https://doi.org/10.31871/WJIR.9.5.12
World Journal of Innovative Research (WJIR)
ISSN: 2454-8236, Volume-9, Issue-5, November 2020 Pages 140-147

Analysis of ISO/IEC 27001 to Encourage its Adoption in Nigerian Businesses

Heman Awang Mangut, Damuut Peter Luhutyit, Aristarkus Datukuk Kalamba, Palang Mangut

***Abstract*— There are several standards for Information Security Management Systems (ISMS) developed to strengthen the security of organizational information assets. ISO/IEC 27001 is one of the ISMS standards that has global acceptance. However, business organizations in developing countries, which Nigeria happened to be one of them, stray away from adopting the standard. In order to encourage Nigerian companies to adopt the standard, a mixed research method was adopted for collecting data, a Strength Weakness Opportunity and Threat (SWOT) analysis of collected data was carried out to show how the standard will improve on Nigerian businesses using Threat Opportunity Weakness and Strength (TOWS) Matrix to tackle vulnerabilities and threats of the standard that stray Nigerian businesses away living them with opportunities to benefit of the standard. Questionnaire responses from researchers, implementation consultants and auditors were used to validate interview responses from certified ISO/IEC 27001 accreditors. In order to check the significance and confidence level of the hypothesis, t-test and analysis of variance were used.**

***Index Terms*— Analysis of ISO/IEC 27001; Benefits of adopting ISO/IEC 27001; SWOT analysis; TOWS Matrix; ISMS .**

I. INTRODUCTION

In today's business world where information technology has taken over businesses, information asset become the lifeblood of a business [1] because it could be evaluated in monetary terms [2]. Businesses stand the risk of losing money if they do not provide security to their information assets. Hence, the need for information security.

Information security is a measure taken by organization to reduce risk of losing money by reason of preventing unauthorized access to information assets, ensuring business continuity and maximizing profit by reason of creating business opportunities [3].

Information security is aimed at ensuring only rightful users have access to information assets of an organisation which in other word refer to confidentiality; data is only modified at when it is supposed to be modified by those who have the right to modify the data which is in other word referred to integrity; and ensures that information assets are available to rightful users only at any time they intend to use them [4]. Hence, in order to effectively utilize business resources to minimize loses and maximized profit using information security, a standard has to be made for businesses to comply with. ISOIEC 27001 is one of the most acceptable global standards for information security. It was developed by the department of trade, United Kingdom as a code of good practice of operating businesses using information security [5].

According to [4] ISO/IEC 27001:2013 has thirteen controls and, these include: access control, organisation of information security, asset management, human resources, cryptography, information security policies, human resource security, physical and environment security, supplier relationship, operation security, communication security, development and maintenance, business continuity management and compliance and incident management. This standard is primarily developed to created, implement, monitor, review, maintain and improve information security management system [6]. Regulatory body's award certificated to businesses that convincingly show compliance to the standard.

The purpose of this research is to carryout SWOT analysis of ISO/IEC 27001 using TOWS Matrix to tackle threats and vulnerability of the standard and check the confidence level of the hypothesis using t-test and analysis of variance to encourage Nigerian businesses to adopt the standard.

II. OVERVIEW OF SWOT ANALYSIS USING TOWS MATRIX

[7] said SWOT analysis is a planning tool that is used for figuring out vulnerabilities, threats, and opportunities in a business organization. It enables companies to pair resources and the adeptness to the competitive atmosphere it runs. The supposition is that, for a company to be successful, it has to aligned its vulnerabilities with its threats and opportunities. SWOT analysis is applied in information security in order to discover vulnerability in existing security to organisational information assets to bridge the gap to meetup to ISO/IEC 27001 standard. Hence, SWOT analysis enables companies to build their business processes in line with security policies [8]. Because SWOT analysis is applied to address most of business organisation's risks, the cost of insurance of a business company have to be reduced [5].

