A Roadmap to ISMS ISO 27001 Implementation Process

Chandradeo Rajak
ITR Chandipur
Defence R&D Organisation
Balasore,India
chandradeor@gmail.com

Jayshankar Bharti
ITR Chandipur
Defence R&D Organisation
Balasore,India
bhartidrdo137@gmail.com

Asfa Mateen
ITR Chandipur
Defence R&D Organisation
Balasore,India
asfamateen10@gmail.com

Nishtha Mehndiratta
ITR Chandipur
Defence R&D Organisation
Balasore,India
nishthamehndiratta007@gmail.com

Jitendra Chauhan
ITR Chandipur
Defence R&D Organisation
Balasore,India
jitendrafz20898@gmail.com

Ranjit Marndi
ITR Chandipur
Defence R&D Organisation
Balasore,India
ranjitmarndi@gmail.com

2023 3rd International Conference on Range Technology (ICORT) | 978-1-6654-9331-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ICORT56052.2023.10249115

Abstract—Due to advancement in ICT systems their usage has increased manifold now a days but at the same time these systems cyber-attacks have also increased at the same pace. In order to safeguard against such threats Information Security Management Systems are being implemented. These ISMS are certified to some standards in order to provide assurance to the customers about effectiveness of information security implementation. Present work outlines a roadmap to implementation of such a standard called ISO 27001. It may be helpful to the information owners in order to implement such standard in their organizations.

Keywords— Information Security, Information Security Management System (ISMS)', ISO 27001 Standard, Risk assessment, ISMS Implementation

I. INTRODUCTION

In the present era of connected world most of the businesses or day to day activities are happening through cyber space. Every day millions of transactions related to banking, business processing, and telemedicine are happening through internet and computing devices. Increasing use of this cyber space has also invited the attention of hackers and attackers steal the precious information or having unauthorized access to these information and resources. In order to prevent or minimize the loss due to such attacks information security mechanisms are being implemented. Information security is analogous to preserving confidentiality Integrity and Availability (CIA)[1] of the information and information resources. The CIA of information may be achieved to some extent by implementation of technical means like cryptographic techniques but information security also depends on People, Policies, Process and Procedures (PPPP).Therefore in order to provide assurance that information assets are sufficiently protected against threats and attacks, Information Security Management Systems (ISMS) have been devised. The ISMS provides a framework for identification of Information security risks, applying appropriate security controls, measuring their effectiveness and continually improve them. To provide greater assurance to customers and stake holder about information security or security of their data, these ISMS need to be certified against some national or international standards. There are various ISMS standards like ISO 27001[2], PCI DSS[3], FINRA[4], HIPAA[5], COBIT 5[6] etc. Out of these standards ISO 27001 is a common standard which is internationally adopted by the organizations. This standard may be applicable to any type of industries for certifying their ISMS. Other standards in this list are applicable to a particular type industry. Therefore in this literature a roadmap for implementation of ISO 27001 standard will be discussed.

In recent past it has been observed that many organizations are suffering from information breaches to outside agencies in spite that stringent technical security measures like firewalls, IDS/IPS[7], cryptographic techniques, SSL/TLS[8], antimalware software, access controls systems etc. have been implemented. After careful examination of the breaches it has been found that human factor was the key role of breaches. Either intentionally or un-intentionally people are involved in data leakage of the organizations. Lack of awareness about the information security practices is the major cause of involvement of people in such activities. It has been found that people don't leak data from the systems inside the office premises but they use their personal gadgets from home for such purpose. Many times honey-pot trapping techniques have been used by the foreign intelligence agencies. It happens because people are unaware of the presence of these agencies behind the scene. Therefore ISMS recommends awareness training to the human resource. Loss CIA of information may happen due to environmental disasters like tsunami, earthquake, fire, and flood. It may also happen due to improper backup policy, power failure, improper cooling of IT infrastructure, improper physical security and many other such reasons. Therefore ISMS recommend the PPT approach as shown in Fig.1 wherein apart from technical measures above mentioned non-technical measures and processes are also taken into account for protecting the CIA of information. Taking care of all the three dimensions of PPT ISMS assures the customers that any organization which is ISMS certified handles the data using internationally recommended standard. It enhances the customer base of the organization and makes it unique among its competitors.

