การออกแบบเครือข่ายสำหรับมาตรฐานการจัดการความปลอดภัยของข้อมูล ขึ้นอยู่กับ ISO 27001
Design Network Model for Information Security Management Standard depend on ISO 27001

Santi Pattanavichai
Rajamangala University of Technology Thanyaburi, RMUTT
39 Village No. 1 Rangsit-Nakornnayok Road, Klong 6 Thanyaburi, Pathumthani, 12110 Thailand
E-mail: Pattanavichai@gmail.com, Santi_p@rmutt.ac.th

บทคัดย่อ

ในบทความนี้รูปแบบเครือข่ายการออกแบบสำหรับ Information Security Management Standard (ISMS) ขึ้นอยู่กับ ISO 27001 โดยใช้ เราเตอร์, ไฟร์วอลล์, ระบบตรวจจับการบุกรุก (IDS) และระบบป้องกันการบุกรุก(IPS) ISO 27001 กำหนดวิธีการสร้างระบบจัดการข้อมูลความปลอดภัยอย่างเป็นทางการ (ISMS) นอกจากนี้งานวิจัยฉบับนี้ได้ทำการวิเคราะห์จุดอ่อนของระบบรักษาความปลอดภัยเครือข่าย (IDS) และ (IPS) ซึ่งเป็นวิธีการกำหนดตำแหน่งอุปกรณ์เหล่านี้ในระบบเครือข่ายสำหรับมาตรฐานการจัดการข้อมูลความปลอดภัยขึ้นอยู่กับ ISO 27001 และรูปแบบเครือข่ายการออกแบบสำหรับองค์กร การขอใบอนุญาตเกี่ยวกับระบบการจัดการความมั่นคงปลอดภัยข้อมูลขึ้นอยู่กับ ISO 27001

โมเดลเครือข่ายนี้ได้รับการออกแบบมาเพื่อสนับสนุนการได้รับใบรับรองจาก Information Security Management Standard (ISMS) ขึ้นอยู่กับ ISO 27001 และได้รับอิทธิพลจากวัตถุประสงค์ทางธุรกิจและขึ้นอยู่กับวัตถุประสงค์ด้านความปลอดภัยและความจำเป็นในการควบคุมกระบวนการสำหรับขนาดและโครงสร้างขององค์กร: ในเอกสารฉบับนี้ การออกแบบเครือข่ายที่ได้รับการทดสอบและมีความปลอดภัยได้รับการเสนอขึ้นอยู่กับความต้องการในทางปฏิบัติและโครงข่ายโครงข่ายที่เสนอนี้สามารถนำมาใช้กับโครงสร้างพื้นฐานที่ปรับเปลี่ยนได้สำหรับระบบการจัดการความปลอดภัยข้อมูล (ISMS) ขึ้นอยู่กับ ISO 27001

Abstract

In this paper a design network model for Information Security Management Standard depend on ISO 27001, using the router, Firewall, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS). ISO27001 defines how to create an official Information Security Management System (ISMS). Also, this paper was conducted the network security weakness in Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), the method set the position these devices in the network for Information Security Management Standard depend on ISO 27001 and design network model for organization to apply for a license about Information Security Management System depend on ISO 27001.

This network model was designed to support obtaining a certificate from Information Security Management Standard depends on ISO 27001 and is influenced by its business objective and depends on security objectives, and the need for process control for the size and structure of the organization: In this paper, a tested and secure network design is proposed based on the practical requirements and this proposed network infrastructure is realizable with adaptable infrastructure for Information Security Management System (ISMS) depends on ISO 27001.

Keywords: Network Security; Firewall; Intrusion Detection System (IDS); Intrusion Prevention System (IPS); ISO27001; ISO 27001

1. Introduction

ISO / IEC27001 is a standard developed by ISO (International Organization for Standardization). It is a requirement for the development of information security management systems for the efficiency and effectiveness of data security. The requirements of ISO / IEC 27001 have divided the content of the requirements into two parts. Part of the information security management part of the control list and is part of the control objectives.