III. RELATED WORK

According to [9], This standard was initiated and established in 1989 by United Kingdom's department of trade

Mr. Heman Awang Mangut, His Department of Computer Science, Plateau State University, Bokkos, Nigeria
Damuut Peter Luhutyit, Computer Science, Plateau State University, Bokkos, Nigeria
Aristarkus Datuku Kalamba, Computer Science, Plateau State University, Bokkos, Nigeria
Mss. Palang Mangut, Computer Science, Plateau State University, Bokkos, Nigeria

and Industry. ISO/IEC 27001 has the wider acceptance around the world most largely because it is capable of mapping business processes into information security and management [10]. A good number of researchers deduct that the model is iterative due to Plan-Do-Check-Act (PDCA). The standard is so flexible that it supports variable organisational sizes devoid of sector in an economy. However, the adoption of the standard is low in developing nations, largely due to poor approach of implementation [11].

[12] suggested that Information Security Management System (ISMS) should be integrated with objectives of information security goals on organizational assets: Confidentiality, Integrity and Availability (CIA). However, [13] buttressed that the standard does not only integrate the main objectives of information security into ISMS but it encompasses IT compliance and governance. Hence, it is rather a programme than otherwise. Although [14] compared the standard with adoption of environmental management systems and quality management and concluded that the global adoption of the standard is low. However, a comparison between ISO/IEC 27001 and other international standards was made by [1] and concluded that the standard has a global acceptance.

In order to minimize loses in a business, an organisation should be able to identify and describe, analyse and evaluate their risks. These would help in decision making as to level of risk the organisation could take to maximize profit. This is called risk assessment. Hence, risk assessment is the framework to ISMS [15]. Some organisations have vulnerabilities in their process flow. Hence, for information security application to be effective in such organisations, such vulnerabilities have to be eliminated. Besides, most times application of information security standard does not seem to produce the desired result because risk assessment was not carried out [16].

According to [17], business organisations go after certification in order to give customers and partners assurance on their investments. Hence, added that it is imperative for a business organization to adopt a standard and be satisfied on event of zero-day attack, it helps in giving customers confidence that an organization had provided all the security measures needed of it to protect it customer's investment. And, it also serves as security for the company due to legal action that should be taken by clients on event of breach of information security [18].

IV. METHOD FOR ANALYSING ISO/IEC 27001

In this research work, review of literature was carried out, it was discovered that vulnerability and threat of ISO/IEC 27001 that stray away companies in Nigeria from adopting the standard was not tackled. Hence, data was collected qualitatively and quantitatively. Data was collected qualitatively from a sample of 8 accreditors that were certified through oral interview and the responses were documented appropriately and the quantitative approach was done using questionnaire with a total of 42 questions of which 6 questions were from opportunities, 13 questions from Strengths, 10 questions from Threats, and 13 question from vulnerabilities of the standard. A provision was made for response to the questions on a scale of 1 – 5; between strongly disagree to strongly agree for easy response to questions. There were 70 respondents in all of which 22 were implementation consultants, 30 were auditors and 18 were researchers. The collected quantitative data was used to validate the qualitative data collected. Data analysis was done using Statistical Package for the Social Sciences (SPSS). Strength, Weakness/Vulnerability, Opportunity and Threat (SWOT) analysis was carried out to identify the benefit for adoption of the standard using TOWS Matrix to tackle the vulnerability and threats of the standard, living Nigerian businesses with the benefits of the standard to enjoy.