This paper is further organized in the following manner. Section II covers literature survey in the area of ISMS 27001 implementation. An overview of 27001 standard structures is presented in section III. Stepwise processes for ISMS implementation is provided in section IV. Section V covers risk management process in detail and section VI covers about Statement of Applicability document. Finally the paper is concluded in section VI.

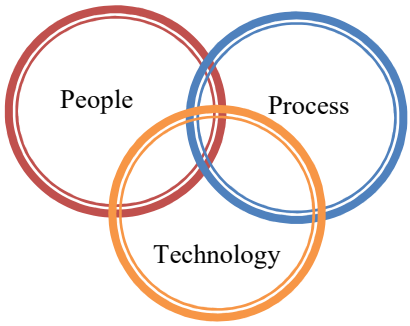

Fig. 1. ISMS PPT Relationship diagram

Literature Survey

ISMS implementation based on 27001 is not a new field. Many professional are working in this area since long time. All of these researchers have worked on the various aspects of this subject. V. Money has proposed a model for Organizational Information Security Maturity Assessment in [2].K. Peciña, et. al in [9] has proposed a model for organization of physical and logical security. A. K. Shrivastava et. al. in [10] have worked on application of Machine learning technique for checking the compliance of 27001 implementation. R. Almeida et. al. in [11] have discussed about a Model for Assessing COBIT 5 and ISO 27001 Simultaneously. A. Longras et. al in [12] have discussed about ISO/IEC 27001:2013 Implementation Difficulties in Portuguese organization. Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements has been discussed by D. S. K. Putra et. al in [13]. All of these works provide a lot of direction in the area of 27001 but very few of them provided a simple roadmap particularly for beginners. Therefore our paper may provide a better roadmap for beginners in the area of ISO 27001 implementation.

II. ISO 27001:2013 Standard Structure

ISO 27001 standard ISO 27001 is a standard for Information Security Management System. It is one of the internationally adopted and most widely used standards. 27001 specify the requirements that an organization should fulfill in order to get certified against it. It is a framework for development, implementation, and operations and continually improves Information Security Management System of any organization. ISO 27001:2013 is mainly oriented towards risk based approach. Identification of the risk, assessment of the risk and treatment of the risk on organizational assets are the key elements of this standard. ISO 27001 focuses on People Process and Technology for achieving information security. Since people play an important role in success of ISMS therefore awareness among the employee and other stakeholders of the information is a must requirement.

There is a series of 27000 standards like 27000,27001,27002,27003,27004,27005,27006 etc. But out of these standards only 27001 can be used for certification and audit. Other standards in this series are like supporting various components of 27001 standards e.g. 27002 specifies 114 controls and their implementation guidelines. These controls are used for risk mitigation identified during the risk assessment process in 27001standard. 27005 provide guidelines for information security risk management. ISO 27006 is guidelines for accredited certification bodies and 27007 is guideline for auditing ISMS. In this manner the complete series is dedicated to providing support for ISMS 27001 standard.

An ISM is not only a purely technical framework for achieving the information security but it comprises of three basic elements like People Process and Technology (PPT). It has been illustrated in brief in Fig.2. Human resource plays a crucial role in ISMS. People within the organization and also external to the organization that are interacting to it for achieving the business objective need to be aware about the ISMS. People have been seen as one of the crucial factor in information security. Successful implementation of Technological measures and processes are dependent on human resource of the organization.

ISO 27001 comprises of mandatory clauses from 4-10 and an Annexure-A. Any organization needs to implement these clauses in order to get certification. Annex-A contains 114 controls which are divided into 14 domain and 35 control objectives. These controls are ICT as well as non –ICT controls and are taken from ISO 27002 standard. Table-I contains mandatory clauses and Table-II contains 14 domain of Annex-A.

TABLE I. Mandatory Clauses of 27001:2013

4	Context of the Organization
5	Leadership
6	Planning
7	Support
8	Operation
9	Performance Evaluation
10	Improvement

TABLE II. 14 Domains of Security Controls

A.5	Information security policies
A.6	Organization of information security
A.7	Human resource security
A.8	Asset management
A.9	Access control
A.10	Cryptography
A.11	Physical and environmental security
A.12	Operations security
A.13	Communications security
A.14	System acquisition, development and maintenance
A.15	Supplier relationships
A.16	Information security incident management
A.17	Information security aspects of business continuity management
A.18	Compliance

Statement of Applicability (SOA) is an important document which indicates the status of 114 controls implementation in the context of a particular organization. As its name indicates it states which controls are applicable and which are not applicable for an organization. SOA must contain all of these controls. If any of these controls are omitted then proper justification has to be given for its omission.

