A Process Frame Work for Information Security Management System

Aditi, Kavita Dhiman

Department of Computer Applications

Chandigarh School of Business, Jhanjeri

Chandigarh Group of Colleges, Jhanjeri, Mohali, India

aditisaryal01@gmail.com, kavita.j1612@cgc.ac.in

Abstract: Organizations are finding that protecting sensitive data is becoming more and more important. A system to handle information security is a scientific technique for creating, carrying out, running, keeping an eye on, and evaluating, keeping, also enhancing a company's data safety. Important factors of an ISMS's functioning are its strategies. But still, regardless because of how crucial an ISMS method structure with an outline of the management system for information security strategies and their interactionin addition to the interplay with different control strategies isn't always to be had inside the literature. Cost advantage evaluation of data safety investments concerning single measures protective data and ISMS strategies aren't inside the awareness of modern studies, generally targeted regarding economies. This piecegoalsto complete this study's hole through offering a system similar that for managing information security method structure for the structure primary contribution. It is primarily based totally on a fixed of agreed-upon ISMS strategies in present requirements such is ITIL and COBIT. In the structure itself, diagnosed strategiesare definedand their interplay and interfaces are specified.Rather than emphasizing measures and controls, this strategy allows awareness of the ISMS's operation. As a result, by this prime discovering, systematic person of the System for the Administration of Information Securityincluding strategies with the belief of applicable the ISMS's roles are reinforced.

Keywords:-Data, Safety, Administration, Framework, monitoring, review

I. Introduction

Information safety is an essential detail of socialresponsibility. The reason for data safety is to guard a company's precious resources, including data. Information safety is likewise diagnosedwithin the context of technical (IT) management [1]. At applicable requirements and structures in addition to within clinical books, the constantly growingdepending on almost everyagencieswith suitable stable data processing turned into nearly within the final years. Requirements for the control of data safety various assortments of fine exercise actions have been evolved and installed inside. The works of literature, such as requirements regarding the improvement and how an ISMS is run are covered under the ISO 27000 series. [2].

Above the previous couple of decades, price advantage conversations are inspired data safety exercises. The cost of data has to justify safety expenses. Modification and price-performance is essential. factors of an effective ISMS. Understanding of the projectwanted The System for Information Security Management in order to align strategies about the company with its project. Consideringwhich enterprise harmony and price-efficiency are critical for a system for information security management to function effectively, studies investments have to cope with each issue by permitting the reduction in complexity of the identification of important, suitable strategies in center factors for each security management system.Differentiating among an ISMSfundamental operation, enabling processes, and administration processes as well as the security measures governed by the system's basic procedures is necessary for this particular process structure for security management. [3]. Two essential components of a good ISMS are cost-effectiveness and adjustment. A suitable interaction of theISMS procedures is ensured by an extensive architecture of input, output, and interaction processes and how they interact at the task level. In order to close this research gap, this study, as the fundamental components of any ISMS, a historical yet

comprehensive framework of ISMS basic procedures is suggested.

It is imperative that this particular process structure for security management makes a clear distinction between the safety precautions governed through the Information Systems Management System procedures and the core, supporting, and management processes of the ISMS.A successful ISMS must have both cost-effectiveness and adjustment. An extensive ISMS process framework. The interaction of (input, output, and interfaces) at the activity level contributes to the proper functioning of the ISMS processes. This paper proposes a comprehensive but precise structure of ISMS fundamental procedures as essential components of all ISMS's to close this research gap.

This paper offers a through structure and a methodical procedure for the oversight of information security through the examination of problems at higher elaboration stack tiers. The primary goals are to ensure cost-effectiveness in the design and execution of security enforcement actions and to offer organizational coordination for the use of security models stable and conflict-free, to offer sufficient security. This study objectives to explain the framework and supply a brief summary of first solutions for significant challenges rather than providing a deep examination of connected topics, despite the provision of particular remedies.