V. TOWS MATRIX

In order to make a better strategic planning to encourage Nigeria business to adopt ISO/IEC 27001 standard, TOWS matrix is employed to tackle the vulnerabilities and threats of the standard as represented in table 1 bellow:

TABLE I. ISO/IEC 27001 TOWS MATRIX SHOWING HOW IT COULD IMPROVE ON NIGERIAN BUSINESSES

SO: Strategy (Maxi-Maxi)	**WO: Strategy (Mini-Maxi)**
As a means for expanding the standard, S1: the standard is internationally recognized and validated. 81.4% of respondents agreed with it & O1 says there is potential that the standard can be expanded which 71.4% of respondents agreed with it. Hence, it means the standard can be expanded to accommodate Nigerian businesses	Although 54.3% of respondents agreed with V1 which says the standard has cost for adoption and 42.9% of respondents agreed with V5 which says there could be misleading due to the intricacy of the standard. However, 71.4% of respondents agree with O1 which says the standard could be expanded and the lighter version of it is obtainable which makes the implementation simpler and, of cause, cost-effective
68.9% of respondents agreed with the statement in S12 which says the standards creates room for interoperability. Also, 72.8% due to O3 agreed that the standard applied to other schemes such as cloud security. Hence, Interoperability of the standard enhances wider adoption	Although the 42.9% agreed with V5 which says the standard is misleading due to intricacy. However, 81.4% of O2 which says the standard can easily be integrated with other standards. Hence, Ease of integration can reduce the complexity.
	54.3% of respondents agreed that the standard has cost for adoption and 45.7% of respondents agreed with V4 which says the standard is rather concerned with the presence of implementation not the effectiveness. However, 77.1% of the respondents agreed with O2 which says businesses will make more income if security policies are standardized. Paying attention to standard security practice have the possibility of minimizing cost. Besides, it also gives confidence to business clients against fear of losses

	In order to tackle security concerns in a company, V6 which says some controls are excluded in the current version of the standard which 30% of respondents agreed with the statement. Similarly, O6 says the standard has the ability to provide security for future information due to its available controls, 64.3% of respondents agreed with it. Hence, O6 crafted an equilibrium with availability of controls to tackle security concerns.
	Although in V3, 51.5% of respondent agreed that there is possibility that the standard could influence the ethos of administration in an organisation but 58.5% of respondents agreed with O5 which says the standard could be applied to any kind of information. Hence, lean management as emphasized by O5 should give Nigerian businesses confidence to adopt the standard.
ST: Strategy (Maxi-Mini)	WT: Strategy (Mini-mini)
T5: 47.5% of respondents agreed that there are other countries with similar standard. S1 says that the standard has global recognition which 81.7% agreed with the statement. Hence, the standard's global recognition will mitigate tendency for confusion with other standards.	
In order to lessen the misunderstanding in T4 which says, compliance means security is 100% guarantied which 48.6% of respondents agreed with it, S9 which say the standard enables businesses to determine the performance of their ISMS which 65.8% of respondents agreed with it implies that performance management could enable the management to check on employees performance due to adherence to the standard. This should tackle aforementioned misconception	
In order to reduce corrosion of values in T7 which 37.1% of respondents agreed with it and let businesses be inform that certification is rather an integral part of business and a marketing tool than just a marketing tool as said in T9 which 50% of respondents agreed with it, S11 says businesses used the standard for advertisement and as a marketing tools. This should create awareness to enlighten business organisations in Nigeria on the need for certification	
Although T2 says Registrars engender conflict of interest by infringing on the roles of implementation consultants and auditors which 47.1% of respondents agreed with statement, organizational top management could mitigate such conflict of interest by defining roles clearly since the standard provides for top-down risk approach in S7 which 62.9% of respondents agreed with the statement in the question.	

VI. Determination of Significance and Confidence Level of the Hypothesis

A. *T-Test*

Although the TOWS matrix glaringly shows that the percentage of strength-opportunity of the standard outweighed the percentage of vulnerability-threat of the standard which should be enough to influence Nigerian businesses to adopt the standard, we used t-test in this research work to decide on whether or not to accept the null hypothesis. The null hypothesis here is, if opinion of two different groups is the same i.e. if both the p-value and the t-test values of two different groups lie within a significant level, the null hypothesis should be accepted else rejected vis-à-vis the results of SWOT analysis assuming the p-value has a significance level of 5%.

