Best Practices of Auditing in an Organization using ISO 27001 Standard

Amogh Phirke, Jayshree Ghorpade-Aher

ABSTRACT--- In recent year with the intensive use of the information technologies, data security has been turned into a critical and important issue in organizational management. Various Standard and rules are there for the security of Information, for example, ISO/IEC 27001, ISO/IEC 27002. However, organization face different challenges for implementing the standard. In this paper, we present the status of the ISO/IEC 27001 execution process in a Small and Medium Sized Enterprise. By executing ISO 27001, organization got the chance to prove authenticity and show the clients that the organization is working according to recognized best practices. It helped the organization "IKSC Knowledge Bridge Pvt Ltd." in reducing cost, risks, and increases the brand value. The outcomes obtained conclude not just the need to think about the technical, legal aspects of organization but also those related to people like training, knowledge, create awareness, to achieve a successful management of information security

Keywords— ISO/IEC 27001:2013, Risk Mitigation, Software Audit, Controls, Compliances

1. INTRODUCTION

In upcoming era data security is one of the most important assets for IT industry. Risk Assessment is one of solution to prevent data from data theft and for recognizing loop holes in the organization that can cause security breaches. There should be a proper set of procedures and policies applied to prevent these security breaches to enter in to the organization. One of the framework which includes Risk Assessment is ISO 27001 Standard which deals with the overall security of the organization. This Standard starts from determining the scope of organization till certification of the Standard, although it is not mandatory that organization should be certified if the organization is following the mandatory policies and control to gain its objective. ISO 27001 Standard is used to implement Information Security Management System (ISMS) in an organization. Since the most of highest effect security breaches originate by employees working in the organization, there should to be a proper training in the organization to shield the system from being compromised internally, the awareness program should be conducted for the employees and staff so that the information security business continuity do not exclusively depends upon a specific individual presence which could lead to serious system halt/crash dependent on the accessibility of specific employees. Information Security Management System (ISMS) give a complete solution for a superior information security encounter by providing the needed procedures, tools, and measures for enhancing and maintaining a protected information organization [1]. The employees and staff of the organization should be given proper awareness and training about the ISO Standard and why it is important to their organization. After compliance with ISO 27001, the organization can give guarantee to their clients and partner that their data is secure within the organization.

2. LITERATURE REVIEW

Koldo Peciña and et al. used two techniques which is ISO 31000 and ISO 27001 resulting in both physical and Logical security evaluation. The only limitation was that there was no security management implemented to ensure protection of all assets. [1]. Carol Hsu and et al. compares the lists of firms with and without ISO 27001 certification with their performance. Only the Financial information was not available in any firm [2]. Manar Abu Talib and et.al. gives the importance of ISO 27001 procedure to execute in an information security management. The future scope was to evaluate the enriched Information Security course, and improve the Information Security Technologies [3]. Elvi Fetrina and et al. collected the data by interview and by literature study. The results of this survey is inventory management information. They used Rapid Application Development and Object Oriented Approach using Unified Modelling language. Problem regarding possibility of Loss or damage data arises in this case while implementing [4]. Awni Itradat and et al. uses ISO 27001 which guarantee an ultimate protected environment for organization. The only limitation arises that the team who is implementing should have all the knowledge of ISO 27001 Standard [5]. Yogesh Verma and et al. highlights the design and development of a web based centralized software asset management systems, reduces the overall development cost, and improves the software value and efficiency. The limitation was that there was no monitoring and Evaluation for periodic built in feedback mechanism towards continuous improvement [6]. Martin Jakubicka, investigates the design of a Software Asset Management created for University purposes and addresses the most noteworthy issues in this situation.. The only limitation was that there was no suitable methodology for creating SAM. Afifah Muftinisa and et al. uses technique that manage their resources, maintain detailed asset record as well as maintain the conditions of the asset. The limitation was there was not much flexible assets [7]. Thomson Martin uses number of ways in which SAM can help an organization to keep assets safe but it takes a lot of

Revised Manuscript Received on July 10, 2019.

Amogh Phirke, Computer Science and Engineering, MIT World Peace University, Pune, Maharashtra, India. (amogh.phirke@gmail.com)

Jayshree Ghorpade-Aher, Computer Science and Engineering, MIT World Peace University, Pune, Maharashtra, India.. (jayshree.aher@mitwpu.edu.in)

time, effort and support from Senior Management. The limitation was that it is not necessary that an expert in SAM may also be expert in Software Licensing. Viktor Shved and et al. proposed a technique that permits distinguishing executable documents assembled from a similar source code for different versions of systems and with minor changes to the source code [8].

