Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X
Volume 3, Issue 6, 2025

EVOLUTION OF INFORMATION SECURITY TOOLS TO PREVENT ID THEFT IN THE BANKING SECTOR OF PAKISTAN

Amna Abro[1], Abdullah Maitlo[*2], Mumtaz Hussain Mahar[3]

*[1,*2]Institute of Computer Science, Shah Abdul Latif University, Khairpur Mir's*
[3]Department of Computer Science, SZABIST University, Larkana Campus

[1]abroamna5@gmail.com, [*2]abdullah.maitlo@salu.edu.pk, [3]mumtaz.mahar@lrk.szabist.edu.pk

DOI: https://doi.org/10.5281/zenodo.15610011

Keywords
ID Theft, Evolution, Information Security Tools, Banking Sector, Financial Institutions, Case Study, Identity theft prevention, Information security Tools, Vulnerabilities, Case study research, Semi-structured interviews.

Article History
Received on 30 April 2025
Accepted on 30 May 2025
Published on 06 June 2025

Copyright @Author
Corresponding Author: *
Abdullah Maitlo

Abstract

Purpose – *Recently information breaches are increased in banking sector of Pakistan. The implementation old and non-effective Information Security Tools to Prevent Identity (ID) Theft pose significant risks to banking sector of Pakistan. The lack of appropriate evolution of these tools in banking sector causes of posing many vulnerabilities in information security infrastructure of and needs to be investigated. The purpose of this paper is to study and investigate the evolution of information security tools to prevent identity theft in banking sector of Pakistan. This paper also identifies the information security weakness in the existing banking infrastructure of Pakistan.*

Design/methodology/approach – *A qualitative case study approach is used to conduct the research. Three case studies are conducted in different banks of Pakistan. The total number of one-to-one semi-structured interviews conducted was 31. A framework for Evolution of Information Security Tools to Prevent ID Theft in banking sector was proposed by extending the guiding framework for knowledge sharing processes for ID theft prevention within organizations proposed by Maitlo et al., (2019)***.**

Findings – *This research found that Banks need to upgrade their Information security infrastructure. As existing information security tools are not sufficient to prevent identity theft in banking sector of Pakistan. Therefore, it is required to volute the ID Theft Prevention, ID Theft Risk Assessment and ID Fraud Identification Tools. A Managerial Support for Information Security is also required.*

Practical implications – *The research evaluates the information security tools for ID theft prevention in banking sector of Pakistan. It identifies the flaws in information security infrastructure in banking sector and provides the solutions to prevent ID theft. A framework for evolution of the information security tools used to prevent ID theft is developed to strengthen the information security infrastructure of banking sector. It guides the managers for effective use information security tools to empower the information security of banking sector.*

Originality/value – *This study provides a new framework which was developed in the new context to evolute information security tools for ID theft prevention in the banking sector of Pakistan.*

INTRODUCTION

Identity (ID) theft in the banking sector of Pakistan is a critical issue in these days (Salman, H. M., 2020). ID frauds are increasing day by day and have become major problem for the financial Institutions of Pakistan (Solove and Washington, 2003; Kahn and Liñares-Zegarra, 2016; Shareef and Kumar, 2012). Federal Board of Investigation (FBI) Pakistan has declared that it is rapidly growing white-collar criminal activity (Malik, A. A., Asad, M., and Azeem, W. 2021; Solove and Washington, 2003; Kahn and Liñares-Zegarra, 2016; Shareef and Kumar, 2012). Currently, Pakistan is facing ID theft issues such as hacking, data breaches, ID theft, ransomware attacks, online fraud and many more cyber frauds (Riaz, A., et al., 2024), which causes many issues in banking sector such as, financial losses, damage to bank reputation, Legal and Regulatory Consequences, increased operational costs, customer disruption and inconvenience (Ibrar and Karim, 2023). Due to the rapid growth of ID theft issues, the banking sector of Pakistan faces a significant challenge in effectively regulating its digital world (Ibrar and Karim, 2023; Khan, 2021) and it requires to evolute the information security infrastructure and cyber security tools to prevent ID frauds (reference).

In the banking sector, evolution of information security tools refers to the continuous development and improvement of technologies, strategies, and practices as information security tools aimed at protecting sensitive information and systems from unauthorized access, misuse, or damage. It involves advancement in tools for identifying new threats, vulnerabilities, and regulatory requirements to ensure the high level of security for banking operations and customer data to protect customers' and banking information. Recently, in Pakistan, increased number ID frauds and attacks IT infrastructure of banks as brought the attention of banking sector and government of strengthen the information security infrastructure in the organizations. At some extent, researchers have investigated the protection of personal and organizational information.

The regulating authorities, such as (provide the names of regulating authorities) are evolving in the managing ID frauds in Pakistan to reduce information security threats in banking sector. However, ID theft attacks are increasing with the passage of time due to the usage of old information security infrastructure having insufficient security tools to prevent ID frauds within banks. It has become a challenge for banking sector to protect from information security breaches and protecting information of banks and their accountholders (Ahmad and Sheharyar Khan, 2022). Due to such a fast growth of ID theft issues in banking sector, it attracts the attention of researchers to find out the reasons of enhancement in the ID frauds in banking sector of Pakistan.

Therefore, this research study Evolution of Information Security Tools to Prevent ID Theft in banking sector of Pakistan makes a theoretical and practical contribution. It bridges a gap in the literature by providing a comprehensive framework to understand the vulnerabilities in the effectiveness of the evolution of information security tools to prevent ID theft in the banking sector of Pakistan. Second, it contributes to the existing literature by developing the framework for Evolution of Information Security Tools to Prevent ID Theft in banking sector. It was developed by borrowing the most appropriate factors of this research study from the guiding framework**.**

The guiding framework was chosen through appropriate criteria of selecting a guiding framework for developing a new framework in the context of this research study. From the perspective of the practical implications, this study investigated the banking sector of Pakistan, identified vulnerabilities in the effectiveness of the evolution of existing information security tools and provided a solution to prevent ID theft in the banking sector of Pakistan. The developed framework can be implemented to improve security practices therefore; this study has a unique contribution in the context of ID theft in the banking sector of Pakistan.

The three (03) factors Information Security Awareness Tool produced form Information Sourcing Opportunities, Managerial Support for Information Security tools produced from Leadership support, Information Security Infrastructure produced from Knowledge Management Infrastructure of the guiding framework proposed by Maitlo et al., (2019), two-factors, ID theft prevention Tools produced from Information Securing Strategy and ID Theft Risk Assessment Tools produced from Risk Management& Assessment Process from Ula, Ismail and Sidek, (2011), and two factors ID Fraud Identification and ID Theft Prevention Barriers were developed from the findings of literature gape.

The remainder of this paper is organized into the following sections: a review of the literature; a discussion of the research methods employed; a presentation of the findings; a discussion of their importance; the theoretical contributions, limitations recommendations for future research; and, finally, the conclusion. Existing literature was reviewed from various electronic databases, search engines, books, Web Pages, newspapers and electronic media. To make it accurate, most articles and books are reviewed and cited in this research study project. In this study researcher has adopted a funnel approach for the research refinement process. Table 2 contains the relevant and frequently cited studies that have investigated information security tools. The information illustrates that although numerous studies have explored ID theft not in the specific context of the evolution of information security tools in the banking sector of Pakistan. Previous studies have investigated information security tools in a different context and reported different causes of ID theft in the banking sector, which implies that these barriers differ in the vulnerabilities in the effectiveness of the information security tools in the banking sector of Pakistan.

2. Literature review

Identity theft issues are rapidly growing and have been a major problem in the banking sector. Due to faster growth in ID frauds, it has increased attention of many researchers around the globe, such as, Naeem, Jawaid and Mustafa, (2023), Ullah, Majeed and Popp, (2023), Ibrar and Karim, (2023), Naseem et al., (2023), Saeed, (2023), Haque et al., (2023), Ahmad and Sheharyar Khan, (2022) Islam et al., (2022), (Malik et al., (2022), Javed, (2020), Altaf et al., (2021), N. Gana, M. Abdulhamid and A. Ojeniyi, (2019), Chinyemba and Phiri, (2018), Hussain et al., (2017), Soomro, Shah and Ahmed, (2016), Chioma Vivian Amasiatu and Mahmood Hussain Shah, (2014) Bose and Leung, (2013), Hoffmann and Birnbrich, (2012), Hoffmann and Birnbrich, (2012). However, ID theft is decreasing day by day and many people are not fully aware of the information security issues which causes violation of ID of bank accountholders which is a major concern of banking sector (Kahn and Liñares-Zegarra, 2016; Shareef and Kumar, 2012; Brody et al., 2007; W.Wang, 2006; Arab News PK, 2023).

However, proper education of security management, technology development, law enforcement and behavior can be helpful to fight against ID theft (WenJie Wang, Yufei Yuan and Archer, 2006). Useful information and appropriate training systems, educating staff on sharing institutional knowledge can prevent form ID theft (Abdullah, Mahmood Hussain Shah, 2016). Whereas, banks are focusing on system physical security which is not sufficient for secured access to the accounts at accountholder side. In Pakistan banks do not consider themselves fully responsible for protection from ID theft, but also account holders can have such a responsibility to protect their accounts from ID thieves.

