Network Security Policy for Higher Education Institutions based on ISO Standards

Jonard B. Bolanio[1], Rolysent K. Paredes[2], Alberto L. Yoldan Jr.[3] & Roy E. Acapulco II[4]

[1,3,4]Management Information Systems, Misamis University, Ozamiz City, Philippines.
[2]College of Computer Studies, Misamis University, Ozamiz City, Philippines. Email: rolysent@mu.edu.ph*

DOI: http://doi.org/10.46382/MJBAS.2021.5101

Article Received: 19 October 2020 *Article Accepted: 01 February 2021* *Article Published: 10 February 2021*

ABSTRACT

Computer network plays a very important role in any organizations or institutions. It becomes a necessary tool, useful for communications, and can be utilized in storing data in various forms and at various locations. However, it intrinsically at risk to breaches from both internal and external attacks, and because of that, there should be an appropriate implementation and management of the network and its security. The study aimed to assess the employed network security of the higher education institutions (HEIs) and check if they conform to the six parts of ISO 27033 international standards. Standardized ISO 27033 assessment questionnaire was the main tool in gathering the data and the respondents were the network security team members of the five (5) HEIs. Results showed that HEIs did not mostly conform to the ISO 27033 requirements. Hence, to have a better guide and implementation of the institutions network security, a network security management policy based on ISO 27033 must be in place.

Keywords: *Network assessment, Protection, Policies, Conformance, Network tool.*

I. Introduction

Computer networks have become necessary tools, useful for communications and can be utilized in storing data in various forms and at various locations [1]. However, computer network systems have been shown in various studies to be characteristically susceptible to breaches from many attacks [2] and network security is one of the most volatile and dynamic entities for enterprises, influenced by technology change trends and with the shifting threat vectors and more sophisticated application level advanced threats [3].

The Internet Security Threat Report (ISTR) of Symantec [4] shows that in 2015 the number of zero-day vulnerabilities revealed more than doubled to 54, a 125 percent increase from the year before. Or a new zero-day vulnerability was found every week in 2015. Cisco published its annual security report, which compares the 2015 survey results with those of 2014 [5]. Cisco found out that chief security officers (CSOs) and security operations (SecOps) managers are less confident that their security infrastructure is up to date, or that they are able to thwart attacks. With the growing numbers of threats and attacks in security, protecting all important resources in the organization or institution is another necessary concept that is needed of any computer systems [6] but protection alone by technical means is not sufficient and needs to be supported by a policy [7]. This policy can be a structure to have a well-established and secured infrastructure which would assist in making the computer network safe from all kinds of intrusion [8].

A security policy comprises a set of objectives for an organization whether commercial or educational, and it is a living document which means that the document is never done and is constantly revised as technology and employee requirements change [9]. An example of this security policy is the network security management policy for Information and Communication Technology (ICT). The network security management policy is imperative to be able to preserve the reliability, authenticity and dependability of a system or network, its data, and its direct environmental infrastructure [10].

In education settings, a network security management policy is to determine administrative control, procedural requirements, and technical support to ensure the proper protection of the university's information handled by computer networks [11]. It facilitates to safeguard the integrity of and alleviate the risks and losses associated with security threats to inside the university's IT resources, including their data that are connected to the network [12]. Thus, it is essential to offer a reliable campus network to conduct the university's business and avoid illegal access to institutional, research or personal data [13]. However, most of the network security measures and policies are not yet incline with any international standards like ISO 27033 since in developing countries, implementation of international standards are still rare [14].

The ISO/IEC 27033 international standard provides detailed support on the security aspects of the administration, process and use of information system networks, and their inter-connections [15]. Further, those individuals within an organization that are accountable for information security in general, and network security in particular, should be able to adjust the standard to meet their particular requirements. ISO 27033 has six parts namely: (1) ISO/IEC 27033-1:2015 - Network security overview and concepts [16], (2) ISO/IEC 27033-2:2012 - Guidelines for the design and implementation of network security [17], (3) ISO/IEC 27033-3:2010 - Reference networking scenarios – threats, design techniques and control issues [18], (4) ISO/IEC 27033-4:2014 - Securing communications between networks using security gateways [19], (5) ISO/IEC 27033-5:2013 - Securing communications across networks using Virtual Private Networks (VPNs) [20], and (6) ISO/IEC 27033-6:2016 - Securing wireless IP network access [21].

