# Effectiveness of banking card security in the Ethiopian financial sector: PCI-DSS security standard as a lens

Lemma Lessa and Daniel Gebrehawariat
*School of Information Science, Addis Ababa University, Addis Ababa, Ethiopia*

Received 12 October 2021
Revised 18 May 2022
21 June 2022
Accepted 2 January 2023

## Abstract

**Purpose** – This study is aimed at assessing the information security management practice with a focus on banking card security in selected financial institutions in Ethiopia, using an international information security standard as a benchmark. It is to identify the gaps and recommend best security practices to help financial institutions meet the required security compliance.

**Design/methodology/approach** – Two financial sectors were purposively selected. A total of twenty-five respondents (IT executives and IT staff) were included in the study. Quantitative data was collected using the PCI-DSS (Payment Card Industry Data Security Standard) security standard questionnaire. In addition, observation and document analysis were made.

**Findings** – The result shows that most of the essential security management activities in the financial sectors do not comply with the international security standard. Similarly, the level of most of the indispensable security requirements that should be in place is found to be below the acceptable level. The study also revealed major security factors that prohibit the financial sectors from PCI-DSS security standard compliance.

**Originality/value** – This study assessed the information security management practice with a focus on banking card security and tried to figure out the limitations of security practices of the organizations surveyed based on the standard adopted. The topic has not been well explored especially in the Ethiopia context. Hence, the result can positively influence security policies, particularly in the banking sector.

**Keywords** Payment card industry, Banking card security, Data security standard, Card data environment, Automatic teller machine

**Paper type** Research paper

## 1. Introduction

In the current competitive business environment, information is the most valuable and fundamental asset in any organization. Therefore, protecting the security of information is so important and becoming a priority for many organizations (Heru *et al.*, 2011). To protect this valuable asset, there should be proper information security practices and management that keep information from a wide range of internal and external threats and preserve its value to the organizations. Financial institutions are subject to insider threats due to the highly sensitive information and their high dependence on information technologies (Yaseen, 2017). The use of electronic banking is increasing from time to time (Khudhur *et al.* (2018) and the growth of e-banking has led to ease of access and 24-hour banking facilities. However, this

A previous version of this manuscript was presented at the 2nd African International Conference on Industrial Engineering and Operations Management Harare, Zimbabwe, December 7–10, 2020; and published in the conference Proceedings by IEOM Society International.

International Journal of Industrial Engineering and Operations Management
Vol. 5 No. 2, 2023
pp. 135-147
Emerald Publishing Limited
e-ISSN: 2690-6104
p-ISSN: 2690-6090
DOI 10.1108/IJIEOM-10-2021-0015

has led to a rise in e-banking fraud which is a growing problem affecting users around the world (Devadiga *et al.*, 2017).

As Shi-Ming *et al.* (2006) noted, if organizations follow guidelines and standards to set up their security policy, they could own a tighter and more complete IT environment. The organization could also safeguard its business value and benefit from IT if there is well-developed information security management. In addition to this, businesses also need to implement rules and controls around the protection of valuable systems that store and process information, and this protection is attained through the proper implementation of information security policies, standards, guidelines and procedures. Data breaches are occurring regularly and the financial sector is a target of attackers who often successfully compromise sensitive information. The financial sector is expected to be compliant with security standards such as Payment Card Industry Data Security Standard (PCI-DSS) to be connected to international payment brands.

As banking card is becoming the most prevailing mode of payment for online as well as regular purchases, fraud-related to them is also increasing (Devadiga *et al.*, 2017). The drastic upsurge in online banking fraud can be seen as an integrative misuse of social, cyber and physical resources. Hence, protecting individuals' financial information is one of the fundamental activities to be undertaken by all financial organizations to enhance their business. Business partners, suppliers and vendors are seeing security as the top requirement, particularly when providing mutual network and information access. To provide a fast and appropriate response to security incidents and to ensure interoperability between the financial sectors, there is a need for systematic and predefined information security management. And to that end, it is crucial to assess the current security management of the financial sectors.

