Manuscript Submitted	Nov 11, 2020
Accepted	Dec 19, 2020
Published	Dec 24, 2020

Information Security Compliance Framework for Data Center in Utility Company

Yuvaraaj Velayutham, Ganthan Narayana Samy, Nurazean Maarop, Noor Hafizah Hassan, Wan Haslina Hassan, Sivakumar Pertheban and Sundresan Perumal

Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, 54100, Kuala Lumpur, Malaysia
Malaysia-Japan International Institute of Technology (MJIIT), Universiti Teknologi Malaysia, Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia
Cyberlynx International College, No.27, Jalan RU 7/1, Section 7, 46050, Petaling Jaya, Selangor, Malaysia
Faculty of Science and Technology, Universiti Sains Islam Malaysia, 71800, Nilai, Negeri Sembilan, Malaysia

ganthan.kl@utm.my

Abstract

The utility organization has already implemented some of security framework and compliance in their data center to secure the data centers of valuable information. However, the implementation of security framework and compliance, still has several issues relates to some restricted areas. There is no effective security framework and compliance, being implemented in their data center such as access control management system at the entrance of the building zone. Therefore, the objective of this research is to develop information security compliance framework in data center in utility company. This research applied qualitative method namely semi-structured interviews for data collection. The contribution of this research will help professionals and security management organizations to understand the best ways they can be used to improve physical security within the context of information security compliance frameworks that play an important role.

Keywords: *Compliance, Data Center, Framework, Information Security Compliance.*

1. Introduction

The data centre is the heart and core of an organization. As per relating to the threats, it's called a honey pot for hackers and intruders. The physical and logical security and compliance are important to secure the information system of an organization to avoid any loss in revenue, halt in production or even stolen important and valuable data [1]. "With the development of the Internet and its use in different dimensions, organizations and institutions have faced invasion with new issues related to information security and computer networks" [2], both physical and logical security as well as the framework and compliance do play a vital role in this emerging and quickly surging network activities. It is important to obtain a proper standard of compliance or framework which will be the first layer defence and readiness towards the threats [2].

Security is the major targets of many companies whom offering in house data center services. However, with the missing security standards and framework could lead to serious catastrophic security related incidents [3]. Such organization handling private and confidential data of their end users, the users must have huge trust and a trust relationship on the data provided to the company in any form.

The end users hoping that these data's will be safeguarded. Protection can be commonly portrayed as the dynamic procedure whereby people manage the level of their receptiveness to other people [4].

2. Literature Review

Data Center Compliance Standard

Basically, there are vast amount of compliance standards available for data center environments. These security compliances existing to cater certain aspects of the data center operational and to maintain its credibility as a date center hosting thousands of servers. Compliance will be given upon a certain criterion being fulfilled or all the business continuity process has been fulfilled [5]. There are a few standards that are closely related to data center, namely Uptime institute certification, ISO/IEC 27001 information security management system standard, EN 50600 and COBIT [3].

Uptime Institute is the main association that affirms data center structures, facilities and operations to the Tier Classification System (I-IV) and Operational Sustainability criteria [6] Uptime Institute has granted 864 certifications in 83 nations around the globe as shown in Figure 1. Uptime Institute is a worldwide expert on server farm and it assists with designing data center that advance granted to different enterprises, governments and colleges. Tiers additionally gives a technique to benchmark the data center. There will never be a one-size-fits-all answer for a data center. This strategy for accreditation enables one to alter the solution for meet the prerequisites of the project. Tiers is acknowledged and regarded around the world. There are no contentions with region code or guidelines. Tier certification terminates two years after the award date. This forces the association to consistently improve its strategies to adjust to the emerging innovation. Uptime Institute likewise gives documentation and instruction to the proprietors and administrators of data center so as to create skill in this field. This guarantees precise everyday activities of the data center [6].