In designing and building a secure network, many factors such as the structure and location of Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) within the network are considered. Select the location of these devices and Careful configuration of each component. Network infrastructure design has become an important part of any IT organization. The key network design for today's networks is to build the capacity to support future growth in a reliable and scalable way. This requires the designer to determine the specific circumstances of the customer, especially the current technology, applications and data architecture. Security may include authentication and authorization and CCTV to protect the integrity, availability, accountability and accuracy of computer hardware or network equipment. [1]

The first method of protection is to identify the true physical layer of the network to ensure that it is installed correctly. Next steps should follow the three network management guidelines [2, 3]. All unnecessary services should be disabled in the router configuration to prevent an attacker from using it to corrupt the network or to steal it. The Important information or network device configuration is set in this article, router attack detection and mitigation or mitigation methods are described with the Intrusion Detection System (IDS), Intrusion Prevention System (IPS), and firewalls as an important part of network and security operations. Of the network intelligent management and intrusion detection (IDS), Intrusion Prevention System (IPS), and firewall functionality can help reduce network downtime. Prevent hacker attacks, minimize network harm, and help analyze unforeseen security breaches. [4] Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. The terms information security, computer security and information assurance are frequently used interchangeably [5-6].

It is important that the information security management system is part of the integration with the organization's processes and the overall management structure and data security that is being considered in the data design and control process. It is expected that the information security management system will be scaled to meet the needs of the organization. [7-8]

2. Information Security Policy.

Information security is the most necessary component in information security because it is responsible for securing all information passed through computers network [9, 10].

2.1 Elements of Information Security

Confidentiality, integrity, and availability, also known as CIA, are three models designed to guide information security within an organization. Data confidentiality is an important element in maintaining information security. Key principles of confidentiality include:

- Confidentiality is closely related to privacy. There are measures to ensure that confidential information is designed to prevent confidential information from reaching the wrong people, while also ensuring that the right person can receive the information [11].
- Integrity is to maintain consistency, accuracy, and reliability of information throughout the life span. [12].
- Availability is best achieved by maintaining all hardware strictly, repairing hardware as needed, and maintaining a working, non-conflicting operating system environment. It is important to keep things up to date. [13]

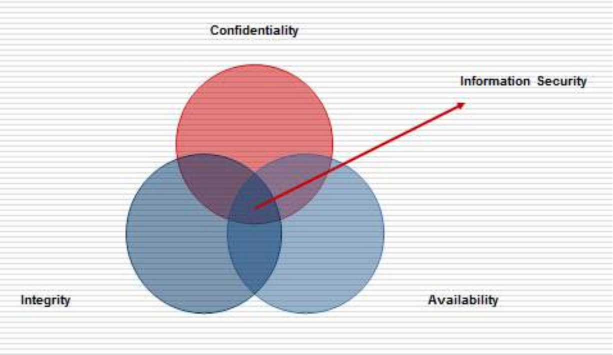

Figure 1. Elements of Information security

In this context, confidentiality is a set of rules that restrict access to data integrity, ie, ensuring that data is reliable and accurate, and that data availability is guaranteed to be credible shown in "Figure 1".

3. Information Security Management System (ISMS) Approach

To administer the Information Security Management System (ISMS) it is driven through the PDCA cycle in “Fig 2”, which consists of

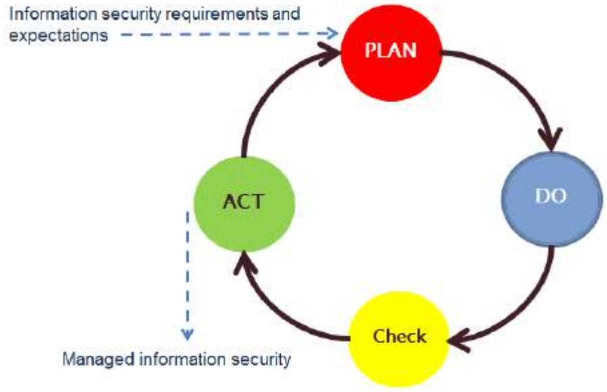
Information security requirements and expectations
PLAN
DO
Check
ACT
Managed information security

Figure 2. PDCA Model

- Plan (establish the ISMS)

Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization’s overall policies and objectives [14]. The process of Plan (establish the ISMS) set scope and Information security management system policy. The additional process manages the guidelines for risk assessment for organizations that are suitable for ISMS and security. Business information Include relevant legal requirements, risk identification and risk Analysis and Assessment, evaluating risk management approaches, control selection and control objectives for risk management and set the document about Statement of Applicability (SOA).

- Do (implement and operate the ISMS)

Implement and operate the ISMS policy, controls, processes and procedures about preparation of risk management plan, implementation of the risk management plan, and implementation of the prescribed control and set the guidelines for measuring the effectiveness of controls.