TABLE II. RESPONDENTS' AVERAGES IN THE THREAT CATEGORY

Auditors	Consultants	Researchers
3.80	3.50	3.10
3.50	2.70	3.60
4.00	3.50	2.80
1.00	3.90	3.50
2.50	2.20	3.40
3.90	4.20	3.00
3.30	3.90	3.00
3.80	3.80	4.10
3.30	4.90	3.70
3.30	3.50	3.40
3.40	4.40	3.80
4.20	4.60	3.80
4.60	3.50	3.10
4.40	3.50	3.00
2.00	2.70	3.00
2.50	4.20	3.90
3.10	4.20	3.90
3.30	3.90	4.00
3.50	2.60	
3.90	3.70	
4.00	2.30	
4.00	3.80	
1.80		
2.50		
3.40		
3.90		
2.60		
3.80		
3.20		
3.50		

From the t-test in table 2 above, comparing the averages of researchers and auditors in table II above, the result is 0.512, comparing the averages of implementation consultants and auditors using t-test the result is 0.195 and comparing implementation consultants and researcher the result is 0.375.

The null hypothesis of the three comparison in the threat category of the standard could be accepted as both the p-value and the t-test value lie with a significant level.

TABLE III. AVERAGES OF RESPONDENTS IN VULNERABILITY CATEGORY

Auditors	Consultants	Researchers
3.85	3.38	3.23
2.23	2.46	3.85
3.54	3.92	3.85
1.00	3.31	3.46
3.54	2.23	2.85
3.77	4.15	3.00
3.46	3.46	3.00
3.62	3.38	3.85
3.23	4.38	3.77
3.00	3.92	3.15
3.15	4.00	3.08
3.38	5.00	3.38
4.00	3.38	3.38
1.69	3.31	3.00
2.00	3.15	3.23
3.54	4.00	3.08
3.31	4.31	3.85
3.62	2.08	3.54
3.31	2.38	
2.77	4.00	
3.54	3.00	
3.62	3.23	
1.69		
2.92		
2.38		
3.62		
2.54		
3.77		
3.92		
3.23		

The t-test values obtained in the vulnerability category from table 3 above shows that the result of comparison between auditors and researchers is 0.117, the result of comparison between researchers and implementation consultants is 0.535 and the result of comparison between implementation consultants and auditors is 0.087. Hence, the null hypothesis can be accepted because the t-test value and p-value lie within a significant level.

TABLE IV. AVERAGE OF EACH RESPONDENTS IN STRENGTH CATEGORY

Auditors	I. Consultants	Researchers
4.85	3.92	3.31
4.00	4.77	4.00
4.46	4.08	2.77
4.69	3.92	3.77
3.69	4.23	3.85
3.85	4.62	3.00
4.00	4.38	3.00
4.00	4.62	3.77
4.00	4.46	3.92
3.00	4.00	3.46
4.00	4.38	3.31
4.23	5.00	4.08
3.92	4.00	3.77
4.46	4.08	2.46
2.00	3.69	3.92
3.77	3.92	3.62
3.15	4.00	4.00
3.31	3.54	3.62
3.85	4.08	
4.15	4.54	
4.00	4.62	
4.15	3.85	
4.85		
3.85		
4.31		
3.92		
3.69		
4.08		
3.31		
3.92		

From table 4 above, the t-test result obtained from the average scores of respondents in strength categories between auditors and researchers is 0.015, between implementation consultants and auditors is 0.027 and between implementation consultants and researchers is 2.012. The t-test results obtained for comparing auditors' and researchers' average scores as well as result of comparison between auditors' and implementation consultants' average scores shows that the null hypothesis could be accepted as the values lie within a significant level. However, the result of t-test obtained for comparison between implementation consultants' and researchers' average scores could be rejected because researchers and auditors seemed to disagree with each other due to strength of the standard.

