

L-7 Data Security, Governance and Compliance

(ACCA7028)

ASSIGNMENT

Madhusudan Ghumare

(2116948)

Table of Contents

Introduction.....	3
1. Conducting the research based on the security framework	3
1.1 Information Infrastructure Library (ITIL).....	3
1.2 Security model.....	4
1.3 ISO	4
2. Understanding and knowledge based on several factors	5
2.1 Designing an approach for meeting requirements.....	5
2.2 Importance of updated regulations in practice	7
2.2.1 Compliance	7
2.2.2 Strategic planning and governance with security	7
2.2.3 Security aspects and policies	8
2.2.4 Risk management	10
2.2.5 Security management models.....	10
2.2.6 Contingency planning.....	11
2.2.7 Protection mechanism.....	12
2.2.8 Service level agreement.....	13
Conclusion	14
Reference list	15

Introduction

Commercial security aspects are generally getting placed in this report for implementing some activities with the help of suitable infrastructure. The creation of each value is getting profound details with those various kinds of values that can take the overall charge to endure the process values. As the infrastructure is generalizing different kinds of authenticated services which can help address issues with authenticated surveys in the project timeline. Different kinds of issues are generalizing each propaganda with the help of authorized terms and sentimental overviews. For creating each estimation various allocative representations in which the values are taking valid details to look after the architectural aspects generally require some framework for establishing various attributes for security aspects in the overall project. Various trust issues are distributed in the framework to enhance the key values which are creating such aspects in the initialization of potentiality. Permissions in which basic allocative terms lie in various specification allocations are taking a few considerations to define *Coffee Blend* company's characteristics in an accurate way of presentation. More likely trust merchants are clearly getting placed in the decorum from which basic terms are managing various complex relationships. Commercial aspects can always be tracked and there is a possibility that it can get attacked by hackers in any case scenario. Getting profound help must take occasional considerations in a wider range of allocation for enduring the market place in an efficient number. Selected segments are placed in this project to endure the compatibilities for adding extra accuracy to the security all the segments are stuffed with thematic analysis which is getting placed in the following.

1. Conducting the research based on the security framework

1.1 Information Infrastructure Library (ITIL)

Creating such aspects might take periodically considered values that are generally suitable to endure each compatibility. According to the viewpoints of Alaa Abdul Al Muhsen Hussain (2022), generalizing these kinds of allocated terms in the project might get used in the timeline with values and exponential terms to enhance compatibility. Generalizing some allocated terms is taking some validated values to ensure the services of the company with great values in allocated terms.

Information Infrastructure Library (ITIL) services are taking some consideration values in the project management methods to ensure compatibility from roots to tips. Gaining in allocated terms in the allocated values must enhance the collaborative aspects for ensuring the services of the **CoffeeBlend** company. The life cycle evolves in the implementation program and that can endure different kinds of compatibilities taking valid allocated terms in order to comprehend the valuable assets which the process might take few considerations for enduring the visualization methods. Practices that can take valid reasons for the library to endure compatibility from the implementation program. Each component that can enhance the key values is generalizing the factors with profound techniques which is ensuring the business objectives. Components that are lending different kinds of values from the library are managing each value to make connections with various objectives in the library.

1.2 Security model

Getting value from the roots can take the overall allocative term in order to engage the key aspects (Allen *et al.* 2022). A generalized framework has been taking valid allocations in order to comprehend the values from the roots, generalization is managing some aspects that are referring to the endurance of each compatibility from the roots. Security aspects that are generalizing the compatibility are generalizing authentication values. Getting allocated with these expanding values is establishing some security models with the help of different kinds of confines which can lend some help to managing the security model. Model allocation generally taking so few authenticated values from the implementation program which takes valid details to manage the confidentiality aspects and authenticity allocations as well. Creation of valid terms is getting placed in order to comprehend the client data using some promulgated pliers which are referring to value endurance aspects. Allocating valid details in valuable terms enhances the key values in terms of getting valid details that can take part for being able in the estimation for a particular client solution. Getting values from the web allocations are taking valid points to enhance the client credentials. Managing the estimation can take the overall factors in an accurate way to lead the accurate terms with profound authentication values.

