ADDIS ABABA UNIVERSITY COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE SCHOOL OF INFORMATION SCIENCE

ENHANCING USABILITY OF PRIVILEGED ACCESS MANAGEMENT SYSTEMS: A CASE STUDY OF IMPLEMENTATION STRATEGIES AT THE COMMERCIAL BANK OF ETHIOPIA

BY

FIKRU AFEWORK ELYAS

AUGUST, 2024

ADDIS ABABA, ETHIOPIA

ADDIS ABABA UNIVERSITY COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE SCHOOL OF INFORMATION SCIENCE

ENHANCING USABILITY OF PRIVILEGED ACCESS MANAGEMENT (PAM) SYSTEMS: A CASE STUDY OF IMPLEMENTATION STRATEGIES AT THE COMMERCIAL BANK OF ETHIOPIA

A Thesis Submitted to The School of Graduate Studies of Addis Ababa University in Partial Fulfilment of The Requirement for The Degree of Master of Science in Information Science and Systems

(Information System Specialization)

Prepared By: - Fikru Afework

ID GSE/4378/14

Advisor: -Getachew H/Mariam (PhD)

ADDIS ABABA UNIVERSITY COLLEGE OF NATURAL AND COMPUTATIONAL SCIENCE SCHOOL OF INFORMATION SCIENCE

Enhancing Usability of Privileged Access Management (PAM) Systems: A Case Study of Implementation Strategies at The Commercial Bank of Ethiopia

Approval of Examination

Name And Signature of Member of The Examining Board

Name	Title	Signature	Date
Getachew H/Mariam	(PhD) Advisor	----------	----------
Lemma Lessa	(PhD) Examiner	----------	----------
Temtim Assefa	(PhD) Examiner	----------	----------

Declaration

I, Fikru Afework Elyas, declare that this thesis, titled " Enhancing Usability of Privileged Access Management (PAM) Systems: A Case Study of Implementation Strategies at The Commercial Bank of Ethiopia" is my authentic work submitted in partial fulfillment of the Master of Science in Information Systems degree at the School of Information Science, Addis Ababa University. This document has not been submitted for the award of any other qualifications at any other university or academic institution.

Name: Fikru Afework

Signature: ----------

This thesis has been submitted for examination with my endorsement as the advisor, confirming its originality meets the required standard.

Name: Getachew H/Mariam (PhD)

Signature: ----------

Acknowledgment

The successful completion of this research paper on the Enhancing Usability of Privileged Access Management (PAM) Systems: A Case Study of Implementation Strategies at The Commercial Bank of Ethiopia would not have been possible without the support and contributions of several individuals and organizations.

First of all, I would like to Thank you, my God, for everything, then my family especially my wife Miss Nardos Taye.

I sincerely thank my supervisor, Dr. Getachew H/Mariam, for his invaluable guidance, expertise, and unwavering support throughout the research process. His insightful feedback and mentorship have been instrumental in shaping the direction and quality of this study.

I would also like to acknowledge the contributions of the Commercial Bank of Ethiopia for granting access to their PAM system and facilitating the user recruitment and data collection process. The cooperation and participation of the 155 users who took part in the PAM system usability were vital to the success of this research.

Additionally, I would like to thank the School of Information Science of Addis Ababa University at for providing the necessary resources, infrastructure, and academic support that enabled me to undertake this research project.

Finally, I am grateful to my friends for their encouragement, moral support, and understanding during this study. Their constant motivation and belief in my abilities have been a constant source of inspiration.

I am truly thankful to all the individuals and organizations who have contributed, directly or indirectly, to the completion of this research paper.

Fikru Afework Elyas

Dedication

This research paper is dedicated to my loving family, my wife Miss Nardos Taye, and my children, who have been a constant source of support, encouragement, and inspiration throughout my academic journey.

Abstract

Privilege Access Management (PAM) systems play a critical role in modern cybersecurity, ensuring secure and controlled access to sensitive organizational resources. However, the usability of these systems can significantly impact their overall effectiveness and user adoption. The research problem addressed was the impact of factors on PAM system usability and the aim to address employees' reluctance to interact with PAM systems due to usability challenges. This study aims to evaluate the usability of a PAM system implemented within the Commercial Bank of Ethiopia (CBE), identify improvement areas, and inform future system design and deployment.

The research design methodology employed a mixed-methods approach, combining quantitative and qualitative data collection techniques. A total of 155 end-users, representing a diverse range of roles and levels of technical expertise, were recruited to participate in the study. Participants are provided feedback through questionnaires and interview questions on PAM usability. The study identified several factors that impacted the usability of the PAM system, including the intuitiveness of the workflow, and the level of integration with existing organizational processes. Based on these findings, the researchers developed a set of recommendations for enhancing the usability of the PAM system, such as simplifying the user support, improving the onboarding and training materials, and better aligning the system with the users' mental models and job responsibilities.

The results of this usability study provide valuable insights for both researchers and practitioners in the field of cybersecurity and PAM system design. The findings can inform the development of more user-centric PAM solutions and contribute to the broader understanding of the human factors that influence the adoption and effectiveness of critical security technologies within organizational settings.

Keywords: PAM, UTAUT (unified theory of acceptance and use of technology), Usability.

Table of Contents

List Of Acronyms

PCI DSS	Payment Card Industry Data Security Standard
GDPR	General Data Protection Regulation
ISMS	Information Security Management System
PAM	Privileged Access Management
ISO	International Organization for Standardization
DLP	Data Loss Prevention
NAC	Network Access Control
SIEM	Information and Event Management
IAM	Identity and Access Management
RBAC	Role-Based Access Control
MFA	Multi-Factor Authentication
SSO	Single Sign-On
PVWA	Password Vault Web Access
CPM	Central Policy Manager
EPV	Enterprise Password Vault
PSM	Privileged Session Manager
PTA	Privileged Threat Analytics
CBE	Commercial Bank of Ethiopia
NCCoE	National Cybersecurity Center of Excellence
WAF	Web Application Firewall
IoT	Internet of Things
PCI DSS	Payment Card Industry Data Security Standard
UTAUT	Unified Theory Of Acceptance And Use Of Technology
PAS	Standard Core Privilege Access Security Components

CHAPTER: I

Introduction

Information systems play a critical role in organizations by facilitating the management and processing of information to support decision-making, improve operational efficiency, and enhance overall productivity (Ezza et al., 2020)**.** Information technology can help financial institutions manage client transactions such as deposits, withdrawals, fund transfers, and payments more efficiently (Mikhaylov & Petrov, 2021). To ensure the accuracy, security, and smooth connectivity of all various financial systems, core banking systems are the central hub for managing these transactions (Bhuvaneswari et al., 2022). Banking information systems improve efficiency, customer service, risk management, and decision-making, creating a secure and competitive environment. Cybersecurity is the protection of information and communication systems from unauthorized access, modification, or exploitation using various processes and safeguards. (Moustafa et al., 2021). Most of the cybersecurity research has focused on improving computer network systems (Nobles, 2018), as many believe that information technology advances and software development are the main ways to increase information security (Sadkhan, 2019; Benson and Mcalaney, 2020). Cyber attackers can manipulate computer users' minds using social engineering and cognitive hacking to spread misinformation and break into a network or system, few studies aim to enhance system analysts' cognitive capabilities and situational awareness (Moustafa et al., 2021).