Following section may be divided by subheadings. It should provide a concise and precise description of the experimental results, their interpretation as well as the experimental conclusions that can be drawn.

https://doi.org/10.31871/WJIR.9.5.12
World Journal of Innovative Research (WJIR)
ISSN: 2454-8236, Volume-9, Issue-5, November 2020 Pages 140-147

TABLE V. AVERAGE OF EACH RESPONDENTS IN OPPORTUNITY CATEGORY

Auditors	Consultant	Researchers
4.83	4.00	3.50
3.83	4.50	4.50
4.00	2.83	4.00
3.83	4.33	3.17
4.33	4.33	3.83
3.83	4.83	3.00
4.33	4.50	3.00
3.33	4.33	4.00
4.17	5.00	3.83
3.00	3.83	3.83
4.00	4.67	4.00
3.67	4.67	3.83
4.17	3.83	3.50
4.33	3.67	3.17
2.00	3.67	3.50
4.83	3.83	3.50
3.00	4.67	3.83
3.33	3.67	3.33
4.33	3.33	
3.67	4.33	
4.17	4.50	
4.50	4.50	
4.50		
3.33		
4.00		
4.17		
3.83		
3.50		
3.50		
3.17		

T-Test was carried out on average scores of respondents on the opportunity category. Comparison was made between researchers and implementation consultants and the value is 0.001, comparison was made between researchers and auditors average scores and the result is 0.137 and comparison was made between implementation consultants and auditors and the value is 0.046 as shown on table 5. The null hypothesis could be accepted of all the comparisons because both the p-values and the t-test values lie with significant levels.

B. Analysis of Variance

In order to find the significant differences among mean values obtained from implementation consultants, researchers and auditors, t-test is extended using analysis of variance (ANOVA). In the analysis of variance, the following statements were considered: if $f_{stat} < f_{crit}$ accept null hypothesis because they are the same; if $f_{stat} > f_{crit}$ reject null hypothesis because they are not the same. Assuming null hypothesis is true, following is the analysis of threat of the standard

TABLE VI. VARIANCE OF THREAT OF THE STANDARD SUMMARY

Groups	Count	Sum	Average	Variance
Auditor	10	33.33333333	3.333333333	0.111605
Implementation Consultant	10	36.13636364	3.613636364	0.140611
Researcher	10	34.5	3.45	0.131996

TABLE VII. INTERPRETATION OF VARIANCE FOR THREAT OF THE STANDARD

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	0.396525865	2	0.198262932	1.54807661	0.230947073	3.354130829
Within Groups	3.457903275	27	0.128070492			
Total	3.85442914	29				

The null hypothesis of the standard could be accepted here since $f_{stat} < f_{crid}$ which are 1.54807661 and 3.3541130829 respectively. And, from the table above, it could be seen that the span of threats of the standard are not the same of each of the three groups of respondents. Hence, the hypothesis is true assuming the null hypothesis is true

Following is analysis for vulnerabilities of the standard:

TABLE VIII. VARIANCE OF VULNERABILITY OF THE STANDARD SUMMARY

Groups	Count	Sum	Average	Variance
Auditor	13	40.4	3.107692308	0.080954416
Implementation Consultant	13	45.18181818	3.475524476	0.086644416
Researcher	13	43.72222222	3.363247863	0.12120133

TABLE IX. INTERPRETATION OF VULNERABILITY OF THE STANDARD USING ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	0.923932461	2	0.461966231	4.798815498	0.0142064	3.259446306
Within Groups	3.46560194	36	0.096266721			
Total	4.389534401	38				

It can be seen that the hypothesis of the vulnerability category is significant as the null hypothesis due to vulnerability of the standard can be rejected since $f_{crid} < f_{stat}$ which are 3.259446306 and 4.798815498 respectively.