ISO 27001 certifications focuses on ensuring robust information security management system (ISMS). This certification is also widely accepted internationally security accreditation by International Organization for standardization (ISO) and international electro technical Commission (IEC) [7]. ISO 27001 is the accreditation is awarded if the organization has implemented, operates and retains the information security management systems (ISMS) together with risk assessment and meet management objectives [8][9]. Information system Management System is a methodical way to deal with overseeing delicate organization data so it stays secure. It incorporates individuals, procedures and IT frameworks by applying a hazard the executive's procedure. It can support little, medium and huge organizations in any part keep data resources secure [10].

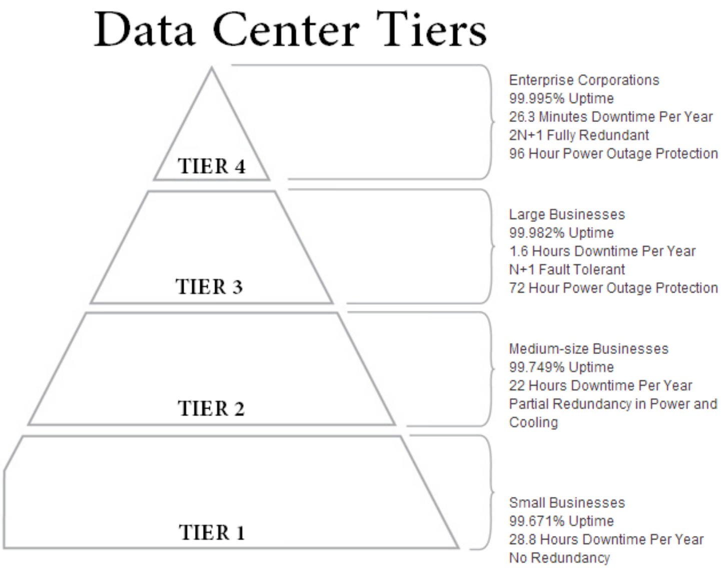


FIGURE 1. Uptime Institute Tiers

The European EN 50600 series “Information Technology - Data center facilities and frameworks" as of now contains seven models that were affirmed by the European Committee for Electrotechnical Standardization (CENELEC) somewhere in the range of 2012 and 2016. The English rendition is distributed by the British Standards Institution (BSI) [11][12]. There are five (5) series in EN 50600 standard. Following Table 1 will provide an overview of the series of EN 50600 components.

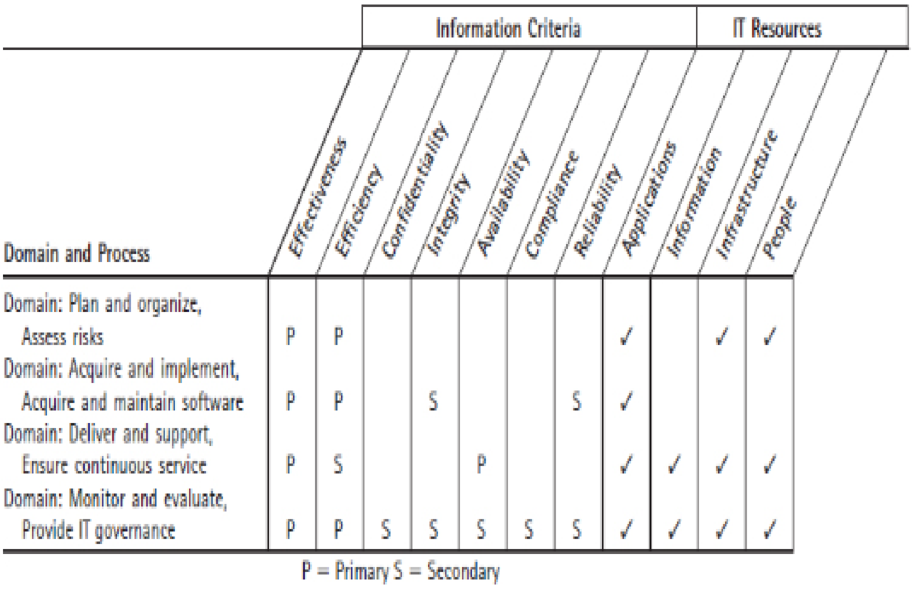
TABLE 1. EN 50600

Publication	Description
EN 50600-1	Defines the operations of the data center
EN 50600-2	Defines the requirements for the data center design.
EN 50600-3	Defines the requirements for the operation and the management of the data center.
EN 50600-4	Defines the key performance indicators for the data center
EN 50600-99-X	Technical Reports cover recommended practices and guidance for specific topics around data center operation and design.