3. PURPOSE OF THE INTERNAL AUDIT FOR ISO 27001 STANDARD

The purpose of audit is understanding with information security management system examining practices. The scope of the audit included an assessment of the information security services, forms, and controls portrayed within the ISMS documentation to secure the privacy, reliability and accessibility of the city's critical information assets inside the scope of the ISMS. A list of twenty information resources was given at the beginning of the audit as the inventory to be considered within the scope of the ISMS.

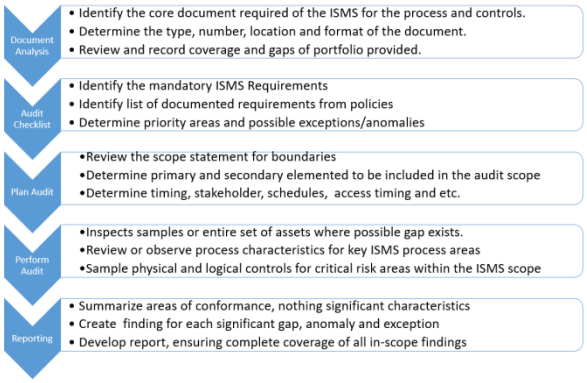

Fig.1 Auditing Methodology

4. IMPLEMENTATION OF ISO 27001 STANDARD

ISO/IEC 27001 gives regulating prerequisites to develop and operate in an ISMS, including a lot of controls for the controls and mitigation of the risks related with the information assets which the organization looks to protect by working its ISMS.

4.1 ISO 27001 Clauses

ISO/IEC 27001:2013 contains 10 clauses which are as follows:

Clause 1 -Scope
Clause 2 -Normative references
Clause 3 -Terms and definitions
Clause 4 -Context of the organisation
Clause 5 - Leadership
Clause 6 -Planning
Clause 7 -Support
Clause 8 -Operation
Clause 9 -Performance Evaluation
Clause 10 -Improvement

4.2 Steps for implementing ISO 27001 Standard in an organization

The ISMS might be certified as consistent with ISO/IEC 27001 by various authorize enlistment centers around the world. The ISO/IEC 27001 certification, as other ISO management system certifications, for the most part includes a three stage audit process:

PDCA is very important for implemetation of the porject. The ISO/IEC 27001 Standard states that for implementing the standard following are the steps which is to be followed

a. Defining the ISMS policy
b. Scope of the ISMS
c. Preparing for Risk Assessment
d. According to risk assessment and identified risk selection of controls which is to be applied
e. Preparation of Statement of Appicability

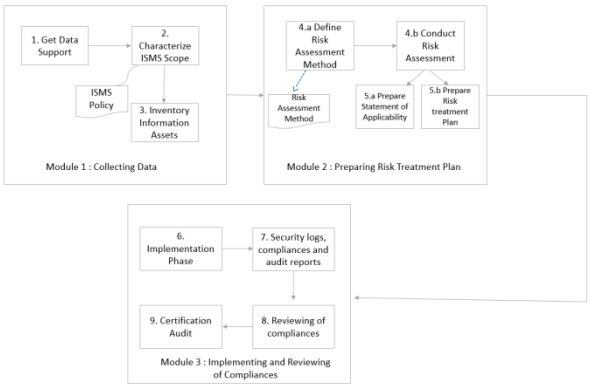

Fig. 2 Block Diagram of ISO 27001 [5].

Stage 1— Find out the Objective of the organization

The objective of the organization is obtained from the company's mission and vision. The goal can be:

1. Assurance to the employees and client that they are fully compiled with the information security.
2. The data which is taken from the employees and client is protected.
3. Continues improvement in productivity of the organization.
4. Ethically running with IT guidlines.

Stage 2— Get Organization Support

The organization should take guarantee that it will cooperate with the implementer while implementing the standard for improvement of the ISMS. Obligation must consolidate exercises, for instance, guaranteeing that the most potential resources are accessible to work with ISMS and that all deligates of the ISMS which are doing trainning.

Stage 3— Charaterize ISMS Scope

According to the ISO 27001 Framework, there are 114 controls , which are organized in 14 Domains and 35 control objectives organization , but the framework states that it is not mandatory to implement all the controls. It depends on the size of the organization and its objective. But it should be mentioned that why that control is not applicable to your organization. ISMS Scope must be specified in order to be get certified from external auditors[14].