II. Literature Review

At the moment, there exists a big quantity of concepts for ISM, proposed throughresearchers, all of themcommon groups, enterprise corporations, political projects in light of protective data safety, as well as others. Everybody those ISM models focus in a particular area and possess their factor of view. The structure choice relies upon numerous elements which include enterprise region and geography. Therefore, in this segment, we can offer an outline of a few applicable ISM frameworks to shape a popular view on present solutions.
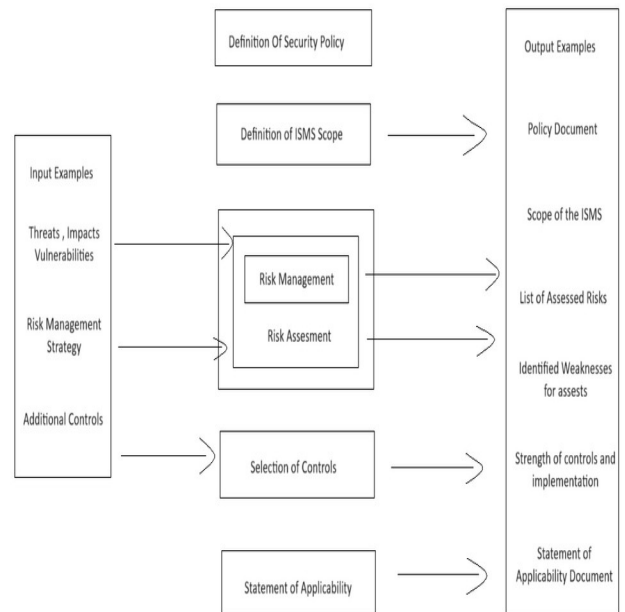
Fig. 1 : Framework of ISMS

Fig.1. Framework– ENISA[4]

Trcek (2003) proposed an essential framework for data structure safety control primarily based totally on layered multi-panes. The writer announces that to guard data, a company has first of all the identity of threats associated with enterprise resources. According to on threat evaluation, he suggested a multi-layered -aircraft strategy [5]. The initial aircraft targeted on exchanges, beginning along safety mechanisms as well as consequently putting in place safety offerings, that connectedto interactions between humans and machines. Lastly, communication between people need to be addressed. Therefore, concurrently, to make matters functioning, the researcher suggests cope with any other viewpoint, encompassing organizational, legislative, and technical spheres.

Bradley and Josang (2004) recommend a framework that is open for company safety control. This structure is meant to rely on innovation and contains a data storehouse, supervisor packages as well as arrangement dealers. Data storehouse shops community, safety coverage data.Supervisor packages are specific to the technology domain, and act as professional structures searching the database and speak with arrangement vendors. Configuration dealers offer the necessary

professional device adaptability [6]. This look suggests an academic way to thedata safety control problems. Given that the suggested structure depends on gadgets, it might no longer offer the kind of adaptability thatcan be necessary in specific circumstances.

Sherwood et al. (2005)indicated the Enterprise Security Architecture is based on the SABSA (Sherwood Applied Business Security Architecture) framework. SABSA is meant over growing danger -pushed company data safety and data integrity structures as well as for turning in safety systems answers assist crucial enterprise endeavours. It's an open standard that includes some designs, structures, techniques, and procedures [7]. The operational life cycle is covered by the SABSA Model skills also it contains 6 levels. Every vertical analysis exists in the horizontal layer primarily foundedtotallyregarding the six inquiries: Which (assets)? Why (the driving force)? How (method or technologies)? Whom (individuals)? Where is that? When is that? This results ina 6-by-6 molecular matricesreferred to asthe Main Structure for SABSA [8].6th level, carrierlayer of management is placed on top of the opposite 5thlevels orin addition, vertical analyzed for provide 5/6 mobileular Framework of SABSA Services Organization. Several of the important thing functionsof the SABSA consist of:that could carried outgradually, canutilized whichever enterpriseindustry or other company if or not privately orbelonging to everyone, may be employed for the improvement many architectural designs and answers whenever degree of range complexity, permitsapplicable present requirements to exist incorporated beneaththe one SABSA architecture, allowing teamed forces, stop-to-stop buildinganswers, it always upheld or evolved additionally updated variations are posted from time to time.