Banking information systems use advanced security measures such as encryption, biometric authentication, and real-time monitoring to protect sensitive financial data and assets (Dhoot et al., 2020). Banks can prevent security breaches by training employees on best practices, phishing

awareness, and social engineering tactics (Aldawood & Skinner, 2019). Firewalls, intrusion prevention systems, PAM, and secure network architecture protect banks from unauthorized access, malware, and other cyber threats (Steingartner et al., 2021). Banks must comply with PCI DSS and GDPR to protect customer data (Razikin & Widodo, 2021). Using advanced security monitoring tools and threat intelligence platforms improves banks' ability to detect and respond to emerging threats in real time, enhancing overall security (Razikin & Widodo, 2021). Banks can enhance security by implementing multi-layered measures and controlling access to sensitive data and systems. One of the most popular and well-respected information security standards in use today is ISO 27001 (Purba & Soetomo, n.d.-b). ISO 27001 helps organizations create and maintain effective information security through continual improvement. It provides a framework for implementing an information security management system (ISMS) that covers nearly every aspect of information security. The standard has controls devoted to security policy, physical security, incident response, and so forth including access controls like PAM (Purba & Soetomo, n.d.-a). Access control is the process of granting or limiting permissions to individuals or systems based on their roles, responsibilities, or need for specific information (Saeed et al., 2020). Access control tools play a critical role in ensuring the security and integrity of sensitive financial information. These tools help enforce access policies, monitor user activities, and prevent unauthorized access to confidential data(Saeed et al., 2020). Some common types of information security tools are

Data Loss Prevention (DLP) systems aid in preventing the unauthorized disclosure of sensitive data by monitoring and controlling data transfers within the bank's network (Thombre, 2020)., Security Information and Event Management (SIEM) Platforms enable comprehensive monitoring, logging, and analysis of security-related events within the bank's IT infrastructure (González-Granadillo et al., 2021). and Identity and Access Management (IAM) systems centralize

control over user identities and access privileges, enabling organizations to respond to incidents, facilitate compliance, and automate use cases for privileged accounts (Alruwies, Mishra, & AlShehri, 2022). These tools offer capabilities such as user provisioning, role-based access control (RBAC), multi-factor authentication (MFA), and single sign-on (SSO). User identity management is a common component that provides security and easy auditable access to some limited assets (Singh et al., 2023). Privileged accounts are used to manage IT infrastructures, resources, and applications, and provide access to high-value applications such as payment and accounting systems, and social media accounts (Waltermire et al., 2018). Privileged accounts have unlimited access to sensitive data, critical systems, and network resources including local and domain administrative accounts, emergency accounts, application management, and service accounts. (Sindiren & Ciylan, 2019a) Hackers target privileged accounts due to their high-level access to IT resources (Egwuche et al., 2022). One of the objectives of cyber-attacks on information systems is to obtain the passwords of such accounts (Sindiren & Ciylan, 2019b). PAM can manage privileged access, log all activity in the form of session recordings or keystroke logging, monitor applications to ensure that a threat actor does not gain inappropriate access, and document all sessions (Mohammed, n.d.) (Haber and Hibbert, 2018). Overall, PAM solutions help banks and financial institutions mitigate the risks associated with privileged access by implementing proactive security measures, enforcing least privilege principles, and ensuring accountability for privileged user actions. By effectively managing and securing privileged accounts, PAM solutions contribute to strengthening an organization's overall security posture and regulatory compliance by properly securing and controlling privileged credentials (Haber & Haber, 2020b). Ultimately protecting sensitive financial data and maintaining customer trust by protecting a company against unintentional or intentional abuse of privileged access.

1.2. Research Motivation

Organizations require a PAM solution that appropriately secures privileged accounts and enforces organizational policies for privileged account use (Memole-doodson, 2018a). Privileged Access Management is the process and technology used to control and monitor privileged entities in the network (Dou et al., 2020). Due to rising data breaches and cyber threats, businesses require strong access control mechanisms. Privileged users should not have access to actual password credentials, which enhances security and reduces the risk of unauthorized access to critical systems (Haber and Hibbert, 2018). PAM privilege session management feature provides real-time monitoring and records of all user activities to prevent incidents and conduct examination analyses and audits (Haber and Hibbert, 2018).

Ensuring compliance with PAM guidelines can greatly improve a CBE security posture. This is achieved by limiting access to sensitive IT resources to authorized personnel only. As a result, the risk of unauthorized data breaches, system compromises, and insider threats can be greatly reduced. Implementing efficient PAM compliance processes can modernize user provisioning, access requests, and role-based access control. This can lead to improved operational efficiency, reduced manual effort, and enhanced organizational productivity.

The research aims to improve PAM system usability, considering security imperatives, organizational impact, user-centric design, and continuous improvement. Strong security measures are necessary, as seen by the increasing frequency and sophistication of cybersecurity threats. PAM system is essential for protecting confidential information and lowering the possibility of unwanted access (Haber & Haber, 2020b). Despite their recognized importance, organizations have noticed a worrying trend of employees becoming reluctant to interact with privileged access management systems due to usability challenges (Walker, 2019).

Usability issues must be addressed to ensure user acceptance and adherence for successful PAM system implementation, as they affect organizational efficiency and security. The success of security initiatives is shaped by employees' experiences, attitudes, and perceptions. To understand why users are hesitant to use the PAM system A preliminary observation the researcher conducted shows that some employees are unwilling to use the system as the desired level of functionality, it is necessary to conduct a quantitative and qualitative analysis of their interactions with the system. The goal of the researcher is to increase the usability of the PAM solution to enhance security and productivity.

Improving the usability of the PAM system is crucial to enhancing organizational resilience against cyber threats. By addressing the usability challenges within the system, employees will be able to incorporate security practices into their daily tasks easily. This research aims to gather feedback from employees to inform targeted improvements and refine security infrastructure based on real-world experiences. privileged access management solutions vary architecturally. However, most offer access management, password management, and session management (Purba & Soetomo, n.d.-a). To guarantee adequate privilege management and access control, it is necessary to identify the subjects who request access to the resources (Gazzarata et al., 2017). Effective PAM compliance mechanisms can help mitigate risks by identifying vulnerabilities, developing controls, and establishing monitoring systems to build trust. PAM is used to control and monitor privileged users, and to defend against the unintentional or intentional abuse or attack on privileged access. PAM solutions safeguard sensitive information and maintain cybersecurity by preventing misuse of privileged credentials, ensuring usability and compliance(Haber & Haber, 2020a). The best method to stop attacks is to restrict and monitor privileged user access to the most important data

and systems. Through this research, the researcher aims to contribute to existing knowledge on PAM by identifying current practice and regulation gaps.

1.3. Statement of the Problem

It is crucial to have effective security measures in place for privileged accounts to prevent malicious activities that could harm an organization's business operations (Waltermire et al., 2018). Privileged accounts pose a significant risk as they are vulnerable to various harmful actions like ransomware, espionage, sabotage, or data theft, often without proper oversight or controls (Waltermire et al., 2018). The lack of protection for high-privilege accounts makes them easy targets for hacking and data breaches (Tirtadjaja et al., 2021). Many organizations, particularly those in the financial sector, struggle with managing privileged accounts, which can lead to up to 80% of cyber incidents caused by privilege misuse (Duessel et al., 2020a). As the number of applications increases, managing multiple identities like employee usernames and passwords becomes more complex (Alruwies, Mishra, Abdul, et al., 2022).