Currently, most of the banks use old Information Technology (IT) infrastructure and workers are not fully aware of evaluating and managing the information security tools to prevent ID theft. Due to lack of advanced knowledge of ID theft prevention both management and account holders are being victimized by ID fraudsters (Maitlo et al., 2019) which causes various ID crimes in banking sector. To reduce such type of issue bank management have a responsibility to manage ID theft information security tools properly and from time to time inside the organization (Farooqi, 2017; Asfour and Haddad, 2014; Altobishi, Erboz and Podruzsik, 2018; Zulkhibri, 2019). According to Shah et al., (2019) and Maitlo et al., (2019) individuals and groups should need to enhance their knowledge for ID theft issue and protect themselves. Previous research suggest that financial institutions should implement the Knowledge-sharing (KS) process inside the bank (Maitlo et al., 2019). Furthermore, banks should have well-thought-out and implemented plans in place to mitigate the risk of data loss and minimize business downtime in the event of an ID theft attack or any service disruption (Marcin Kubacki, 2023). According to Selimić and Radivojević, (2017) application level protection, operating system level protection, network infrastructure level protection, and procedural and operational level protection can prevent form information security issues so to secure the customer's data bank should make a protective system and tighten up their defense methods and countermeasures.

Table 2 shows the existing literature has identified two main barriers, namely ID Fraud Identification and ID Theft Prevention to prevent ID theft in the banking sector. However, still research is required on barriers to preventing ID theft in banking sector of Pakistan in the context of ID theft. Therefore, this study have identified various barriers to prevent ID theft in Pakistan which include Information Sourcing Opportunities, Leadership support, Knowledge Management Infrastructure from (Preventing ID theft: Identifying major barriers to knowledge-sharing in online retail organizations) (Maitlo et al., 2019), and Information Securing Strategy and Risk Management and assessment Process from (The Initial Design of the Proposed ISG Framework) (Ula, Ismail and Sidek, 2011). If these 07 enablers are absent then the evolution of information security tools could not be effective and prevention cannot take place. In the context of ID theft prevention, several frameworks were reviewed (see Table 1). The KS enablers framework developed by Maitlo et al., (2019) was selected as a guiding framework. The guiding framework was selected based on below criteria:

1. **Functionality:** The framework should be capable of fulfilling the research objectives and functioning effectively.

2. **Comprehensiveness:** The framework should cover the factors for the prevention of ID theft but should not be overly complex.

3. **Adaptability:** The frameworks must be flexible and able to be modified or have adoptable factors for this study.

4. **Ongoing improvement:** The framework should focus on ongoing improvements, enabling the banking sector to further evolve the existing tools to make them more effectiveness in the tools.

5. **Empirically derived:** The framework should be derived from previous research and have empirical evidence supporting its effectiveness.

6. **Focused components:** The framework should have components that specifically address the research objectives.

Table 1 Reviewed Frameworks

S.#	Reviewed Framework	Information Infrastructure Security	ID Theft Prevention Tools	ID Theft Risk Assessment Tools	ID Fraud Identification Tools	ID Theft Prevention Barriers	Managerial Support for Information Security	Information Security Awareness Tool
1	Altaf et al., (2021)	X	X	✓	X	X	X	X
2	Maitlo et al., (2019)	✓	X	X	X	X	✓	✓
3	Baz, Samsudin and Che-Ahmad, (2017)	X	X	X	X	X	X	✓
4	Abdullah and Mahmood Hussain Shah, (2016)	✓	X	X	X	X	✓	✓

5	Aydın, (2014)	X	X	X	X	X	X	✓
6	Mahmood Shah, (2011)	X	X	X	X	X	✓	X
7	Ula, Bt Ismail and Sidek, (2011)	X	✓	✓	X	X	X	X
8	Salleh, (2010)	X	X	X	X	X	✓	✓
9	Srivastava and Rajesh, (2007)	X	X	X	X	X	✓	✓
10	Wilhelm, (2004)	X	X	X	X	X	X	✓

To select the appropriate guiding framework for this research study, various frameworks were closely studied

Table 2 Literature Findings

Vulnerabilities	**Source**
Information Security Infrastructure The infrastructure of some banks has not fully evolved yet because as a developing country, Pakistan is one step back in adopting technological advancement due to limited resources, and untrained staff for technology adoption or performing any security operation. Developing and implementing effective security measures is an industry-wide concern and requires that the STATE Bank of Pakistan (SBP) conduct audits of commercial banks' security protocols and investigate the underlying reasons for their weak governance structures. Additionally, the SBP needs to address the issue of data hacks not being reported to the central bank. By doing so, the SBP can identify and rectify vulnerabilities, strengthen governance practices, and ensure that data breaches are promptly reported, leading to improved security in the banking sector.	Naeem, Jawaid and Mustafa, 92023), Ahmad and Sheharyar Khan, (2022), Haque et al., (2023), Ibrar and Karim, (2023) and Reporter, (2022)
ID Theft Prevention Tools The banking sector of Pakistan is using various ID theft prevention tools and measures to protect customer information and prevent ID theft. The banking sector of Pakistan does not have security parameters (lack of awareness about tools, and technology) to prevent form ID theft which is increasing more challenges for financial Institutions of Pakistan. IT security team management ensures for regular nationalities all incoming emails and the information of all clients are safe and secure, updates advanced authentication techniques, adopts the latest technology, develops policies, and implements strategies to safeguard cyberspace and properly trains employees can protect from ID theft.	Mohsin et al., (2019), Lodder, (2023), Bhasin and Reporting, (2016), N. Gana, M. Abdulhamid and A. Ojeniyi, (2019), Azhar-Ibrahim, (2023), Bhasin and Reporting, (2016), Malik et al., (2022), Ahmad and Sheharyar Khan, (2022), Chioma Vivian Amasiatu and Mahmood Hussain Shah, (2014), Malik et al., (2022) and Ahmad and Sheharyar Khan, (2022)
ID Theft Risk Assessment Tool most of the banks are utilizing only mapping techniques, key risk indicators, and self-assessment tools to identify risk. Further improvement on the authentication methodologies requires adherence to security standards as may be spelt out by the banking information security framework. Some possible methods for ID theft prevention and fraud detection suggested by different researchers such as Firewall and filtering software to be installed on the computer system, Operational audits, Performance audits, Ethics officers, Internal control review and improvement, Cash reviews and Password protection. Strong monitoring mechanisms are necessary for an effective risk management system.	Altaf et al., (2021), N. Gana, M. Abdulhamid and A. Ojeniyi, (2019), N. Gana, M. Abdulhamid and A. Ojeniyi, (2019), Zamzami, Nusa and Timur, (2016), Bologna, (1993), Haugen and Selin, (1999), Bierstaker, Brody and Pacini, (2006), J., (2004) and Mufti, Arshad and Haqqani, (2023).
ID Fraud Detection Tools	Rahman and Anwar, (2014), Shah,

There are different fraud mechanisms used by the banking sector to detect fraud, the most common techniques are ethics training, inventory observations, fraud hotline, password protection, continuous auditing, data mining and reference checks on employees Fraud detection is a set of activities to stop ID theft before it is detected, so the above fraud detection tools are not enough to prevent ID theft, but increasing information security tools, and implementing organizational ID theft prevention methods (thread assessment, firewall database, and network access) and awareness about strong information flow encryption may prevent from ID theft and can be helpful to detect the fraud earlier. Furthermore, developing new fraud detection techniques and prevention is not possible until customers know about theft and the way of attack.	Ahmed and Soomro, (2016), Chinyemba and Phiri, (2018) and Hoffmann and Birnbrich, (2012)
Managerial Support for Information Security The laws and regulations supporting online banking in Pakistan are insufficient, lacking in compensating customers for any financial losses during transactions. To address these challenges, financial institutions and government agencies should prioritize training cybersquatting professionals and increasing general awareness among citizens through campaigns in educational institutions and public spaces. Pakistan is at risk of being targeted by state-sponsored hackers, highlighting the need for better risk management by managers and higher authorities to make informed operational and strategic decisions.	Naeem, Jawaid and Mustafa, (2023), Ibrar and Karim, (2023) and Ullah, Majeed and Popp, (2023)
Information Security Awareness Tool Pakistan banks face several social challenges, including low levels of education, poverty, and a lack of access to technology, which make it difficult for people to protect themselves from cyber threats. Untrained staff and lack of awareness among staff about the latest information security threats faced by the online banking industry in Pakistan	Ibrar and Karim, (2023), Naeem, Jawaid and Mustafa, (2023), (Ibrar and Karim, (2023), Ahmad and Sheharyar Khan, (2022), Javed, (2020) and Hussain et al., (2017)

Table 2 provides a summary of the literature reviewed. It identifies seven main vulnerabilities in the effectiveness of ID theft in the banking sector of Pakistan. Based on an analysis of the studies in Table 1, it can be argued that Preventing ID theft: Identifying major barriers to knowledge-sharing in online retail organizations (Maitlo et al., 2019) does not cover all the vulnerabilities existing in the effectiveness of the ID theft in the banking sector of Pakistan, So three-factor Information Security Awareness Tool produced form Information Sourcing Opportunities, Managerial Support for Information Security tools produced from Leadership support, Information Security Infrastructure produced from Knowledge Management Infrastructure of the guiding framework proposed by Maitlo et al., (2019), two-factor, ID theft prevention Tools produced from Information Securing Strategy and ID Theft Risk Assessment Tools produced from Risk Management& Assessment Process from Ula, Ismail and Sidek, (2011), and two factors ID Fraud Identification and ID Theft Prevention Barriers were developed from the literature gap. The seven barriers proposed in the framework for this study are discussed in the following sections.