Li He and Wang Shu-yang determines a few fundamental ideas in the field of security evaluation, such as assets, the worth of assets, threats, and vulnerability, followed by a few principles to guide the measurement of these concepts. At last, it offers an operational framework for the security of information systems evaluation along with vulnerability management [9]. In the meantime, a detailed introduction is also given to this functioning model, the combined approach for risk computation, and other associated formulas. In addition to improving the quality of risk assessment and providing a supporting platform for evaluating enterprises' security of information, the study seeks to offer theoretical foundations for the assessment of information security and vulnerability mitigation. It may also

yield some helpful recommendations towards the advancement of enterprises' details safety evaluation oversightsystems [10].

Maciej Kiedrowicz, J. Stanik states that the information system within the company (SIO) properly manages the security system's parameters. The basic components of the security system (SS) concept have been explained to preserve the information resources' present level of protection. The procedure of producing suitable security technological and administrative settings from the list of acceptable solutions will yield the intended present security characteristic of the SIO [11]. The author's suggestion can be seen by the suggested concept, which considers the effects of not only the fundamental security components of the data assets (such as resource types, security attributes, risks, and vulnerability) but also modifications to the information system's and security system's operational parameters as well as the organization's overall safety and quality direction environment.

III. Research Methodology

According to Susanto et al., the maximum critical and maximum extensively common worldwide projects regarding the improvement and an ISMS's functioning are ISO 27000 collection, ITIL, and COBIT.As these projects is additionally applicable to factors similar to data, safety control.For gain a decided foundation of Security Management strategies of those requirements, more than one method reference fashions want to be harmonized [12]. To balance more than one method reference styles a scientific stepwise method offered through Baldassarre turned into utilized in a mapping look at through Haufe et al.

For the evaluation of the diagnosed safety control requirements, a version of the Similarity Study between Models and Standards technique through J. A. Calvo-Manzano et al. turned into work. Thi0073technique turned into as follows:

1.Choose the fashions ,requirements being examined.

2.Select the citation version – thecitation versionthe 27000 ISO collection selected due to the fact due to the awareness of this popularcollectionthe largest insurance within ISMS strategies is anticipated.

3.Choose the method.

4.Decide on an element degree – as everyone examined requirements are worldwide requirements as well as relevant to everyone agencies impartial in their dimensions and goals,

enterprise model, place, and so forth - the enclosed data approximately ISMS strategies were standardized. Consequently, a comparable degree of element is selected to investigate the requirements.

5.Make an outline for interaction– rather than an in-depth pattern for interaction amethod feature model turned intoproduced.

6.Find the commonality amongst fashions – method models have been finishedalongside data receivedoriginating with the requirements.

7.Display received outcomes.

For the identification of processes, the following method was used:

1. Initiallythe ISO 27000 series was analyzed regarding the mentioned processes.

2. The ISMS processes that have been recognized in the series of ISO 27000 additionally potential new ISMS procedures were examined (matched) between ITIL and COBIT.With COBIT and ITIL, a matched database of potential ISMS operations was produced.

Following queries were posed about the matching:

a. Are there any details regarding ISMS procedures in other standards that are connected to the ISMS procedures of the ISO 27000 series reference standard? What further details could be useful to implement the reference standard's ISMS process?

b. Is there any information about possible additional ISMS processes in the other standards? What is this information/what is the possibleadditional ISMS process?

3. A mapping table that documents the outcomes of stages one and two can be found in Haufe et al. Haufe et al. provide a full description of the mapping study's methodology.