Following is analysis for strengths of the standard using ANOVA:

TABLE X. VARIANCE OF STRENGTH OF THE STANDARDS SUMMARY

Groups	Count	Sum	Average	Variance
Auditor	13	50.9	3.915384615	0.05011396
Implementation Consultant	13	54.77272727	4.213286713	0.118245391
Researcher	13	45.94444444	3.534188034	0.125276986

TABLE XI. STRENGTH OF THE STANDARD INTERPRETATION USING ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	3.012669874	2	1.506334937	15.38980104	1.47862E-05	3.2594463
Within Groups	3.52363605	36	0.097878779			
Total	6.536305924	38				

Observe that the hypothesis of strength of the standard is significant as the null hypothesis due to strength could be rejected because $f_{stat} > f_{crid}$ which are 15.38980108 and 3.25944 respectively.

Following is analysis for opportunities of the standard using ANOVA:

TABLE XII. VARIANCE OF THE OPORTUNITY OF THE STANDARD SUMMARY

Groups	Count	Sum	Average	Variance
Auditor	6	23.1	3.85	0.04922222
Implementation Consultant	6	25.04545455	4.17424242	0.02183196
Researcher	6	21.77777778	3.62962963	0.14773663

TABLE XIII. OPPORTUNITY OF THE STANDARD INTERPRETATION USING ANOVA

Source of Variation	SS	df	MS	F	P-value	F crit
Between Groups	0.900598692	2	0.450299346	6.174382172	0.011057364	3.682320344
Within Groups	1.093954018	15	0.072930268			
Total	1.99455271	17				

Observe that the hypothesis of opportunities of the standard is significant as the null hypothesis due to opportunity could be rejected because $f_{stat} > f_{crid}$ which are 6.174382172 and 3.682320344 respectively.

A. Confidence level error margin

In order infer the reliability of the survey, the error of margin and confidence level have to be calculated using the total sample size of 70. Using Raosoft calculator, assuming we are using sample size of 20, 000, the confidence level of this study should be 90% and the required sample sized should be 68. In this research work, the sample size for the survey is 70. From Roasoft calculator, the margin error is 9.81% which is the maximum error that could be tolerated in this research work that should not pose significant effect on population of sample size greater than 20, 000.

B. Further study

Although in this study SWOT analysis and analysis of variance were used to encourage Nigerian businesses to adopt ISO/IEC 27001 standard, the standard has different versions, the like of 2005, 2013, 2018. further research will study each of the versions, analyse and validate them. Also, work could also be done to determine the t-test of each respondent to a questions and determine the analysis of variance for each respondent in a category.

VII. CONCLUSION

In order to influence Nigerian business companies to adopt the ISO/IEC 27001 standard, a mixed research approach was adopted. Result of quantitative approach was used to validate the result obtained from qualitative approach. Result obtained from the quantitative research approach show that the standard should strengthen Nigerian businesses as there are more strength and opportunities in the standard than threats and vulnerabilities as shown by TOWS Matrix analysis of the SWOT which should encourage Nigerian businesses to adopt the standard. In order to prove the validity of the hypothesis that strength and opportunity of the standard outweighed the vulnerabilities and threats of the standard, t-test and analysis of variance were used to determine the significant difference among the means of the observed samples. A sample size of 70 was used and the obtained confidence level is 90%.

REFERENCES

[1] Heru Susanto, M. N. A., Tuan, Y. C., Aksoy, M. S. & Syam, W. P., (2012). Integrated Solution Modeling Software: A New Paradigm on Information Security Review. Level International Journal of Engineering and Technology, Issue 2, pp. 67-74.

[2] Loloei, I., Shahriari, H. R. & Sadeghi, A., (2012). A model for asset valuation in security risk analysis regarding assets' dependencies. Tehran, IEEE, pp. 763-768.

[3] Livshitz, I. I. et al., (2016). The optimization of the integrated management system audit program. Nalchik, IEEE.