Hence, to continually improve the network security of the higher education institutions, an assessment is conducted to the network utilizing the ISO 27033 standards which assessed the level of security of the network. In addition, the study aimed to give inputs to the network security team of the institution by developing a Network Security Management Policy. Thus, a policy cycle model designed by Young and Quinn [21] was utilized to develop such policy. The policy which is based on ISO 27033 international standards can be used by any Higher Education Institutions and it can be a tool to review and assess their current network security policies. Furthermore, it can contribute in enhancing the poorly secured and managed network infrastructure of the institution and should improve the capabilities of the network security teams in dealing with many issues that they may face in the schools network.

II. Related Literature

Keane et al, [2] revealed that computer networks are vulnerable at all often derives from the actual users and administrators of the systems. As IT managers differ on the makers for security in their products, so does the hacker hang on the manufacturers for exploitable vulnerabilities in their products. The IT administrator considers for particular behavioral strengths in end-users while the hackers look for behavioral weaknesses in the same end-users. The totality in the safety of the network lies in the balance between the IT administrator's knowledge/skills and the hacker's knowledge/skills as well.

According to Mohammed et al, [6], network security and management policy in communication is the need to preserve the reliability, validity and stability of a system or network, its data and its immediate environmental infrastructure. Well established and secured infrastructure would benefit in no means making the network secure from all forms of intrusion. Safeguarding all these assets is another significant concept that is required of any computer system. Further, Brophy [22] said that a day-to-day checking is going to be critical to having a secure infrastructure. In the layered defense method to network security, network monitoring acts as the tripwires that notify IT that there is a minor problem - before more a serious issue occurs.

A campus network is a valuable part of campus life and network security is essential for a campus. Campus network faces challenges to address core problems of security which are governed by network architecture. Secured network defends an organization from security attacks associated with network. A university network has a number of uses, such as teaching, learning, research, management, e-library, result publishing and connection with the external users. Network security will thwart the university network from distinct types of threats and attacks [23].

Oguntunde [24] reviewed or assessed the challenges the University of Ibadan (Nigeria) Information Technology Unit has faced from inception till present which can be applied to provide better support for the completion of the University ICT goals. Further, the study delivers few suggestions such as to how the network can beat its challenges for better realization of the set institutional goals and policy as well. Policy-motivated management especially for the network and security management is getting popular today, primarily due to the ever-growing scale and density of large networked systems. In these structures, policies are typically employed to streamline the tasks of the system management, thus making way for further system enlargement [25]. A security policy includes a set of ideas for an institute whether commercial or educational, and it is a dwelling document which means that the document is never completed and is endlessly revised based on the current requirements [9]. Policies can be derived from international standards like ISO since they are more easily implemented and well recognized. Thus, compliance to the international standards is highly recommended with a variety of reasons. Moreover, the standard is designed in order to assure the privacy, reliability and accessibility of ICT assets [26]. In addition, there is an extreme need of standardization which regulates governance over security. Young and Quinn [21] developed policy cycle model which guides, or heuristic, for policy enhancement; it makes a system and a rhythm to a world that might otherwise be found chaotic and unordered [27], [28]. Thus, a policy cycle is a unceasing method or iterative and collective [13], therefore the need to monitor the implemented policy is very much necessary.

III. Research Framework

The research framework of the study is anchored on the policy cycle model designed by Young and Quinn [21]. A policy cycle is a guide, or empirical, for policy advancement; it takes a system and a rhythm to a world that might otherwise appear chaotic and unordered [27, 28]. The steps of the policy cycle are: agenda setting, policy formulation; and policy implementation and monitoring. Figure 1 shows the research framework of the study.