- Check (monitor and review the ISMS)

Assess and, where applicable, measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

- Act. (Maintain and improve the ISMS)

Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

3.1 Document requirements

Preparation ISMS document consists of

1. ISMS policy document and objectives.
2. ISMS scope.
3. The working process And control to support ISMS.
4. Description of how to assess risk.
5. Risk Assessment Report.
6. Risk Management Plan.
7. The required work procedures documentation for the organization.
8. Statement of Applicability. (SOA)

Records must be stored and maintained to prove compliance with the terms of service. ISMS performance must be protected and controlled. It must be considered. It's clearly stated and easy to use for control guidelines must be documented. Clear the operating procedure. Content must cover data, identifying storage, prevention, use, maintenance, and storage [15].

3.2 The Measurement of Information Security Management

Define how to measure the effectiveness of controls so that executives and employees can define good controls to achieve planned control objectives.

1. Information security policies:
2. Organization of information security
   - 2.1 Internal organization
   - 2.2 Mobile devices and teleworking
3. Human resource security
   - 3.1 Prior to employment
   - 3.2 During employment
   - 3.3 Termination and change of employment
4. Asset management
   - 4.1 Responsibility for assets.
   - 4.2 Information classification
   - 4.3 Handling of assets
5. Access control
   - 5.1 Business requirements of access control
   - 5.2 User access management
   - 5.3 User responsibilities
   - 5.4 System and application access control

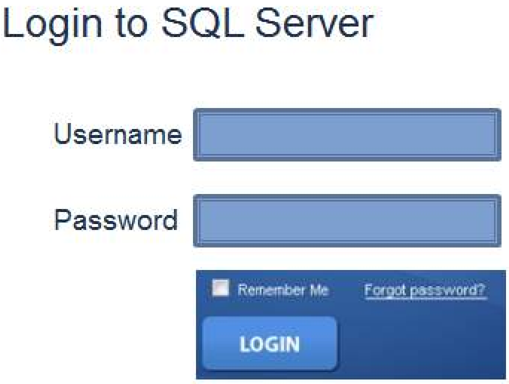

Figure 3. Login to SQL Server Authentication

In this paper, set the SQL Server Authentication is used as the means of connecting to use network model for access control policy and support for User access management process in “Fig 3”

6. Cryptography
   6.1 Cryptographic controls
7. Physical and environmental security
   7.1 Secure areas
   7.2 Equipment
8. Operations security
   8.1 Operational procedures and responsibilities.
   8.2 Protection from malware
   8.3 Backup
   8.4 Logging and monitoring
   8.5 Control of operational software
   8.6 Technical vulnerability management
   8.7 Information systems audit considerations
9. Communications security
   9.1 Network security management
   9.2 Information transfer
10. System acquisition, development and maintenance
    10.1 Security requirements of information systems
    10.2 Security in development and support processes
    10.3 Test data
11. Supplier relationships
    11.1 Information security in supplier relationships
    11.2 Supplier service delivery management
12. Information security incident management
    12.1 Management of information security incidents and improvements:
13. Information security aspects of business continuity management
    13.1 Information security continuity
    13.2 Redundancies
14. Compliance
    14.1 Compliance with legal and contractual requirements
    14.2 Information security reviews

4. Firewall, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) Policy

Security policy is the definition of security functions with network intrusion. Security appliances include Firewall, Intrusion Detection System (IDS) and Intrusion Prevention System (IPS), and have packet filtering security, authentication, access control, intrusion detection and intrusion detection. Examination routing in the kernel region of the router [16, 17]

4.1 Firewall

The firewall can be an important function in filtering; it allows them to help protect computers and other network components. A firewall can protect a particular network from external attacks by monitoring all packets of messages attempting to pass through the network and refusing to send packets unsuitable for security reasons.. However, firewalls cannot protect against internal network attacks.

4.2 Intrusion Detection System (IDS).

Intrusion Detection Systems (IDS) can alert the system administrators to attack the network in real-time by monitoring traffic on the wires and generating alerts if suspicious activity is identified. Intrusion Detection System (IDS) is a device or software program that monitors a network or system for malicious activity or policy violations. Typically, any activity or breach is reported to the system administrator or centralized using the Information Security Management System (SIEM). [17] IDS consist of two types.