Changes in the regulations worldwide, changing technology, changing business process and hence changing risk to information compelled the ISO to update its 27002:2013 standards to 27002:2022. This standard has been updated in February 2022. The previous name of the standard “Information technology – Security techniques –

Code of practice for information security" has been changed to "Information security, Cyber security and privacy protection – Information security controls". The Annex-A of 27001:2013 standard has been taken from 27002 hence changes in 27002 automatically invites changes in 27001. It is being discussed that 27001 will be updated and published in October 2023. The updated version of 27002 contains 93 controls instead of 114 controls. There are 11 new controls which have been introduced in the new version. Some of the controls in older version have been combined together to avoid the redundancy. The controls in the new version have been categorized into four domain called "themes". These themes are Organizational, People, Physical and Technological. Once an organization is certified for 27001 standards, it is valid till next three years. Therefore any organization which have already been certified against 27001:2013, they will have to apply the changes during their re-certification after three years. Any organization which is in the process of certification will have to apply the changes according to the new standard.

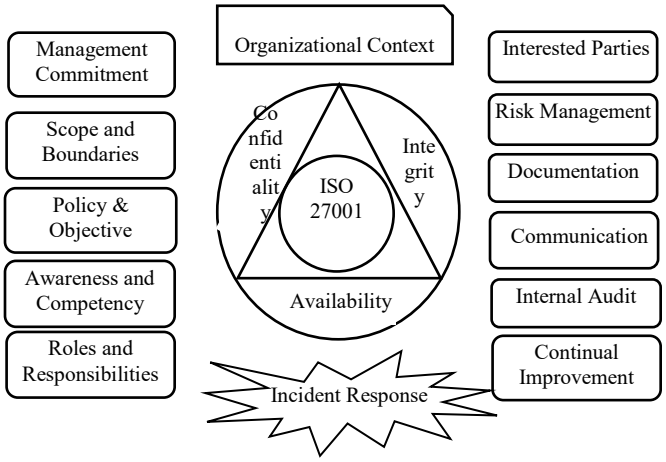

Fig. 2. Key Components of ISMS

III. Steps for ISMS Certification Process

1. Identification of context of the Organization: It means identification of business are of the organization and its core activities. Since 27001 standards may be implemented for many types of organisation it needs to be customised for specific type of organisation. It also includes identifying internal and external issues of the organisation. The legal and contractual obligations in which the organisation operates are identified. 2. Defining the scope of certification: An organisation may have many sites, multiple premises and it may have different types of networks. ISMS 27001 may be implemented for a particular site or premises. In scope of implementation it is determined that what areas will be covered for certification.3. Once scope is determined a policy for ISMS has to be drafted in consultation with the top management. 4. Training and awareness to the employee and other stakeholder: Awareness is key to information security hence each and every employee of the organization and service providers should be aware about ISMS policy. Information security awareness programs need to be conducted time-to-to time. Posters and banners should be displayed everywhere in the organisation so as to develop an information security culture. 5. Asset management: The ultimate goal of ISMS is protection of organisational assets. Therefore it is mandatory to make an inventory of all assets so that each and every asset is easier to trace and it is not left unattended. Every asset should be allotted to some person in the organisation. 6. Risk Assessment and risk treatment plan: It is one of the important steps for ISMS implementation. ISMS 27001 are basically risk oriented system and hence risk management plays an important role. This step is elaborated in detail in the coming sections of the paper. 7. Document preparation: ISMS Implementation process demand a lot of documents and records to be generated. It is necessary to document the policy and procedures of organizations and communicate it to all interested parties. The Major documents for ISMS implementation includes but is not limited to Scope of ISMS implementation, ISMS Gap Analysis Report, Inventory of all assets, ISMS Policy and Procedure Manual ,Risk assessment documents, Statement and Applicability. Once risk assessment is done, appropriate controls need to be applied in order to minimise the risk. The SOA document is a clear indication of implementation of controls. The SOA preparation is also discussed in detail in further section. Since document