2.1. Information Security Infrastructure Tools

The information security infrastructure of the banking sector refers to the combination of technologies, policies, and practices implemented to safeguard sensitive data, prevent unauthorized access, detect and respond to security incidents, and ensure the confidentiality, integrity, and availability of information within the banking industry. However, during the literature review we found that Pakistan is way back in technological advancement due to limited resources, and untrained staff for technology adoption and performing information security operations (Naeem, Jawaid and Mustafa, 2023). Currently, Pakistan is facing numerous challenges, including a lack of cyber security awareness, a shortage of trained personnel, and a weak IT investigation infrastructure (Haque et al., 2023). Ahmad and Sheharyar Khan, (2022) highlighted that banking sector in Pakistan have not fully stablished cyber security infrastructure which causes more challenges for Pakistani banks (Saeed, 2023). Therefore, it is accessory to evolute information security infrastructure and its tools for effective and secured Cyber security infrastructure in banking sector of the country have robust security tools .

2.2. ID Theft Prevention Tools

The banking sector of Pakistan is using various ID theft prevention tools and measures to protect customer information and prevent ID theft. According to Mohsin et al., (2019), Lodder, (2023), Bhasin and Reporting, (2016), N. Gana, M. Abdulhamid and A. Ojeniyi, (2019), Azhar-ibrahim, (2023), Bose and Leung, (2013), Qureshi, Baqai and Qureshi, (2018) and Bhasin and Reporting, (2016) several evolved tools are used banking sector. However, banks in Pakistan use old conventional information security tool, which may cause rapid growth of ID theft in Pakistan (Malik et al., 2022; Ahmad and Sheharyar Khan, 2022). Therefore, it is required to investigate existing cyber security tools to prevent ID theft and evolve them as per requirements of current time.

ID Theft Risk Assessment Tools

In the banking sector, risk assessment tools are essential for identifying, evaluating, and managing various ID theft threats (Mufti, Arshad and Haqqani, 2023; Mufti, Arshad and Haqqani, 2023 and Lin, 2023). According to N. Gana, M. Abdulhamid and A. Ojeniyi, (2019) and N. Gana, M. Abdulhamid and A. Ojeniyi, (2019) the use of biometric authentication during transaction processing can perform significant role in managing risk factor in the banking sector. However, banks of Pakistan are utilizing only mapping techniques, key risk indicators, and self-assessment tools to identify risk (Altaf et al., 2021; N. Gana, M. Abdulhamid and A. Ojeniyi, 2019) which is not sufficient to assess the risk before it perform. Therefore, it is required to identify the risk assessment process and evolve its tools to prevent ID theft in banking sector of Pakistan.

2.3. ID Fraud Identification Tools;

Several security challenges are faced by Pakistan that impact its development and progress (Ibrar and Karim, 2023). During literature review we found that various prevention systems have been implemented i.e. Secure Electronic Transaction protocol (SET) and Sockets Layer (SSL) (Parusheva, 2009 and Dandash et al., 2008) and Fraud Detection Systems. Banks employ sophisticated fraud detection systems that use machine learning algorithms and artificial intelligence to identify potential instances of identity fraud (Pakistan, 2023). The common types of customer authentication methods to detect fraud are fingerprint (DeVries, 2011), Token-based authentication (Lodder, 2023; Balaj, 2017; and Tiller, 2008), Knowledge-based authentication and Biometric -based authentication (Tiller, 2008), several security-related technologies are including (Azhar-Ibrahim, 2023) and automated analysis tools, data visualization tools, sector-oriented benchmarking solutions, behavioral analytic, the internal audit function, and deep learning tools (Bhasin and Reporting, 2016). All the above tools play a crucial role in ensuring the security and protection of sensitive information in the banking industry. Different fraud detection mechanisms have evolved which are under the usage of the banking sector (Rahman and Anwar, 2014). Instead of having tools and technologies for ID fraud detection, theft issues are increasing day by day (Chinyemba and Phiri, 2018). Therefore, we need to evaluate fraud detection tools to prevent ID theft in banking sector of Pakistan.

2.4. Managerial Support for Information Security Tools

In an organization support of management is mandatory. While talking about managerial support for information security within and organization, it is inevitable to secure the infrastructure and resources of bank without managerial support. According to Abdullah et al (2019) without managerial support it is not possible to secure the information and resources within organization. In Pakistan banking sector requires huge need for strategic planning for ID theft prevention. Banks require major support for arranging, implementing and monitoring information security tools to prevent ID theft. Therefore, it requires to identify the managerial support for evaluating information security tools to bring in robust information security infrastructure with fully capable security tools (Ibrar and Karim, 2023).

2.5. Information Security Awareness Tools

In an organization it is important to have skillful and knowledge oriented employees working in the organization. Lack of awareness can be major issue for organization including banks. Therefore, employee awareness of information security infrastructure and its tools is a mandatory element in banking sector. Employees may be familiar about the problems but not the solutions to resolve the information security issues (Hong et al., 2011). According to Riege (2007), employees should be aware of the requirements and knowledge gaps of the other employees, teams and organizations who are receiving the knowledge (reference). Employees, including senior managers, must be aware of the importance (Van den Hooff et al., 2003) of an effective use of information security tools in a bank. However, in many banks, raising awareness of the benefits of information security is a challenge (Zahedi et al., 2016). Communicating about the bank's security policy and developing awareness programs are main sources of increasing staff awareness of information security to prevent ID theft (Flores et al., 2014). However, according to Ibrar and Karim, (2023) in Pakistan people face many challenges, including low level of education, poverty, and a lack of access to technology, which make it difficult for people to protect themselves from cyber threats. Untrained staff and lack of awareness among staff about the latest information security threats faced by the banking industry in Pakistan (Naeem, Jawaid and Mustafa, 2023; Ibrar and Karim, 2023; Ahmad and Sheharyar Khan, 2022; Javed, 2020 and Hussain et al., 2017). Due to such type of weakness non-technical personnel system always remains under target by the cyber-criminals (Hussain et al., 2017). Therefore, it is required to investigate existing information security awareness tools to prevent ID theft in banking sector of Pakistan.

Table 2 summaries the literature review of this paper. During research refinement we found seven essential aspects required for the evolution of information security tools in preventing ID theft in the banking sector of Pakistan. These aspects include information security infrastructure, ID theft prevention tools, ID theft risk assessment tools, ID fraud identification tools, ID theft prevention barriers, managerial support for information security, and information security awareness tools. It is required to investigate the identified aspects for information security tool evolution. Furthermore, there is a need for research that identifies vulnerabilities in the effectiveness of information security tools specifically in the banking sector of Pakistan. Despite numerous studies on ID theft prevention, there is a lack of research on the evolution of information security tools in the context of preventing ID theft in Pakistani banks which is a gap in existing body of knowledge. This study aims to bridge this gap by investigating the effectiveness of information security tools in preventing ID theft in the banking sector of Pakistan. It proposes a framework and provides solutions for addressing vulnerabilities in the effectiveness of these tools. The study aims to provide comprehensive answers to unanswered questions in the existing literature.

1) How effective evolution of information security tools to prevent ID theft in the banking sector of Pakistan?

2) What is the vulnerability in the effectiveness of the information security tools to the prevention of ID theft in the banking sector of Pakistan?

3) How can the banking sector overcome the existing vulnerabilities which may cause of ID theft in the banking sector of Pakistan?

2.6. Research Methodology

The main sources of data are documentation, archival records, interviews, direct observations and participant observation (Yin, 1994, 2011). This research has used the case study to find out the accurate results (Merriam, 2001). According to Yin (1994), whrn you design the case study it must have these five basic components. 1. Research question,2. propositions, 3. The units of analysis pf the study, 4. Its determination about how the data is linked with the above component one and two to interpret the research findings. Yin (1994, 2011) the case studies are very important strategy which are preferred when "how" and "why" questions are posed. Therefore, the case study approach is very suitable for this research study to gain the accurate knowledge about the existing information tools and its evolution in the banking sector of Pakistan. The case study approach includes data collection, data analysis, and reporting and presenting the results of the analysis (Yin, 2011). This research used several data-collection methods: analysis of internal and external documents from the selected banks in Pakistan (including memos and survey reports); analysis of the banking sector of Pakistan websites; an investigation of news about the banks in print and electronic media; and interviews with employees. Both internal and external documents from the banks were analyzed.

Using the archival analysis method, these documents were examined in order to understand the bank's existing information security tools to prevent ID theft and evolution process of cyber security for ID theft prevention in banking sector. The analysis focused on any evidence of identity theft, reasons for stealing data from bank accounts, the steps taken to overcome these problems, and existing information security policies and processes for preventing identity theft in banks. The external documents investigated included news reports on the organizations published in print and digital media, including STATE Bank of Pakistan, Financial Monitoring Unit, Banking Muhatasib Pakistan, Federal Muhatasib Pakistan, Federal Investigation Agency, Cabinet Division and Financial Monitoring Unit, GEO NEWS, DAWN NEWS and others. These reports were examined for any evidence of or clues about identity theft and its prevention. Furthermore, various websites were studied, focusing on publications about information security tools to prevent identity theft in banking sector of Pakistan. The qualitative method used also included interviews. Therefore, interviews were conducted with individual employees to identify how they experienced concerns about information security in the context of preventing identity theft and evolution of information security tools.