In Ethiopia, most of the banks have implemented a core banking system that interconnects all branches with the headquarters, and few banks and electronic payment system processors are connected to the national and international payment system to transact electronic payment services using ATM and point of sale (POS) machine. For all these, technology plays a vital role in carrying out the delivery of financial services, whereas the risk followed by the implementation of these technologies and the problem associated with it are not well considered. According to Spremic (2011), adopting the industry's best practices (e.g. CobiT, ISO 27000, PCI-DSS) and adjusting IT infrastructure with high-level executive objectives helps companies to lower IT risks, which are related to infrastructure and operational risks. The security standard, PCI-DSS, is used to assess the information security status of organizations and provide a mitigation and road map to make the organization secure and compliant. The PCI-DSS was developed to encourage and enhance payment card account data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect bank account data. While specifically designed to focus on environments with payment card account data, PCI DSS can also be used to protect against threats and secure other elements in the payment ecosystem (PCI Security Standards Council, 2018).

The electronic banking system addresses several demands for anytime and anywhere service with complex integration challenges. However, the increase in the use of ICT facilities results in an increase in cybercrime like spamming, credit card fraud, ATM fraud, Phishing, identity theft, denial of service and many more. Hence, ensuring a high level of security for electronic banking platforms will have a motivation for the consumers' protection of electronic services and consequently the protection of the financial institutions' interests (Marinela and Liana, 2010).

The financial sector is expected to be compliant with security standards such as PCI-DSS to be connected to the international payment brands. In addition to that, being a security standard complaint will enable the financial sectors to protect their valuable asset from the current internal and external attacks. Assessing those controls using the PCI-DSS standard checklist could have prevented costs in business disruption as well as monetary fines and made the financial sectors competitors in the international market by enabling them to provide international card services such as VISA International, MasterCard, Union Pay and the like. PCI-DSS security standards reduce the risk of electronic payment, including debit card, credit card and Internet banking data loss by preventing, detecting and reacting to potential breaches or hacks that lead to an account data compromise, since one of the goals of PCI-DSS is to protect electronic payment system from risk and threats and minimize data breach risk. Electronic banking has many security issues which include fraud, data loss and a lack of information security in general (Shaikh, 2014). To address these information security issues related to card banking security, this study aimed at assessing the effectiveness of information security practice and management of card banking security in the financial sector and to identify the factors that prohibit the Ethiopian financial sectors from PCI-DSS security standard compliance.

Security compliance is one of the major issues in information security management (Munirul *et al.*, 2011). Different frameworks, guidelines and standards were proposed by researchers, practitioners, consultants and professionals to protect an organization's information assets (Choobineh *et al.*, 2014). The most widely used international standards are COBIT, ISO 27001&2 and PCI-DSS. Among these widely used standards, PCI-DSS is an industry-wide standard that focuses on the credit card industry that aims at achieving strong protection of sensitive consumer and card data, and preventing major security issues. The standard sets mandatory requirements in many aspects, including secure networks, card data protection, access control, vulnerability management, security assessments and reporting (PCI Security Standards Council, 2018). To that end, any bank that runs an ATM, POS machine, issues debit cards, credit cards and electronic payment sector that do business with the merchants need to be compliant with PCI-DSS security standard security compliance. As the PCI-DSS standard is used to improve the security of electronic and online banking data and to facilitate consistent security measures to mitigate data breaches and fraud, the researchers used the PCI-DSS security standard checklist to assess the current information security management in the Ethiopian financial sector focusing on the card banking security.

## 2. Methods

As Chang *et al.* (2016) mentioned, security controls can be a very complicated and resource-intensive process that requires special resources and expertise. Hence, proper consideration and follow-up are required on the security tool to address the security issues. There should also be a way of assessing the proper functionality of the deployed tools and the security status of the financial organization. In this regard, the researchers employed a quantitative approach and a survey method. The researchers used the purposive sampling technique as it provides a deliberate choice based on the qualities the participant possesses to address the objective of the research (Etikan *et al.*, 2016). Besides, purposive sampling technique involves selecting certain cases based on a specific purpose rather than random selection (Teddlie and Yu, 2007). In addition to the four banks with card banking services, two electronic card payment service sectors are established under the Ethiopian national bank license to provide the electronic payment service which serves as a switch among the banks and print the electronic payment card (debit card) and PIN. The researchers also selected one electronic payment processor among the two financial sectors using purposive sampling. Hence, 50% of the banks that issue electronic cards and PINs, and 50% of the electronic payment processors are selected for this study using the purposive sampling method. A total of 25 respondents (IT executives and IT staff) in the IT department were selected to answer the questions.