Centralized identity and access management present major challenges for organizations aiming to ensure secure and compliant access to IT resources (Singh et al., 2023). Failing to secure privileged accounts can result in severe operational, legal, and reputational consequences for organizations (Walker, 2019). Allowing unlimited access to privileged accounts for IT personnel can lead to significant IT security issues within a company (Sindiren & Ciylan, 2019a). Safeguarding and monitoring privileged access is essential to prevent attacks by insiders and outside hackers (Haber & Haber, 2020b). Human errors contribute to 95% of cyber and network attacks, making company employees the weakest link in system security efforts (Moustafa et al., 2021).

Monitoring and managing digital identities and their authorization across system and enterprise boundaries are vital for enhancing security and productivity (Devlekar & Ramteke, 2021).

Despite the importance of privileged access management systems in maintaining security protocols, employees are often reluctant to engage with these systems (Haber & Haber, 2020b). Key challenges in implementing a complete and manageable access control framework for distributed control systems include difficulty adhering to the least-privilege principle and managing policies across heterogeneous systems (Huh et al., 2016). Various security solutions integrated by banks, such as firewalls, SIEM, DLP, NG screeners, and WAF, effectively prevent cyberattacks due to their successful implementation and user-friendly systems (Ankele et al., 2020). However, there is a gap in the literature evaluating the usability of PAM within organizations, highlighting a need for further research in this area.

A preliminary observation we conducted shows that some employees are reluctant to use the system as the desired degree of functionality in contrast to other banking applications. If users are not using the system to its full potential, there's a risk of significant changes to IT systems, leading to compliance violations, security incidents, and lost revenue and the entire system will be vulnerable, so it's essential to understand why some employees are resist to use the PAM system. That is why the study aims to identify the usability issues within the PAM system, and the root causes of employee unwillingness, in getting actionable recommendations on how to improve the overall user experience by gathering input from users to identify usability issues and propose solutions aligned with best practices.

PAM solutions are utilized by system administrators to control access to critical infrastructure, enforce security compliance, monitor privileged activities, and manage access from third parties. Understanding the common challenges faced by users when using PAM tools is essential to improving overall effectiveness and usability, identifying areas for enhancement, and implementing strategies for better utilization.

1.4. Research Question

- What factors impact the usability of privileged access management (PAM) systems at the Commercial Bank of Ethiopia (CBE)?
- How usability of PAM will be improved at CBE?

1.5. Objective of the Study

1.5. 1 The General Objective

The main objective of the research is to investigate the factors influencing the usability of Privileged Access Management Systems within the Commercial Bank of Ethiopia and explore strategies to enhance PAM system usability.

1. 5.2. Specific Objectives

1. Identify factors that impact the usability of CBE's privileged access management (PAM) systems.
2. Investigate best practices and recommendations for improving the usability of PAM systems within CBE.
3. To Propose actionable insights for optimizing PAM usability, improving security posture, and ensuring compliance adherence within the CBE.

1.6. Scope of the Study

The scope of this study is focused only on a comprehensive analysis of CyberArk privilege access management systems solution usability at Commercial Bank of Ethiopia, by analyzing the PAM

usability dimension on operations and performance to archive organizational performance and enhance information security.

1.7. Significance of the Study

Privileged accounts grant access levels to corporate resources and critical systems beyond that of regular user accounts. IT administrators and managers utilize these accounts for essential system actions such as maintenance, system management, and access control. These accounts provide sensitive and often unrestricted access to a company's most critical assets (Waltermire et al., 2018). The set of policies and technologies employed to identify and prevent unauthorized access to privileged accounts is referred to as privileged account management (Waltermire et al., 2018).

Upon analysis of the research findings, the researcher aims to propose recommendations for enhancing PAM strategies. This study will play a fundamental role in assisting the organization in assessing the return on investment derived from the PAM system, pinpointing optimization opportunities through PAM techniques, and inspiring proactive measures to reinforce information security.

This research holds significant importance due to its multifaceted impact on an organization’s security posture, operational efficiency, and user experience with PAM systems. The core objective of the research is to reinforce the effectiveness of the PAM system in safeguarding privileged access and sensitive data, thereby mitigating the risk of security breaches. Additionally, the research explores addressing usability challenges within the PAM system, aiming to enhance user acceptance and adherence. Addressing usability challenges underscores the organization's dedication to creating a workspace that prioritizes security and user experience. Ultimately, this research aids in stimulating organizational resilience against cybersecurity threats, equipping the

organization to proactively navigate dynamic security landscapes and reinforce defences against risks associated with privileged access. By disseminating these findings, valuable insights will be provided to other organizations grappling with similar challenges. Ultimately, the researcher's objective is to ensure that employees operate in a secure and user-friendly environment that fosters their well-being and promotes responsible management of sensitive data.

CHAPTER II

Literature Review and Related Work

Introduction

This chapter examines a few works of literature that have links to the study's objective. There is a discussion of the main ideas, advantages, causes, impacts, and components of information system usability. The review of the literature offers a thorough explanation of the range of usability, including information system usability, information system security measures usability, privileged access management (PAM) usability, and other usability models and parameters.

2.1. Literature Review

2.1.1. Overview of Privileged Access Management (PAM)

Identity Access Management (IAM) ensures the job identities and nature of the right people are easily accessed through relevant tools (Singh et al., 2023). Identity and access management includes privileged account management (PAM), a domain dedicated to tracking and managing privileged account usage (Memole-Doodson, 2018b). The acronym PAM is used as a reference to privileged access management and privileged account management. Privileged identity management (PIM) and privileged user management (PUM) are also terms often used interchangeably. PAM was developed especially for protecting the local administrator accounts' passwords from Pass the Hash attacks, and for ensuring the control and management of those passwords (Sindiren & Ciylan, 2019b). Privileged accounts include local and domain administrative accounts, emergency accounts, application management, and service accounts. Privileged access management is a part of the identity governance (IG) framework and complements IAM.

Optimally, PAM is part of the organization's IAM model, but it can also be implemented independently (Tuononen, 2023). The PAM system is deployed so that it is available from production networks only. PAM is configured to create a comprehensive audit trail of all connections and to store the trail files encrypted in a highly available external storage system. Connection targets are imported into the system from the configuration management database (CMDB) via automation, but the system allows adding targets manually too (Tuononen, 2023).

Organizations encounter various challenges in managing high-privileged accounts, including the risk of data breaches due to compromised superuser accounts, the potential for human error in manual privilege assignment, a lack of oversight leading to difficulty in detecting unauthorized activities, the complexity of managing accounts across multiple systems in large IT environments, and the additional complexity of ensuring compliance with regulatory requirements. Implementing effective privileged access management solutions can help organizations improve their security posture and mitigate the risks associated with highly privileged accounts (Tirtadjaja et al., 2021). Privileged Access Management is essential for enhancing network security by restricting access, monitoring and auditing privileged user activities, centralizing password management, enforcing least privilege, and automating password rotation. Implementing PAM solutions helps organizations strengthen their security posture, mitigate risks related to privileged access, and improve overall security resilience (Sindiren & Ciylan, 2019a).

