus Project).

The Data Interlinking service allows users to add data from an external source as evidence. The evidence is used to support data defined in the KG. Evidence is interlinked through DCAT records. A DCAT record is generated through the privacy-aware metadata factory. The resulting DCAT record will be available only to the data owner and collaborators.

D. Subgraph Generation

The Subgraph Generation service (Figure 1, Subgraph Generation) provides the functionality of sharing data as private (owner and collaborators), or public (any agent in the system). The owner and/or collaborators of a KG have the ability to change the sharing permissions of the data subgraph.

The ARK-Virus Project defines a collaborative environment where different users can share data from their own KGs using a privacy-aware sharing mechanism whereby confidential or sensitive data cannot be shared outside an organization. This sharing functionality helps to reuse information to enrich related KGs. In this sense, the Subgraph Generation service helps to extend or complement information from one KG to another.

V. SECURITY EVALUATION OF THE ARK PLATFORM

This section presents a security evaluation of the ARK platform considering the requirements of the ISO 27001 standard. The ISO 27001[9] (ISO/IEC 27001) is a specification for information security management systems (ISMS). The ISO 27001 helps to increase the reliability and security of systems and information, and improved customer and business partner confidence, by means of a set of requirements.

The security evaluation of the ARK Platform[10] was conducted using the ISO 27001 Gap Analysis Tool (GAT)[11]. The ISO 27001 GAT can be used to identify gaps in ISO 27001 compliance, and to prioritize areas for future work. Some features of the ISO 27001 GAT are listed below:

- The tool contains a set of sample audit questions.
- It lists all ISO 27001:2013 requirements, identifying what documentation is mandatory for compliance.

The ISO 27001 GAT consist of 41 questions divided into seven clauses. Each clause is divided into sub-clauses, containing one or more requirements (questions). For example, the clause “Leadership” is divided into three sub-clauses, the first sub-clause is *leadership and commitment*, containing three requirements. The first requirement is: “are the general ISMS

[8] https://www.w3.org/TR/2013/NOTE-prov-primer-20130430/

[9] https://www.iso.org/isoiec-27001-information-security.html

[10] The evaluation was performed by three computer scientists with strong backgrounds in Linked Data and security systems. The first evaluation was performed in February 2021 and the second was performed in April 2021

[11] https://www.itgovernance.eu/en-ie/shop/product/iso-27001-gap-analysis-tool

objectives compatible with the strategic direction?", a positive answer means that the ISMS supports the achievement of the business objectives.

The ISO 27001 GAT was conducted on the ARK Platform both before and after implementing TIKD. Before implementing TIKD, the ARK Platform only used access control, based on authentication process, to provide access to the platform. The results of both evaluations can be seen in Table III where *#Req.* defines the number of requirements for each sub-clause, *Impl* defines the number of implemented requirements, and *%Impl.* defines the percentage of implemented requirements.

It can be seen that compliance with the ISO 27001 standard increased, from 53.66% to 85.37%, after implementing the TIKD on the ARK platform. There was a notable increase in the "Operation" and "Performance evaluation" clauses after the TIKD was employed. However, there are still some requirements that are yet to be addressed in order to achieve an increased level of compliance with the ISO 27001 standard. Table IV outlines these unaddressed requirements as well as the action needed to implement them.

VI. Conclusions

In this paper the Trusted Integrated Knowledge Dataspace (TIKD) was presented as an approach to securely share data in collaborative environments by considering personal data handling, data privileges, access control context specification, and a privacy-aware data interlinking.

TIKD was implemented in the ARK platform, considering the security requirements of the ARK-Virus project, to explore the extent to which an integrated sharing dataspace, based on linked data technologies, personal data handling, data privileges, and interlinking data, contributes to building a trusted sharing dataspace in a collaborative environment. In comparison with state-of-the-art works, TIKD integrates solutions for security aspects, data interlinking, GDPR-compliant personal data handling as part of the data security infrastructure, and evidence interlinking.

The security evaluation of the ARK platform was conducted using the ISO 27001 Gap Analysis Tool (GAT). The evaluation compared two versions of the ARK platform, a version before TIKD implementation and a version after TIKD implementation. According to the results, the implementation of the TIKD achieved a 85.35% ISO 27001 compliance score, improving the security aspects of the ARK platform as compared to the version before TIKD implementation.