Preparation takes a lot of time and hence it is advised to take consultation with some expert having experience in this domain. 8. Conducting Auditing: Initially Internal Audit of the ISMS implementation is conducted by the people within the organisation. Once internal audit is completed and all the non-conformities are closed then external audit is conducted by third party. 9. Certification phase: During this phase all the NCs found by external auditors are closed and organization gets the Certification. 10. Re-certification or Surveillance audit: ISMS 27001 certificate is valid for three years hence during this three year period the surveillance audits are conducted to continue the Certificate validity. As ISMS is a continual process it is generally followed in a Plan-Do-Check-Act (PDCA) [14] manner. Mmandatory clauses of the Standard from Clause 4 to 10 are followed in different phases of PDCA cycle as shown in Fig-03. *Plan*: Context of the Organization, Leadership, Planning and Support i.e. clause 4 to 7 are carried out during this phase. *Do*: This phase covers clause 8 i.e. Operation. Check: Clause no 9 i.e. Performance evaluation is covered during Check phase of PDCA. Act: It covers clause 8 i.e. Improvement.

Fig. 3. PDCA Cycle of ISMS 27001 Standard

IV. Risk Assessment

Clause 6.1.2 of the standard discusses about the information security risk assessment [15]. It says that organization shall define and apply an information security risk assessment. The process of risk assessment may be defined by the organization according to their context. The standard doesn't mention any specific risk assessment

methodology. Generally the risk assessment has two approaches namely quantities and qualitative approach. In qualitative approach the values of various risk factors like asset value, threat, vulnerability and impact and finally risk values are taken as very high, high, medium, low and very low but in quantitative approach these values are taken on a scale of 1-5 or 1-3.Fundamentally in asset based risk assessment approach,

TABLE III. IMPACT AND LIKELIHOOD FOR RISK CALCULATION

		Likelihood				
		Rare	*Unlikely*	*Possible*	*Likely*	*Certain*
Impact	*Insignificant*	1	2	3	4	5
	Minor	2	4	6	8	10
	Moderate	3	6	9	12	15
	Major	4	8	12	16	20
	Catastrophic	5	10	15	20	25

first of all we list all the organizational assets. Then threats, vulnerabilities, impact and likely hood of the exploiting the vulnerabilities are determined. It is important to clearly understand the these terms as described below

a) Assets: Asset is anything which is of value to the organization or anything that we want to protect. The assets of an organization may include people asset, infrastructure, information processing, transmitting and storage systems, outsourced services etc. The assets affect the Confidentiality, Integrity and Availability of information of an organization. The values of these assets are determined according to their importance or criticality for the organization. We may also assign CIA values of these assets. The asset value may be calculated with CIA values either by taking maximum of three values or by multiplying or adding them.

b) Threat: Threat is what against which we are trying to protect our assets. We may be fire, earthquake, computer viruses, theft, damage, unauthorized access. So we ask a question that what can happen to the asset?

c) Vulnerabilities: These are weakness or loopholes in the security control implementation of an asset. To figure out the vulnerabilities we ask the question why that threat can happen and the answer may be due to lack of antivirus, lack of physical boundaries, lack of fire extinguisher system etc.

d) Impact: Depending upon the importance or criticality of an asset for the organisation, the impact of loss may be determined. Once the threat is materialised into attack , how that is going to affect the organisation. Its value may be low to high depending upon how the loss of CIA of an asset affect the cashflow, legal or contractual obligations or the reputation of the organisation.

e) Likelyhood: It is the probability of the threat exploiting the vulnerability. It may be frequently, rarely , twice in a day, once in a month or once in a year etc.

An asset may have multiple threats and a threat may be associated with multiple vulnerabilities. Risk is defined as function of Asset value, Threat, Vulnerability.
The Impact is dependent on asset value of the organization and the probability of threat exploiting the associated vulnerabilities. Table-01 shows the calculation of risk with multiplication of impact and likelihood. Table-04 shows how actual risk may be calculated by taking into account asset values, impact and likelihood, taking into account the threat and associated vulnerabilities. All the parameters are measured on a scale of 1to 5 where 5 is the maximum value.
Risk=Impact x Likelihood

Risk can't be eradicated completely therefore we will have to accept some risk, avoid some risks and mitigate the major risks which are above the threshold values decided by the organization. The threshold value depends upon the risk appetite of the organization means up to what extent the organization can accept the risk.