Financial institutions depend on privileged accounts to allow authorized users, such as system administrators, to carry out critical tasks (Waltermire et al., 2018). System administrators utilize privileged superuser accounts to manage IT infrastructures and resources or to gain access to high-value applications such as payment systems, and accounting systems, as well as core systems such as human resources, database access, and access control (Waltermire et al., 2018). There are so

many malicious adversarial threads in the world that can easily destroy an organization by stealing credentials and information data (Singh et al., 2023). Since security is the main concern of any organization, the level of security features available with the access management scheme should be well organized and arranged according to the time requirements (Alruwies, Mishra, Abdul, et al., 2022b). Many commercial application solutions are utilized to protect the passwords of computers in the directory structure, to manage privileged accounts to protect them from cyber-attacks, and to ensure compatibility with IT security procedures (Sindiren & Ciylan, 2019a).

The PAM software's primary attributes include providing web interface support for the RDP, SSH, VNC, and HTTP/S protocols; supporting native clients for SSH and RDP; supporting remote networks' RDP and SSH protocol targets by use of an extender component that is installed in the target network; the ability to document clipboard usage and file transfers in audit trails; Target hosts' granular role-based access management; allows SSH keys and passwords for local PAM authentication; gives PAM access to credentials and Kerberos tokens for LDAP authentication; encourages keeping target system login information private; assistance with target system password rotation; Application programming interface (API) access to all system parameters (Tuononen, 2023).

2.1.2. Importance of Usability in Privileged Access Management (PAM)

Implementing effective security measures through privileged account management is crucial for mitigating both insider and external threats. By limiting access to authorized personnel, monitoring and auditing account activities, providing regular cybersecurity awareness training, enforcing security policies, and integrating PAM into the overall security strategy, organizations can effectively reduce the risks associated with insider threats and strengthen their cybersecurity

defenses (Sindiren & Ciylan, 2018). One effective way to mitigate the risks associated with insider threats is through the management of privileged accounts. Organizations can easily be destroyed by malicious threats that steal important credentials and information. Therefore, good cybersecurity requires effective identity management and governance, with role-based access control being a crucial aspect of identity and access management. Organizations can improve their cybersecurity posture and lessen their susceptibility to insider attacks by managing privileged accounts well with these procedures (Sindiren & Ciylan, 2018). To effectively manage access requests, authorizations, accreditations, provisioning, and restoration for privileged users, organizations should implement identity governance and privileged access management (Alruwies, Mishra, Abdul, et al., 2022b). To prevent insider attacks, it's important to have a comprehensive privileged account management approach.

The usability and accessibility of PAM solutions can be enhanced by integrating the experience of both security and usability experts to identify and resolve usability and security problems in access control security services (Naqvi et al., 2018). Control and management of privileged accounts, determination of passwords, the establishment of stronger passwords, clarification of IT personnel duties, decrease in workload, and increase in IT security awareness (Sindiren & Ciylan, 2019a). The most dangerous threats faced by organizations are insider attacks Since insiders are aware of the underlying system, handling insider attacks is a most deterring task. Insider attacks have become the most devastating threat in today’s world. According to Forrester's research, 36% of the attacks are due to arrogant or careless user actions (Sindiren & Ciylan, 2018). Implementing a robust privileged account management approach in organizations involves following best practices to enhance security measures and prevent insider attacks (Mr. Siddhesh Bhargude, 2023). These practices include ensuring appropriate task distribution and authorization limitation for IT

personnel, implementing access control and monitoring mechanisms, providing regular training and awareness programs, enforcing strong password policies, integrating privileged account management with information systems, conducting regular security audits, and involving executives in the IT security process. By implementing these best practices, organizations can strengthen their privileged account management approach and reduce the risk of insider attacks on their information systems**.**

2.1.3. CyberArk Privileged Access Management Components

Standard Core Privilege Access Security Components (PAS)

Table 2.1. Core PAS Components

Secure Digital Vault	• A hardened and secured server used to store privileged account information • Based on a hardened Windows server platform
Password Vault Web Access (**PVWA**)	• The web interface for users to gain access to privileged account information • Used by admins to configure policies
Central Policy Manager (**CPM**)	• Performs the password changes on devices
Privileged Session Manager (**PSM**)	• Isolates and monitors privileged account activity.
Privilege Threat Analytics (**PTA**)	• Monitors and detects malicious privileged account behavior.

CyberArk's privileged account security solution became advertises as a security provider that offers the industry’s most comprehensive answer, for protecting, controlling, and monitoring privileged access across on-premises, cloud, and hybrid infrastructure”(Baxter & Martinez, 2020).

CyberArk states that 80% of security breaches involve a compromised privileged account.(Baxter & Martinez, 2020). The white paper uses the Office of Personnel Management and Bangladesh Bank breaches as examples of how an administrator account was compromised, allowing hackers to obtain access to privileged accounts.(Baxter & Martinez, 2020). CyberArk can support a wide range of technologies, including network devices, databases, security appliances, cloud environments, directories, and applications, among others. (Baxter & Martinez, 2020).

CyberArk Privilege Session Manager Architecture

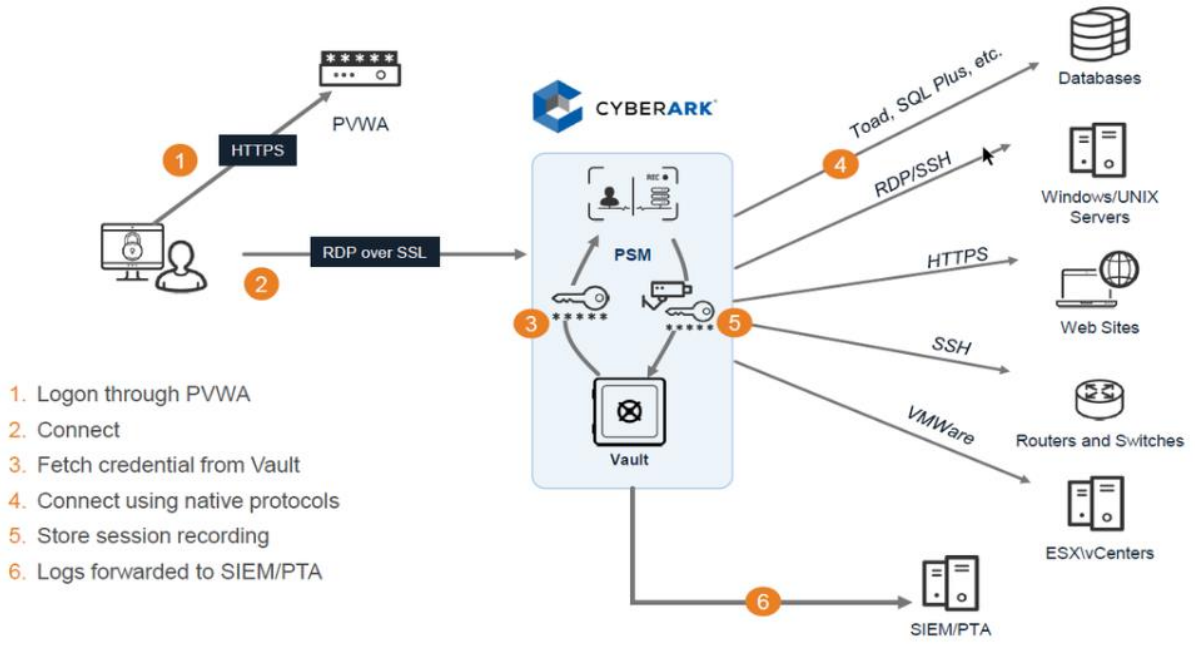

Figure 2.1 CyberArk Privilege Session Manager Architecture

Adopted from CyberArk Core PAS

2.1.4. Usability Challenges in Privileged Access Management

When implementing privileged access management solutions to meet ISO 27001 control requirements, organizations commonly face challenges such as a lack of knowledge in deploying PAM tools effectively, inadequate baseline understanding of current privileged access management practices, and the complexity of meeting ISO 27001 security controls (Purba & Soetomo, n.d.-b). Integration issues with existing IT systems, user resistance to change, and resource constraints in budget and skilled personnel also hinder successful PAM implementation (Purba & Soetomo, n.d.-b). Proactively addressing challenges and following best practices can enhance security posture and ensure compliance with ISO 27001 standards.