IV. Process Framework of ISMS

ISMS strategies and their interplay at an excessive degree foundation are proven in Fig. 1. ISMS method structure. A few interfacesaren't demonstrated to allow a higher clarity of Fig. 1. ISMS method structure: Each ISMS method offers entry to records and data management method. The ISMS making plans in addition to the configuration

control method offers to enter for each ISMS method.

As a result of the mapping look the subsequent strategies have been diagnosed as ISMS strategies [13]

Table 1. ISMS strategies

Process/standards	Process category
Process/standards	Process category
ISMS making plans method	Management method
Information safety governance method	Management method
Information safety danger evaluation method	ISMS center method
Information safety danger remedy method	ISMS center method
Resource control method	ISMS center method
Process to guarantee important attention and competence	ISMS center method
Communication method	ISMS center method
Documentation and data management method	ISMS center method
Requirements control method	ISMS centre method
Information safety extrude control method	ISMS center method
The process to manipulate outsourced strategies	ISMS center method
Performance assessment method	ISMS center method
Internal audit method	ISMS center method
Information safety incident control method	ISMS center method
Information safety development method	ISMS center method
Information safety client dating control method	ISMS center method
Configuration management process	Support process

The ISMS-making plan's method is the method the ISMS requirements, as well as layout from the beginning till the manufacturing of strategies for execution. The records as well as information management method is the method to recognize, produce, replace, manage data decided to existimportant about the ISMS's efficacy [14]. The essential to attaining the ISMS goals are updated knowledge of the wishes and expectancies of fascinated parties applicable to data safety and the ISMS. Thisis found in the necessities control method, which offers diagnosed legal, statutory, regulatory, and contractual necessities for thedanger evaluation method, the inside-out examination method, along with the method manipulate externalized procedures.

Within thedata safety danger remedy method, danger remedy alternatives which include

managing goals while the keys were diagnosed and decided on.Results from this method are listing with decided onregulates and manage goals a manage Strategy for execution and demands for modifications for data safetyextrude control method, that are used as enter in diverse ISMS strategies. Resources had to put in force the controls in addition to running the ISMS strategies are diagnosed and allocated. Output of the aid control method are planned assets to put in force and run decided-on control and oversight classification concerning Who sets the spending managesand recorded assets to maintain the ISMS center strategies, reviews concerning aid utilization of ISMS center strategies, and for the data safety dating control method: reviews on aid utilization. The implementation of controls usually outcomes in modifications. The data safety extrude control method is the method to manage modifications of ISMS factors and evaluate the results of accidental modifications. Output of this method are important modifications, proposed and important modifications in addition to outcomes of modifications, initiation of danger evaluation whilelargemodifications are proposed or arise, and the outcomes of modifications to data safety incident control method, as they have been initiated through that method.

The ISMS strategies are mentioned in an extra element insidethe subsequent sections:

A. ISMS making plans

Within the ISMS-making plans method, contributionsjustsimilar to the imaginative and prescient among the stakeholdersare convertedinto resultsjust like the control acclaim regarding the ISMS or its application. Several results from this method – such as control acceptance, and defining the range – want to be registered an ordinary foundation concerning their fact and appropriateness, however, the method itself is the number one preliminary method that is done as soon as a project [15]. Ordinary sports like renewing the control approval also are incorporated inside the control evaluation and development strategies. The ISMS making plans method is a method of the scheme segment inside the Plan Do Check Act (PDCA) cycle this implies that the method isn't always done at the same time as running the ISMS (DO segment).

B. Information safety governance

Data safety administration from an all-encompassing attitude is needed for domesticate a suitable degree of data safety tradition and minimize data safety risks. The control must

provoke control review to always enhance the suitability, sufficient, and efficacy of the ISMS [16]. The results of the control evaluationconsistsof selections associated with controlling the ISMS. Considering consideration goal of in charge of the ISMS, the data safety leadership method has to be carried out again on an ordinary foundation. This method is likewise a part of the carrier control device. The integration of an ISMS with a carrier control device allows synergy results primarily based totally on the mixing of those processes.