- Intrusion Detection Systems (HIDS): HIDS monitors incoming and outgoing packets from devices only and alerts users or system administrators if suspicious activity is detected.
- Network Intrusion Detection (NIDS): Located at points or strategic points within the network to monitor traffic from all devices on the network.

4.3 Intrusion Prevention System (IPS).

IPS devices are responsible for detecting and intercepting penetration and attacks by intruders and malicious malware applications. They should be installed in the network path between potential risk sources and critical IT resources. Intrusion Prevention System (IPS) is network threat prevention / prevention technology that monitors traffic flows on the network to detect and prevent vulnerabilities. Vulnerability attacks often come in the form of malicious inputs to the target application or service that the attackers use to interrupt and control programs or machines. [18] IPS consists of two types.

- Intrusion Prevention (HIPS): HIPS is an IPS protection or intrusion prevention system designed for security on host systems that are vulnerable to attack and infection at each workstation level. Provide more effective security. [19]
- Intrusion Prevention (NIPS): Network intrusion prevention (NIPS) systems are used to monitor networks and

protect confidentiality, integrity, and network availability. Its main functions include protecting networks from threats such as denial of service (DoS) and unauthorized use. [20]

5. Design Network Model for Information Security Management Standard depend on ISO 27001

An important step in designing our network is to define a network structure. The topology is the physical and logical form of the network. We consider designing a network model from device selection and placement to network device installation.

5.1 Installing Host-Based IDS.

Because of the subnet is an important part of IDS installation and host IDS installation method, depending on the IDS feature in "Figure 4".

- IDS installation on the main backbone of the network

  Location 1

- Installing IDS on a high-risk Subnet demilitarized DMZ

  Location 2

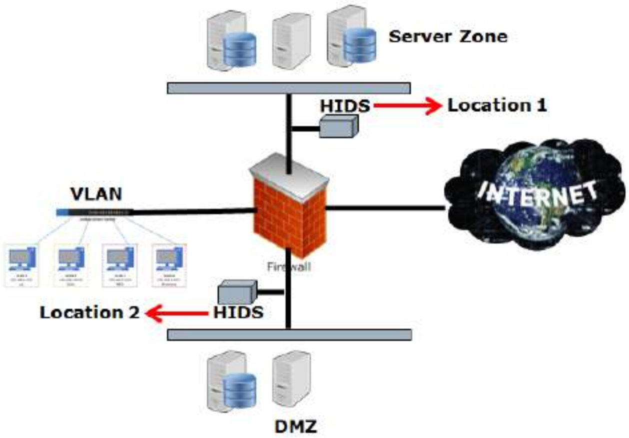

Figure 4. nstalling Host-Based IDS

Demilitarized Zone (DMZ) is a physical or logical subnet, and makes external organizations turn to services with unreliable networks, typically large networks such as the Internet. The purpose of the DMZ is to add additional security to the organization's local area network (LAN). External network nodes can only access what is in the DMZ, while the rest of the organization's networks are firewalls.

5.2 Installing Network-Based IDS.

The nature of the network must be studied and analysed to determine which sites are critical to security. The installation technique consists of Network-Based IDS 4 characteristics shown in "Figure 5"

- Installing NIDS behind Firewall

  Location 1

- Installing NIDS in front of Firewall

  Location 2

- NIDS installation on the main backbone of the network

Location 3

- Installing NIDS on a high-risk Subnet demilitarized DMZ

Location 4

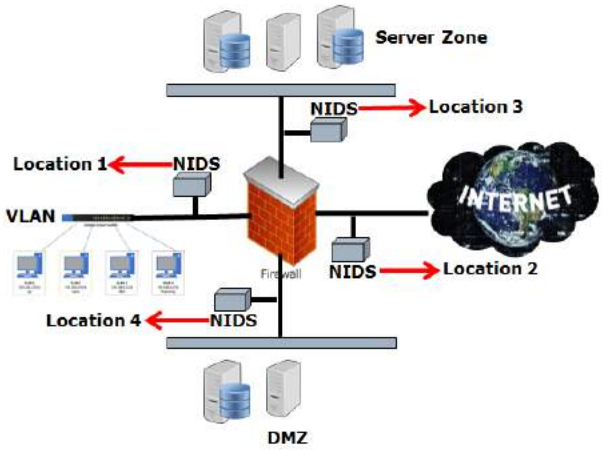

Figure 5. nstalling Network-Based IDS

In this paper, we have selected a device for designing network models for firewall. Network-Based IDS (NIDS) and host-base IPS (HIPS).set the location to install these devices in "Figure 6" and set up the SQL Server Authentication on the DMZ depends on the configuration in the firewall to send all users to the DMZ which set to Honeypot "or" target machine catch refers to the server machine on SOL Server Authentication in DMZ.