1.3 ISO

Allocating valid details in order to manage various values is lending some valuable terms to expand the quality values. For the coursework of Anu (2022), performances that can take the values from the roots are generalizing the compatibilities with the help of some measurement standards in hand. The creation of each allocation must rely on an occasional measuring system that can measure compatibility with the help of quality standards. All the standards that can endure the compatibility are taking some measurements in the allocation. *ISO* is generally a certification that can take various accomplishments in the allowances with deep measurements to measure the quality standards. Creation of comparing the business performances some detection methods are taking place in the allocation to enhance the key allocations for the company (Guggenmos *et al.* 2022). Taking out the certification must rely on a few aspects of developing measurement in the certification areas. Lending various allocations must take little consideration in the project which can create values from the roots with the help of appropriate terms.

2. Understanding and knowledge based on several factors

2.1 Designing an approach for meeting requirements

A basic allocation can take the entire approach in an accurate manner which can lead to the appropriate values of the project. Security design for estimating the components are generalizing various allocated terms which can lead to an accurate path for competence in each significant measure. Development values are generally taking valid reasoning in the system decorum to endure capabilities with continuous testing measures and authentication values (Hong-Jing Lin *et al.* 2022). Programming practices in which each value is generally made are willingly estimated in different kinds of possibilities that are referred to by a design allotment to lead in an accurate route. As the development process takes the overall charges to endure the capabilities in order to comprehend the values. Considering various terms are generally authenticated in the safeguards to estimate a diagram for enhancing the possible attack expenditure terms. All the values that are taking some authenticated value in the case scenarios are taking deep consideration in the allocative terms which are taking place in the following to estimate valid key aspects for the defined project significance.