Future work will focus on addressing the remaining ISO 27001 standard requirements. Additionally, the TIKD will be evaluated by the project stakeholders, and their feedback will be used to distill further requirements.

References

[1] X. Yang, T. Li, X. Pei, L. Wen, and C. Wang, "Medical data sharing scheme based on attribute cryptosystem and blockchain technology," *IEEE Access*, vol. 8, pp. 45 468–45 476, 2020.

[2] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A blockchain-based medical data sharing and protection scheme," *IEEE Access*, vol. 7, pp. 118 943–118 953, 2019.

[3] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," *J. Med. Syst.*, vol. 42, no. 8, p. 1–11, Aug. 2018. [Online]. Available: https://doi.org/10.1007/s10916-018-0993-7

[4] X. Zou, "A survey on application of knowledge graph," *Journal of Physics: Conference Series*, vol. 1487, p. 012016, mar 2020. [Online]. Available: https://doi.org/10.1088/1742-6596/1487/1/012016

[5] H. L.-r. XU Zeng-lin, SHENG Yong-pan and W. Ya-fang, "Review on knowledge graph techniques," *Journal of University of Electronic Science and Technology of China*, vol. 45, no. dzkjdxxb-45-4-589, p. 589, 2016. [Online]. Available: http://www.juestc.uestc.edu.cn//article/id/41

[6] M. Franklin, A. Halevy, and D. Maier, "A first tutorial on dataspaces," *Proc. VLDB Endow.*, vol. 1, no. 2, p. 1516–1517, Aug. 2008. [Online]. Available: https://doi.org/10.14778/1454159.1454217

[7] S. R. Jeffery, M. J. Franklin, and A. Y. Halevy, "Pay-as-you-go user feedback for dataspace systems," in *Proceedings of the 2008 ACM SIGMOD International Conference on Management of Data*, ser. SIGMOD '08. New York, NY, USA: Association for Computing Machinery, 2008, p. 847–860. [Online]. Available: https://doi.org/10.1145/1376616.1376701

[8] M. Franklin, A. Halevy, and D. Maier, "From databases to dataspaces: A new abstraction for information management," *SIGMOD Rec.*, vol. 34, no. 4, p. 27–33, Dec. 2005. [Online]. Available: https://doi.org/10.1145/1107499.1107502

[9] F. K. Dankar and R. Badji, "A risk-based framework for biomedical data sharing," *J. Biomed. Informatics*, vol. 66, pp. 231–240, 2017. [Online]. Available: https://doi.org/10.1016/j.jbi.2017.01.012

[10] E. Curry, W. Derguech, S. Hasan, C. Kouroupetroglou, and U. ul Hassan, "A real-time linked dataspace for the internet of things: Enabling "pay-as-you-go" data management in smart environments," *Future Generation Computer Systems*, vol. 90, pp. 405–422, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167739X1732887X

[11] L. McKenna, J. Liang, N. Duda, N. McDonald, and R. Brennan, "Ark-virus: An ark platform extension for mindful risk governance of personal protective equipment use in healthcare," in *Companion Proceedings of the Web Conference 2021 (WWW '21 Companion), April 19–23, 2021, Ljubljana, Slovenia. ACM, New York, NY, USA*, 04 2021.

[12] A. C. Jr., M. Basereh, Y. M. Abgaz, J. Liang, N. Duda, N. McDonald, and R. Brennan, "The ARK platform: Enabling risk management through semantic web technologies," in *Proceedings of the 11th International Conference on Biomedical Ontologies (ICBO), Italy, September 17, 2020*, ser. CEUR Workshop Proceedings, J. Hastings and F. Loebe, Eds., vol. 2807. CEUR-WS.org, 2020, pp. 1–10. [Online]. Available: http://ceur-ws.org/Vol-2807/paperM.pdf

[13] S. Corrigan, A. Kay, K. O'Byrne, D. Slattery, S. Sheehan, N. McDonald, D. Smyth, K. Mealy, and S. Cromie, "A socio-technical exploration for reducing & mitigating the risk of retained foreign objects," *International Journal of Environmental Research and Public Health*, vol. 15, no. 4, 2018. [Online]. Available: https://www.mdpi.com/1660-4601/15/4/714

[14] N. McDonald, "The evaluation of change," *Cogn. Technol. Work*, vol. 17, no. 2, pp. 193–206, May 2015.