The organizations selected for this study are from the financial sectors in which one is from the banking industry and the other is from electronic payment processing. In the banking sector, bank X [1] provides all the major banking services that a commercial bank is expected to provide with the vision to be the bank of choice for customers, employees and shareholders and the mission to be customer-focused financial services through competent, motivated employees and modern technology to maximize the value of its stakeholders. The bank is among the four banks that issue electronic payment cards and PIN security numbers at its premises to provide card banking services to its customers. The second financial sector where this research is conducted is Y S.C. It is a consortium owned by six Ethiopian private banks established in 2009 by visionary banks to save the high investment cost of the modern payment platform and deliver electronic payment services to financial institutions with a shared system. It commenced operation officially on July 5, 2012. Thus, this research focuses on information security management in the financial sectors focusing on card banking services. The empirical data were analyzed using thematic analysis technique.

## 3. Results

### *3.1 Security scoping*

The security scoping questions provided to the financial sectors comprise how their inventory device is updated, and whether it included all the necessary information regarding the devices information such as the model of the device, location of device, serial number asset identification tag and classification of item type. In addition to this, it verified if there is a detailed network diagram covering all boundaries in scope including network segmentation if there are boundaries between trusted and untrusted networks, wireless and wired networks, type of devices, device interfaces, protocols and security controls in the scope. The result in Table 1 shows that hardware and software asset inventory has been maintained in the organizations but the existing inventory is not updated to include all the essential assets which should be under the security scope.

Furthermore, the existing inventory did not have a detailed description and function of use. The network diagram was not updated with cardholder data components of the organizations since the following were not well illustrated within the diagram.

(1) The card data environment (CDE) and non-card data environment (non-CDE) data flow are not well mentioned in the network diagram.

(2) Demilitarized zone (DMZ) is configured on the premises; however, some components are not included in the DMZ.

(3) ATM and POS transaction connectivity (Type of connection, systems involved within operation) is not clearly defined to include the end-to-end connectivity for storing, processing and transmission of transaction data.

### *3.2 Media and facilities security*

The media and facility security part of the questionnaire includes how the removable media that contains sensitive information is properly labeled to protect the information from unauthorized access, how the media are destroyed using procedures supported by legal reasons such as retention period based on business justification, how onsite personnel is identified from visitor and the entry control security as a whole using different technologies such as CCTV and Access control.

**Table 1.**
Security scoping of hardware and software inventory

| | Frequency | Percent |
|---|---|---|
| Less secure | 8 | 32.0 |
| Partially secure | 6 | 24.0 |
| Fully secure | 11 | 44.0 |
| Total | 25 | 100 |

The result in Table 2 shows that there is a gap in the documentation procedure in the organization to include the below requirements.

(1) Maintaining a list of media devices periodically.

(2) Periodic inspection of media devices to look for tampering or substitution.

(3) Training personnel to be aware of suspicious things and to report tampering or substitution of devices.

### *3.3 Network and security*

The network and security category consists of both wired and wireless network security on top of the technologies applied to protect the premises from unauthorized access and periodic vulnerability assessment and penetration test. As shown in Table 3, there is a notable gap in network and security. Internet connection is separated from the internal network through a firewall and router and there is no direct connection between the Internet and the internal network of the organizations.

Furthermore, the production and test environment are segmented to protect the production environment from any security risk using VLAN technology. However, the firewall and router configuration standard has not been documented to include roles, responsibilities and access privileges to the network components. Furthermore, services and ports are not restricted for inbound (incoming) and outbound (outgoing) traffic in the card data environment. There is no successive quarterly wireless scanning and analysis activity that identifies unauthorized access points at the premises. In addition, there is no all-inclusive vulnerability assessment and penetration test conducted regularly to verify the security of the whole perimeter, and the security system to monitor and respond to networks intrusions, vulnerabilities and irregularities behaviors are not monitored on a 24/7 basis; hence, it will not be easier to take immediate action if any internal or external incident occurs.