C. Information safety danger evaluation

The data safety danger evaluation method is the general method of danger evaluation and danger assessment. The data safety danger evaluation method has to be monitored, reviewed, and repeated regularly. Several iterations of this method are frequently conducted. Inputs from ISMS making plans method, data belongings, and former method outcomes are convertedinto recorded and assessed dangers or danger owners [17]. Data safety danger evaluation methodas a part of the data danger control method is an essential a component of an ISMS and has to implementedwith continued the way an ISMS operates. The data safety danger evaluation method is a supply of price for the pinnacle control at the same time as it offers a fixed of documented dangers in addition to a documented assessment of these dangers to assist the choice making.

D. Resource control

The aid control method is to determine, assign, and display necessary assets to maintain the ISMS center strategies in addition to putting in force and running the chosen controls. An aid control method is likewise a part of the ISMS-making plans method. This method focuses on the assets importantto function as the ISMS's operator. Nothing particular data approximatelymethodis included in ISO/IEC [18]. The aid control method wishes to be done on an ordinary basis,due to the fact it's far incorporated inside the ISMS and constantly helps the ISMS strategies.This method likewise helps the controls through the designation, distribution, and tracking of necessary assets.Thus, this isn't always a single assignment.

E. Process to guarantee important attention

The method to guarantee important attention is composed of the improvement and implementation of data safety attention, education, and schooling programs.Objectives of the method are to make sure that every employee obtains the important safety education and/or schooling. Employees will

be privy to the data safety policy, and their part in making ISMS more effectivewhich includes advantages of stepped-forward data safety overall effectiveness as well as its consequences of now no longermeeting ISMS criteria [19]. Direction of this method wishes to be done systematically, due to the fact requirements, dangers, and controls in addition to the workers. Employees are constantly shifting. This method additionallychanges supplies such that attention specifications, rules or safety goals into attention methods, substances,and lastly, a good enough attention degree for all employees.

F. Communication

Risk verbal exchange is the method to gain settlement on the way to control dangers through replacing and/or sharing all data approximatelydangers among the decision-maker and different stakeholders. Risk verbal exchanges have to be performed continually. In the danger verbal exchange method inputs like data approximately dangers and data wishes of stakeholders are converted into danger verbal exchangestrategies. Details wishes of the parties involved are happy. The verbal exchange method,is a component of the data danger control method, is an essential component of running an ISMS [20].The danger verbal exchange method is price-producing for the pinnacle control at the same time as it without delay satisfies the data wishes of the pinnacle control.

G. Documentation and Information Management

The documentation and information management methodsare the methodsto recognize, produce, replace, manage data resolved to be importantregarding the ISMS's efficiency [21]. As modernizing and keepingapplicable records are a portion of the method, it has to be doneon frequently. Within the records and information management method results of different ISMS, strategies are converted into suitable,controlled recording. As you process information,differentthrough records, the method by itself is operational as well. In actuality, record control is frequently no longer to the centerproficiency of ISMS employees. However, to control suitable records as well as information is a duty of the data safety official,due to the fact this documentation allows her or him to offer proof of the right ISMS.

H. Internal audit

The outcomes due to this method are components of the frequent assessment within the ISMS, it method has to be done regularly. Inputs like

manage lists, manage goals and occurrence reviews are convertedentering assessment schedules, assessment reviews, and lastly, control reviews.Internal examinations concerning data safety In oversight, there's an essential a portion of the check segment inside the ISMS's PDCA cycle [22]. Similar to the size method, inner examination method must become a part of the ISMS. Thus, it's by far really part of the ISMS and done at the same time as running the ISMS.