[15] Y. Sun, L. Yin, Z. Sun, Z. Tian, and X. Du, "An iot data sharing privacy preserving scheme," in *39th IEEE Conference on Computer Communications, INFOCOM Workshops 2020, Toronto, ON, Canada, July 6-9, 2020*. IEEE, 2020, pp. 984–990. [Online]. Available: https://doi.org/10.1109/INFOCOMWKSHPS50562.2020.9162939

[16] W. Sun, Z. Huang, Z. Wang, Z. Yuan, and W. Dai, "A method and application for constructing a authentic data space," in *2019 IEEE International Conference on Internet of Things and Intelligence System, IoTaIS 2019, Bali, Indonesia, November 5-7, 2019*. IEEE, 2019, pp. 218–224. [Online]. Available: https://doi.org/10.1109/IoTaIS47347.2019.8980430

[17] A. Munoz-Arcentales, S. López-Pernas, A. Pozo, Álvaro Alonso, J. Salvachúa, and G. Huecas, "An architecture for providing data usage and access control in data sharing ecosystems," *Procedia Computer Science*, vol. 160, pp. 590–597, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919317429

[18] B. Otto, M. t. Hompel, and S. Wrobel, *International Data Spaces*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2019, pp. 109–128. [Online]. Available: https://doi.org/10.1007/978-3-662-58134-6_8

[19] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2009. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf

TABLE III
ARK PLATFORM SECURITY EVALUATION, BEFORE AND AFTER IMPLEMENTING THE TIKD, BASED ON THE ISO 27001 GAT.

Clause	**Sub-Clause**	**#Req.**	**Before TIKD**		**After TIKD**	
			Impl.	%Impl.	Impl.	%Impl.
Context of the organization	Understanding the organization and its context	3	2	66.67%	2	66.67%
	Understanding the needs and expectations of interested parties	2	2	100%	2	100%
	Determining the scope of the information security management system	1	0	0%	1	100%
	Information security management system	1	0	0%	1	100%
Leadership	Leadership and commitment	3	3	100%	3	100%
	Policy	2	0	0%	2	100%
	Organizational roles, responsibilities and authorities	1	1	100%	1	100%
Planning	Actions to address risks and opportunities	3	1	33.33%	3	100%
	Information security objectives and planning to achieve them	2	1	50%	2	100%
Support	Resources	1	1	100%	1	100%
	Competence	1	1	100%	1	100%
	Awareness	1	1	100%	1	100%
	Communication	1	1	100%	1	100%
	Documented information	3	2	66.67%	3	100%
Operation	Operational planning and control	3	3	100%	3	100%
	Information security risk assessment	1	0	0%	1	100%
	Information risk treatment	2	0	0%	1	50%
Performance evaluation	Monitoring, measurement, analysis and evaluation	2	0	0%	2	100%
	Internal audit	2	0	0%	1	50%
	Management review	2	2	100%	2	100%
Improvement	Nonconformity and corrective action	3	0	0%	0	0%
	Continual improvement	1	1	100%	1	100%
TOTAL		**41**	**22**	**53.66%**	**35**	**85.37%**

TABLE IV
UNADDRESSED CLAUSES AND THE ACTION NEEDED TO COMPLY WITH ISO 27001 REQUIREMENT.

Clause	**Requirement**	**Action to Perform**
Context of the organization	Did the organization determine how internal and external issues could influence the ISMS ability to achieve its intended outcomes?	Organization stakeholders will be define how internal and external issues can affect the security model.
Operation	Is there a documented list with all controls deemed as necessary, with proper justification and implementation status?	A set of actions, to address risks, will be established. This will be periodically reviewed, tested and revised where practicable
Performance evaluation	Are internal audits performed according to an audit program, results reported through an internal audit report, and relevant corrective actions raised?	An internal audit will be performed.
Improvement	Does the organization react to every nonconformity? Does the organization consider eliminating the cause of the non-conformity and, where appropriate, take corrective action? Are all non-conformities recorded, together with corrective actions?	Non-conformity data will be collected from the stakeholders. A document with the procedure(s) to address non-conformities, including the identification of causes and actions to prevent recurrence, will be prepared. The results will be recorded for future reference and corres -ponding documentation will be prepared.