Stage 4— Define risk assessment methodology

After studing and Analysing objective and risk assosiated with the organization we have to formulate a proper risk asessment methodology. The methodology should contains the proper treatment of risk which includes resolution and controlling of risks faced by the organization. We also have to identify and distinguish the resources from which the risk occurs and harm the organization security [14].

Stage 5— Prepare Risk Treatment Plan

After identifying the risk associated with the organization, probability and consequences of each risk is measures or analyz and drown in the table. Depending on the probability and consequences of risk, prority of treatment of each risk is decided. Risk treatment Plan includes basic Risk Mitigation Strategic which includes accepting, avioding, transferring or reducing the risk to a certain level of acceptance.

Stage 6— Developing ISMS Implementation Program

As mentioned in step 3, controls should be selected with respect to size of organization and the organization objectives. Not all the controls are mandatory to implement the ISMS framework. According to the objective of the organization among 114 controls specific controls which is needed to implement Information Security Management System [14].

Stage 7—Documentation of adopted controls in an organization.

For the controls applied, as mentioned in the SOA, the organization will require articulation of arrangement or a complete procedure strategies and report to recognize client role for relaiable and execution of approaches and techniques.

List of documents and practices which is also called as Statement Of applicability(SOA) is mandatory document for certification of ISO 27001.

Stage 8— Reviewing of compliances

After implementing all the controls in the organization, it should be reviewed periodically whether the controls implemented in the organization suitable for the objective of the organization. Monitoring of objective, control, measurement methodologies comes together in this phase [14].

Stage 9— Preparing for Internal Audit

Sometimes the employee knowingly and unknowingly takes wrong discussion while achieving the objective of the organization, which leads to decrease in performance of the organization so it is important to perform an internal review. So corrective and preventive action is to be taken to meet the required objective. [14].

Stage 10— Preodic Management Review

Periodic Management Review deals whether the implemented policies and procedures are being followed or not to achieve organization's objective. This step is always important for taking action against the employee who are violating the policies and procedures [14].

5. RESULTS AND ANALYSIS

It's a E- learning based institute. Previously, there was no ISMS policies and controls applied in an organization. There was lack in proper documentation and procedures in an organization due to which it was facing with many difficulties and internet threats. Even there was no supervision on network security. Firstly, we did the gap analysis and studied about the existing procedures and control applied in the organization. After doing the gap analysis we come to know that there are many mandatories processes and control which are good to have in an organization for network security purpose.

Firstly, we make a list of mandatory controls which is to be implemented from ISO 27001 Standard checklist. We get to know that there are many softwares used in organization so the handling and enhancing the purchase, deployment, maintenance, cosumption, and removal of software is required in an organization. Along with this solution for Risk management, MIS reporting, disaster management was also required.

Along with this we also applied the policy to deleted unwanted data after a particular period of time, policy to alert when internet data allotted to each student exceeds, policy if data theft occurs, policy to block and check whether anyone is uploading files on dropbox and blocking the USB port to avoid altering of computer system and data theft along with policy to measure the productivity of each student is also applied. As information security becomes a public concern, certification would benefit the certified firms through competitive advantages. All these issues can be eliminated by implementing ISO 27001 Standard in an organization. Hence, we have studied about ISO 27001 and started with establishing ISMS Scope according to the requirement of an organization. Along with these, we also studied about different policies that is to be applied in organization, which will help to implement ISO, 27001 framework.

After implementing the project, we get to know that it helps the organization to save cost and time in Software Audit, IT related Configuration, overall management done by higher authority and IT effort done by network Administrator. The organization easily do monitoring of all the assets (which also includes human) and softwares installed in the systems. After implementing the Standard, the organization can easily check the productivity of each student on daily basis as well as on monthly/yearly basis. This comes under Human Resource Management which can help business to gain a competitive advantage.

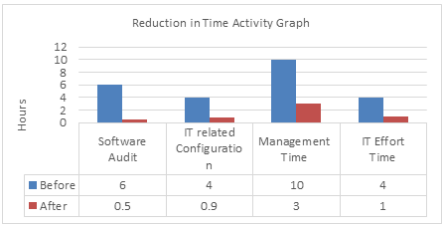

Fig. 3. Reduction in Time Activity Graph.