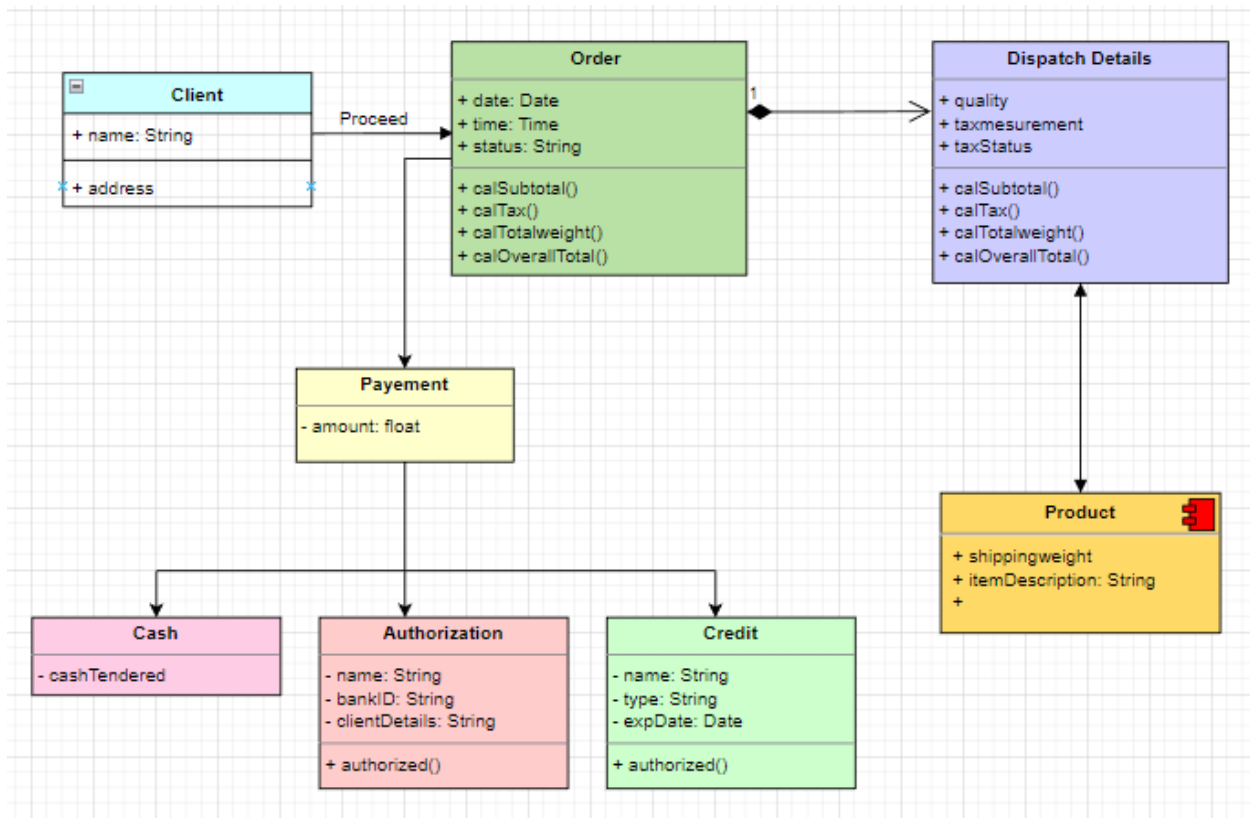


Figure 2.1.1: Class Diagram of Client and Services Interaction Methods in the Company

(Source: Self-created)

Graphical representations are taking place in this allocation with profound techniques and valuable assets in them (Wu *et al.* 2022). The creation of these kinds of allocative terms might be useful allocation in order to comprehend each value and systematic viewpoint. Several considerations are gradually made in the process for getting various values in the diagram representation, overlooking aspects are getting placed in the following.

- In the initial state, various attributes are taking valid elements to be more accurate from the beginning. The customer allocative terms are predefined in the allocation for generalizing each name and address of the clients (Kemendi *et al.* 2021). Storing these types of data is a useful allocation to enhance the key aspects of the ordering system.

- Presentations of a static value are generally getting placed in the diagram with compound materials. Creation of these kinds of allocations might take occasional overviews in order to create an appropriate allocation of the ordering table. All the above figures are present to expand each value from the roots which can take occasional overviews to calculate subtotals with the help of tax and weight of the overall product allocation.
- The details during the order are generally measuring the qualities with the help of each taxation status (Kirss, 2022). Values that can lend different kinds of shipping items in the allocation are generally measuring the overall price of the product. Managing these kinds of allocations in order to measure the values is generalizing the taxation overviews as well to enhance each key aspect.
- Essential values which are establishing different kinds of allocation in order to comprehend the elemental details are taking valid reasons for payment allocation. The payment process generally offers to clients three mediums of payment types: cash, check, and credit. All the methods which can measure compatibility are generating some valid values with the help of some mapping process representation.

2.2 Importance of updated regulations in practice

2.2.1 Compliance

Measuring safety can lend some strong helping hands to measure the public goods and services which is important to endure the project values. Taking out the allocational terms must take a few considerations which can measure the values in an effective way to endure the compatibilities (Mindlin *et al.* 2022). Each service that can measure the values are taking out some accurate reasonings to function some possible outcomes in the project timeline.

2.2.2 Strategic planning and governance with security

The main purpose of the strategic planning for introducing effective security measures that provide the management of "*CoffeeBlend*" with the necessary information to take informative decision-making statements. Additionally, the term "*governance*" refers to wide set of responsibilities and practices that are required to be exercised by the executive management of the organization to

enhance the strategic directions. Effective management of strategic planning provides inevitable processes for enhancing security management as it ensures *effective risk management* so that the data in the underlying staff will be managed effectively. Moreover, it is also essential to maintain *confidentiality, and the factor of the integrity* of the data available so that the factor of *nonrepudiation* will be preserved in throughout the management structures (Szczepaniuk *et al.* 2020).