We use the Honeypot system to intercept hacker hacking, so we learn how to penetrate the hacker system, and we can know before the hacker will penetrate our real system. And we also use the ability "Stealth Logging" of the Honeypot system to record evidence for the hacker to be able to see that the installation of Honeypot in the system. We have studied Hacker hacking and learned new attacks. To be included in the system as well as Worm-like behavior, the Honeypot system can detect it as well.

The IPS and Honeypot studies are interrelated and a new technology to apply to prevent hackers because we can be aware before the hacker to attack our real system and us. This is called "Active Defense". The problem with IPS and Honeypot is that it is still in the early stages and there are things to fix. Get updates on several points. We should continue to monitor the application to protect our system.

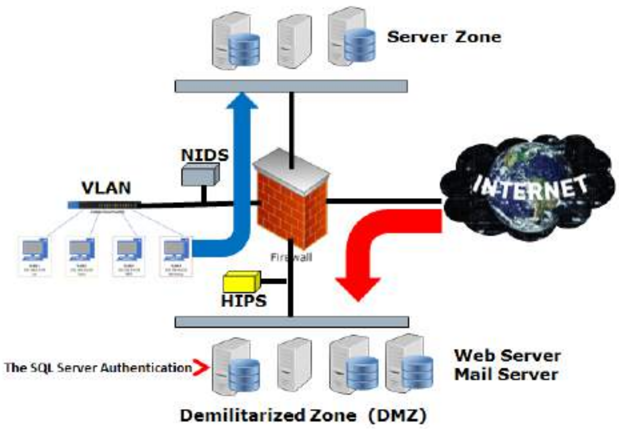

Figure 6. Design Network Model for Information Security Management Standard depend on ISO 27001

The reason to set installing NIDS behind Firewall

- Can detect intrusion from the outside. This can be penetrated through the firewall. (Location 1)
- Confidential firewall can be validated to increase the effectiveness of the firewall in preventing intrusion.
- NIDS can be an internal packet monitor. (Location 1)
- NIDS is installed based on the coverage of network segments associated with specific attacks.

The reason to set installing HIPS on a high risk Subnet demilitarized DMZ zone

- Detects attacks on target machines that are critical Honeypot "or" target machine catch refer to the server machine on SOL Server Authentication in DMZ.
- Traffic Monitor can monitor only high-risk sensitive areas.
- Monitor all users to login to The SQL Server Authentication.
- Use HIPS on high-risk Zone of Network to prevent all attack in the network.

In this article, we have adopted the principle of passage of the standard of information security management, based on ISO 27001. Prior to the certification, organizations should perform ISMS and SOA system auditing thoroughly, the organization must demonstrate compliance. The entire PDCA cycle and Article 14 of the ISO27001 standard is a requirement for continuous improvement. This network model based on the principles in the measurement of information security management (ISMS) on topic 5, 7, 8, 9, and 12 in chapter 3 of this paper. The certification examiner will find evidence. (In the form of process notes such as access control, Physical and environmental security, operations security, communication security and information security incident management at ISMS is ongoing and continually improving.

The organization shall continually improve the effectiveness of the ISMS through the use of:

- The information security policy;
- Information security objectives;
- Audit results;
- Analysis of monitored events;
- Corrective and preventive actions;
- Management review.

The reason for not installing Host-Based IPS on server zone is as a result of the firewall settings only users within the network can only access to the server zone, as shown in Figure 6.

Table 1. The measurement of information security management System (ISMS) in ISO 27001 follow by this network model for the reason

The measurement of information security management System (ISMS)	Installing Network-Based IDS	Installing Host-Based IPS.
access control	-	User access management
Physical and environmental security	Equipment IDS	Equipment IPS
operations security	Logging and monitoring	Logging and monitoring
communication security	Network security management	Network security management
information security incident management	Management of information security incidents and improvements:	Management of information security incidents and improvements:

6. Conclusion

This paper examines several network design strategies for Information Security Management Standard, based on ISO 27001. We have identified the need for security positioning in security appliance installations. Network architects need to be cautious in planning to install security devices and pay attention to the details in order to increase network security while meeting the organization's communications needs. Select Firewall, Network-Based IDS (NIDS) and Host-Based IPS (HIPS) provide additional access control and set up SQL Server Authentication to monitor network traffic and monitor users. Using Network-Based IDS (NIDS) and Host-Based IPS (HIPS) to set up locations on the network can provide better security depend on many reasons mentioned in chapter 5.