#	Publisher	Name	Version	Computer
1	10-Strike Software	10-Strike Bandwidth Monitor Agent	3.51	A1 a2 A3 B1 C2 C3 D1 D3 D7 DEVELOPMENT E4 h3 h4 ho J1 krishna punebranch2
2	10-Strike Software	10-Strike LANState Pro	8.8	PUNESERVER
3	10-Strike Software	10-Strike Network Inventory Explorer	8.5	PUNESERVER
4	AccelWare, Inc.	Unit Conversion Tool 5.1		A1 a2 A3 B1 C3 D1 D3 d5 D7 E4 h3 h4 punebranch2
5	Adobe Systems Incorporated	Adobe Acrobat DC	19.008.20074	J1
6	Adobe Systems Incorporated	Adobe Flash Player 10 ActiveX	10.0.22.87	A1 a2 A3 punebranch2
7	Adobe Systems Incorporated	Adobe Flash Player 15 Plugin	15.0.0.152	A1 a2 A3 B1 D1 D3 d5 E4 h3 h4 ho J1 punebranch2
8	Adobe Systems Incorporated	Adobe Flash Player 26 ActiveX	26.0.0.131	J1
9	Adobe Systems Incorporated	Adobe Flash Player 26 ActiveX	26.0.0.137	C2 krishna
10	Adobe Systems Incorporated	Adobe Flash Player 29 ActiveX	29.0.0.171	D7
11	Adobe Systems Incorporated	Adobe Flash Player 29 NPAPI	29.0.0.171	D7
12	Adobe Systems Incorporated	Adobe Flash Player 31 NPAPI	31.0.0.122	C3
13	Adobe Systems Incorporated	Adobe Reader 9.3	9.3.0	iksc-backup
14	Adobe Systems Incorporated	Adobe Reader X (10.1.16)	10.1.16	C3
15	Adobe Systems Incorporated	Adobe Reader X	10.0.0	A1 a2 A3 B1 C2 D1 D3 d5 D7 DEVELOPMENT E4 h3 h4 ho J1 krishna punebranch2 PUNESERVER
16	Adobe Systems Incorporated	Chinese Simplified Fonts Support For Adobe Reader X	10.0.0	C3
17	Altair Engineering, Inc.	Altair HyperWorks Desktop 13.0 (Local 64-bit)	13.0	C3
18	Altair Engineering, Inc.	Altair HyperWorks Master Installer 13.0 (Local 64-bit)	13.0	C2 E4 krishna
19	Altair Engineering, Inc.	Altair HyperWorks Master Installer 14.0 (Local 64-bit)	14.0	C2 C3 D1 D3 d5 E4 krishna
20	Altair Engineering, Inc.	Altair HyperWorks Student Edition 14.0 (Local 64-bit)	14.0-edu	C3 d5
21	Altair Engineering, Inc.	Altair HyperWorks Student Edition 2017 (Local 64-bit)	2017-edu	D1 D3 d5
22	Altair Engineering, Inc.	Virtual Wind Tunnel 13.0 46	13.0.46.0	C2 E4 krishna
23	Altair Engineering, Inc.	Virtual Wind Tunnel 13.1 1270	13.1.1270.0	C2 D1 D3 d5 E4 krishna

Fig. 4. Implementation of procedure to show installed software in an organization

Link Order	GPO	Enforced	Link Enabled	GPO Status	WMI Filter	Modified	Domain
1	USB-BLOCKED-USER	Yes	Yes	Enabled	None	17-04-...	kb.in
2	Block Websites	No	Yes	Enabled	None	07-04-...	kb.in