### *3.4 Application security*

About application security, it is tried to evaluate the software development process, security patches management, application log monitoring and application change detection mechanisms. As evidenced in Table 4, not all system components were installed with the latest patches on time to fix the application from recent virus definitions. There is no application vulnerability assessment and application penetration test conducted periodically or at the time of significant change, and the application firewall is not deployed on a perimeter location.

| | Frequency | Percent |
|---|---|---|
| Less secure | 9 | 24.0 |
| Partially secure | 10 | 40.0 |
| Fully secure | 6 | 36.0 |
| Total | 25 | 100.0 |

**Table 2.** Media and facility security

| | Frequency | Percent |
|---|---|---|
| Less secure | 2 | 8.0 |
| Partially secure | 11 | 44.0 |
| Fully secure | 12 | 48.0 |
| Total | 25 | 100.0 |

**Table 3.** Network and security

Furthermore, the file integrity and log monitoring tool are not fully integrated with all the application systems to alert unauthorized access and modification. It is examined that cardholder data components including Windows servers, Linux servers, Oracle Database, Application, Cisco firewall, Router and Switch are configured to enable audit track and send all logs to a centralized system which are file integrity monitoring and log monitoring to monitor the system components. However, not all the component in the scope is integrated and configured to send logs to the log monitoring system. Moreover, logs are not analyzed periodically to examine the security status of the system components.

### *3.5 Card data security and encryption*

The card data security and encryption questionnaire include both cardholder data security and the encryption technology used to protect sensitive data from being exposed to authorized access. While data are transmitted over the public network, security protocols such as IP Security (IPSEC) and Secure Shell (SSH) are used to secure the end-to-end connectivity nevertheless, it is not fully implemented (as revealed in Table 5) with all the connections and some of the application components don't use cryptography technologies such as Secure Socket Shell (SSH).

Access to sensitive areas is not strictly limited to individuals whose job requires visiting this area and there is no formal and periodic security awareness training though, there is a security briefing on the hiring of new staff. Regarding the network diagram that identifies the connections between the cardholder data environment and other networks, all the cardholder components are included in the network diagram. However, the network diagram does not show the cardholder data flows across systems and networks.

### *3.6 Logging and monitoring*

As shown in Table 6, the logging and monitoring category consists of time synchronization technology (NTP), password management, access management, user management process and account management.

**Table 4.**
Application security

| | Frequency | Percent |
|---|---|---|
| Less secure | 6 | 24.0 |
| Partially secure | 9 | 36.0 |
| Fully secure | 10 | 40.0 |
| Total | 25 | 100.0 |

**Table 5.**
Card data security and encryption

| | Frequency | Percent |
|---|---|---|
| Less secure | 6 | 24.0 |
| Partially secure | 13 | 52.0 |
| Fully secure | 6 | 24.0 |
| Total | 25 | 100.0 |

**Table 6.**
Logging and monitoring

| | Frequency | Percent |
|---|---|---|
| Less secure | 10 | 40.0 |
| Partially secure | 10 | 40.0 |
| Fully secure | 5 | 20.0 |
| Total | 25 | 100.0 |

(1) Some users have not logged in for more than 60 days and are not disabled and removed from the system.

(2) Account lockout has not been configured on some of the components (Servers and Network) based on the requirement.

(3) It is verified that there are system components not configured with minimum password length.

(4) Some system components are not configured with password complexity enabled (alphanumeric characters).

(5) There are system components that are not configured with password history

(6) In some of the components, the password is not interactive to enforce a strong password.

### *3.7 Policy and procedure*

The organizations are not providing security training and do not provide refresher training every year as is documented in the information security policy. Information classification policy is not defined within the organization to maintain proper control of all assets identified with the correct classification and Table 7 magnifies this issue.

As a part of the recruitment and training policy, all employees signed on commitment form, which mentioned that they understood the policy and procedures. Non-Disclosure agreements with all employees are maintained. Changes are not being routed through change management. Access rules are being modified based on specific requests from different departments; however, structured formal change management was not followed for systems, firewall and router configuration changes.