Certifications are involved in the ISMS of organizations that are assessed to be in compliance with ISO27001. Certification authorities must be confident that the organization's security risk assessment reflects the business activities of the organization. For the full scope of the ISMS, a certificate of compliance from an accredited certification is credible with the ISO 27001 organization to Certification Audit. This network model can support to verify for certification with ISO27001 about access control, operations security, communications security and information security incident management in the standard of information security management, based on ISO 27001. This network model can set for the information security policy, analysis of monitored events, corrective and preventive actions and management review in the process of ISMS in the ISO27001.

This network model was designed to utilize resources and equipment about Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to a minimum resource in line with the measurement of Information Security Management System (ISMS) but in the best way of the security system should be installed equipment about Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) on 4 positions in the network (location 1-4).

In this design network model for security management standards; this information is based on ISO 27001 as a management tool to verify the organization's ISMS certification in ISO 27001. The network security area may need to be updated very quickly to deal with threats and attacks in the future.

Acknowledgement

This research was financially supported by Rajamangala University of Technology Thanyaburi, RMUTT

References

[1] M.N.Bin Ali, M.E. Hossain, and M.M. Parvez, "Design and Implementation of a Secure Campus Network," International Journal of Emerging Technology and Advanced Engineering, vol. 5, no.7, pp. 370-374, 2015.

[2] P. Rybaczyk., "Cisco Router Troubleshooting Handbook ", M&T Books, 2000.

[3] S. Jo. "Security Engine Management of Router based on Security Policy," Proceedings of world academy of science, engineering and technology. vol. 10, ISSN 1307-688, 2005.

[4] S. Alabady, "Design and Implementation of a Network Security Model for Cooperative Network," International Arab Journal of e-Technology, vol. 1, no.2, pp. 26-35, 2009.

[5] S. Kadry, W. Hassan., "Design Implementation of System and Network Security for an Enterprise with Worldwide Branches," Journal of Theoretical and Applied Information Technology, pp. 111-118, 2008.

[6] ISO/IEC 27001:2013, Information technology — Security Techniques — Code of practice for information security controls.

[7] ISO/IEC 27001:2013. Information Technology - Security Techniques – Information Security Management Systems – Requirements. Known as ISO 27001.

[8] A. Calder, S. Watkins, "IT Governance: an International Guide to Data Security and ISO27001/ISO27002" 5th edition. Kogan Page Publishing, 2012.

[9] S. Chen, R. Iyer, and K. Whismant, "Evaluating the Security Threat of Firewall Data Corruption Caused by Instruction Transient Errors," In Proceedings of the 2002 International Conference on Dependable Systems & In Proceedings of the 2002 International Conference on Dependable Systems & Network, Washington, D.C., 2002.

[10] H. Kim, “Design and Implementation of a Private and Public Key Crypto Processor and Its Application to a Security System,” IEEE Transactions on Consumer Electronics, vol. 50, no. 1, 2004.

[11] Information on https://www.techopedia.com/definition/10254/confidentiality

[12] Information on http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

[13] Network Security 1, Cisco system,Inc. 2006.

[14] A. Chakraborty “Importance of PDCA cycle for SMEs,” International Journal of Mechanical Engineering (SSRG-IJME), vol. 3, no. 5, pp. 30-34, 2016.

[15] E. Gidey, K. Jilcha, B. Beshah,D. Kitaw, “The Plan-Do-Check-Act Cycle of Value Addition,” Ind Eng Manage 3: 124, 2014, doi: 10.4172/2169-0316.1000124.

[16] Y. Wa, The design and implementation of router security subsystem based on IPSEC, Proceedings of IEEE TENCON'2002.

[17] Information on https://en.wikipedia.org/wiki/Intrusion_detection_system

[18] Information on https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-prevention-system-ips

[19] Information on http://www.webopedia.com/TERM/H/HIPS.html

[20] Information on http://www.webopedia.com/Thttps://www.techopedia.com/definition/4030/network-based-intrusion-prevention-system-nipsERM/H/HIPS.html