I. Information safety extrude control

Information safety extrude control is the method to manipulate modifications of ISMS factors and evaluate the results of accidental modifications. This method most effectively focuses on extrude control of the ISMS. As the operational surroundings of the company modifications on an ordinary foundation, ISMS factors such as safety features additionally must be modified systematically [23]. Contributions as suggested modifications or wishes for themodifications are converted into carried out and recordedmodifications. Modifications arise in any respect stages: tactical, tactical, as well as functional. Consideringthe point of interest of alteration control method on modifications of security management factors, data safety officials must become the proprietor of this method.Due to thepoint of interest of the method, it has to additionallyact as a central proficiency of theISMS [24]. As though each extrude controlled through the extrude control method is meant to enhance or keep the data safety degree of the company and data safety has an immediate fine effect on the enterprise of the company, the extrude control offers an immediate price for the stakeholders.

V. Conclusion and Future Scope

The suggested experimental program's deployment ISMS method methodology shown that a method-orientated perspective that ISMS is able to assist inconcentrating on how an ISMS operates and enhance its performance at the same time as making plans for such strategies.As a result, by this primary discovering, the systemic person within the ISMSincludingstrategiesand belief of applicableThe ISMS's responsibilities are reinforced. The trial's execution additionally confirmed that a few upgrades within the structure want to carried outand that the structure's improper application will no longerbe enough.

Future Scope will included three steps:-

Step 1:Enhancement of the structure inthefuture, primary or additional outcomes for assessment of

the suggested ISMS method structure have to be examined and put to use in enhance the structure. It particularly established to be had outcomesof the experimental execution could be usedand method "Documents and information manage method" could be divided into the "Security coverage control method" (ISMS center method) from Veiga and Eloff and the "Records manage method". The ones strategies could be incorporated into the structure [25].

Step 2:Creation of a technique to regulate and create charges in light of running the ISMS center strategies obvious. Openness of data safety charges can be in addition stepped forward through tailoring the adulthood degree within ISMS strategies to necessities of the company [26].Thinking About restricted assets in addition to making sure a green use of assets, now no longer each ISMS method has to be installed and operated on the identical degree of adulthood. By considering the adulthood degree version for ISMS strategies mixed with a technique for the willpower of the important adulthood degree, the appropriateness of an ISMS may be made obvious in addition to needless charges of data governance maystay away.

Step 3:Obtain a fundamental method structure for decreasing adulthood stages. The suggested ISMS's experimental installation method structure confirmed that, particularly when it comes to agencies, general adulthood degree of ISMS isn't always better "defined", the suggested method structure is also complex as well as excessively large. Because the one's agencies, a changed fundamental ISMS center method framework has to be derived. This framework can also be a milestone for agencies that need to set up a better adulthood through an iterative approach.

References

[1]Broderick, J. S. (2006). *ISMS, security standards, and security regulations. information security technical report, 11(1), 26-31.*

[2]Saucier, G. (2000). *Isms and the structure of social attitudes. Journal of personality and social psychology, 78(2), 366.*

[3]Höpfl, H. M. (1983). *Isms. British Journal of Political Science, 13(1), 1-17.*

[4]Joint Task Force, 2018. *Risk Management Framework for Information Systems.*

[5] M. Kittel, T. J. Koerting and D. Schött, Kompendium für *ITIL-Projekte. read, 2006.*

[6] *German Federal Office for Information Security*, BSI-Standard 100-1. Bonn, 2008.