Organizations can improve security and minimize data breaches by implementing a high-privileged account management system to safeguard their privileged accounts (Tirtadjaja et al., 2021)**.** Managing high-privileged accounts presents organizations with notable obstacles, such as the threat of data breaches from compromised superuser accounts, the possibility of human error in manual privilege allocation, insufficient oversight resulting in unauthorized activities, the complexity of handling multiple accounts, and the necessity to adhere to regulatory mandates (Tirtadjaja et al., 2021). Privileged Access Management aims to keep organizations safe from misuse of privileged credentials, but its usability challenges may arise due to the complexity of its systems and various privileged users (Cobia, n.d.). Privileged access management projects often fail due to usability challenges and the potential for breaches of sensitive company information (Walker, 2019). Projects related to Privileged Access Management (PAM) often fail due to several reasons such as a lack of understanding of security risks associated with privileged accounts, incorrect focus on technical features instead of essential business requirements, over-reliance on agent-based technology, insufficient integration of PAM components that lead to under-delivery, a

lack of governance and strategic alignment, and the absence of a consistent approach to managing these accounts (Walker, 2019). To improve PAM initiatives, organizations should address these drawbacks by prioritizing business needs, avoiding over-reliance on specific technologies, adopting a holistic approach, and emphasizing governance and strategic alignment (Walker, 2019).

Most security systems fail to address usability in their design. The flow of communication within the organization and outside invites many security and privacy challenges for the user.(Parveen et al., 2021). IAM continues to present a major challenge for organizations, as efforts to enhance the security of their employees' passwords often prove ineffective. Employees experiencing security fatigue often find password policies and management onerous, making enterprise IT systems more vulnerable (Cram et al., 2021). Challenges in implementing the PAM system include insufficient planning, lack of management support, poor user role management, misapplication of access management roles, lack of attention, and absence of relevant perspectives. (Singh et al., 2023). Granting unrestricted access to privileged accounts for IT personnel may result in significant IT security risks for the organization (Sindiren & Ciylan, 2019a). Stolen credentials are often used in data thefts, which makes securing privileged accounts a crucial task (Carson 2019.) Insider attacks on privileged accounts can pose significant risks to an organization's information systems and data. Unauthorized access to sensitive data, Insiders with privileged access can manipulate or destroy data, causing significant damage to an organization's operations and reputation can disrupt critical systems and services, causing downtime and hackers can access and steal sensitive information, including financial data, trade secrets, and customer records. A cyber-security culture framework focusing on the human factor can help detect both malicious and unintentional insider threats, considering technical, behavioral, cultural, and personal indicators(Georgiadou et al., 2022).

Overall, insider attacks on privileged accounts can have severe consequences for an organization, making it crucial to implement effective security measures to prevent and detect such attacks.

Organizations are continually improving their safety measures to protect their information systems, while attackers are simultaneously exploring various methods to breach or bypass these precautions (Sindiren & Ciylan, 2018).The reason for targeting privileged accounts is that these accounts have broad authorizations on the information systems (Sindiren & Ciylan, 2018)**.** Effective management of privileged accounts is crucial for preventing insider attacks. These accounts have elevated access rights and can be exploited by malicious insiders to gain unauthorized access to confidential information or systems. Thus, companies must prioritize the management of these accounts to mitigate the risk of insider threats (Sindiren and Ciylan (2018). they have emphasized the significance of this issue in the IT landscape. To prevent insider threats, organizations should address the human factor in addition to leveraging technological solutions. It's crucial to provide regular cybersecurity training to employees to enhance their awareness.

2.1.5. Best Practices for Usability in Privilege Access Management

Improve the ability to revoke access or permissions granted to users to ensure better control over data access and security (Lessa & Etoribussi, 2023). Organizations can improve their threat management by promoting collaboration and breaking down silos between IT and security operations. This can be achieved through implementing integrated tools and processes, providing cross-training opportunities, and establishing clear roles and responsibilities. These efforts foster a culture of collaboration that enhances information sharing, improves threat detection and response capabilities, bridges departmental gaps, and ensures a coordinated approach to security**.** The system for controlling privileged account access was designed to improve the management,

monitoring, and protection against attacks on local administrator and directory service privileged accounts (Sindiren & Ciylan, 2019b). Many organizations consider it crucial to provide employees with easy and reliable access to digital resources and software applications. Privileged Access Management (PAM) systems not only offer improved password management for employees, but also provide enterprises with tools to oversee a growing number of identities, including external partners, customers, and smart devices. This is especially important with the rise of the Internet of Things (IoT). (Mohammed, n.d.-b).

2.1.6. User Experience in PAM Systems

The concept of Privilege Management has been extensively researched and developed within the IT industry, with numerous academic works and patents (Sindiren & Ciylan, 2019b). Privileged Access Management can effectively prevent unauthorized access to sensitive information, even when security best practices are followed (Haber, M., & Hibbert, B. 2018). Multiple commercial application solutions exist to protect computer passwords within the directory structure, manage privileged accounts, and ensure compatibility with IT security procedures.

2.1.7. User-Friendly PAM Solutions

User interfaces should prioritize both security and usability from the design phase, with users taking into account system security and functionality since security measures may already exist within the application. Involve users in the design and implementation of security features to ensure that they meet user expectations and requirements (Lessa & Etoribussi, 2023). PAM solutions effectively mitigate information security risks and threats from insider activities in IT environments. Privileged Access Management provides secure access control, auditing, alerting, and recording for any privileged account through an automated password and session management

solution (Purba & Soetomo, n.d.-b). The technology is created to oversee various types of accounts, including local or domain-shared administrator accounts, a user's personal admin account, service, operating system, network device, database, and application accounts. Additionally, it can also handle SSH keys, cloud, and social media accounts (Purba & Soetomo, n.d.-b). Privileged Access Management (PAM) involves various methods for securing, managing, and monitoring privileged access to resources (Tuononen, 2023). PAM ensures that only authorized users can administer secure systems and maintains a record of the use of privileged accounts. It provides effective controls against both external and internal threat actors. Internal actors gain legitimate access to systems with PAM, but the unalterable audit trail acts as a deterrent for any deliberate misuse of privilege. The PAM product uses a role-based model for access management to assign permissions (Tuononen, 2023). Access roles are designed to minimize the number of groups while still adhering to the principle of least privilege. PAM is configured to create a comprehensive audit trail of all connections and to store the trail files encrypted in a highly available external storage system. The PAM product offers two connection options: a web interface for all supported protocols and native clients for RDP and SSH targets. Note that SSH tunneling is not available in the web client, but it could be useful for managing network devices.