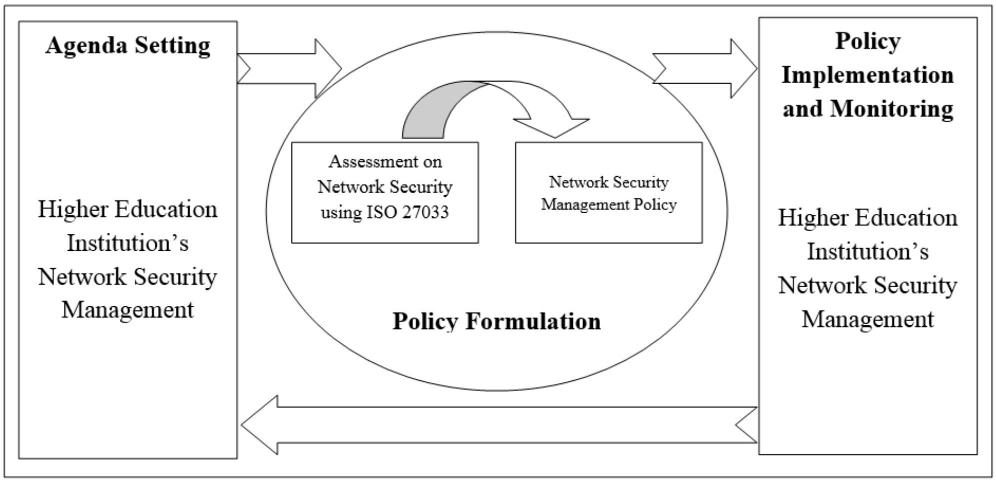
Agenda Setting
Higher Education Institution's Network Security Management
Assessment on Network Security using ISO 27033
Network Security Management Policy
Policy Formulation
Policy Implementation and Monitoring
Higher Education Institution's Network Security Management

Fig.1. Research Framework of the Study

A. Agenda Setting

As a starting point in making a policy, problems or issues must be identified with regards to the higher education institutions network security management which requires solutions. The phase deals as well in reviewing the current network security policy of the institutions for the purpose of revisions.

B. Policy Formulation

To have a proper support to the identified problems, an assessment to the current network security is done. Standardized questionnaire was given to the network security teams from different schools or institutions. Questions from the questionnaire are derived from ISO 27033 standards. Once the nature of the problem is sufficiently detailed, a draft to a new or revised policy is done. This paper formulated a suggested policy which can be used by any higher education institution. This policy is subject for approval by the management.

C. Policy Implementation and Monitoring

In the policy implementation and monitoring phase, the policies are implemented whereby an actual action is taking place. In the other side, an on-going process of monitoring is also conducted. Thus, a policy cycle is a continuous process or iterative and collaborative [27], therefore the need to monitor the implemented policy is very much necessary. Further, monitoring is a great help in establishing the usefulness of the employed network security policies, and in presenting the basis for recommendations and potential decision-making.

IV. Results and Discussions

A. ISO 27033 Standards-Evaluation Results

Table 1 presents the results of an assessment on the network security management of the five (5) higher education institutions that are included in the study. The results are rank from highest to lowest according to the positive responses of the respondents.

Table I: Assessment on the Network Security Management

Indicators	Assessment Results	
	Yes	No
The institution and its context	4	1
Needs and expectations of interested parties	7	3
Scope of the network security	7	3
Roles and responsibilities	7	3
Design and implementation of the network	15	10
Network security policy	5	5
Wireless network security	21	29
Security and support controls	53	97
Documented information	4	11
Awareness and communication	2	8

Operational planning and control	3	17
Network security risk and controls identification	4	26
Corrective action and continual improvement	5	40
Internal Audit	1	19
Monitoring, measurement and evaluation	0	15
Management Review	0	15

Table II: Network Security Management Policy

Network Security Policy
Network Security Organization/Team in the HEIs
a. The university/college president is mainly responsible for the security.
b. The Chief Security Officer (CSO) or Chief Operating Officer (COO) is responsible for forming, keeping, executing, managing, and understanding organization-wide network systems security policies, standards, guidelines, and procedures. Thus, the COO and other members of the team, shall execute network risk evaluations, prepare network systems security plans, evaluate network security products, and perform other activities necessary to assure a secure computer network environment.