TABLE IV. RISK CALCULATION USING ASSET VALUES

Asset	**End User PCs**	**Servers**	**CCTV Camera**	**Power System**
C	1	1	1	1
I	2	3	4	2
A	3	3	4	4
Asset Value	3	3	4	4
Threat (What may happen)	Browser not working properly	Not serving the web page	Not storing video	Short-circuit
Vulnerability (Why may that Happen)	Updates for browser not installed	Mis-configuration	Storage full	Wiring problem
Impact	1	1	2	1
Likeli-hood	2	1	1	2
Risk Value	6	3	8	8

V. STATEMENT OF APPLICABILITY (SOA):

Once the risk analysis is completed, the identified risks are prioritized according to their impact and likelihood of happening. The controls are decided to patch up the vulnerabilities which have been pointed out. These controls are taken from Annex-A of the 27001 standard but apart from this list of controls other controls as decided by the organization may also be implemented. The SOA [16] document is one of the most important documents for getting ISO 27001certification [17]. It basically list out all the controls from Annex-A and then indicates whether a particular control has been implemented or not. If controls are being omitted then proper justification is given in SOA. If controls are applicable then also it has to be clarified that in which context it is applicable like; is it applicable for password policy or for physical controls. Table -05 provides a basic structure of SOA document.

TABLE V. STATEMENT OF APPLICABILITY

Annex-A Clause No.	A.10.1.1
Control Domain	Cryptography
Control	Policy on the use of cryptographic controls
Inclusion	Yes
Justification	Confidentiality and Integrity of sensitive
Reference Documents	ISMS Policy, 27001, Standard, NIST Cryptographic Standard
Responsibility	CISO
Implementation Status	Implemented on Jan 2022

VI. CONCLUSION:

This paper basically aims to highlight the importance of ISMS implementation in any organization and provides a roadmap to anyone who wants start ISMS 27001 implementation in their organization. It emphasizes on the fact that bare implementation of technological measures will not ensure the information security in the organization. It is explained how the information security may be completely achieved by the People Process and Technology strategy. Using the PPT will ensure Confidentiality Integrity and Availability of Information security in any organization. The paper provides an overview of 27001 standard structures and its family of standards. Various steps for ISMS implementation processes have been illustrated. Major steps of ISMS 27001 implementation like Risk assessment and risk treatment has been explained in detail. Implementation of control for risk mitigation and then preparing Statement of Applicability (SOA) document has been highlighted. Plan Do Check and Act (PDCA) cycle as applicable to 27001 standard has been explained. Therefore this literature may provide be a good roadmap to start ISMS 27001 implementation in any organization. It is very important to provide proper resources for implementation of ISMS 27001. It has been found that many organisations started the implementation process but could not succeed because they could not define the scope properly. It is therefore important to start with limited scope and then expands it once the team gets confidence over it. Management support in this regard becomes very crucial to keep the team focused on their work. Particularly in public organisations [18][19] where heterogeneous types of systems are available and awareness about ICT systems is comparatively low, it becomes a little difficult in the implementation process.

VII. REFERENCES

[1] R. Kumar and M. P. S. Bhatia, "A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability," 2020 IEEE International Conference on Computing, Power and Communication Technologies (GUCON), 2020, pp. 334-337, doi: 10.1109/GUCON48875.2020.9231255.

[2] V. Monev, "Organisational Information Security Maturity Assessment Based on ISO 27001 and ISO 27002," 2020 International Conference on Information Technologies (InfoTech), 2020, pp. 1-5, doi: 10.1109/InfoTech49733.2020.9211066.

[3] S. Ramkhelawan, B. Gobin-Rahimbux and Z. Cadersaib, "PCI-DSS requirements in the Mauritian Hospitality Industry," 2016 IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech), 2016, pp. 199-205, doi: 10.1109/EmergiTech.2016.7737338.

[4] Black, B. (2013). Punishing bad brokers: Self-regulation and finra sanctions. Brook. J. Corp. Fin. & Com. L., 8, 23.