Initially, the researchers conducted a review of the related literature to assess the extent of the work on information security tools to prevent identity theft. Based on this analysis, a list of interview questions was developed. The interview questions were underpinned by knowledge sharing framework to prevent ID theft proposed by Abdullah et al. (2019) and A Framework for the governance of information security in banking system proposed by Ula, Ismail and Sidek, (2011). A pilot study was conducted using ten semi-structured interviews with MS/MPhil and PhD research students in the relevant field at a University of Pakistan. Following the pilot study, irrelevant and duplicated questions were removed, the sequence of questions was altered, and the wording was amended to ensure clarity for participants. The researchers conducted thirty-one semi-structured interviews with employees in three banks in Pakistan: Bank X, Bank Y and Bank Z (renamed for anonymity). These banks were selected because they have digital infrastructure along with online transaction processes. The participants ranged from senior management to support staff, and they were working in teams and groups. The detail of the participants is showing in table 4 and 5. A total of 13 interviews were conducted in various branches in bank X. At bank Y, the researchers conducted 12 face-to-face interviews. In addition, 6 interviews were conducted with participants working at bank Z. Appendix 1 includes information about each of the three banks.

The semi-structured interviews were conducted face to face and lasted for between 40 and 60 mints. In some cases, additional questions were asked to clarify the interviewees' responses and obtain clear data for analysis. The sequence of the questions was also altered during the interviews depending on the responses of the interviewees. Before the data collection started, a confidentiality agreement was signed with the management of the bank. The researchers obtained consents from interview participants via e-mail and telephonic call before conducting the interviews. Thematic analysis was conducted using a qualitative coding process (Braun and Clarke, 2006). The data collected from employees in the three banks were coded to establish patterns. NVivo software and manual coding were used for the thematic analysis. Various nodes (codes) were generated from group participants' interview responses, which were based on the themes that emerged in the literature review.

3. Findings

Existing Information security tools are discussed below in the context of the literature review.

3.1. Information Security Infrastructure Tools

Researchers found that banks have security infrastructure at some extent but it is not maintained appropriately. The infrastructure is not up-to-date (R1, Bank-X). Furthermore, participants from all case banks informed that:

"Infrastructure requires further evolution because it has several security tools are not updated".

Participants of Bank (Y and Z) said that till to any incident happens infrastructure stops doing work or when fraud accurse then the centralized security team is aware of it, and updates the security infrastructure, before that, it not possible for the bank to update or do further evolution. Whereas (R3, Bank-Y and R4, Bank-Z) responded that:

We admit that fraudsters are one step ahead of us as they use most up dated tools and techniques to breach in infrastructure of banks".

For the above issue, it was highlighted that all three banks should have up-to-date and updated infrastructure as more than more prevention can be possible.

3.2. ID Theft Prevention Tools

Researchers found that banks have few security tools. However, most of them have limitations, such as, neither they are up to date nor user-friendly. Respondents from the banks (X, Y and Z) responded that:

"Tools are difficult to use and employees do not follow the controls/ rules which may cause the ID theft issues in the bank".

Participants of Bank X and Y were briefed and informed that:

"Several tools are available but all are useless until employees of banks don't know the security importance".

The (R4, R6 Bank-X, R2, R3, R6, R10 Bank-Y and R1, R2, and R5 Bank-Z) admitted that most of the bank employees are skipping the security tools due to the locality, so to prevent ID theft issues regulators should develop an effective strategy for properly monitoring, accurate usage of tools, implementation of lines of defense architecture and coordination of the tools may help to achieve more security.

3.3. ID Theft Risk Assessment Tools

While exploring commonly used risk assessment tools, Bank X-Y and Z have identified areas where improvements can be made. Currently, they do not have a specific assessment tool in place, but they have assigned certain employees to handle risk-checking duties. They check the Risk at the time of the customer complaints or any incident that happens before they are not responsible or bound to check. Further, it identified by Bank (X, Y and Z) that:

"Only banks have manual risk assessment/self-assessment which evaluate during audit or surprise visits".

(R2, Bank-X, R5, Bank-Y, R3, R5, and Bank-Z) don't have any tools any check when transactions are performed. The Bank is aware only of the customer's complaints about ID theft issues (R6, Bank-Y) because the identity of the customer is not identified by the customer.

3.4. ID Fraud Identification Tools

In the banking sector of Pakistan, there are some identity fraud identification tools and measures in place to mitigate the risk of ID theft but all three banks don't have any fixed tool to identify the fraud without biometrics, CBC, or signature verification as well as they are using their experiences and they identify the fraud.

Just banks have very normal security tools such as authentication, and card (NIC) systems, Key factors are in the area of cash, two-factor authentication and customer thumb impressions (R5, Bank-Z). Participants of three banks admitted:

"Banks have accounts in thousands so daily we can't see or check".

This is not possible for the bank can identify any fraud before it is so, the customer should take care by self (R5, Bank-X and R2, R7, Bank-Y) because on the branch level, we have normal security tools such as authentication, card (NIC) system. Key factors are in the area of cash, two-factor authentication and customer thumb impressions are implemented (R2, Bank-Z).

3.5. Managerial Support for Information Security Tools

During this study it was analyzed that management supports a lot but still focuses on their business, till any mishap does not happen management cannot be serious (R7, Bank -Y). When any incident happens then the bank realizes and starts evolution in any strategy or tools (R10, Bank-X). All three banks admitted that management does not provide sufficient budget for developing new strategies, plans or tools. Banks need to further evolution in the software/tools as more than more prevention can be possible (R3, R6, Bank-X and R7, R9, Bank-Y) and management should provide sufficient budget for developing new strategies or new tools as security can be possible and can prevent from ID theft issues before it commits or performs (Bank-Z). There is much difference in our training and lower employees' understanding, there is a dire need for management to train the employees through the training sessions conducted by the experts of the bank to prevent ID theft issues (R3, R8, Bank Y).

3.6. Information Security Awareness Tools

During the investigation of the causes of the vulnerabilities in the effectiveness of the evolution of information tools, it was admitted by all three banks that bank employees have the most common source of awareness email, centralized email, WhatsApp group Facebook, etc. Head office to head office means Bank-X head office to Bank-Y head office circulates the email for fraud. Regular training is being arranged by the MDC – Management Development Center in the bank to disseminate the latest information regarding ID theft and its prevention. Management monthly dispatch emails and they arrange the meetings and inform about ID theft issues (Bank X, Y and Z). The phish rod tool is most commonly used (R3, Bank-Z). Bank have awareness tools such as meeting, group discussion, experience shared, WhatsApp group, morning or evening meetings and huddles (R2, R6, Bank-X, R1, R3, Bank-Y and R5, R2, Bank-Z). The bank provides training, time to time training for different departments, The Bank has fraud and forgery departments individually they also guide timely (R10, R11, Bank X, R3, Bank-Y and R7, Bank-Z).

3. Cross-case comparison of Bank-X, Bank-Y and Bank-Z

All three banks are compared to cross-verify the results of banks X, Y and Z.

Information Security Tools to Prevent ID Theft	Availability in Three Banks	Bank-X	Bank-Y	Bank-Z	Recommendations of this study
Information Security Infrastructure	Yes	Yes	Yes	Yes	Banks always face three to four risks, such as operational risk, reputational risk, and financial risk, because several things are not systematically implemented in some banks. system maintenance or update on the time of requirement by a third party 70% of infrastructure should improve more as per the latest technology.
ID Theft Prevention Tools	Yes	Head Office Level and Branch Level	Head Office Level and Branch Level	Head Office Level and Branch Level	Bank employees skip the security tools due to the shortage of staff, and no seat work one main cause of skipping security tools is the locality which may cause ID theft issues in the banking sector. Banks should tighten up security rules, develop good strategies and bind employees to follow rules and regulations by using security tools. Awareness of the latest technology is very important which should be in each employee from top to low level employee.

ID Theft Risk Assessment	Yes	Manual Assessment	Manual Assessment	Manual Assessment	The banking sector of Pakistan has self-risk assessment techniques, which have not evolved yet. Banks don't have any evolved tool to assess the theft risk, still adopting earlier generation tools such as manual performing, bank employees aren't aware of ID theft before it is committed. Banks should develop a risk assessment process and adopt it regularly so they can be aware of the fraud at the time of risk or fraud happening. When any employee inserts any entry, it should go to the BM for supervision
ID Fraud Identification Tool	Yes	Head Office Level	Head Office Level	Head Office Level	Bank should implement biometric and CBC security tools on each transaction or any customer activity such as getting a cheque book, depositing an amount or withdrawing an amount regularly whether the limit exceeds or not.
Managerial Support for Information Security Tool	Yes	Yes	Yes	Yes	The existing system needs to be upgraded and needs to change the software Up-to-date. Globally attack patterns are running, so banks should make them part of the defense strategy. Banks should invest in security programs, security staff, and security strategies to improve or mature security.
Information Security Awareness Tool	Yes	Yes	Yes	Yes	100% of employees have needed to get training. Training must be provided in any case either staff member is out of the city or busy

Table- 3 Cross-Case comparison of Bank-X, Bank-Y and Bank-Z

Table 3 highlights the security measures which are adopted by the banking sector of Pakistan. Banks (X, Y and Z) have security tools to prevent ID theft but lack awareness about the latest technology. To detect fraud banks (X, Y and Z) have tools but all are operating only at the head office level, Banks (X, Y and Z) don't have any risk assessment process through which they can identify the ID theft risk before it is performed. When it was investigated it found that banks have managerial support available but not at a high level. Banks (X, Y and Z) are providing ID theft prevention awareness training but not arranged by the experts of the IT department and don't have any awareness campaign for the bank customers.