c. Network Architects and Designers or Network Engineers are liable for establishing, preserving and adapting an IP network's hardware, software and virtualized components. They are also required to maintain expert-level knowledge regarding network hardware and software technology, and they must also be able to convert a network's technological requirements into solutions that benefit an organization or institution.

d. Network Managers are responsible for maintaining and installing the school's computer networks. They are also responsible to train staff to provide first rate technical support. They should have a recovery plan in mind to lessen any trouble to the business transactions.

e. Network Security Officers are in charge with the physical security and individual safety. They are accountable for managing investigations into any suspected computer or network security compromises, incidents, or problems with the members of the network department. All potential compromises must be reported immediately to the Chief Operating Officer (COO). These persons are responsible for establishing appropriate user privileges, monitoring access control logs, and performing similar security actions for the networks they administer.

f. Network Administrator or systems administrator is accountable for preserving an institution's computer network running smoothly and up to date. An organization that uses multiple computers or software platforms needs a network admin to coordinate the different systems.

g. Network Technicians are information technology professionals involved in numerous businesses to build and troubleshoot computer networks. They focus on setup, repair, and troubleshooting of both hardware and software products incorporated into the institution's operations.

h. Directors and Deans are to guarantee that proper communication and computer system security measures are observed in their areas. Thus, distributing enough resources and time to meet the requirements of the policies, departmental managers are responsible for ensuring that all employee users were aware of institutional policies related to computer and communication system security.

i. The Dean shall ensure that students observe proper computer and communication system security measures. The Dean is accountable for ensuring that all student users are aware of the institutions policies related to computer and communication system security.

j. Users are responsible for conforming with this policy and all other institutional policies relevant to network security measures. All users also are responsible for bringing all known information security violations and vulnerabilities that they notice to the attention of the network department.

Network Security and Supporting Controls

a. The network security team performs activities concerning the security of the network. Thus, a key requirement for any network is to maintain it through the safety management activities, which initiates and

monitors the implementation and operation of safety. The activities include: - identification of all duties related to network security and the appointment of a person responsible for security - documented network security policy, together with documented specialized security architecture - documented SecOPs - compliance check security, including security testing, to provide assurance that security is maintained at the required level - documented conditions of security for network connections that must be met before you will receive, if necessary, permission to connect to the employees of the organization, or outside organizations or persons - documented conditions of security for remote network users - management of network security incidents plan - documented and tested plans to ensure business continuity / recovery interrupt; - the rules of safe use of specific network resources, services and applications - the consequences of noncompliance of safety rules - relations organizations to misuse the network; and the rationale of policies and specific safety rules
b. The network management team regularly monitors the network since it is very crucial to network management [30]. Thus, network monitoring is a process of ongoing monitoring and verification of recorded data on the network activities and operations, including audit trails and dangers, and the detailed analysis. Monitoring that includes: - audit logs of firewalls, routers, servers, etc. - danger warnings or alarms of audit trails, preconfigured for notification of certain events, for example, firewalls, routers, servers, etc. - the output of the intrusion detection systems - the results of operations for the scanning of network security - information on events and incidents reported by users , and support staff - the results of the security compliance audits.
c. The network management team performs periodic network security assessment because it is one way to look at the current state of the network, and determine if any new vulnerability exist, or if any policies or procedures can be refined to achieve a greater level of security. Further, the team executes systematic steps to audit existing security measures and monitoring and controls about the set of control points, including security testing vulnerability scan, etc.

d. There should be a technical vulnerability management which includes timely information about technical vulnerabilities, assessment of exposure to networks such vulnerabilities, the definition of appropriate measures and means of control and security management to address the issue associated with these vulnerabilities, and the implementation and verification of specific measures and means of control and security management.

e. To have a protected network, identification, and authentication of the users in accessing the network are necessary [31]. Both should be applied to remote login, enhanced authentication, and a secure one-time sign-on. Thus, a proper monitoring of these users is mandatory.

f. It is vital to ensure the effectiveness of network security through the conduct of audit trails and continuous monitoring of the rapid detection, investigation and notification of security events and response to them, and then on the incidents. Without conducting audit trails and continuous monitoring cannot be sure of the continued effectiveness of measures and network security monitoring and management tools, as well as the fact that security incidents will not occur with the resulting adverse effects on the operation main activities of the organization.