There are several scopes of EN 50600 standards. This standard is mainly focused on to portray the general standards for server farms whereupon the prerequisites of the EN 50600 arrangement is based, characterizes the normal parts of data center including terminology, parameters and reference models (practical components and their convenience) tending to both the size and multifaceted nature of their proposed reason. Besides, it also portrays general parts of the offices and frameworks required to help data center. Determines an order framework, in view of the key criteria of "accessibility", "security" and "energy efficiency" over the arranged lifetime of the data center, for the arrangement of viable offices and infrastructure [14].

Moreover, subtleties the issues to be tended to in a business risk and working cost analysis enabling application of the characterization of the data center provides reference to activity and the executives of data center and presents the ideas of Key Performance Indicators (KPIs) for resource management of data center facilities and infrastructure.

Control Objectives for Information and Related Technology (COBIT) is created by Information Systems Audit and Control Association (ISACA) as shown in Figure 2. COBIT is a worldwide proficient participation relationship for people intrigued or utilized in IT review, IT hazard, and IT administration fields. ISACA was established in 1967 and has developed into a universally perceived association which as of now checks in excess of 150,000 individuals around the world. COBIT was at first created to support (money related) review experts who were progressively faced with computerized situations. ISACA discharged the primary version of COBIT in 1996 as a structure for executing IT review assignments. COBIT was formed further into a more extensive IT management framework [15][16]. It is firmly lined up with and supplements COBIT, yet conveys an incentive to undertakings in its own right. While COBIT guarantees that IT is filling in as adequately as conceivable to expand the advantages of innovation speculation, Val IT assists endeavors with settling on better choices about where to contribute, guaranteeing that the speculation is predictable with the business system [15][16].



	Information Criteria							IT Resources			
Domain and Process	Effectiveness	Efficiency	Confidentiality	Integrity	Availability	Compliance	Reliability	Applications	Information	Infrastructure	People
Domain: Plan and organize, Assess risks	P	P						✓		✓	✓
Domain: Acquire and implement, Acquire and maintain software	P	P		S			S	✓			
Domain: Deliver and support, Ensure continuous service	P	S			P			✓	✓	✓	✓
Domain: Monitor and evaluate, Provide IT governance	P	P	S	S	S	S	S	✓	✓	✓	✓

P = Primary S = Secondary

FIGURE 2. COBIT Framework

Threats in Data Center

Internal threats happen when somebody has approved access to the system with either a record on a server or physical access to the system. A danger can be internal to the association as the after effect of worker activity or disappointment of an association procedure [17]. External threats can emerge from people or associations working outside of an organization. They don't have approved access to the PC frameworks or system. The clearest outside dangers to information systems and the inhabitant information are catastrophic events: storms, flames, floods and seismic tremors. Outer assaults happen through associated systems (wired and remote), physical interruption, or an accomplice arrange [17]. This class incorporates dangers brought about by human activities, for example, insiders or programmers which cause damage or hazard in information system [17].

Ecological dangers are dangers brought about by non-human. It comes, first, from cataclysmic event dangers like earthquakes, flood, fire, lightning, wind or water and, likewise, because of creatures and natural life which cause serious harm to information system like floods, lightning, tidal waves (like Tsunami) and fire. In reality, this class incorporates other dangers, for example, uproars, wars, and psychological oppressor assaults [18]. Technological threats are brought about by physical and concoction forms on material. Physical forms incorporate the utilization of physical intends to pick up section into confined zones, for example, building, compound room, or some other assigned region like burglary or harm of equipment and programming. Not with standing, compound procedures incorporate equipment and programming advances. It, additionally, incorporates indirect system gear like power supplies [18].