Fig. 5. Figure showing USB port blocked in an organization

Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Pre-Windows 2000 Compatible Acc...
Act as part of the operating system	Not Defined
Add workstations to domain	Authenticated Users
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SERVI...
Allow log on locally	Administrators,Backup Operators,...
Allow log on through Remote Desktop Services	Not Defined
Back up files and directories	Administrators,Backup Operators,...
Bypass traverse checking	Everyone,LOCAL SERVICE,NETW...
Change the system time	LOCAL SERVICE,Administrators,Se...
Change the time zone	Not Defined
Create a pagefile	Administrators
Create a token object	Not Defined
Create global objects	Not Defined
Create permanent shared objects	Not Defined
Create symbolic links	Not Defined
Debug programs	Administrators
Deny access to this computer from the network	Not Defined
Deny log on as a batch job	Not Defined
Deny log on as a service	Not Defined
Deny log on locally	Not Defined
Deny log on through Remote Desktop Services	Not Defined
Enable computer and user accounts to be trusted for delegation	Administrators
Force shutdown from a remote system	Administrators,Server Operators
Generate security audits	LOCAL SERVICE,NETWORK SERVICE
Impersonate a client after authentication	Not Defined
Increase a process working set	Not Defined
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators,Print Operators
Lock pages in memory	Not Defined
Log on as a batch job	Administrators,Backup Operators,...
Log on as a service	Not Defined
Manage auditing and security log	Administrators
Modify an object label	Not Defined
Modify firmware environment values	Administrators
Perform volume maintenance tasks	Not Defined
Profile single process	Administrators
Profile system performance	Administrators,WdiServiceHost
Remove computer from docking station	Administrators
Replace a process level token	LOCAL SERVICE,NETWORK SERVICE
Restore files and directories	Administrators,Backup Operators,...
Shut down the system	Administrators,Backup Operators,...
Synchronize directory service data	Not Defined
Take ownership of files or other objects	Administrators

Fig. 6. Policy applied to control different operation in an organization

From January2019 To April2019 Student Record

ID	BIO_ID	STUD_NAME	BRANCH	PER DAY UTILIZED	AVG_IN_TIME	AVG_OUT_TIME	TOTAL HOURS	ATTENDANCE
1	991	Nikhil Shrikant Jadhav	IKSC PUNE	11.47 Hrs	9 AM	7 PM	195.0 Hrs	Total 17 Day's Present
2	985	Sakshi Sunil Bhosale	IKSC PUNE	11.29 Hrs	9 AM	6 PM	237.0 Hrs	Total 21 Day's Present
3	885	Mansing Manohar Badadare	IKSC PUNE	9.69 Hrs	9 AM	7 PM	310.0 Hrs	Total 32 Day's Present
4	967	Tushar Suresh Khuje	IKSC PUNE	13.42 Hrs	6 PM	7 PM	349.0 Hrs	Total 26 Day's Present
5	737	Amey S. Pavaskar	IKSC PUNE	14.0 Hrs	6 PM	7 PM	98.0 Hrs	Total 7 Day's Present
6	964	Hirosing Suksing Thakur	IKSC PUNE	10.33 Hrs	8 AM	7 PM	310.0 Hrs	Total 30 Day's Present
7	921	Roshan Ravindra Kirange	IKSC PUNE	15.43 Hrs	6 PM	5 PM	216.0 Hrs	Total 14 Day's Present
8	927	Nikhil Arun Dalvat	IKSC PUNE	5.28 Hrs	9 AM	4 PM	95.0 Hrs	Total 18 Day's Present
9	970	Shrikant Jagannath Suryavanshi	IKSC PUNE	8.69 Hrs	9 AM	6 PM	313.0 Hrs	Total 36 Day's Present
10	969	Satyajeet Alka Patil	IKSC PUNE	8.98 Hrs	10 AM	7 PM	404.0 Hrs	Total 45 Day's Present
11	861	Anand Jalindar Kumbhar	IKSC PUNE	8.94 Hrs	10 AM	7 PM	277.0 Hrs	Total 31 Day's Present
12	931	Kirti Rajaram Bhagat	IKSC PUNE	8.03 Hrs	9 AM	6 PM	289.0 Hrs	Total 36 Day's Present
13	973	Ajit Dadasaheb Kakade	IKSC PUNE	9.68 Hrs	9 AM	7 PM	387.0 Hrs	Total 40 Day's Present
14	767	Akshaykumar J. Patil	IKSC PUNE	8.53 Hrs	9 AM	6 PM	128.0 Hrs	Total 15 Day's Present
15	956	Vishal Mohan Parade	IKSC PUNE	9.56 Hrs	9 AM	7 PM	306.0 Hrs	Total 32 Day's Present
16	940	Mahesh Nivrutti Chaudhari	IKSC PUNE	10.89 Hrs	8 AM	8 PM	305.0 Hrs	Total 28 Day's Present
17	926	Haribhau Ramkrishna Patil	IKSC PUNE	10.58 Hrs	8 AM	7 PM	349.0 Hrs	Total 33 Day's Present
18	847	Shantanu Milan Gawli	IKSC PUNE	10.31 Hrs	7 AM	5 PM	134.0 Hrs	Total 13 Day's Present

Fig. 7. Productivity of each student in an organization

6. CONCLUSION

As information security becomes a public concern, ISO 27001 certification on information security management system (ISMS) would benefit the certified firms through competitive advantages. All these issues can be eliminated by implementing ISO 27001 Standard in an organization. Hence, we have studied about ISO 27001 and implemented the ISO 27001 framework according to the requirement of an organization. Along with these, we also studied about different policies that is applied in organization, which will help company to protect from security threats and helps to increase its productivity.