1. Discussion

The primary aim of this research was to investigate the effectiveness of the evolution of information security tools and find out the vulnerabilities in the evolution of information security tools to prevent ID theft in the banking sector of Pakistan:

1) How effective evolution of information security tools to prevent ID theft in the banking sector of Pakistan?

2) What are the vulnerabilities in the effectiveness of the information security tools in the prevention of ID theft in the banking sector of Pakistan?

3) How can the banking sector overcome the existing vulnerabilities which may cause of ID theft in the banking sector of Pakistan?

By answering these questions, this research sought to fill the gap in the literature and banking sector to prevent ID theft by improving the effectiveness of the evolution of information security tools. Identifying theft is becoming an increasing concern, with rising numbers of cases.

Through the extensive literature review, six main vulnerabilities were identified (see Table 2). Data were collected from thirty-one semi-structured interviews and an examination of the internal documents of the banks under study. The research has developed a new framework by developing (06) factors: Information security infrastructure, ID Theft Prevention Tools, ID Theft Risk Assessment Tool, ID Fraud Identification Tool Managerial Support for Information Security; Information Security Awareness Tool by borrowing two factors Information sourcing opportunities, Leadership support and Knowledge Management Infrastructure from the guiding framework proposed by (Maitlo et al., 2019), two factors information securing strategy and risk management & assessment process from (Ula, Ismail and Sidek, 2011), and two were developed through findings of this research study.

To answer the 1st and 2nd questions certain banking sectors are neglecting the implementation of security tools due to their locality. Despite having strategies in place, these security measures are not being properly implemented, leaving vulnerabilities within the banking systems (The summary of the Perceived Effectiveness of the tools is given in Table 3). In addition to the previous findings, it is important to highlight that there is a significant lack of awareness among individuals regarding the potential security issues and risks related to ID theft. This problem is further compounded by the absence of awareness campaigns by banks. Furthermore, my research uncovered that banks do not have a formalized risk assessment process in place. Instead, bank employees tend to assess risks on an ad hoc basis, with some conducting assessments only once every one or two years. The absence of a fixed time frame for risk assessment in banks can expose them to potential threats and raise the risk of security breaches. Relying solely on audits or surprise visits to identify risks may not offer a comprehensive and proactive approach to risk management. Banks need to establish regular and systematic risk assessment processes to effectively mitigate potential threats and enhance security measures.

This study highlights the importance of implementing and updating information security tools in the banking sector. Banks should prioritize the security of their systems and effectively implement strategies to protect against potential threats. Public education and awareness about information security and ID theft risks are also crucial. By addressing these issues, the banking sector can enhance its overall security and better protect customer interests. It is further recommended that banks establish a structured and regular risk assessment process to identify and address vulnerabilities on time. Implementing a standardized risk assessment framework, along with effective information security tools, will safeguard against potential threats and ensure the integrity and confidentiality of customer data.

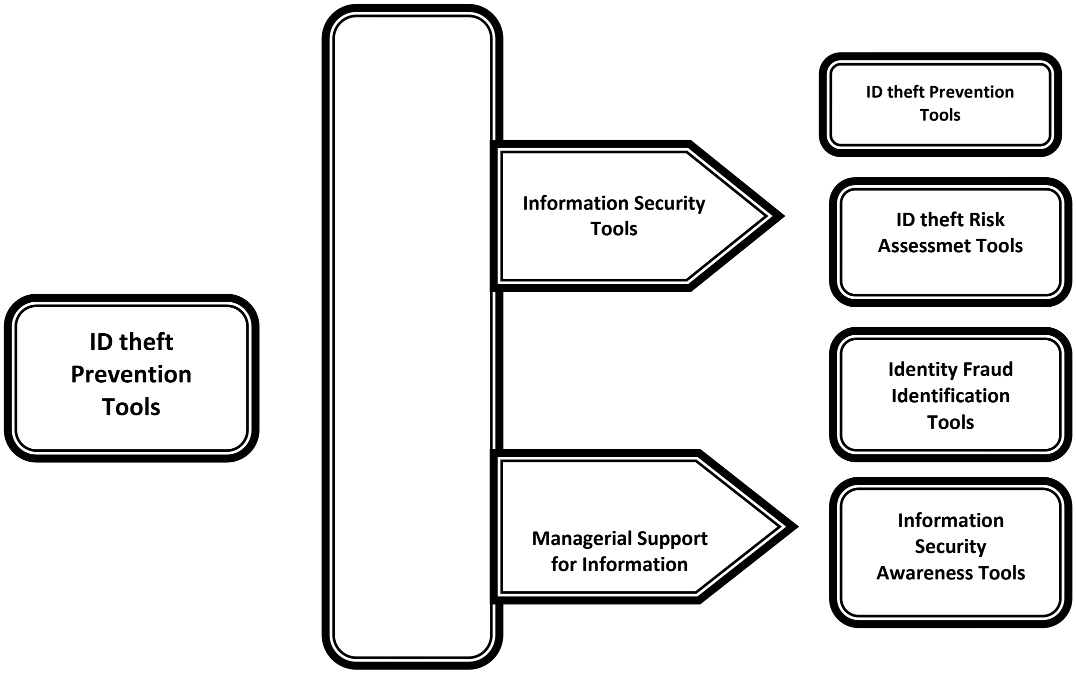

ID theft Prevention Tools
Information Security Tools
Managerial Support for Information
ID theft Prevention Tools
ID theft Risk Assessmet Tools
Identity Fraud Identification Tools
Information Security Awareness Tools

Figure 1. Effectiveness of IS Tools to prevent ID Theft in Banking Sector of Pakistan Framework

In response to the second research question, the findings have revealed that 2nd research question, based on the findings from analyses of the data collected in this research, the framework shown in (Figure-1) is proposed. This framework includes the major vulnerabilities in the effectiveness of the evolution of information security tools for the prevention of ID theft in the banking sector of Pakistan and is based on the conceptualization and development of Preventing ID Theft: Identifying Major Barriers to Knowledge-sharing in online retail organizations proposed by (Maitlo et al., 2019).

The developed framework consists of six factors Information security infrastructure, ID Theft Prevention Tools, ID Theft Risk Assessment Tools, ID Fraud Identification Tools, Managerial Support for Information Security and Information Security Awareness Tools.

6. Theoretical contributions and practical implications

This study examines the evolution of information security tools in the banking sector of Pakistan to prevent ID theft. Before this study, no research had been done on this topic in Pakistan's banking sector. The findings reveal that while the banking sector has evolved information security tools, there is a lack of security awareness among employees and customers. Some employees lack the necessary knowledge to effectively use the existing tools, leading to potential ID theft. The study also found that banks do not have specialized tools for detecting fraud early or a formal risk assessment process. Additionally, there is a lack of awareness campaigns for the general population to educate them about ID theft. This study fills a gap in the existing research and provides a new framework for preventing ID theft in the banking sector of Pakistan.

7. Limitations and future work

The findings of this study are based on three reputational banks in Pakistan. Therefore, further research is required using an empirical method and focusing on larger numbers of banks. This study is limited by the use of the case study approach, the small number of interviews conducted, the number of internal bank documents examined, and the lack of availability of existing literature and data from the banks due to confidentiality concerns. Therefore, future research can adopt quantitative research methods to test the validity of the research outcomes across the banking sector of Pakistan. The researchers card out this study in the banking sector of Pakistan. Further research is recommended for the expansion of this study to include other countries.

8. Conclusion

The research highlights the need for greater emphasis on implementing and updating information security tools within the banking sector. Banks must prioritize the security of their systems and ensure that strategies are effectively implemented to protect against potential threats. Additionally, efforts should be made to educate and raise awareness among the public about the importance of information security and the risks associated with ID theft. By addressing these issues, the banking sector can enhance its overall security posture and better protect the interests of its customers. Further emphasizes the need for banks to establish a structured and regular risk assessment process. By conducting frequent assessments, banks can identify and address potential vulnerabilities on time, reducing the chances of security incidents. Implementing a standardized risk assessment process will enable banks to proactively identify, evaluate, and mitigate risks, ultimately enhancing the overall security of their systems and ensuring the protection of customer information. It is recommended that banks prioritize the development and implementation of a robust risk assessment framework, in conjunction with the adoption of effective information security tools, to safeguard against potential threats and ensure the integrity and confidentiality of customer data.

REFERENCES

Abbasi, A., Zahedi, F. and Chen, Y. (2012) 'Impact of anti-phishing tool performance on attack success rates', ISI 2012 - 2012 IEEE International Conference on Intelligence and Security Informatics: Cyberspace, Border, and Immigration Securities, (July 2016), pp. 12–17. doi: 10.1109/ISI.2012.6282648.

Abdullah, Mahmood Hussain Shah, W. A. (2016) 'Identity theft prevention in online retail organisations: a knowledge sharing framework', The Business and Management Review, 8(August), p. 71. Available at: http://www.abrmr.com/myfile/conference_proceedings/Con_Pro_27018/conference_53625.pdf.

Ahmad, B. and Sheharyar Khan, M. (2022) 'Cyber Threat to Pakistan National Security: National Security and Threat Perception', Pakistan Review of Social Sciences, 3(1), p. 2022.

Akhtar, M. I. (2016) 'Research design Research design', Research in Social Science: Interdisciplinary Perspectives, (September), pp. 68–84.