[5] Xiaomeng Chen, Jianguo Zhang, Dongjing Wu and RuoLing Han, "HIPPA's compliant Auditing System for Medical Imaging System," 2005 IEEE Engineering in Medicine and Biology 27th Annual Conference, 2005, pp. 562-563, doi: 10.1109/IEMBS.2005.1616473.

[6] S. J. Hussain and M. S. Siddiqui, "Quantified Model of COBIT for Corporate IT Governance," 2005 International Conference on Information and Communication Technologies, 2005, pp. 158-163, doi: 10.1109/ICICT.2005.1598575.

[7] Ling Leng and Lin Wang, "The fusion method of the IDS and IPS based on IMS," 2012 International Conference on Computer Science and Information Processing (CSIP), 2012, pp. 727-730, doi: 10.1109/CSIP.2012.6308956.

[8] S. -M. Kim, Y. -H. Goo, M. -S. Kim, S. -G. Choi and M. -J. Choi, "A method for service identification of SSL/TLS encrypted traffic with the relation of session ID and Server IP," 2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2015, pp. 487-490, doi: 10.1109/APNOMS.2015.7275373.

[9] K. Peciña, R. Estremera, A. Bilbao and E. Bilbao, "Physical and Logical Security management organization model based on ISO 31000 and ISO 27001," 2011 Carnahan Conference on Security Technology, 2011, pp. 1-5, doi: 10.1109/CCST.2011.6095894.

[10] A. K. Shrivastava, A. Kumar, A. K. Rai, N. Payal and A. Tiwari, "ISO 27001 Compliance via Artificial Neural Network," 2013 5th International Conference and Computational Intelligence and Communication Networks, 2013, pp. 339-342, doi: 10.1109/CICN.2013.77.

[11] R. Almeida, R. Lourinho, M. Mira da Silva and R. Pereira, "A Model for Assessing COBIT 5 and ISO 27001 Simultaneously," 2018 IEEE 20th Conference on Business Informatics (CBI), 2018, pp. 60-69, doi: 10.1109/CBI.2018.00016.

[12] A. Longras, T. Pereira, P. Carneiro and P. Pinto, "On the Track of ISO/IEC 27001:2013 Implementation Difficulties in Portuguese Organizations," 2018 International Conference on Intelligent Systems (IS), 2018, pp. 886-890, doi: 10.1109/IS.2018.8710558.

[13] D. S. K. Putra, S. Tistiyani and S. U. Sunaringtyas, "The Use of ISO/IEC 27001 Family of Standards in Regulatory Requirements in Some Countries," 2021 2nd International Conference on ICT for Rural Development (IC-ICTRuDev), 2021, pp. 1-6, doi: 10.1109/IC-ICTRuDev50538.2021.9656529.

[14] B. Xu, "Performance Management Model of Public Expenditure Based on PDCA Cycle Theory," 2020 International Conference on E-Commerce and Internet Technology (ECIT), 2020, pp. 216-221, doi: 10.1109/ECIT50008.2020.00056.

[15] Angraini, Megawati and L. Haris, "Risk Assessment on Information Asset an academic Application Using ISO 27001," 2018 6th International Conference on Cyber and IT Service Management (CITSM), 2018, pp. 1-4, doi: 10.1109/CITSM.2018.8674294.

[16] M. Coetzee, "Towards a Holistic Information Security Governance Framework for SOA," 2012 Seventh International Conference on Availability, Reliability and Security, 2012, pp. 155-160, doi: 10.1109/ARES.2012.62.

[17] C. Carvalho and E. Marques, "Adapting ISO 27001 to a Public Institution," 2019 14th Iberian Conference on Information Systems and Technologies (CISTI), 2019, pp. 1-6, doi: 10.23919/CISTI.2019.8760870.

[18] P. P. Roy, "A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard," 2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSTEA), 2020, pp. 1-3, doi: 10.1109/NCETSTEA48365.2020.9119914.

[19] K. I. Alshitri and A. N. Abanumy, "Exploring the Reasons behind the Low ISO 27001 Adoption in Public Organizations in Saudi Arabia," 2014 International Conference on Information Science & Applications (ICISA), 2014, pp. 1-4, doi: 10.1109/ICISA.2014.6847396