REFERENCES

1. Amogh Phirke , Prof. Jayshree Ghorpade-Aher, "Risk Assessment of Software Compliances using ISO 27001 Standard", JASC: Journal of Applied Science and Computations, Volume 6 Issue 3, March 2019
2. Koldo Peciña, Ricardo Estremera, Alfonso Bilbao, Enrique Bilbao, "Physical and Logical Security Management Organization Model Based on ISO 31000 and ISO 27001", IEEE Carnahan Conference on Security Technology, 18-21October 2011
3. Carol Hsu, Tawei Wang, Ang Lu, "The Impact of ISO 27001 Certification on Firm Performance", IEEE, 2016 49th Hawaii International Conference on System Sciences (HICSS), 5-8 January 2016
4. Manar Abu Talib, Adel Khelifi, Tahsin Ugurlu, "Using ISO 27001 in Teaching Information Security", IEEE, IECON 2012 - 38th Annual Conference on IEEE Industrial Electronics Society, 25- 28 October 2012
5. Elvi Fetrina, Eri Rustamaji, Tatat Nuraeni , Yusuf Durrachman, "Inventory Management Information System Development at Bprtik Kemkominfo Jakarta", IEEE 5th International Conference on Cyber and IT Service Management (CITSM), 8-10 August 2017
6. Awni Itradat, Sari Sultan, Maram Al-Junaidi, Rawa'a Qaffaf, Feda'a Mashal, and Fatima Daas, "Developing an ISO 27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study", JJMIE (Jordan Journal of Mechanical and Industrial Engineering) ISSN 1995-6665 Volume 8, April. 2014
7. Yogesh Verma, R. Nandakumar, "Development of Software Asset Management System to Facilitate Software Reuse", IET (Institution of Engineering and Technology) International Conference on Software Engineering and Mobile Application Modelling and Development (ICSEMA 2012), 19-21 December 2012
8. Afifah Muftinisa, Rosalina, Rikip Ginanjar, RB. Wahyu, Nur Hadisukmana "Development and Implementation of Fixed Asset Management System", IEEE (Second International Conference on Informatics and Computing (ICIC)), 1-3 November 2017
9. Viktor Shved, Pavel Kuzmich, Viktoria Korzhuk , "The Method of an Audit of Software Containing in Digital Drives", IEEE he Method of an Audit of Software Containing in Digital Drives, 15-17 October 2014
10. Paul Hopkin, "Fundamentals of Risk Management Understanding, evaluating and implementing effective risk management", Kogan Page, July 2018
11. Tsan-Ming Choi, Hing Kai Chan, Xiaohang Yue, "Recent development in Big Data Analytics for Business Operations and Risk Management", IEEE Transactions on Cybernetics, 12-16 January 2017

12. Benno E. Albert, Rodrigo P. dos Santos, Cláudia M. L. Werner, "Software Ecosystems Governance to Enable IT Architecture Based on Software Asset Management", IEEE 7th IEEE International Conference on Digital Ecosystems and Technologies (DEST), 24-26 July 2013
13. ISO/IEC/IEEE 26531, International Standard, "System and Software Engineering – Content management for product life –cycle, user and service management documentation", May 2015
14. ISO/IEC19770-1, "International Standard, Informational Technology – IT asset management", December 2017
15. SYNC RESOURCE (2018) ISO 27001 (ISMS) Metrics And Step By Step Implementation Guide 2018. [Online].Available: https://blog.sync-resource.com/2018/04/19/iso-27001-implementation-step-by-step-guide/
16. NEWS WEB ZONE (2017) A Brief Guide to Controlling Risks In The Workplace [Online]. Available: https://www.newswebzone.com/brief-guide-controlling-risks-workplace/
17. Envato tuts+ [2014] The Main Types of Business Risk [Online]. Available : https://business.tutsplus.com/tutorials/the-main-types-of-business-risk--cms-22693
18. Simplicable [2016] 6 Types of Compliance Risks [Online]. Available : https://simplicable.com/new/compliance-risk.
19. THYCOTIC | ISO 27001[Online]. Available : http://www.esdebe.com/perch/resources/iso-27001-annex-s-control-mapping.pdf