### *3.8 Anti-malware*

As indicated in Table 8, antivirus has been installed on most of the components, including servers and client machines but it may not protect all the machines from all types of malicious software since the antivirus is not updated in some components with new virus definitions and new updates.

| | Frequency | Percent |
|---|---|---|
| Less secure | 5 | 20.0 |
| Partially secure | 11 | 44.0 |
| Fully secure | 9 | 36.0 |
| Total | 25 | 100.0 |

**Table 7.**
Policy and procedure

| | Frequency | Percent |
|---|---|---|
| Less Secure | 5 | 20.0 |
| Partially Secure | 8 | 32.0 |
| Fully Secure | 12 | 48.0 |
| Total | 25 | 100.0 |

**Table 8.**
Anti-malware

The antivirus has not been enabled and configured to generate logs to store log files since it is not configured to be integrated with the log monitoring server. Moreover, there was no anti-malware procedure or virus prevention procedure documented to make the action easier when such kind of attack happens on the premises.

## 4. Discussion

According to Bradley and Dent (2010), organizations have struggled to adequately protect their most sensitive information assets with many cases of breaches of security and the loss or disclosure of sensitive data. Many widely publicized incidents of high-profile data losses occurred across the globe in recent years in which of the 90% confirmed breaches that were investigated, 285 million records were compromised and 80% of these records involved payment card data. The report confirmed that fraudulent use of the payment card data occurred in 83% of these cases. Thus, financial organizations should work hard in securing their premises from unauthorized access and protect their sensitive information and business as well. Periodic vulnerability scanning is mandatory for financial organizations to identify gaps and mitigate them on time before the occurrence of any damage.

As Lokhande and Meshram (2013) pointed out, vulnerability is a weakness that allows an attacker to reduce a system's information assurance by intersecting the system flaw, access to the flaw and exploiting the flaw. As per PCI-DSS Reference Guide (2010), security vulnerabilities in application systems may allow criminals to access Primary Account Number (PAN) and other cardholder data. Many of these vulnerabilities are eliminated by installing security patches, which perform a quick repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation. Entities should apply patches to less-critical systems as soon as possible, based on a risk-based vulnerability management program. Secure coding practices for developing applications, change control procedures and other secure software development practices protect the application system if it is properly followed.

One of the key success factors in analyzing and measuring the effectiveness of information security is to ensure that the organization has a thorough understanding of the assets which are most valuable to them and that those assets have been allocated an appropriate level of classification based on the criticality of the asset relative to prioritized risk (Khan, 2010). If all the valuable assets are not included in the scope for security management, there will not be effective information security management in the organization. As Liu *et al.* (2010) stated, the media inventory should be stored securely and while those media are useless for legal or business reasons, they must be destroyed permanently.

For the network devices, the security policy was not defined properly and default services were allowed for inbound and outbound traffic. In addition to this, personal firewalls were disabled by users. According to Omariba and Wanyembi (2012), when a computer is connected to the network, it becomes vulnerable to attack. A personal firewall helps to protect the computer by limiting the types of malicious traffic initiated.

Data retention and disposal policy and procedure have not been well documented in the organizations, and the practice is not exercised properly. Hence, data retention requirement such as secure deletion of cardholder data was not addressed descriptively in the security policy and there are some system components where full PAN was displayed. One of the major security protections for the organization is password security. Since common types of attacks are occurred by week password management practice in the organizations. As Liu *et al.* (2010), passwords should be changed every 90 days, and the minimum length should be seven characters, where alphabetic and numeric characters are both required and the user whose repeated access attempts are over six times should be locked out from accessing the system.

Information security policies and procedures are in place but it is not carried out on a day-to-day basis. The organizations were not providing security awareness training for their employees periodically as per the information security policy. As Shi-Ming *et al.* (2006) noted, if organizations follow the guidelines and standards to set up their security policy, they could own a tighter and more complete IT environment.