Security Compliance and Framework Issues and Challenges

Physical or environmental security domain addresses the threats, vulnerabilities, and countermeasures that can be utilized to physically protect an enterprise’s resources (people, facility, data, equipment, support systems, media, supplies) and sensitive information [19][20]. Permission to access a resource is called authorization [21]. Physical security often refers to the measures taken to protect building, systems and the related supporting infrastructure against threats that are linked to the physical environment [5].

Several issues and challenges in framework and compliance relate to perimeter protection and access control subject to risks associated with data center requires more attention to avoid future threats to assets [22][23]. Dangers may happen from outer or potentially inner of the border, for example, unapproved access through passage purposes of the structures. Consequently, such activity to restrain the quantity of passage focuses and decrease its quantity considerably further twilight or amid the end of the week when not the same number of representatives are around are significant so as to avoid vulnerabilities/holes made in the advantages' security and relieve interruption for affecting the benefits' misfortune or harm [23].

The basic security compliance that can be obtained and practiced for a data center is ISO/IEC 27001 which covers the physical aspect, people, processes and technologies are in place, and facilitates a proactive approach to managing security and risk and through the observations that SME companies are not ready to adopt ISO27001 as many gaps were identified [24]. The gaps are, the companies require to interdepend on each other (vendor, client and users), as more emerging technologies occur, it's getting more competitive to adopt emerging and immature technologies which may carry security threats and an augmenting hole between expanding dangers and the inadequacy of countermeasures to adapt to them [25]. Even if compliance is followed and implemented it solely diminished by human factor [26].

There was one occurrence happened where The United States office of personnel management had data breaches twice ranging from 4.2 million to 18 million United States personnel's data were exposed [8]. This data breach happened from the year 2014 as the first occurrence and 2015 were the second occurrence while doing the investigations this was identified due to lack of investments on modern technologies and poor management from the institutions [8]. These circumstances can be well-overseen if the associations practice a successful physical security framework ISO 27001, intrusion surveillance, layered security, and systems integration [9]. ISO27001 is a standard setting out the necessities for a data security management framework. It helps identify, manage and limit the scope of dangers to which data is routinely oppressed.

An information security management system (ISMS) is a methodical way to deal with overseeing delicate data so it stays secure. Data security does not finish at actualizing the most recent firewall, or employing a 24-hour sub contracted security firm. Rather, the general way to deal with data security and incorporation of various security activities should be overseen all together for every component to be best. That is the place a data security the management framework comes in. It permits organizing your security endeavours successfully [28]. As a conclusion, ISO 27001 is good but it doesn't comprise and does not tackle all the aspects of information security components and it is manipulative as well as require fast adaptation on the changes or emerging technologies.

3. Research Methodology

Semi Structured interview from qualitative research methodology is chosen to be used to conduct the research in order to achieve the research objectives by conducting the interview with a number of interviewees. Field setting, detailed method uses and also sample interview questions are being discussed in the following. This method was chosen as this research will seek for expert reviews and interviewing would be the best fit in order to measure and understand the environment better from the organization staffs and security members. Figure 3 illustrates the research procedures compromise of four stages which are literature review, Qualitative data collection and analysis, proposed model and reporting.

This research will be conducted using the semi structured interview approach from the qualitative research methodology. Data is collected through interview to identify the factors contributing to information security compliance framework in data center. To develop the information security compliance framework then analysis will be conducted on interview results to evaluate and suggest an information security compliance framework to ensure research objectives are achieved.

This research is performed using the Qualitative Research Design approach. The interview is then to gather further information on the understanding and to understand further about the data center operation and information security compliance framework.