g. To counteract the institutions computer and networking attacks and misuses or an attempt to compromise CIA (Confidentiality, Integrity and Availability), intrusion detection systems have become a demanding component in terms of computer and network security. Thus, there are many commercial intrusion detection systems available today [32]. Thus, intrusion detection is the method of monitoring the events happening in a computer system or network, and examining them for signs of intrusions. With that, intrusion detection can prevent disastrous events that may happen in the network or computer systems [33].

h. Typically, web, email and other applications that can be accessed immediately through the internet are placed in demilitarized zone (DMZ) or perimeter network. The purpose of a DMZ is to add an additional layer of security to the institution's internal network; an external attacker only has access to equipment in the DMZ, rather than any other part of the internal network.

i. The institution has a business continuity management since it is important to measure and control and management tools used to ensure confidence in the continuity of the functioning of the organization in the event of a disaster by providing the conditions for the possibility of restoring each part of the process of the main activities of the organization after the breach of its stroke, the corresponding time interval.

j. The network security team is responsible in utilizing stateless packet filtering, stateful packet inspection, application firewall, content filtering, intrusion prevention system and intrusion detection system, and security management API in the institutions network.

k. The network security team with the used of intrusion detection systems, monitoring, audit logging etc. must be able to handle illegal access, packet sniffing, rogue wireless access point, denial of service attack, bluejacking, bluesnarfing, and threats brought by Adhoc networks.

Design and Implementation of Network Security
a. To guide the network security team in planning and employing a concrete security to the network, a reference architecture like ITU-T X.805 [34] can be their basis. Thus, it can help in securing the whole IT infrastructure.
b. There are a clear criterion in choosing the products or vendors and the network components to be used.
c. During the application of the network security, the network security team must have a proper network management, logging, monitoring, and incident response.
d. A proper documentation is required during the implementation.
e. There is an identification of assets which include both information and network assets.
Threats, Design Techniques and Control Issues
a. Since internet gives a competitive advantage to the institution by having it fully utilized by the students, faculty, staff, and other users, it is a responsibility of the network security team to manage the threats associated to/from these users.
b. With the help of the intrusion detection systems, audit logging, network monitoring, technical vulnerability management, firewall protection, proper network security design and implementation, and other network security techniques or appliances, threats can be managed or controlled pertaining to the institutions business to business services, business to customer services, mobile communication, and outsourced services.
c. The network security team is responsible in designing techniques and control issues related to threats. But, those are already been included during the planning of the network security with the use of a reference architecture. Thus, a reference architecture determines security issues that need to be addressed to prevent both intentional threats as well as accidental threats. These threats are: - destruction of information and/or other resources; - corruption or modification of information; - theft, loss or removal of information and/or other resources; - disclosure of information; - interruption of services.
d. To prevent threats, the institution has a strong policy in regulating the use of the internet and make sure that all users utilize it for educational and professional purposes in accordance with the mission statement of the institution. Since bandwidth is shared by all users, users must make reasonable efforts to use this resource in ways that do not negatively affect other employees and students (SANS, 2013). Thus, all campus users must act in a responsible, efficient, courteous and legal manner.
e. All outsourced services that may use the institutions internet or network are subject for monitoring, audit