Antivirus was not installed on some of the components, including servers and clients and antivirus was not updated on some critical components with up-to-date signatures. Malicious software such as viruses, worms and Trojans can give access to unauthorized and malicious people by entering into the computer system and antivirus software is capable of removing or quarantining known malware, and it can generate audit logs actively (Susanto *et al.*, 2011). In addition, sensitive information should be encrypted, while it is transmitted internally or externally for a business need. Encrypted data are intrinsically protected because it is unreadable. This is the major reason that it is required in so many compliance guidelines and industry standards (Lokhande and Meshram, 2013). The use of IPSEC (IP Security) encryption ensures secure private communication over the IP networks by facilitating direct IP connectivity between sensitive hosts through untrusted networks (Singh *et al.*, 2014). As Desisa and Beshah (2014) pointed out, layered security control in the communication channel is recommended for the financial sector while using the public network like the Internet. Cryptography technology should also be used to protect sensitive information in the financial sector. According to Singh *et al.* (2014), cryptography is used in information security to protect information from unauthorized or accidental disclosure while the information is in transit or storage. Information security uses cryptography technology to transform useable information into a form that is unusable by anyone other than an authorized user. One of the major security protections for the organization is password security. Since common types of attacks are occurred by week password management practice in the organizations. Organizations should have a password management policy that is adhered to by all the staff and there should be password enforcement on every system component. Hackers can guess passwords locally or remotely using either a manual or automated approach as there are many tools available that can automate the process of typing password after password. Password cracking methods also capture password hash and convert it to its plaintext original. For password cracking, an attacker uses tools like extractors for hash guessing, rainbow tables for looking up plaintext passwords and password sniffers to extract authentication information. Password crackers sniff authentication traffic between a client and server and extract password hashes or enough authentication information to begin the cracking process (Lokhande and Meshram, 2013).

Change and release management policies ensure adequate testing and roll-back policies (Liu *et al.*, 2010). It defines the authorization and escalation processes, incident classification and exception management with centralized log management, reviews and continuous monitoring with appropriate audits. The information security policy should also include the basic requirements such as assigning risk ranking to vulnerabilities including high, medium, and critical risk status in addition to that; there should be a clearly stated incident management procedure to be followed. As Susanto *et al.* (2011) stated that information security incident management involves the identification of resources that are needed for incident handling. Good incident management will help with the prevention and awareness of incidents.

Antivirus software is capable of removing or quarantining known malware, and it can generate audit logs actively (Susanto *et al.*, 2011). The periodic wireless scan is also mandatory for organizations to identify insecure connections available on the premises and take action accordingly. As Lokhande and Meshram (2013), many people may think about logging in to a random and unprotected wireless network just to get some work done. That is all it takes for someone with ill intent to capture a user's login credentials and work his way onto the wireless network. There are security policies and procedures prepared and documented to manage and control the organization’s information security from unauthorized internal and external access but the policies and the procedures are not maintained to be executed in the day-to-day activities of the organization. In general, information security management and practices in the Ethiopian financial sectors are not well addressed and maintained regarding the current security threat and risks associated with the financial sectors. In this study, in addition to assessing the effectiveness of information security management in the Ethiopian financial sectors focusing on the card banking security, the factors prohibiting the effectiveness of information security management toward PCI-DSS are identified. As the result implies, the effectiveness of information security management and practice focusing on card banking security is below the acceptable level.

## 5. Conclusion and recommendations

The study is aimed at assessing the information security management practice with a focus on the electronic banking systems in selected financial institutions in Ethiopia using an international information security standard as a benchmark. It is to identify the gaps and recommend best security practices to help financial institutions meet the required security compliance. The result shows that most of the essential security management activities in the financial sectors do not comply with the international security standard. Similarly, the level of most of the indispensable security requirements that should be in place is found to be below the acceptable level. The study also revealed major security factors that prohibit the financial sectors from PCI-DSS security standard compliance. Based on the major findings, suggestions are presented below considering best practices.

The absence of one vital asset from the security scoping implies that the organization has not used its resources to its best advantage in addressing security risk exposure (Zhi *et al.*, 2013). The study revealed that device inventory needs to be updated with detailed descriptions and functions to identify and classify assets easily and protect them from loss and unauthorized access. Device security operation procedure needs to be documented to include requirement as maintaining a list of devices, periodic inspection of devices to look for tampering or substitution, and training personnel to be aware of suspicious behavior and to report tampering or substitution of devices.