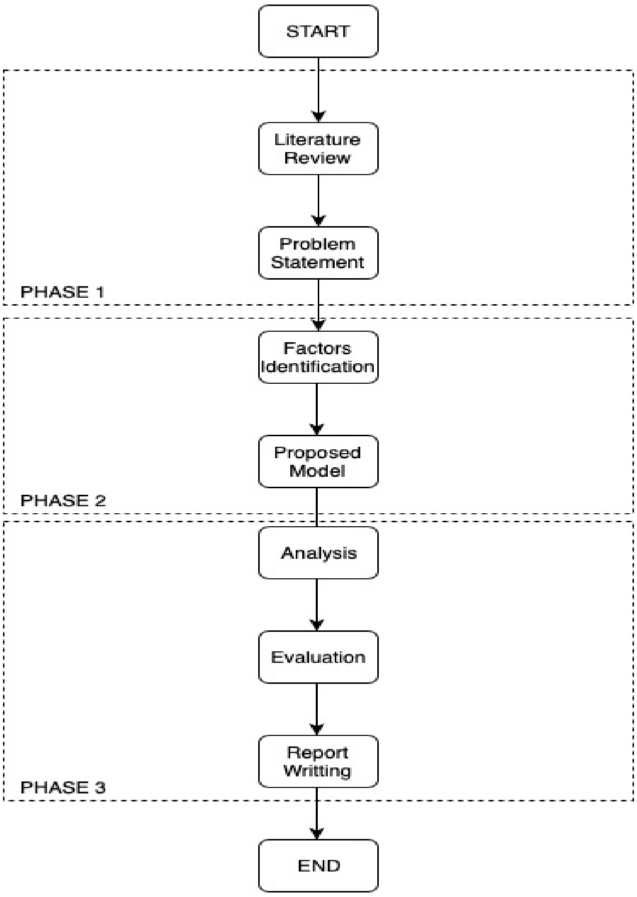


FIGURE 3. Research Procedure

Based on the identified weaknesses or deficiencies in the existing information security compliance framework, literature review was done to provide recommendations on the required information security compliance framework. Literatures related to information security compliance framework have been searched in the Internet and Google Scholar database. Searches has also been done using UTM's e-Journals, e-Books, and online databases. The literatures were searched using combination of keywords "ISMS", "ISO 27001", "Security Framework Data Center", "Data Center Compliance", "Data Center Security Challenges", "information security standards", "information security compliance for data center "and "Basic Compliance of Data Center". Literatures from established international standards and best practices such as Uptime institute certifications, ISO 27001, EN 50600, COBIT, have also been reviewed.

4. Proposed Framework

Based on the literature review, Figure 4 below is the proposed information security compliance framework to safe guard the date center environment and obtain compliance for the data center. As the main objective of this research is to identify the current gaps on information security compliance in data center, to develop appropriate information security compliance framework in data center and to validate the proposed information security compliance framework for data center. The proposed model contains a combination of three compliance model and standards. ISO27001, EN 50600 and also Uptime Institute. As this proposed model may cater all three segments in terms of high-level information security, data center facilities and infrastructures as well as tier certifications correlates infrastructure availability.