Figure 1: Aspects of strategic planning

Ensuring the data security of all employees and customers requires framing a subset of the information governance that deals with a wide range of protecting corporate data both in the unstructured as well as in the structured form. It is evident to abide by all the procedures and policies in the governance framework so that all of these will be effectively implemented throughout the management structures.

2.2.3 Security aspects and policies

The main terminology of the "**Data Security policy**" is based on framing designing, implementing, guiding, managing and monitoring the security system in such a manner that it will create effectiveness in organizational data.

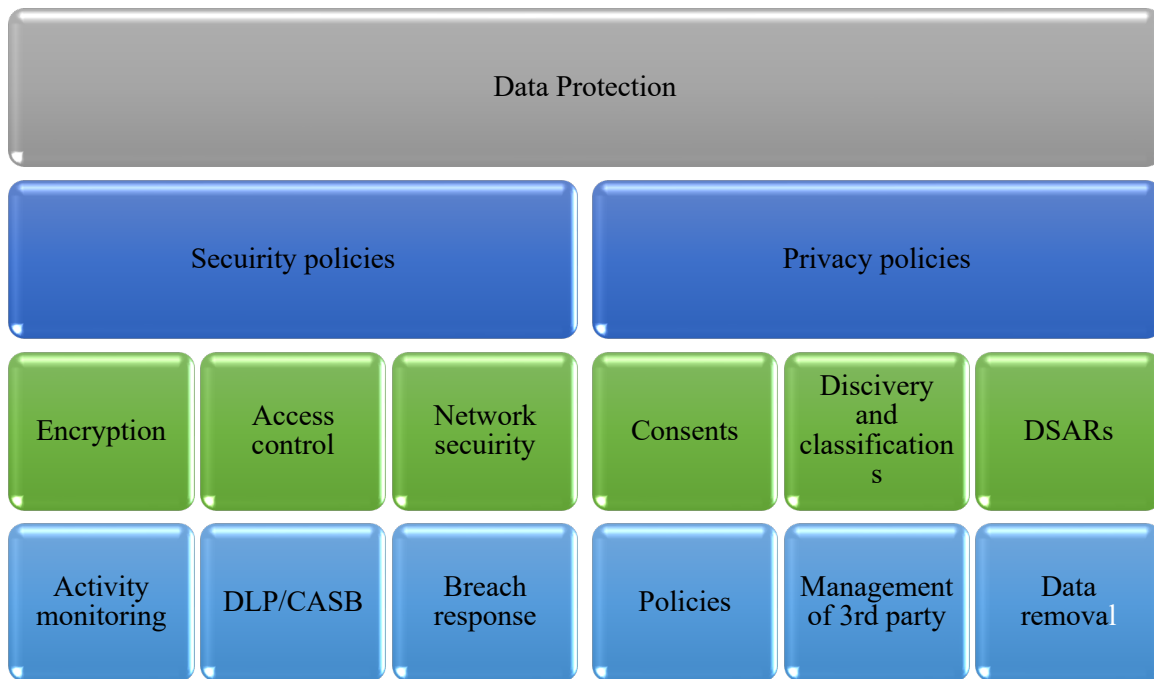


Figure 2: Components of security policies

Based on the **Data Protection Act (DPA), 2020** in Jamaica, seeks to provide privacy to the underlying personal information of the valuable dataset of clients so that security principle has been preserved throughout the process (Japarliament.gov.jm, 2022). This act also empowers the associated individuals to take effective control of the personal data so that it will support the organization's lawful aspects of the personal data. In this present research context, the organization of "**CoffeeBleand**" expressed their effective concern based on protecting the **intellectual properties of the staff along with the client data**. The personal data of the employees have been required to protect based on implementing the encryption method along with doing the access control along with the Network security process (Kumar *et al.* 2018). Privacy aspects of the clients require to be maintained based on applying the General Data Protection Regulation (GDPR) so that it will ensure effective preservation of the data.