Media inventory should be stored securely and while those media are useless for legal or business reasons, they must be destroyed permanently (Liu *et al.*, 2010). Regarding physical security, there should be entry controls to limit and monitor physical access to systems using video cameras and access control mechanisms that monitor individual physical access to sensitive areas such as the data center, card printing room and PIN printing room. As Susanto *et al.* (2011) mention, physical and environmental security is used to protect systems, buildings and related supporting infrastructure against threats associated with their physical environment, buildings and rooms to protect the environment and to avoid damage or unauthorized access to information and systems. All network device configurations need to be changed using defined change management. This change management should include testing and approval of the new access rule and connection before it is implemented on the production system. Organizations should develop change management forms that include detailed business justification for the requested change such as which ports and protocols are required and for what purpose and a rollback procedure should also be maintained. According to Pinder (2006), risk initiated by unexpected events and changes will be mitigated by adequate change management processes. When a computer is connected to the network, it becomes vulnerable to attack. A personal firewall helps to protect the computer by limiting the types of traffic initiated and directed to the computer. The intruder can also scan the hard drive to detect any stored passwords (Omariba and Wanyembi, 2012).

Organizations must have a formal process to approve and test external connections and changes to firewall configurations. The standard demands justified documentation of unapproved or risky protocols, a description of network managing groups, roles and their responsibilities, and lists of services and ports needed to operate the business. It also requires a review of the firewalls and router settings every quarter. Every connection from an un-trusted area must be blocked by the firewall (Liu *et al.*, 2010). System components in the organization should be configured with secured services such as SSH, RDP-SSL, IPSEC VPN and strong encryption technology such as VPN and RDP-SSL. In general, to protect sensitive cardholder data during transmission, strong cryptographic and security protocols like Internet Protocol Security (IPsec) and SSL/TLS must be used (Susanto *et al.*, 2011).

According to Lokhande and Meshram (2013), it is not considered to log onto a random and unprotected wireless network to get some work done. That is all it takes for someone with ill intent to capture a user's login credentials and work his way onto the wireless network. Patch management procedure should be documented to include the installation of critical vendor patches within one month and all applicable patches should be installed within the vendor-defined timeframe. As Susanto *et al.* (2011) stated that security patches fix the majority of bugs by installing the latest official security patches no later than one month after the release. Moreover, all of the patches must be tested before deployment.

In the software development process, development and test environments should be separated and there should be a separation of duties between personnel assigned to the development or test environments and those assigned to the production environment. Furthermore, production data should not be used for testing and test data and accounts should be removed before a production system becomes active. Generally, there should be separate environments and duties for development, testing and production in the organization (Susanto *et al.*, 2011) and the databases and applications must have a production environment that is physically and logically separated from the test and development environment (Liu *et al.*, 2010).

Card data encryption policy and procedures should also be documented to include full PAN to only be displayed to specific roles and users with business needs. And no PAN data should be stored without encryption in addition to this, SSL/TLS or another cryptography method should be used for cardholder data transmission since insecure channels should not be used for cardholder data transmission. According to Susanto *et al.* (2011), the organization should render the PAN into an unreadable form when stored via using pads, index tokens, truncation and should use strong hash functions or strong cryptography with an appropriate key-management procedure. Cardholder data should be encrypted while sending it over end-user messaging technologies. And no clear text PAN data should be shared over email or any end-user messaging technology. In addition to this, all unnecessary default IDs, and user accounts need to be disabled or removed. This includes all system components (Firewall, Router, switch, application and database).

## Note

[1] Case organizations are named X and Y for anonymity.

## References

Bradley, M. and Dent, A. (2010), *Payment Card Industry Data Security Standard (PCI DSS) – What it is and its Impact on Retail Merchants*, Royal Holloway Series, Southfield, MI, pp. 16-19.

Chang, C., Ho, J. and Wu, A. (2016), "The effects of culture and contextual information on resource allocation decisions", *Review of Accounting and Finance*, Vol. 15 No. 2, pp. 174-197.

Choobineh, J., Dhillon, G., Michael, R.G. and Jackie, R. (2014), "Management of information security: challenges and research directions", *Communications of the Association for Information Systems*, Vol. 20, pp. 958-971, 2007.