logging etc. If an update or any transactions that will be done remotely, a temporary username and password will be given to the vendor or a person that will handle the updates which will be deleted once all tasks are finished.
Securing Communications between Networks using Security Gateways
a. The network security team is responsible in implementing security gateways in the institution. This is considered during the security planning. A security gateway is placed at the boundary between the schools internal network and a public network, to filter the traffic flowing across the boundary in accordance with the documented security gateway service access policy for that boundary.
b. In designing security gateways, security gateway components and deploying of the security controls are necessary. The security gateway components are: Switches, Routers, Application level gateway, Security appliances, and Security management. Deploying security gateway controls include: Packet filter firewall architecture, Dual-homed gateway architecture, Screed host architecture, and Screen subnet architecture.
c. There is a proper selection of switches which will be used to allow high-speed communications delivering full network bandwidth to each physical port. Generally, switches are layer 2 devices which are extensively used to segment local area networks. Further, they can provide subnet isolation when VLAN techniques are implemented.
d. Routers are used to filter the respective data communication data packets based on packet filtering techniques. Also, routers can perform NAT and packet filtering.
e. Application level gateways are specifically designed to restrict access between two separate networks. Primarily two techniques are used for implementing application level gateways: Stateful Packet Inspection and Application Proxy.
f. To meet diverse security needs, from the smallest remote locations to large corporate networks, and data centers, a security appliance is best. Security Appliances are network devices (routers, switches, modems etc.) equipped with hardened operating systems, all dedicated to security purposes.
g. In the schools network, a packet filter firewalls should be implemented since they are essentially routing devices that include access control functionality for system addresses and communication sessions. They are often referred to as screening routers.
h. The dual-homed gateway should be considered as well since it represents a more qualified type of security gateway because it hides internal IP addresses from systems of external networks and it provides logging capability which can be used in conjunction with an Intrusion Detection System (IDS) to detect possible intruder activities.
i. The packet filtering on the screening router is set up in such a way that the bastion host is the only system that hosts of external networks can open connections to. Such a bastion host as an application-level firewall consists

of proxy services that pass or block the services according to the sites policy. The router filters inherently dangerous protocols from reaching the firewall and site systems.
j. The screened subnet architecture is a variation of the dual-homed gateway and screened host architectures. It adds an extra layer of protection to the screened host architecture by adding a perimeter network that further isolates the internal network from external networks like the Internet. Thus, it is more appropriate for sites with large amounts of traffic or sites that need very high-speed traffic.
Securing Communications Across Networks using Virtual Private Networks (VPNs)
a. VPNs are implemented in a way that ensures the: - confidentiality of data and code in transit between VPN end-points, - integrity of data and code in transit between VPN end-points, - authenticity of VPN users and administrators, - authorization of VPN users and administrators, - availability of VPN end-points and network infrastructure.
b. VPNs can be implemented entirely within a private network under the control of the institution, they can be implemented across networks in the public domain, or they can be implemented across combinations of the two as long as the connection is secured.
c. VPNs can easily be switched on or off as required without any change to the underlying physical network infrastructure.
d. A VPN created with tunnels is therefore more flexible than a network based on physical links. Tunnels can be created by using: - virtual circuits - label switching, or - protocol encapsulation.
e. Encryption is implemented to all tunnels.
f. In selecting VPNs, the following architectural aspects should be addressed: - endpoint security, - termination security, - malicious software protection, - authentication,

- intrusion detection system, - security gateways (including firewalls), - network design, - other connectivity, - split tunneling, - audit logging and network monitoring, - technical vulnerability management.
g. Typical technologies and protocols used to implement VPNs: - Frame Relay - Asynchronous Transfer Mode (ATM) - Multi Protocol Label Switching (MPLS) - Point-to-Point Protocol (PPP) - Layer 2 Forwarding (L2F) Protocol - Layer 2 Tunneling Protocol (L2TP) - IPsec - Secure Socket Layer (SSL) - Secure Shell
Securing Wireless IP Network Access
a. In wireless networks, the network security team considers threats such as: - unauthorized access - packet sniffing - rogue wireless access point - denial of service attack - bluejacking - bluesnarfing - adhoc networks - and other threats