2.2.4 Risk management

Factors	Likelihood	Severity	Impact	Mitigation strategies
Data tempering	Moderate	Low	Moderate	- Using firewalls - Controlling the network traffic
Password related threats	High	Moderate	High	- Monitoring all the activity - Enforcing steps in managing the password issues - Provide consistent training to the employees
Lack of accountability	Moderate	Low	Moderate	- Setting the team goals - Scaling the feedback skills - Creating a culture for two-way feedback
Falsifying the user identities	Moderate	Moderate	Moderate	- Provide features for frequent change in password - Monitoring the authorised transactions
Issues in managing the intellectual property	High	High	High	- Focusing on scrutiny - Maintaining a record - Protect the IP-related delay

Table 1: Analysing Risk Register

2.2.5 Security management models

This model ensures a mechanism of holistic management to assist all the transactional along with the multidimensional threats so that the security features will be effective in coordinating with the changes incorporated in the overall process. Moreover, *security management practices* entail the processes of identification of all the information in the organizations to be developed so that it will help in detecting the standards along with the policies incorporated to ensure the availability of the underlying data (Lidster and Rahman, 2018). It also ensures the confidentiality and integrity of the data to the employees along with the clients so that it will be effectively implemented in throughout the management procedures. It requires to implementation of data security processes based on the "NIST cybersecurity model" in this context that ensures effective data management. It includes:

Factors	Discussions
Identify	Establishing an effective business approach to security management including the current risks of maintaining sensitive data
Protect	Developing the program maturity to organize the data to protect the security program
Detect	This process drives all the cybersecurity management processes in encompassing the monitoring processes for identifying the risks in an effective manner
Respond	This step entails the aspects of tackling all the steps underlying the present practices so that the impact of malicious activity will get reduced
Recover	Requires to get the scheduled time to recover so that it will reflect on damages based on the real tasks of data security

Table 2: Security management models

2.2.6 Contingency planning

Contingency planning involves the processes of the restructuring the organizational policies to be ready in any case of circumstances. It must be capable of mitigating the issues faced by the current organization of "*CoffeeBlend*" so that it must equal the time saved by the disaster strikes.

Phase	Factors	Discussions
1	Notification and Activation	• Focused on activity criteria • Outage assessment • Notification of all affected parties
2	Recovery	• Sequence of activities • Awareness • Recovery escalation notices • Procedure of recovery
3	Reconstruction	• Validation of data • Testing the system functionality • Focusing on the system recovery • Recovering and deactivating the present systems along with data backups

Table 3: Contingency planning

This planning context underlying the recovery along with the reconstruction processes is required to be ensured throughout the management process (D'Agostino *et al.* 2019). It requires testing the functionality of the planning procedure so that it can deal with the issues faced by the organizations.

2.2.7 Protection mechanism

The protection mechanism lies in building the overall computer architecture in supporting the enforcement so that the security policies will be implemented throughout the management

procedures. Maintaining physical security along with the authentication processes so that the data encryption will be effectively implemented throughout the tasks. It requires eliminating access to the key network resources so that they will be secured from the other prospects. The *step of authentication* also involves requesting the network services to be restored in between the processes so that it will handle all the software processes (Zhang and Chen, 2019). It is also quite evident in maintaining the security features based on the login ID and password so that the same will be implemented in securing the data of the employees along with the data of the client. The step of *authorization* also helps in controlling the network resources so that it will help in doing the security administration in the main part of the network. This type varies with the conception of the users that also depends on the job functions for effective accounting throughout the processes. Encryption of all the underlying data requires to be done in such manner so that effectiveness among all the datasets will be preserved. Implementing the firewall in the data protection processes also allows for enhancing the security measure in throughout contexts.