Desisa, A. and Beshah, T. (2014), *Internet Banking Security Framework: the Case of Ethiopian Banking Industry*, HiLCoE, Computer Science College, Addis Ababa, pp. 8-13.

Devadiga, N., Kothari, H., Jain, H. and Sankhe, S. (2017), "E-banking security using cryptography, steganography and data mining", *International Journal of Computer Applications*, (0975-8887), Vol. 164 No. 9, pp. 26-30.

Etikan, I., Musa, S. and Alkassim, R. (2016), "Comparison of convenience sampling and purposive sampling", *American Journal of Theoretical*, Vol. 5 No. 1, pp. 1-4.

Heru, S., Almunawar, M.N. and Tuan, Y.C. (2011), "Information security management system standards: a comparative study of the big five", *International Journal of Electrical and Computer Sciences*, Vol. 11, pp. 21-27.

Khan, R. (2010), *Practical Approaches to Organizational Information Security Management*, SANS Institute Info Security, SANS Institute.

Khudhur, D.Y., Hameed, S.S. and Al-Barzinji, S.M. (2018), "Enhancing e-banking security: using whirlpool hash function for card number encryption", *International Journal of Engineering and Technology*, Vol. 7 No. 2, pp. 281-286.

Liu, J., Xiao, Y., Chen, H., Ozdemir, S., Dodle, S. and Singh, V. (2010), "A survey of payment card industry data security standard", *IEEE Communications Surveys and Tutorials*, Vol. 12 No. 3, pp. 287-303.

Lokhande, P.S. and Meshram, B.B. (2013), "E-commerce applications: vulnerabilities, attacks, and countermeasures", *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, Vol. 2, pp. 499-509.

Marinela, V. and Liana, A.P. (2010), *Consideration Regarding the Security and Protection of E-Banking Services Consumers interest*, Academy of Economic Studies, Bucharest, pp. 388-403.

Munirul, U., Ismail, Z. and Sidek, Z. (2011), "A framework for the governance of information security in banking system", *Journal of Information Assurance and Cyber Security*, pp. 1-12.

Omariba, Z.B. and Wanyembi, G. (2012), "Security and privacy of electronic banking", *International Journal of Computer Science Issues*, Vol. 9, pp. 432-446.

PCI Security Standards Council (2018), *Payment Card Industry (PCI) Data Security Standard: Requirements and Security Assessment Procedures Version 3.2.1*, PCI Security Standards Council, LLC, Wakefield, MA.

Pinder, P. (2006), "Preparing Information Security for legal and regulatory compliance (Sarbanes–Oxley and Basel II)", *Information Security Technical Report*, Vol. 11 No. 1, pp. 32-38.

Shaikh, M.A. (2014), "Ethiopian banker's perception of electronic banking in Ethiopia – a case of Adama city", *International Journal of Scientific and Research Publications*, Vol. 4, pp. 1-7.

Shi-Ming, H., Lee, C. and Kao, A. (2006), "Balancing performance measures for information security management", *Industrial Management and Data Systems*, Vol. 106, pp. 242-255.

Singh, A., Vaish, A. and Keserwani, P. (2014), "Information security: components and techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, Vol. 4 No. 1, pp. 1072-1077.

Spremic, M. (2011), "Standards and frameworks for information system security auditing and assurance", *Proceedings of the World Congress on Engineering*, London, Vol. 1, pp. 978-988.

Susanto, H., Almunawar, M. and Tuan, Y. (2011), "Information security management system standards: a comparative study of the big five", *International Journal of Electrical and Computer Sciences*, Vol. 11 No. 5, pp. 21-27.

Teddlie, C. and Yu, F. (2007), "Mixed methods sampling: a typology with examples", *Journal of Mixed Methods Research*, Vol. 1 No. 1, pp. 77-100.

Yaseen, Q. (2017), "Insider threat in banking systems", in Aljawarneh, S.A. (Ed.), *Online Banking Security Measures and Data Protection*, IGI Global.

Zhi, X.N., Atif, A. and Sean, B.M. (2013), "Information security management: factors that influence security investments in SMEs", *Australian Information Security Management Conference*, Edith Cowan University, pp. 60-73.

**Corresponding author**
Lemma Lessa can be contacted at: lemma.lessa@aau.edu.et