[7]Ochoa, D. M., & Barnes, D. (2020). *The SABSA® Conceptual Security Architecture.*

[8] Shore, M., & Deng, X. (2010, September). *Architecting Survivable Networks Using SABSA. In 2010 6th International Conference on Wireless Communications Networking and Mobile Computing (WiCOM) (pp. 1-7). IEEE.*

[9] Kazemi, M., Khajouei, H., & Nasrabadi, H. (2012). *Evaluation of information security management system success factors: A case study of Municipal organization. African Journal of Business Management, 6(14), 4982.*

[10] Eloff, M. M., & Von Solms, S. H. (2000). *Information security management: an approach to combine process certification and product evaluation. Computers & Security, 19(8), 698-709.*

[11]Miyachi, M., Yamamoto, H., Kawai, H., Ohta, T., & Shirakata, M. (2005). *Analysis of SiO anodes for lithium-ion batteries. Journal of the Electrochemical Society, 152(10), A2089.*

[12] Asosheh, A., Hajinazari, P., & Khodkari, H. (2013, April). *A practical implementation of ISMS. In 7th International Conference on e-Commerce in Developing Countries: with focus on e-Security (pp. 1-17). IEEE.*

[13] Mukeshimana, M. C., Zhao, Z. Y., & Nshimiyimana, J. P. (2021). *Evaluating strategies for renewable energy development in Rwanda: An integrated SWOT–ISM analysis. Renewable Energy, 176, 402-414.*

[14] Asosheh, A., Hajinazari, P., & Khodkari, H. (2013, April). *A practical implementation of ISMS. In 7th International Conference on e-Commerce in Developing Countries: with focus on e-Security (pp. 1-17). IEEE.*

[15] Candra, J. W., Briliyant, O. C., & Tamba, S. R. (2017, October). *ISMS planning based on ISO/IEC 27001: 2013 using analytical hierarchy process at gap analysis phase (Case study: XYZ institute). In 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA) (pp. 1-6). IEEE.*

[16] Białas, A. (2005). *A UML approach in the ISMS implementation. In Security Management, Integrity, and Internal Control in Information Systems: IFIP TC-11 WG 11.1 & WG 11.5 Joint Working Conference 7 (pp. 285-297). Springer US.*

[17]Ghilay, Y., & Ghilay, R. (2015). *ISMS: A new model for improving student motivation and self-esteem in primary education. Ghilay, Y. & Ghilay, 383-398.*

[18]ISO, I. (2011). ISO. IEC, 25010, 2011.

[19]Broderick, J. S. (2006). *ISMS, security standards and security regulations. information security technical report, 11(1), 26-31.*

[20]Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). *ISMS core processes: A study. Procedia Computer Science, 100, 339-346.*

[21]Moses, F., & Sandkuhl, K. (2023). *ISMS in small public sector organisations: requirements and design of a procedural approach. In 22nd International Conference on Perspectives in Business Informatics Research Workshops and Doctoral*

Consortium, BIR-WS 2023, Ascoli Piceno, 13-15 September 2023 (pp. 1-10). CEUR-WS.

[22]Lee, S. W., & Cheung, C. S. (2020). *The effects of ISO 22301 and ISMS certification requirements on business performance: Focusing on mediation of corporate culture. Journal of the Society of Disaster Information, 16(3), 558-576.*

[23]Achmadi, D., Suryanto, Y., & Ramli, K. (2018, May). *On developing information security management system (isms) framework for iso 27001-based data center. In 2018 International Workshop on Big Data and Information Security (IWBIS) (pp. 149-157). IEEE.*

[24]Haufe, K., Colomo-Palacios, R., Dzombeta, S., Brandis, K., & Stantchev, V. (2016). *ISMS core processes: A study. Procedia Computer Science, 100, 339-346.*

[25]Lyubimov, A., Cheremushkin, D., Andreeva, N., & Shustikov, S. (2011, August). *Information security integral engineering technique and its application in ISMS design. In 2011 Sixth International Conference on Availability, Reliability and Security (pp. 585-590). IEEE.*

[26]De Abrew, K. M. N., & Wickramarachchi, R. (2021). *Organizational Factors Affecting the ISMS Effectiveness in Sri Lankan IT Organizations: A Systematic Review. In Proceedings of the International Conference on Industrial Engineering and Operations Management (pp. 702-713).*