2.2.8 Service level agreement

Service level agreement (SLA) evolves into a contract that is framed between the services or wider along with the underlying customers based on maintaining the standard of services throughout the context (Subramanian and Jeyaraj, 2018). The main purpose of making the SLA agreement lies in expecting all the metrics of the vendors that help in measuring the assessment along with the remedies that should be implemented based on the prescribed services. It also defines specific responsibilities adopted by the service provider so that they fulfil the requirement of the customers. It requires adopting some precautionary principles so that all the valuable data has been stored in the cloud for future data processes. Storing the information in the cloud ensures it to be retrieved at any point in time based on adopting the SLA negotiation (Kumar et al. 2018).

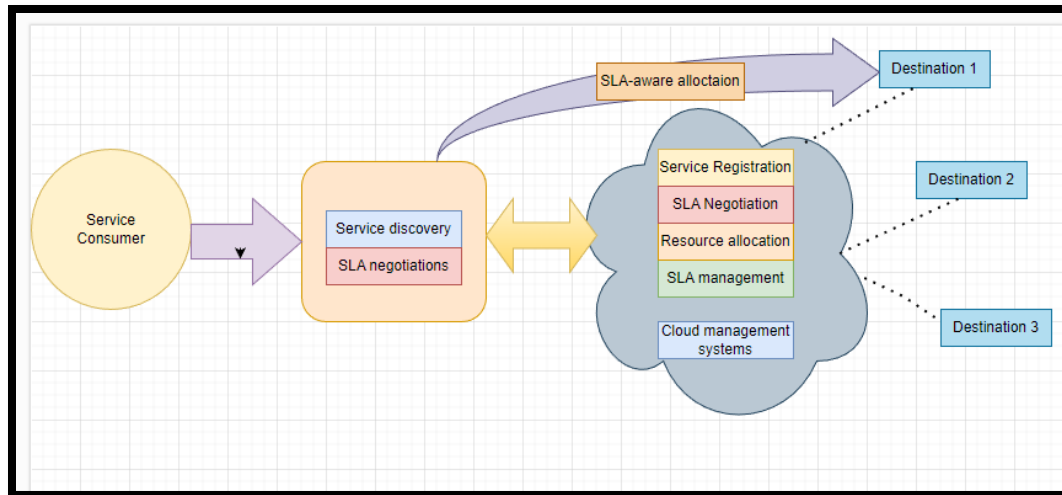


Figure 3: SLA structure

It also requires to do effective service registration along with resource allocation so that it will demonstrate an effective cloud management system so that the requirements of the enterprise will be assured by implementing the modern technologies in the present context.

Conclusion

It concludes that all the discussed factors require to be implemented in the overall context so that the effectiveness will be enhanced in meeting the issues identified in "*CoffeeBlend*". Data encryption is required to be done in such a manner so that it will ensure an enhanced rate of data security throughout the management contexts. In this provided case study, their identified organization has faced severe issues in handling the data of the clients along with the data of the employees. It is also quite problematic in wider to protect intellectual properties throughout the management process. The same will reach into the severe context in case all the management processes have been wireless. Maintaining the data in such a manner so that it will be presented online along with social media so that it will effectively maintain the data underlying in the associated contexts. Implementing the NIST architecture in the system processes also enhances the security measure in the underlying systems that enhance the security principles in the present business contexts.