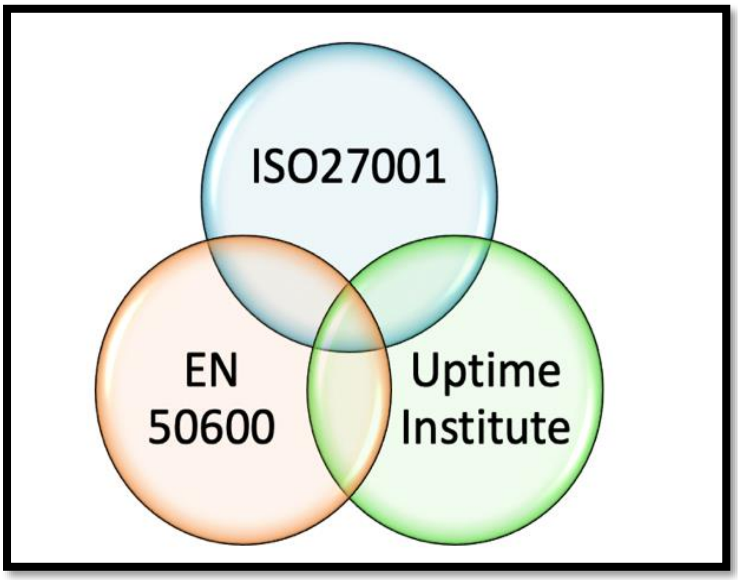


FIGURE 4. Proposed Framework

This proposed framework will have an interrelation between those three models to achieve the state-of-the-art data center information security compliance. ISO27001 covers the high level but not the specific segment of the components, however EN 50600 and uptime institute standards do focuses on data center facilities and data center tier on the availability. We can conclude that there are number of security features do overlap all three security standards. However, the private sector is much more beneficial from the implementation and development of ISO27000 and EN 50 600. Unique security feature from EN 50 600 and Uptime Institute adds up to the gaps on 27001 which then fulfills fifty-one (51) security features making it as a robust information security compliance framework to be adapted by the industry or data centers.

There are many components involved in the proposed framework. The description of each components as per will be elaborated further as illustrated in Figure 5. Security policy, A lot of approaches for information security must be characterized, endorsed by the board, distributed and imparted to workers and applicable to external parties. The strategies must be driven by business needs, together with the appropriate guidelines and enactment influencing the association as well [27]. Organizational security, to set up a management framework to start and control the execution and activity of data security inside the association. Asses classification and control, any assets related with data and data handling offices should be recognized and oversaw over the existence cycle, consistently updated. A register or stock of those advantages must be assembled that shows how they are overseen and controlled, based around their significance [27].