2.1.8. Impact of Usability on Information Security Practices

The main challenge is to balance the interests of usability and security in system development. To address this issue, a comprehensive methodology has been developed that promotes collaboration between experienced systems designers and experts from the usability and security domains. The approach emphasizes the early alignment of usability and security principles during the system design phase with the ultimate goal of enhancing the usability and security of global information

systems. The effectiveness of security measures in e-health applications through the examination Expert analysis of all e-health applications found that learnability, aesthetics, minimalist design, and user language, out of the thirteen criteria analyzed, were found to be compliant with security features (Lessa & Etoribussi, 2023). Human-centered cyber security, focusing on user, usage, and usability, is a growing trend, offering insights for both users and system designers (Grobler et al., 2021).To assess the usability of security measures in software, a heuristic approach is used. This involves a joint model that evaluates both usability and security and a tool-supported evaluation process to optimize the security measures. The evaluation process is refined and improved regularly to ensure effectiveness and usability (Feth & Polst, 2019). Heuristics can be effectively used to evaluate the usability of security measures by providing a set of guidelines or principles that help assess the user-friendliness and effectiveness of security mechanisms in software. In the context of evaluating security measures, heuristics serve as a structured approach to identify potential usability issues and improve the overall user experience (Feth & Polst, 2019). By integrating contextual enhancements to promote secure behavior, highlighting the significance of user-centered design, and ensuring that security measures remain user-friendly without sacrificing effectiveness. This approach challenges top-down security policies that may not align with user behaviors and promotes an understanding of user needs to cultivate robust security practices. User decisions in cybersecurity are impacted by the usability of systems, underscoring the pivotal role of usability in shaping user choices online. This approach seeks to bridge the divide between usability and security in systems, advocating for a comprehensive strategy that incorporates user behaviors, system design, and behavioral interventions to elevate cybersecurity practices.

2.1.9. Information System Usability

Ethiopian software development organizations face significant challenges in usability, including a lack of user focus, awareness, and education on usability principles, infrastructure, and technical limitations, cultural considerations, insufficient organizational support, and the complexity of integrating usability into agile methods. Addressing these challenges is crucial for improving the effectiveness and user satisfaction of products developed by Ethiopian software companies (Teka et al., 2016). The study discovered that the system's usability was low and there were significant links between quality components and user characteristics, such as position, education level, field of education, age, and practice experience, impacting learnability, efficiency, helpfulness, and overall usability (Rangraz Jeddi et al., 2020). In system analysis and design, it's important to consider user groups' diverse needs for usability. Recommendations include developing national health information system requirements, providing support for older and less educated users, and streamlining system activities for physicians (Rangraz Jeddi et al., 2020).

2.2. International And Vendor Standards and Models Of PAM

2.2.1. International Organization for Standardization (ISO)

Privileged Access Management is a critical part of an organization's cybersecurity strategy. It aims to secure privileged accounts, control access to sensitive data, and enhance overall security posture through effective management and monitoring. PAM solutions play a crucial role in meeting compliance requirements, such as those outlined in standards like ISO 27001, by providing mechanisms for controlling and monitoring privileged access. The ISO standards stress the importance of Privileged Access Management (PAM) usability for effective implementation and

compliance with information security requirements (Culot et al., 2021). Key points from the ISO standards regarding PAM usability include:

1. *Compliance:* PAM ensures compliance with internal policies, legal obligations, regulatory schemes, and contractual requirements related to information security.
2. *Automation:* PAM solutions automate password and session management for privileged accounts, enhancing access control, auditing, alerting, and recording across systems and applications.
3. *ISO 27001 Compliance:* PAM aids in ISO 27001 compliance by establishing an access gateway for system administrators, enforcing access policies, managing access rights, and documenting privileged access controls.
4. *Risk Mitigation:* PAM helps mitigate risks of unauthorized access and misuse of privileged accounts, thereby strengthening the overall security posture.
5. *Real-time Monitoring:* PAM solutions provide real-time visibility into privileged user activities, enabling prompt monitoring and response to security incidents for ISO standards compliance.
6. *Documentation:* PAM tools offer detailed audit logs and session recordings of privileged user activities, facilitating demonstration of ISO standards compliance during certification audits.
7. *Integration:* ISO standards emphasize seamless integration of PAM solutions with existing IT systems and processes to ensure compatibility with various platforms and applications.

By adhering to these principles and effectively leveraging PAM solutions, organizations can enhance their security posture, fulfill compliance requirements, and oversee privileged access by ISO standards.

2.2.2. National Institute of Standards and Technology (NIST)

The National Institute of Standards and Technology (NIST) is a US federal agency that develops and promotes measurements, standards, and technology to advance economic security and improve quality of life. NIST is known for its work in cybersecurity, providing guidelines, standards, and best practices to help organizations protect their information systems and data. Some key NIST standards and publications that address PAM usability include: NIST's emphasis on usability guidelines for Privileged Access Management (PAM) underscores the importance of making PAM solutions user-friendly and effective (Memole-doodson, 2018b). Here's a breakdown of the key points:

1. *Clear and Accessible Content*: NIST stresses the need for PAM guidelines and documentation to be clear and easily understandable for a wide range of stakeholders, including business decision-makers, program managers, cybersecurity practitioners, and IT professionals. Clear content ensures that users can easily grasp the concepts and requirements of PAM, leading to better implementation and adoption.
2. *Practical Implementation Guidance:* NIST advocates for practical implementation guidance that helps organizations translate theoretical concepts into actionable steps. Practical guidance includes detailed instructions, best practices, and real-world examples that enable organizations to implement PAM solutions effectively. By providing practical guidance, NIST ensures that organizations can apply PAM principles in a meaningful way within their specific environments.
3. *Alignment with Industry Standards*: NIST underscores the importance of aligning PAM usability guidelines with industry standards and best practices. By aligning with established standards such as the NIST Cybersecurity Framework and other relevant guidelines,

organizations can ensure that their PAM solutions meet industry expectations and requirements. Alignment with industry standards also facilitates interoperability and consistency across different organizations and sectors.

In summary, NIST's usability guidelines for PAM focus on making PAM solutions accessible, practical, and aligned with industry standards to enhance their effectiveness and adoption within the financial services sector. By following these NIST standards and publications, organizations can enhance the usability of their PAM solutions, and improve access control, monitoring, auditing, and enforcement of policies related to privileged accounts, ultimately strengthening their cybersecurity posture (Memole-doodson, 2018b).

2.2.3. Payment Card Industry Data Security Standard (PCI-DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a globally recognized information security standard. It specifies measures for safeguarding cardholder data and is aimed at ensuring that any organization handling credit card information maintains a secure environment (Jere, 2017) The standard mandates protecting the cardholder data environment by taking preventive measures to secure privileged account access and passwords. The solution for privileged access management is designed to comply with the requirements of the PCI DSS standard, specifically those clauses related to privileged or administrative account access.The solution comes equipped with pre-defined and customizable reports that can be used to provide evidence of compliance with PCI DSS requirements. (Jere, 2017).

The PCI-DSS standards are The Following

- Access to the systems should be secured.
- Only authorized personnel should be allowed to enter.

- Each user must have a unique user account and password.
- Avoid using groupwide authentication.
- Implement multi-factor authentication.
- Only those who require access should be allowed to access cardholder data.
- Document all policies.