Altaf, K. et al. (2021) 'Do operational risk and corporate governance affect the banking industry of Pakistan?', Review of Economics and Political Science, ahead-of-p(ahead-of-print). doi: 10.1108/reps-12-2019-0156.

Altobishi, T., Erboz, G. and Podruzsik, S. (2018) 'E-Banking Effects on Customer Satisfaction: The Survey on Clients in Jordan Bankingand Sector', International Journal of Marketing Studies, 10(2), p. 151. doi: 10.5539/ijms.v10n2p151.

Arab News PK (2023) Inadequate Cyber Security a Threat to Banking Sector. Available at: https://www.arabnews.pk/node/1404776/business-economy (Accessed: 27 July 2023).

Asfour, H. K. and Haddad, S. I. (2014) 'The Impact of Mobile Banking on Enhancing Customers ' E-Satisfaction : An Empirical Study on Commercial Banks in Jordan', International Business Research;, 7(10), pp. 145–169. doi: 10.5539/ibr.v7n10p145.

Aydın, D. (2014) 'Customer Perception towards the Internet Banking Services Performed by the Turkish Banking System', Institute of Graduate Studies and Research, (February).

Azhar-ibrahim, B. (2023) 'Secure Socket layer : Fundamentals and certificate verification', (June), pp. 9–14. doi: 10.20944/preprints202306.0869.v1.

Balaj, Y. (2017) 'Token-Based vs Session-Based Authentication : A survey', research gate, (September), pp. 1–6.

Baz, R., Samsudin, R. S. and Che-Ahmad, A. (2017) 'The Role of Internal Control and Information Sharing in Preventing Fraud in the Saudi Banks', Journal of Accounting and Financial Management, 3(1), pp. 7–13. Available at: www.iiardpub.org.

Bhasin, M. and Reporting, I. (2016) 'Integration of Technology to Combat Bank Frauds: Experience of a Developing Country', WULFENIA JOURNAL KLAGENFURT, AUSTRIA, 23, n.2(February).

Bierstaker, J. L., Brody, R. G. and Pacini, C. (2006) 'Accountants' perceptions regarding fraud detection and prevention methods', Managerial Auditing Journal, 21(5), pp. 520–535. doi: 10.1108/02686900610667283.

Bose, I. and Leung, A. C. M. (2013) 'The impact of adoption of identity theft countermeasures on firm value', Decision Support Systems, 55(3), pp. 753–763. doi: 10.1016/j.dss.2013.03.001.

Brody, R. G. et al. (2007) 'PHISHING , PHARMING AND IDENTITY THEFT', Academy of Accounting and Financial Studies Journal, 11(3), pp. 43–56.

Chinyemba, M. K. and Phiri, J. (2018) 'An investigation into information security threats from insiders and how to mitigate them: A case study of Zambian public sector', Journal of Computer Science, 14(10), pp. 1389–1400. doi: 10.3844/jcssp.2018.1389.1400.

Chioma Vivian Amasiatu and Mahmood Hussain Shah (2014) 'First party fraud : a review of the forms and motives of fraudulent consumer behaviours in e-tailing', International Journal of Retail & Distribution Management, 42(9), pp. 805–817. doi: 10.1108/IJRDM-05-2013-0112.

Dandash, O. et al. (2008) 'Fraudulent internet banking payments prevention using dynamic key', Journal of Networks, 3(1), pp. 25–34. doi: 10.4304/jnw.3.1.25-34.

DeVries, P. D. (2011) 'The problem of fraud in the banking industry: Are biometrics the answer?', International Journal of Services and Standards, 7(3/4), pp. 310–327. doi: 10.1504/ijss.2011.045055.

Draucker, C. B. et al. (2007) 'Theoretical sampling and category development in grounded theory', Qualitative Health Research, 17(8), pp. 1137–1148. doi: 10.1177/1049732307308450.

Farooqi, R. (2017) 'IMPACT OF INTERNET BANKING SERVICE QUALITY ON CUSTOMER SATISFACTION', Journal of Internet Banking and Commerce, 22(1), pp. 1–17.

Fielding & Thoma (2011) Qualitative Research Interviewing, Qualitative Research Interviewing. doi: 10.4135/9781849209717.

Gemmell, R. M., Boland, R. J. and Kolb, D. A. (2012) 'The Socio-Cognitive Dynamics of Entrepreneurial Ideation', https://doi.org/10.1111/j.1540-6520.2011.00486.x, 36(5), pp. 1053–1073. doi: 10.1111/J.1540-6520.2011.00486.X.

Haque, E. U. L. et al. (2023) 'Cyber Forensic Investigation Infrastructure of Pakistan : An Analysis of the Cyber Threat Landscape and Readiness', IEEE Access, 11(March), pp. 40049–40063. doi: 10.1109/ACCESS.2023.3268529.

Hoffmann, A. O. I. and Birnbrich, C. (2012) 'The impact of fraud prevention on bank-customer relationships: An empirical investigation in retail banking', International Journal of Bank Marketing, 30(5), pp. 390–407. doi: 10.1108/02652321211247435.

Hussain, M., Reza, H. and Yasin, N. M. (2014) 'The determinants of individuals ' perceived e-security : Evidence from Malaysia', International Journal of Information Management, 34(1), pp. 48–57. doi: 10.1016/j.ijinfomgt.2013.10.001.

Hussain, Z. et al. (2017) 'E-Banking Challenges in Pakistan: An Empirical Study', Journal of Computational Chemistry, 05(02), pp. 1–6. doi: 10.4236/jcc.2017.52001.

Ibrar, M. and Karim, S. (2023) 'Tackling Pakistan ' s Cyber Security Challenges : A Comprehensive Approach Tackling Pakistan ' s Cyber Security Challenges : A Comprehensive Approach', (May). doi: 10.6633/IJNS.202305.

Islam, U. et al. (2022) 'Detection of Distributed Denial of Service (DDoS) Attacks in IOT Based Monitoring System of Banking Sector Using Machine Learning Models', Sustainability 2022, Vol. 14, Page 8374, 14(14), p. 8374. doi: 10.3390/SU14148374.

J., G. G. (2004) 'Identity theft: the US legal environment and organisations' related responsibilities', Journal of Financial Crime. Edited by H. William, 12(1), pp. 33–43. doi: 10.1108/13590790510625043.

Javed, A. (2020) 'Prospects and Problems for E-commerce in Pakistan Prospects and Problems for E-commerce in Pakistan', (December).

Kahn, C. M. and Liñares-Zegarra, J. M. (2016) 'Identity Theft and Consumer Payment Choice: Does Security Really Matter?', Journal of Financial Services Research, 50(1), pp. 121–159. doi: 10.1007/s10693-015-0218-x.

Kaplan, B. and Maxwell, J. A. (2005) 'Evaluating the Organizational Impact of Healthcare Information Systems', Evaluating the Organizational Impact of Healthcare Information Systems, (January), pp. 29–55. doi: 10.1007/0-387-30329-4.

Khan, M. F. (2021) 'CYBERSECURITY AND CHALLENGES FACED BY', Pak. Journal of Int'L Affairs, 4(4), pp. 865–881.

Lin, J. (2023) 'The impact of environmental disclosure and the quality of fi nancial disclosure and IT adoption on fi rm performance : Does corporate governance ensure sustainability ?', (January), pp. 1–16. doi: 10.3389/fenvs.2023.1002357.

Lodder, M. (2023) Token Based Authentication and Authorization with Zero- Knowledge Proofs for Enhancing Web API Security and Privacy.

Mahmood Shah, R. I. O. (2011) 'A framework for internal identity theft prevention in retail industry', Proceedings - 2011 European Intelligence and Security Informatics Conference, EISIC 2011, pp. 366–371. doi: 10.1109/EISIC.2011.29.

Maitlo, A. et al. (2019) 'Preventing identity theft: Identifying major barriers to knowledge-sharing in online retail organisations', Information Technology and People, (March), pp. 0959–3845. doi: 10.1108/ITP-05-2018-0255.

Malik, Z. U. A. et al. (2022) 'Cyber security situation in Pakistan: A critical analysis', PalArch's Journal of Archeology, 19(1), p. 23.

Marcin Kubacki, C. at S. (2023) Cyber Attacks on the Banking Sector - National Bank of Pakistan. Available at: https://storware.eu/blog/cyber-attacks-on-the-banking-sector-on-the-example-of-the-national-bank-of-pakistan-what-can-banks-do/ (Accessed: 31 July 2023).

Mohsin, A. H. et al. (2019) 'Blockchain authentication of network applications: Taxonomy, classification, capabilities, open challenges, motivations, recommendations and future directions', Computer Standards and Interfaces, 64, pp. 41–60. doi: 10.1016/j.csi.2018.12.002.

Mufti, M. A., Arshad, M. and Haqqani, F. A. (2023) 'Assessment of corporate governance practices & its impact on financial performance: a case of banking sector of pakistan', 4(2).

N. Gana, N., M. Abdulhamid, S. and A. Ojeniyi, J. (2019) 'Security Risk Analysis and Management in Banking Sector: A Case Study of a Selected Commercial Bank in Nigeria', International Journal of Information Engineering and Electronic Business, 11(2), pp. 35–43. doi: 10.5815/ijieeb.2019.02.05.