[4] Gutiérrez-MartínezEmail, J., Núñez-Gaona, M. A. & Aguirre-Meneses, H., (2015). Business Model for the Security of a Large-Scale PACS, Compliance with ISO/27002:2013 Standard. Journal of Digital Imaging, 28(4), p. 481–491.

[5] Disterer, G., (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. Journal of Information Security, 4(2), pp. 92-100.

[6] Anttila, J., Jussila, K., Kajarva, J. & Kamaja, I.,(2012). Integrating ISO/IEC 27001 and other Managerial Discipline Standards with Processes of Management in Organizations. Prague, IEEE

[7] Gholami, M. F. & Ramsin, R., (2012). Strategies for Improving MDA-Based Development Processes. Liverpool, IEEE.

[8] Chander, M., Jain, S. K. & Shankar, R., (2013). Modeling of information security management parameters in Indian organizations using ISM and MICMAC approach. Journal of Modelling in Management, 8(2), pp. 171-189.

[9] Fal, A. M., (2010). Standardization in information security management. Cybernetics and Systems Analysis, 46(3), p. 512–515.

[10] Aginsa, A., Edward, I. Y. M. & Shalannanda, W., (2016). Enhanced information security management system framework design using ISO 27001 and zachman framework - A study case of XYZ company. Yogyakarta, IEEE.

[11] Alshitri, K. I. & Abanumy, A. N., (2014). International Conference on Information Science & Applications (ICISA). Seoul, IEEE.

[12] Jo, H., Kim, S. & Won, D., (2010). A Study on Comparative Analysis of the Information Security Management Systems. Berlin, pringer, pp. 510-519.

[13] Kilic, N. & Metin, B., (2012). Importance of education in information technology governance. Smolenice, IEEE.

[14] Gillies, A., (2011). Improving the quality of information security management systems with ISO27000. The TQM Journal, 23(4), pp. 367-376.

[15] Goldes, S., Schneider, R., Schweda, C. M. & Zamani, J., (2017). Building a Viable Information Security Management System. Exeter, IEEE.

[16] Kirwan, B., 2017. A Guide To Practical Human Reliability Assessment. 1st ed. London: CRC Press.

[17] Tariq, M. I., (2015). Providing Assurance to Cloud Computing through ISO 27001 Certification: How Much Cloud is Secured After Implementing Information Security Standards. 1st ed. s.l.:The ACM Guide to Computing Literature.

[18] Al-Ahmad, W. & Mohammad, B., (2013). Addressing Information Security Risks by Adopting Standards. International Journal of Information Security Science, 2(2).

Mr. Heman Awang Mangut, MSc. Information Security and Computer Forensics, University of East London; B.Sc. Computer Science, University of Jos, Jos, Arrp Cache Poisoning Mitigation and Forensic Investigation, CCNA, CPN, IBM

Assoc. Prof. Damuut Peter Luhutyit, PhD University of Essex, M.Sc. Software Technology, Robert Gordon University, Aberden, United Kingdom, B.Tech., ATBU Bauchi, Bauchi, Nigeria; X-raying discovery in a wireless sensor network comprising non-homogenous node, Comparative analysis of FCFC, SJN & RR job scheduling algorithms, determining the uptimum maturing of maize using computational intelligence technique; CCNA, IEEE, ISOC, FOSSFA

Dr. Aristarkus Datukun Kalamba, PhD University of Science and Technology, Selangor, Malaysia; M.Sc. Information Technology, National Open University of Nigeria; B.Sc. University of Jos, Jos, Nigeria; Diagnosing Salem University Lokoja network performance, Towards better bandwidth subscription in Plateau State University, Harnessing telemedicine through video conferencing; CCN, NCS.

Mss. Palang Mangut, M.Sc. Information Security, University of Staffordshire, Staffordshire, B.Tech. ATBU, Bauchi; Quality of Ka-Band Internet Service based on users' experience; CCNA, NCS