2.3. Theoretical Framework

The research's theoretical framework is crucial in providing a solid foundation and structure for interpreting and analyzing data (Heale & Noble, 2019). It helps researchers to understand and contextualize their findings within existing knowledge, theories, and concepts relevant to the research topic. By drawing upon established theories and frameworks, researchers can develop hypotheses, define variables, and identify relationships between different factors. Theoretical frameworks also assist in shaping the research design, methodology, and data analysis strategies, ensuring that the study is coherent and logically organized. Additionally, a well-developed theoretical framework aids in identifying gaps in the current literature, suggesting new avenues for further research, and contributing to the advancement of knowledge in the field. Ultimately, the theoretical framework serves as a roadmap for researchers, guiding them through the research process and supporting the generation of meaningful and relevant insights that can contribute to the academic community and society at large (*MAKING SENSE OF THEORETICAL FRAMEWORKS (1)*, n.d.).

The Unified Theory of Acceptance and Use Of Technology (UTAUT) is a theoretical research model developed in 2003 by Viswanath Venkatesh, Michael G. Morris, Gordon B. Davis, and Fred

D. Davis. The UTAUT model aims to explain user intentions to use an information system and subsequent usage behavior. The UTAUT model consists of four key constructs.

The Unified Theory of Acceptance and Use of Technology (UTAUT) model is a popular framework in the field of information systems that seeks to explain and predict individuals' acceptance and use of technology. The model integrates elements from various prior theories and models to create a comprehensive framework for understanding user behavior. The UTAUT model consists of four key constructs, which are:

1. Performance Expectancy: This refers to the extent to which an individual believes that using a technology will improve their ability to perform tasks. If a user believes that a new software system will make them more efficient at work, they are likely to have high expectations for its performance.

2. Effort Expectancy: Effort expectancy refers to the ease or difficulty of using the technology. Individuals prefer easy systems over complex ones, which are less likely to be adopted.

3. Social Influence: refers to the impact of social factors on an individual's decision to use technology. This encompasses the influence of peers, colleagues, or superiors on the intention to adopt technology. Positive influence encourages adoption, while negative influence hinders it.

4. Facilitating Condition: Facilitating conditions refer to the support that individuals perceive from the organizational and technical infrastructure while using technology. This support includes resource availability, technical assistance, training, and compatibility with existing systems. When users observe these conditions being met, they are more inclined to adopt the technology.

The UTAUT model consists of four main constructs that work together with external variables to influence people's intentions and actual use of technology. Researchers and practitioners can gain valuable insights into the factors that affect technology acceptance and adoption by considering these constructs together. The model also includes four moderating variables that can impact the relationships between the main constructs and behavioral intention and usage behavior.

1. Gender: Gender may influence the effects of the main factors on behavioral intention and usage behavior.

2. Age: Age may influence the effects of the main factors on behavioral intention and usage behavior.

3. Experience: Familiarity with the technology may influence the effects of the main factors on behavioral intention and usage behavior.

4. Voluntariness of Use: The extent to which the use of the technology is seen as voluntary or mandatory may influence the effects of the main factors on behavioral intention and usage behavior.

The UTAUT model has been widely used in information systems research to understand and predict user acceptance and usage of various technologies, such as enterprise resource planning (ERP) systems, mobile banking, e-government services, and social media platforms, among others. The model provides a comprehensive framework for understanding the complex factors that influence technology adoption and use. The Unified Theory of Acceptance and Use of Technology (UTAUT) is a well-known theoretical research model that explains how individuals adopt and use

technology. This model proposes that four main factors influence an individual's intention to use technology, ultimately impacting their actual usage behaviors.

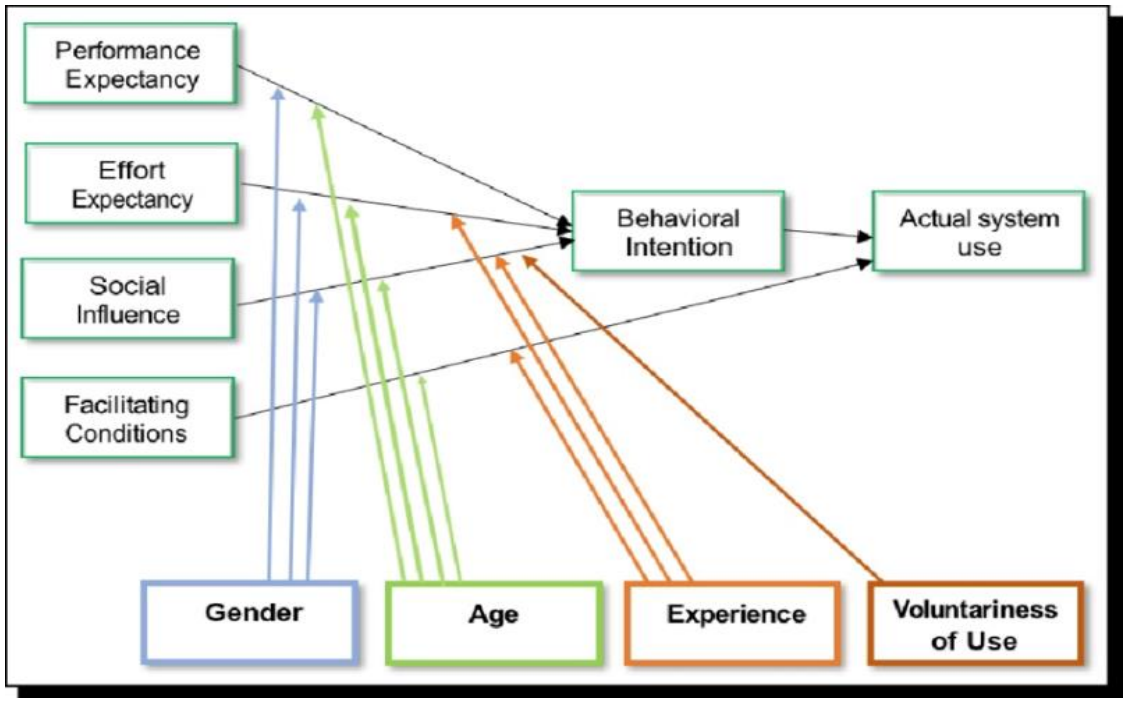

Figure 2.1. The UTAUT Theoretical Model

Adopted from (Venkatesh et al., 2003)

It is important to investigate the usability of Privileged Access Management (PAM) using the UTAUT theoretical model. This model considers factors such as performance expectancy, effort expectancy, social influence, and facilitating conditions. By extending the model, the researcher includes additional concepts from the literature and usability model, such as perceived security features, error handling, and audit and reporting capabilities. Analyzing these elements can offer valuable insights into the user-friendliness of PAM systems, leading to the development of improved solutions. This research aims to understand the factors that influence users' acceptance and usability of the PAM system, to create more user-friendly PAM systems.

2.3.1 Theoretical Model Framework Comparison

The UTAUT model is the most appropriate theoretical framework for this study compared to other available models.

- **Comprehensiveness**: The UTAUT model is a comprehensive framework that integrates key constructs from several prominent technology acceptance theories, including the Technology Acceptance Model (TAM), the Theory of Reasoned Action (TRA), and the Theory of Planned Behavior (TPB). This broad integration allows the UTAUT model to offer a more complete explanation of the factors that influence technology adoption.
- **Empirical Validation:** The UTAUT model has been thoroughly tested and confirmed across various technologies and situations. Numerous studies have shown that the model can significantly explain both the intention to use technology and actual usage. This solid empirical basis enhances the reliability and validity of the model for our current study.
- **Relevance to the Context:** The UTAUT model comprises four key constructs: performance expectancy, effort expectancy, social influence, and facilitating conditions. These constructs are particularly pertinent when it comes to comprehending the adoption of the PAM system within the context of its usability. In contrast, other models like TAM or TPB may not encompass the complete array of influential factors in this specific context.
- **Moderating Variables:** The UTAUT model includes moderating variables such as gender, age, experience, and voluntariness of use. This enables a deeper understanding of how user characteristics and contextual factors influence the relationships between key concepts and technology adoption. This level of detail is essential for developing specific strategies to encourage the acceptance and use of the PAM system's usability.