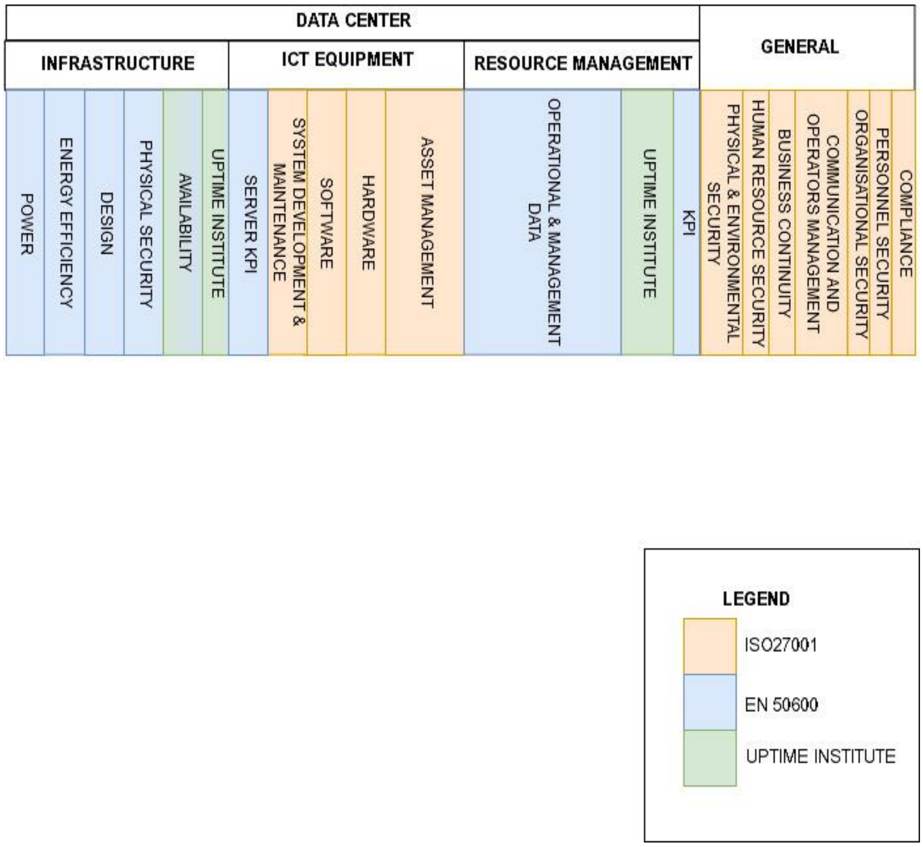


FIGURE 5. Breakdown of Proposed Framework

Access control, an access control strategy must be set up, recorded and investigated routinely considering the necessities of the business for the benefits in scope. Access control rules, rights and confinements alongside the profundity of the controls utilized ought to mirror the data security hazards around the data and the association's risk for overseeing them. Put essentially get to control is about who has to know, who needs to utilize and the amount they gain admittance to. Compliance, a decent control depicts how all important administrative statutory, administrative, legally binding prerequisites, and the organizations way to deal with meet these necessities ought to be unequivocally distinguished, reported and updated with the latest for every information system in the association. Put in straightforward terms, the association needs to guarantee that it is staying up with the latest with and recording enactment and guideline that influences accomplishment of its business destinations and the results of the ISMS [27].

EN 50600 represents to the main European standard that uses an all-encompassing way to deal with make thorough particulars for the new development and activity of a data center. It characterizes necessities for the development, power supply, cooling and ventilation, cabling, security frameworks, and characterizes criteria for the activity of data center. Uptime Institute, Uptime Institute Tier Certification gives an autonomous, demonstrated proportion of the capacity of your foundation to meet the presentation level your business relies upon. With Tier Certification, data center will have the option to convey the business benefits the organization needs, all day every day. Tier Standards are a fair arrangement of foundation and working criteria that are one of a kind in the business for their thoroughness and completeness. No other accreditation conveys the weight and stature of Tier Certification, and no other data center standard is really affirmed by the standard's creator itself. Personnel security, the goal is to guarantee that workers and contractual workers comprehend their duties and are reasonable for the jobs for which they are considered. It likewise covers what happens when those individuals leave or change jobs. Physical and environmental security, the goal is to guarantee that workers and contractual workers comprehend their duties and are reasonable for the jobs for which they are considered. It likewise covers what happens when those individuals leave or change jobs [27].

System development and maintenance, Security prerequisites of information system. The target is to guarantee that data security is a basic piece of information system over the whole life cycle. This additionally incorporates the prerequisites for information system which are provided over the internet. Communication and operation management, Network security management. The goal is to guarantee the insurance of data in systems and its supporting data handling offices. Business continuity management, Information security progression. The target is that information security coherence will be installed in the association's business continuity management systems [27].

5. Conclusion

This study is to determine the appropriate information security compliance framework for data center in utility company. The framework could be improved by incorporating more adaptation from other standards. This research only examines the critical standards require for information security. The following are the contributions of the proposed framework to existing literature on information security compliance framework for data center in utility company it is to be a major attempt at identifying a comprehensive security framework which meets the compliance and secure the environment even further.