Reference list

- [1]Alaa Abdul Al Muhsen Hussain Al Zubaidi and Pro. Florentin Ipate, “Application Programming Interface (API) Security: Cybersecurity Vulnerabilities Due to the Growing Use of APIs in Digital Communications,” *International Research Journal of Innovations in Engineering and Technology*, vol. 6, no. 6, p. 108–, 2022, doi: 10.47001/IRJIET/2022.606014.
- [2]M. T. Allen and S. P. Fraser, “Gates, guards and patrols: Impacts of community security features on home values,” *Managerial Finance*, 10-Jun-2022. [Online]. Available: <https://www.emerald.com/insight/content/doi/10.1108/MF-04-2022-0177/full/html>. [Accessed: 23-Dec-2022].
- [3]V. Anu, “Information security governance metrics: a survey and taxonomy,” *Information security journal.*, vol. 31, no. 4, pp. 466–478, 2022, doi: 10.1080/19393555.2021.1922786.
- [4]D’Agostino, G., Di Pietro, A., Giovinazzi, S., Porta, L.L., Pollino, M., Rosato, V. and Tofani, A., 2019. Earthquake simulation on urban areas: Improving contingency plans by damage assessment. In *International Conference on Critical Information Infrastructures Security* (pp. 72-83). Springer, Cham.
- [5]F. Guggenmos, B. Häckel, P. Ollig, and B. Stahl, “Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT Security in Digitalization Projects,” *Computers & security*, vol. 118, p. 102747–, 2022, doi: 10.1016/j.cose.2022.102747.
- [6]H. Lin, C. Chen, Y. Chiu, and T. Lin, “How financial technology (fintech) can improve the business performance of securities firms by using the dynamic data envelopment analysis modified model,” *Managerial and decision economics*, vol. 43, no. 4, pp. 1113–1132, 2022, doi: 10.1002/mde.3443.

[7]Japarliament.gov.jm , 2022. *The Data Protection Act, 2020.pdf* - Houses of Parliament. Available at: <https://japarliament.gov.jm>. [Accessed on: 27.12.2022]

[8]Á. Kemendi, P. Michelberger, and A. Mesjasz-Lech, “ICT security in businesses - efficiency analysis,” *Entrepreneurship and Sustainability Issues*, vol. 9, no. 1, pp. 123–149, 2021, doi: 10.9770/jesi.2021.9.1(8).

[9]A. Kirss, “Interest or ideology? Why American business leaders opposed the Vietnam War,” *Business and politics*, vol. 24, no. 2, pp. 171–187, 2022, doi: 10.1017/bap.2021.22.

[10]P. R. Kumar, P. H. Raj, and P. Jelciana, “Exploring Security Issues and Solutions in Cloud Computing Services – A Survey,” *Cybernetics and information technologies : CIT*, vol. 17, no. 4, pp. 3–31, 2017, doi: 10.1515/cait-2017-0039.125, pp.691-697.

[11]W. w Lidster and S. S. M. Rahman, “Obstacles to implementation of information security governance | IEEE ...,” *ieeexplore*, 03-Aug-2018. [Online]. Available: <https://ieeexplore.ieee.org/document/8456144/>. [Accessed: 20-Dec-2022]. (pp. 1826-1831). IEEE.

[12]Y. Mindlin, M. Novikov, and O. Ignatyeva, “Clusters and cooperatives as a tool of sustainable food security: a comparative analysis,” *IOP conference series. Earth and environmental science*, vol. 1043, no. 1, p. 12038–, 2022, doi: 10.1088/1755-1315/1043/1/012038.

[13]N. Subramanian and A. Jeyaraj, “Recent security challenges in cloud computing,” *Computers & electrical engineering*, vol. 71, pp. 28–42, 2018, doi: 10.1016/j.compeleceng.2018.06.006.

[14]E. K. Szczepaniuk, H. Szczepaniuk, T. Rokicki, and B. Klepacki, “Information security assessment in public administration,” *Computers & security*, vol. 90, p. 101709–, 2020, doi: 10.1016/j.cose.2019.101709.

[15]Y. Wu, M. Xu, D. Cheng, and T. Dai, “Information security strategies for information-sharing firms considering a strategic hacker,” *Decision Analysis*, vol. 19, no. 2, pp. 99–122, 2022.

[16]X. Zhang and X. Chen, “Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network,” IEEE access, vol. 7, pp. 58241–58254, 2019, doi: 10.1109/ACCESS.2018.2890736.