b. Proper authentication and authorization in using the wireless network are considered to maintain CIA.
c. These are the security controls for the wireless network in the institution: - Encryption control and implementation - Integrity evaluation - Authentication - Access control (permission control and network-based control) - Denial of service attack resilience - DMZ segregation via firewall protection - Vulnerability management though secure configurations and hardening of devices - Continuous monitoring of wireless networks
d. There is a proper regulation on the use of Bluetooth and other wireless technologies in the institution.
Risk Assessment and Treatment
a. HEIs approach to network security should be based on risk assessments standards.
b. HEIs should continuously assess the risk and evaluate the need for protective measures. Measures must be evaluated based on HEIs role as an establishment for education and research and with regards to efficiency, cost, and practical feasibility.
c. An overall risk assessment of the information systems should be performed annually.
d. Risk assessments must identify, quantify and prioritize the risks according to relevant criteria for acceptable risks.
e. Risk assessments are to be carried out when implementing changes impacting information security. Recognized methods of assessing risks should be employed, such as ISO/IEC 27033.
f. The Chief Security Officer (CSO) or Chief Operating Officer (COO) is responsible for ensuring that the risk management processes at the HEIs are coordinated in accordance with the policy.
g. The system owners are responsible for ensuring that risk assessments within their area of responsibility are implemented in accordance with the policy.
h. Risk management is to be carried out according to criteria approved by the management of the HEIs.
i. Risk assessments must be approved by the management.
j. If a risk assessment reveals unacceptable risks, measures must be implemented to reduce the risk to an acceptable level.

Guidelines in Selecting Network Components
a. All network components that will be employed in the school's computer network should comply with the standards and needs of the institution. It is the responsibility of the network security team to investigate the best solutions for the network which later be approved by the president or CEO of the institution.
b. All requisitions and purchases should follow the institutions policies and guidelines.
Compliance
a. All employees must conform to the network security policy and rules. Enforcement is the obligation of line management. Students must comply with IT regulations.
b. Employees and students should be aware that evidence from security incidents will be stored and may be handed over to law enforcement agencies following court orders.
c. Network audits should be planned and arranged with the involved parties to minimize the risk of disturbing the activities of HEIs

V. Conclusions and Recommendations

Based on the assessment, the five (5) Higher Education Institutions (HEIs) did not mostly conform to most of the ISO 27033 indicators. Thus, network security policies are present but those were not properly imposed throughout the institution. Moreover, the study crafted a policy for the HEIs pertaining to the campus network security. The policy can serve as a baseline for the HEIs improvement on the security measures for their network infrastructure.

In addition, HEIs should perform corrective actions on the indicators which showed non-conformity. A proper monitoring of the implemented network security management policy because it helps in establishing the effectiveness of it, and in providing the basis for recommendations and future decision- making. Further, HEIs may utilize the developed policy based on the ISO 27033 standards in preparation for their ISO certification.

References

[1] R.P.S. Ahuja and F. Lakhani. System and method for data mining and security policy management., U.S. Patent No. 8,447,722. 21 May 2013.

[2] A. Keane and J. Flood. How to Improve Network Security Using Gamification., Proceedings of the 12th European Conference on Information Warfare and Security: ECIW 2013. Academic Conferences Limited, 2013.

[3] Communications Today. Network security: Changing dynamics. (January 2014) [Online]. Available: http://search.proquest.com/docview/1491080112? accountid=33262 [July 8, 2016].

[4] Symantec. Symantec's Internet Security Threat Report (ISTR) 2016. (2016) [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/ reports/istr-21-2016-en.pdf [July 8, 2016].

[5] Cisco. Cisco 2016 Annual Security Report. (2016) [Online]. Available: http://www.cisco.com/c/en/us/products/ security/annual security report.html [July 8, 2016].

[6] A. Mohammed, S. Mohd Nor, and M. N. Marsono. Analysis of Network Security Policy-Based Management. International Journal of Computer Science and Information Security 11.3 (2013): 143.

[7] C. K. Kee. Security Policy Roadmap-Process for Creating Security Policies. Sans Institute Electronic Library Available online at http://rr.sans.org/policy/roadmap.php Sourced on the 29th 2002.

[8] C. Tang and S. Yu. Assessment of network security policy based on security capability. Communication Systems, 2008. ICCS 2008. 11th IEEE Singapore International Conference on. IEEE, 2008.

[9] C. Paquet. Network Security Concepts and Policies. (Feb. 5, 2013) [Online]. Available: http://www.ciscopress.com/articles/article.asp?p=1998559&seqNum=3 [July 9, 2016].

[10] J. G. Kolo and U. S. Dauda. Network Security: Policies and Guidelines for Effective Network Management., Leonardo Journal of Sciences, July-December 2008, Issue 13.