Naeem, M., Jawaid, S. T. and Mustafa, S. (2023) 'Development of Online Banking Services in Pakistan : Applications of', South Asian Journal ofManagement Sciences, 17(1), pp. 1–14. doi: 10.21621/sajms.2023171.01.

Naseem, M. H. et al. (2023) 'Utilizing Fuzzy AHP in the Evaluation of Barriers to Blockchain Implementation in Reverse Logistics', Sustainability (Switzerland), 15(10). doi: 10.3390/su15107961.

Nasri, W. (2011) 'Factors Influencing the Adoption of Internet Banking in Tunisia', International Journal of Business and Management, 6, no.8(8), pp. 143–160. doi: 10.5539/ijbm.v6n8p143.

Pakistan, S. B. of (2023) 'State Bank of Pakistan'. Available at: https://www.sbp.org.pk/epd/2008/index.htm (Accessed: 2 August 2023).

Parusheva, S. (2009) 'Identity Theft and Internet Banking Protection', Economic Alternatives, (January 2009).

Qureshi, J. A., Baqai, S. and Qureshi, M. A. (2018) 'Consumers ' attitude towards usage of debit and credit cards : evidences from the digital economy of Pakistan', International Journal of Economics and Financial Issues, 8(5), pp. 220–228.

Rahman, R. A. and Anwar, I. S. K. (2014) 'NB.Effectiveness of Fraud Prevention and Detection Techniques in Malaysian Islamic Banks', Procedia - Social and Behavioral Sciences, 145(June), pp. 97–102. doi: 10.1016/j.sbspro.2014.06.015.

Reporter, W. (2022) 'Bank Data Breaches', https://www.nation.com.pk/. Available at: https://www.nation.com.pk/27-Jul-2022/bank-data-breaches (Accessed: 31 July 2023).

Robert K. Yin (2014) 'Case Study Research Design and Methods', Sage, 30(March 2016), pp. 1–5. doi: 10.3138/CJPE.BR-240.

Saeed, S. (2023) 'A Customer-Centric View of E-Commerce Security and Privacy', Applied Sciences (Switzerland), 13(2). doi: 10.3390/app13021020.

Salleh, K. (2010) 'Tacit knowledge and accountants: Knowledge sharing model', IEEE Computer Siciety, 2, pp. 393–397. doi: 10.1109/ICCEA.2010.227.

Selimić, M. and Radivojević, M. (2017) The New Approach of Observing Data and the Information Systems' Protection With the Use of Databases and the Semantic Web, International Journal of Trend in Research and Development. Available at: www.ijtrd.com.

Shah, M. H. et al. (2019) 'An investigation into agile learning processes and knowledge sharing practices to prevent identity theft in the online retail organisations', Journal of Knowledge Management. doi: 10.1108/JKM-06-2018-0370.

Shah, M. H., Ahmed, J. and Soomro, Z. A. (2016) 'INVESTIGATING THE IDENTITY THEFT PREVENTION STRATEGIES IN M-COMMERCE', international conference ITS, ICEduTech and STE, pp. 59–66.

Shareef, M. A. and Kumar, V. (2012) 'Prevent/Control Identity Theft', Information Resources Management Journal, 25(3), pp. 30–60. doi: 10.4018/irmj.2012070102.

Solove, D. J. and Washington, G. (2003) 'Identity Theft , Privacy , and the Architecture of Vulnerability', HASTINGS LAW JOURNAL, 54(August), pp. 1–48.

Soomro, Z. A., Shah, M. H. and Ahmed, J. (2016) 'Information security management needs more holistic approach: A literature review', International Journal of Information Management, 36(2), pp. 215–225. doi: 10.1016/j.ijinfomgt.2015.11.009.

Srivastava, R. K. and Rajesh (2007) 'Customer ' s perception on usage of internet banking', Innoative Marketing, 3(April), pp. 67–73.

Stuckey, H. (2014) 'The first step in Data Analysis: Transcribing and managing qualitative research data', Journal of Social Health and Diabetes, 02(01), pp. 006–008. doi: 10.4103/2321-0656.120254.

Tiller, J. S. (2008) 'Identity Theft', Journal of Economic Perspectives, 22, No,2, pp. 171–192. doi: 10.1081/e-eia-120046290.

Ula, M., Bt Ismail, Z. and Sidek, Z. M. (2011) 'A Framework for the Governance of Information Security in Banking System', Journal of Information Assurance & Cybersecurity, 2011, p. 12. doi: 10.5171/2011.726196.

Ula, M., Ismail, Z. and Sidek, Z. M. (2011) 'A Framework for the governance of information security in banking system(data basse)', Journal of Information Assurance & Cyber Security, 2011, pp. 1–12.

Ullah, S., Majeed, A. and Popp, J. (2023) 'Determinants of bank's efficiency in an emerging economy: A data envelopment analysis approach', Science of Totaol Enviroment, 18(3), p. e0281663. doi: 10.1371/journal.pone.0281663.

W.Wang, Y. Y. A. N. A. (2006) 'A Contextual Framework for Combating Identity Theft', IEEE Security & Privacy, (Marc/April).

WenJie Wang, Yufei Yuan and Archer, N. (2006) 'A contextual framework for combating identity theft', IEEE Security & Privacy Magazine, 4(2), pp. 30–38. doi: 10.1109/MSP.2006.31.

Wilhelm, W. K. (2004) 'The Fraud Management Lifecycle Theory : A Holistic Approach to Fraud Management .', Journal of Economic Crime Management, 2(2), pp. 1–38.

Zamzami, F., Nusa, N. D. and Timur, R. P. (2016) 'NB.The effectiveness of fraud prevention and detection methods at universities in Indonesia', International Journal of Economics and Financial Issues, 6(3), pp. 66–69.

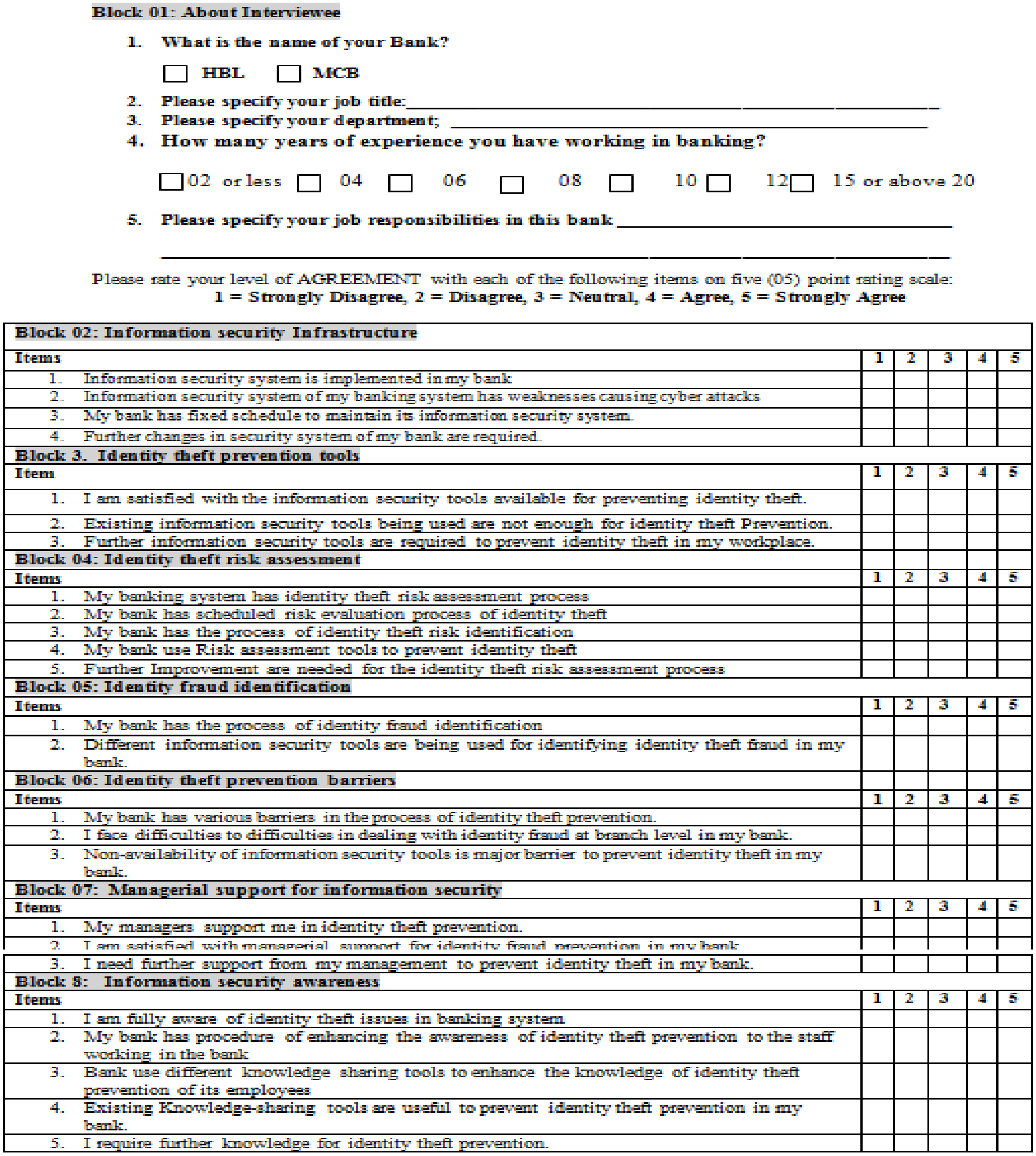
Zulkhibri, M. (2019) 'Macroprudential policy and tools in a dual banking system: Insights from the literature', Borsa Istanbul Review, 19(1), pp. 65–76. doi: 10.1016/j.bir.2018.04.001.