References

1. Achmadi, D. Suryanto, Y & Ramli, K. (2018). *On Developing Information Security Management System (ISMS) Framework for ISO 27001-based Data Center*, 2018 International Workshop on Big Data and Information Security (IWBIS), Jakarta, 149-157.
2. Sayana, S.A. (2003). Approach to Auditing Network Security, *Information Systems Control Journal*, 5.
3. Doelitzscher, F. (2014). *Security audit compliance for cloud computing*.
4. Krishnan, R. (2017). *Security and Privacy in Cloud Computing*. Master's Thesis.
5. Trappe, W. (2015). *The challenges facing physical layer security. IEEE Communications Magazine*. 6, 16-20.
6. Boehmer, W. (2008) Appraisal of the efectiveness and efciency of an information security management system based on ISO 27001. *The second international conference on emerging security information, systems and technologies*. IEEE, 224–231.
7. Brenner, J. (2007). *ISO 27001: Risk Management and Compliance*.
8. Ismail, W., Alwi, N.H.M., Ismail, R., Bahari, M. and Zakaria, O. (2018). Readiness of Information Security Management Systems (ISMS) Policy on Hospital Staff Using e-Patuh System. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*. 10, 47-52.
9. The Stationery Office. (2007). *Office of Government Commerce, Service Operation Book (Itil)*. No. 978-0113310463.
10. Haes. D, Van Grembergen S., , Joshi. W. A. & Huygh, T. (2020). *COBIT as a Framework for Enterprise Governance of IT.* Springer, Cham.
11. Purba, A. & Soetomo. M. (2018). *Assessing Privileged Access Management (PAM) using ISO 27001: 2013 Control*. ACMIT Proceedings. 5, 65-76.
12. Ramgovind, S. Eloff, M & Smith, E. (2010). *The management of security in Cloud computing.* 10.1109/ISSA.2010.5588290. 1-7.
13. ISO. (2019). *ISO/IEC 27001 Information security management. From https://www.iso.org/isoiec-27001-information-security.html.*
14. Van Grembergen S., , Joshi. W. A. & Huygh, T. (2020). *Enterprise governance of information technology*. Springer, Cham. 25-162.
15. Mubashir, A. S. (2014). Integration of information security essential controls into information technology infrastructure library-A proposed framework. *International Journal of Applied*. 4.

16. Singhal, H., and Kar, A. K. (2015). *Information Security concerns in Digital Services: Literature review and a multi-stakeholder approach*. International Conference on Advances in Computing, Communications and Informatics (ICACCI), IEEE. 901-906.
17. Gergely, A. Claude C. & Lecat. W. (2011). *Protecting against physical resource monitoring*. Proceedings of the 10th annual ACM workshop on Privacy in the electronic society (WPES '11).
18. Tipton, H.F., & Hernandez, S. (2012). *Business Continuity & Disaster Recovery Planning.*
19. Bauer, L. and Kerschbaum, F. (2014). *What are the most important challenges for access control in new computing domains, such as mobile, cloud and cyber-physical systems?* Proceedings of the 19th ACM symposium on Access control models and technologies. ACM. 127-128.
20. Silva, F. F. & Carlos, A.G.F. (2014). *Smart City Security Issues: Depicting Information Security Issues in the Role of an Urban Environment.* Proceedings of the 2014 IEEE/ACM 7th International Conference on Utility and Cloud Computing (UCC '14). IEEE Computer Society. 842-847.
21. Lavy, S. & Dixit, M.K., (2010). Literature review on design terror mitigation for facility managers in public access buildings. *Facilities*, 28, 542-563.
22. Fomin, V.V., Vries, H. & Barlette, Y. (2008). *ISO/IEC 27001 information systems security management standard: exploring the reasons for low adoption*. EUROMOT 2008 Conference, France.
23. Y. Barlette & V. V. Fomin. (2008). *Exploring the Suitability of IS Security Management Standards for SMEs*. Proceedings of the 41st Annual Hawaii International Conference on System Sciences (HICSS 2008). 308-308.
24. Kurnianto, A. Isnanto R.& Aris P. W. (2013). *Assessment of Information Security Management System based on ISO/IEC 27001:2013 On Subdirectorate of Data Center and Data Recovery Center*. Ministry of Internal Affairs E3S Web Conf.
25. ISO. (2019). *ISO/IEC 27001 Information security management, from https://www.iso.org/isoiec-27001-information-security.html.*
26. Nobody at OPM to blame for massive data breach.(2015), *from https://www.usatoday.com/story/news/politics/2015/06/23/opm-hack-senate-archuleta-hearing/29153773/*
27. *What Is Information Security*. (2019).*Cisco. From https://www.cisco.com/c/en/us/products/security/what-is-information-security-infosec.html.*