[11] Texas Wesleyan University. Network Protection and Information Security Policy. (2012) [Online]. Available: txwes.edu/media/twu/content-assets/documents/it/Network-Protection-and-Info-Security-Policy.pdf [August 14, 2016]

[12] Ryerson University. Network and Server Security Management Policy. (2007) [Online]. Available: http://www.ryerson.ca/policies/administration/ networksecuritypolicy.html [August 14, 2016].

[13] Villanova University. Network Security Policy (2016) [Online]. Available: http://www1.villanova.edu/villanova/unit/policies/Acceptable Use/security.html [August 14, 2016].

[14] C. Candiwan. Analysis of ISO27001 Implementation for Enterprises and SMEs in Indonesia., The International Conference on Cyber-Crime Investigation and Cyber Security (ICCICS2014). The Society of Digital Information and Wireless Communication, 2014.

[15] ISO. ISO/IEC 27033-1. Information technology - Security techniques - Network security - Part 1: Overview and concepts, August 15, 2015.

[16] ISO. ISO/IEC 27033-2. Information technology Security techniques Part 2: Guidelines for the design and implementation of network security., August 1, 2012.

[17] ISO. ISO/IEC 27033-3. Information technology Security techniques Part 3: Reference networking scenarios – threats, design techniques and control issues., December 15, 2010.

[18] ISO. ISO/IEC 27033-4. Information technology Security techniques Part 4: Securing communications between networks using security gateways., March 1, 2014.

[19] ISO. ISO/IEC 27033-5. Information technology Security techniques Part 5: Securing communications across networks using Virtual Private Networks (VPNs)., August 1, 2013.

[20] ISO. ISO/IEC 27033-6. Information technology Security techniques Part 6: Securing wireless IP network access., June 1, 2016.

[21] E. Young and L. Quinn. Writing effective public policy papers." Open Society Institute, Budapest (2002).

[22] M. Brophy. Security and the infrastructure: Take the time to review your network. Inside Counsel. Breaking News, July 10, 2014. [Online]. Available: http://search.proquest.com/docview/1544015396? accountid=33262. [July 27, 2016].

[23] M.N. Bin Ali, M.E. Hossain, and Md. M. Parvez. Design and Implementation of a Secure Campus Network. International Journal of Emerging Technology and Advanced Engineering, Volume 5, Issue 7, July 2015.

[24] T. Oguntunde. Challenges of Managing Higher Academic Institution Information and Communication Technology (ICT) Unit from Cradle: The University of Ibadan Experience. African J. of Computing ICT March 5. 2 (2012): 25-30.

[25] W. Han and C. Lei. A survey on policy languages in network and security management. Computer Networks 56. 1 (2012): 477-489.

[26] H. Susanto12, M.N. Almunawar, and Y.C. Tuan. Information security management system standards: A comparative study of the big five. International J. of Electrical Computer Sciences IJECSIJENS 11.5 (2011): 23-29.

[27] C. Althaus, P. Bridgman, and G. Davis. The Australian policy handbook. Allen Unwin Australia, 2013.

[28] B. Freeman. Revisiting the Policy Cycle, Association of Tertiary Education Management [ATEM], Developing Policy in Tertiary Institutions. Northern Metropolitan Institute of TAFE [NMIT], Melbourne, Australia, June 21, 2013.

[29] F.M. Avolio, S. Fallin. and D.S. Pinzon. Producing your network security policy. Watchguard.com. July (2007).

[30] S.R. Chowdhury, et al.. Payless: A low cost network monitoring framework for software defined networks. 2014 IEEE Network Operations and Management Symposium (NOMS). IEEE, 2014.

[31] B. Daya. Network security: History, importance, and future. University of Florida Department of Electrical and Computer Engineering (2013).

[32] M. Hoque, et al. An implementation of intrusion detection system using genetic algorithm. arXiv preprint arXiv:1204.1336 (2012).

[33] H. Liao, et al. Intrusion detection system: A comprehensive review. Journal of Network and Computer Applications 36.1 (2013): 16-24.

[34] ITU-T. ITU-T X.805. Part 6: Security dimension. 2008.