Salman, H. M. (2020). Identity theft on social media for the system of banking sector in Islamabad. Available at SSRN 3679244.

Malik, A. A., Asad, M., & Azeem, W. (2021). Requirement of Strong Legal Framework and Procedures to Contest with Cybercrime in Pandemic Situation. International Journal for Electronic Crime Investigation, 5(1), 7-16.

Riaz, A., Ramay, S. A., Abbas, F., Hussain, A., Naveed, N., & Abbas, T. (2024). Analyzing the Impact of Cybercrime and Its Security in Banking Sectors of Pakistan by Using Data Mining. Journal of Computing & Biomedical Informatics.

Appendix 1. Case descriptions



Block 01: About Interviewee

1. **What is the name of your Bank?**

   □ **HBL** □ **MCB**

2. **Please specify your job title:**______________________________
3. **Please specify your department;** ______________________________
4. **How many years of experience you have working in banking?**

   □02 or less □ 04 □ 06 □ 08 □ 10 □ 12□ 15 or above 20

5. **Please specify your job responsibilities in this bank** ______________________________

   ____

Please rate your level of AGREEMENT with each of the following items on five (05) point rating scale:
1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree

Block 02: Information security Infrastructure					
Items	**1**	**2**	**3**	**4**	**5**
1. Information security system is implemented in my bank					
2. Information security system of my banking system has weaknesses causing cyber attacks					
3. My bank has fixed schedule to maintain its information security system.					
4. Further changes in security system of my bank are required.					
Block 3. Identity theft prevention tools					
Item	**1**	**2**	**3**	**4**	**5**
1. I am satisfied with the information security tools available for preventing identity theft.					
2. Existing information security tools being used are not enough for identity theft Prevention.					
3. Further information security tools are required to prevent identity theft in my workplace.					
Block 04: Identity theft risk assessment					
Items	**1**	**2**	**3**	**4**	**5**
1. My banking system has identity theft risk assessment process					
2. My bank has scheduled risk evaluation process of identity theft					
3. My bank has the process of identity theft risk identification					
4. My bank use Risk assessment tools to prevent identity theft					
5. Further Improvement are needed for the identity theft risk assessment process					
Block 05: Identity fraud identification					
Items	**1**	**2**	**3**	**4**	**5**
1. My bank has the process of identity fraud identification					
2. Different information security tools are being used for identifying identity theft fraud in my bank.					
Block 06: Identity theft prevention barriers					
Items	**1**	**2**	**3**	**4**	**5**
1. My bank has various barriers in the process of identity theft prevention.					
2. I face difficulties to difficulties in dealing with identity fraud at branch level in my bank.					
3. Non-availability of information security tools is major barrier to prevent identity theft in my bank.					
Block 07: Managerial support for information security					
Items	**1**	**2**	**3**	**4**	**5**
1. My managers support me in identity theft prevention.					
2. I am satisfied with managerial support for identity fraud prevention in my bank					
3. I need further support from my management to prevent identity theft in my bank.					
Block 8: Information security awareness					
Items	**1**	**2**	**3**	**4**	**5**
1. I am fully aware of identity theft issues in banking system					
2. My bank has procedure of enhancing the awareness of identity theft prevention to the staff working in the bank					
3. Bank use different knowledge sharing tools to enhance the knowledge of identity theft prevention of its employees					
4. Existing Knowledge-sharing tools are useful to prevent identity theft prevention in my bank.					
5. I require further knowledge for identity theft prevention.					

The selected companies were all reputable banks of Pakistan. A brief description of each selected bank is follows:

1. Bank-X

The case study one of this study was completed in the first commercial bank established in Pakistan, which has a wide network of over 1400 branches within the country and more than 50 branches worldwide. This bank-X holds a dominant position in the commercial banking sector, with a domestic market share of over 40%. It excels in inward foreign remittances, capturing 55% of the market, and provides loans to small industries, traders, and farmers. Additionally, the bank operates internationally in multiple countries, offering a comprehensive range of banking services including Commercial, Corporate, Investment, and Retail Banking, Treasury, and Islamic banking.

2. Bank- Y

The second case study in this research project was conducted on one of the largest banks in Pakistan, which serves over 7 million customers and has exceeded their limit. This Bank-Y has a vast network of over 1400 branches across the country, ensuring extensive coverage. It also operates more than 1350 ATMs throughout Pakistan. With a presence in the industry since 1947, the bank has established itself as a leader in the region and has received recognition for its achievements, including the esteemed "Best Bank in Pakistan" award from Finance Asia.

3. Bank-Z

The third case study in this research project involved collecting and analyzing data from employees of a highly reputable bank in Pakistan. Bank-Z is a prominent multinational commercial bank with its headquarters in Karachi, Pakistan. It holds a significant position in the private sector of Pakistan's banking industry. The bank has an extensive network of over 1,400 branches throughout the country and operates 19 branches internationally. With a customer base exceeding 4 million, Bank Z serves a substantial number of individuals and businesses.

Table 4 Interview Participants Detail of Bank –X

Participant Code	Department	Designation	Job Responsibilities	Experience
X-P1	Operation Manager	Operation	Look after the overall operations of the branch	07-Years
X-P2	Team Leader	IT Department	Network support, leading the 250 to 270 users using PC and I look and handle all issues and provide them with network facility, engage our team for implementing the newly introduced technology or work, and engage people to deployment.	07-Years
X-P3	Branch Operation Manager	Operations	All over work performed inside this branch is my responsibility. To recheck new account openings, to check cashier to check guards to check the CCTV attached and everything.	06-Years
X-P4	Branch Manager	Business - CRBG	Managing and growing customer base, and business activities of branch	09-Years
X-P5	assistant Manager 2	IT center	To handle all IT-relegated Issues	32 -Years
X-P6	System Support Officer	IT Department	To resolve IT issues	08-Years
X-P7	Branch Manager	Branch	As a Co, all things to look after are my responsibility.	14-Years.
X-P8	Area manager	Business Department	To Plan, implement and monitor the regional operational strategy	35-Years
X-P9	Branch Operation Manager	Operation Department	Overall branch operation, team leader	07-Years
X-P10	Branch Manager	Branch Banking	Look after the branch portfolio, deposit	14-Years

			mobilization, forward the new things to the customers, and sell out them.	
X-P11	Deputy General Manager and Area Manager	Business Department	to look after all business areas on the assets side, customer care, To look after the RM and BM.	35-Years
X-P12	Branch Operation Manager	Operations	Look after all operations, all counter services, complaint regulations, services timeline, etc. all look after.	06-Years
X-P13	Head of SOC (security operation centre inside the information security team)	Security Operation Department	to run the incident management framework, and design a playbook, Everything of my job responsibility moves around incident management and hunting if any information is utilized against a Bank or employee on the dark web or deep web, or if the parent card is selling any place so how it will be identified, we have such type of responsibilities to monitor them.	21-Years

Table 5 Interview Participants Detail of Bank-Y.

Participant Code	Designation	Department	Job Responsibilities	Experience
Y-P1	Operation Manager	Operation department	To look financial mater of branch, to look after all, to monitor the security issues.	07-Years
Y-P2	TSO	RBG	Cash handling, ATM, Balancing. Cash related all entries.	05-Years
Y-P3	Relationship Manager	Credit Card Department	support for financing and perform all documentation, legal documentation.	06-Years
Y-P4	Branch Operation Manager	Operation Department	Over all activities of Bank, general Banking, cash, clearance etc… Mean over all operation of the department.	15-Years
Y-P5	Branch Manager	Sell Department	to look after all branch matters	25-Years
Y-P6	General Banking Officer OG-2	Operation	New account opening, transfer, clearing.	04-Years
Y-P7	Manager	Retail Banking Group	Branch manager targets such as deposit, accounts, ATM, credit cards.	10-Years
Y-P8	Branch Manager	Retail Banking Group	Core responsibilities (activity performing inside the bank and monitor it).	11-Years
Y-P9	Branch operation manager	Operation Department	All relevant issue of operation and all performing task are come under to the branch operation manager.	08-Years
Y-P10	General Banking Officer	Retail Banking	Managing client bank accounts	04-Years
Y-P11	Branch Manager	Marketing	To achieve the targets just targets, and look after all branch matters. Main is to achieve targets	08-Years

Y-P12	Branch Operation Manager	Operation Department	All operational work of the branch	05-Years

Table 4 Interview Participants Detail of Bank-Z

Participants Code	Designation	Department	Responsibilities	Experience
Z-P1	chief information security officer	Information security department.	To manage the overall security	17-Years
Z-P2	Head of Governance Assistant Director	Project Governance	Project management, project governance and project planning. These three are my responsibilities.	19-2- Years
Z-P3	Head of Information Security	Information Security Department	To take care information security risk.	13- Years
Z-P4	Information security analysist.	Information Security Division	Looking and developing policies, frameworks and strategies to prevent ID theft issues.	10-Years
Z-P5	Chief Information Security Officer	Information Security Department	To protect the information assets. If I am talking on top level so this is the main responsibility. Mean to protect the information assets. So we are from defense side.	08-Years
Z-P6	senior security risk specialist	Information Security	Caring all governance related issue. For example which multiple standards we have like PSIDs.	05-Years