- **Established Measurement Instruments:** The UTAUT model has well-developed and validated measurement instruments, which can be adapted for the current study. This ensures the reliability and validity of the data collection process, allowing for more robust and meaningful findings.

By adopting the UTAUT framework, this study will build upon the extensive existing knowledge in the field of technology acceptance and use, while also providing valuable insights specific to the PAM system usability. The UTAUT model's comprehensiveness and empirical grounding make it the most suitable theoretical foundation for this research.

2.4. System Usability

Usability evaluation is crucial for the successful implementation and optimization of an information system (Khajouei & Farahani, 2020). The usability of software systems is a pivotal factor defined by researchers and international standards like ISO/IEC 25010 and IEEE. Usability denotes the extent to which users can employ a product to accomplish specific goals, taking into consideration effectiveness, efficiency, and user satisfaction (Khajouei & Farahani, 2020). Usability is a quality attribute that evaluates how easy it is to use user interfaces. The goal of usability evaluation is to identify and prioritize the issues that affect the user's experience, to improve the system's usability (Khajouei & Farahani, 2020). The two widely recognized definitions of usability are the ISO standard concerning usability and Jacob Nielsen's usability attributes. The ISO 9241-11 standard provides guidelines for identifying the necessary information required to evaluate usability. It aims to create a consistent and widely accepted framework for measuring the key parameters of usability. The International Organization for Standardization (ISO) defines usability as the ability to fulfill users' needs through usability engineering. It is measured through three core factors: effectiveness, efficiency, and satisfaction. Effectiveness assesses how well a user can

accomplish a task, efficiency focuses on speed and resources, while satisfaction measures the overall user experience. Usability is further evaluated based on learnability, efficiency, memorability, error prevention, and user satisfaction. Usability evaluation aims to identify and prioritize system usability problems to improve the user experience.

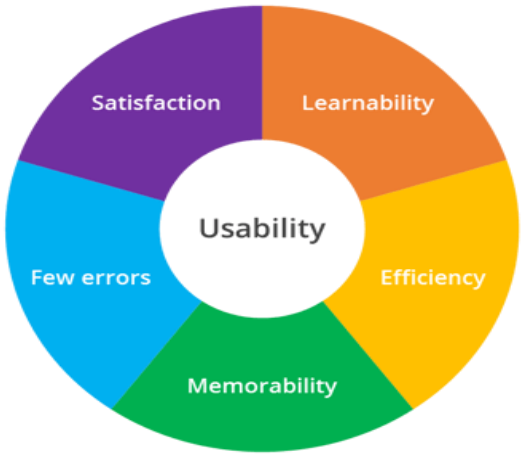

Figure 2.2. Jacob Nielsen's Usability Attributes

Adopted from Jacob Nielsen's Usability Model.

2.5. Usability Models

2.5.1. ISO Usability Model

The ISO 9241-11 standard identifies three key usability attributes: effectiveness (the level of accuracy and completeness in achieving goals), efficiency (how well resources are used to achieve effectiveness), and satisfaction (positive user experience while using the software). The standard also outlines the usability factors that need to be considered: the user (the person interacting with the software), the goal (or main objective), and the context of use (including users, tasks, tools

used, and the environment). Each of these factors influences how the software will be designed and specifically impacts user interaction with the system.

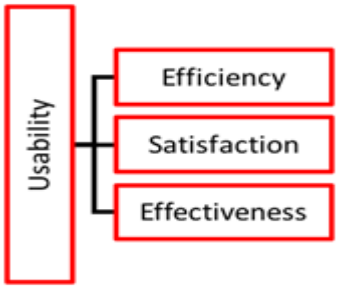

Figure 2.3. The ISO usability model

Adopted from the ISO Usability Model

2.5.2. Nielsen Usability Model

Nielsen initially identified four attributes of usability: effectiveness, efficiency, satisfaction, and learnability. However, he later revised the model by removing "effectiveness" and adding "memorability" and "errors." The attributes he identified are as follows:

- **Efficiency:** Resources used to accurately complete a task in order to achieve user goals.
- **Learnability:** The ease with which the system can be learned so that users can perform tasks in minimal time.
- **Satisfaction:** The product should provide comfort and a positive attitude towards its use.
- **Errors:** The system's error rate should be minimal, and any errors that do occur should be easily recoverable. Catastrophic errors should be avoided.
- **Memorability:** Users should be able to easily memorize the system so that even after a long period, they can use it without having to relearn everything.

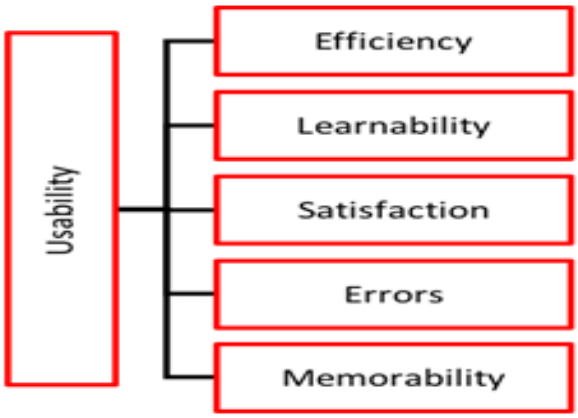

Figure 2.4. Nielsen Usability Model

Adopted from Jacob Nielsen's Usability Model

2.5.3. PACMAD Usability Model

The PACMAD (People at the Centre of Mobile Application Development) model addresses issues that have emerged due to the rise of mobile apps.

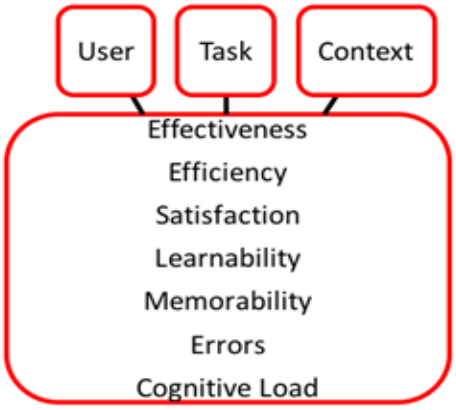

Figure 2.5. PACMAD Usability Model

Adopted From PACMAD Usability Model

2.6. Related Work

Protecting credentials and managing privileged access effectively are crucial in preventing security breaches. By focusing on the human element in security measures, providing appropriate user training, and implementing robust credential management systems, an organization can enhance its security posture and mitigate risk associated with data exposure and unauthorized access (Cobia, n.d.). The critical role of privileged account management in mitigating insider threats and stresses the importance of comprehensive security measures to safeguard information systems from internal vulnerabilities (Sindiren & Ciylan, 2018). The implementation of an effective PAM solution can empower organizations to enhance their security posture and mitigate the associated risks of highly privileged accounts (Tirtadjaja et al., 2021). The significance of a holistic approach to PAM that addresses specific sector requirements, leverages practical examples, assesses and mitigates risks, sets clear objectives, utilizes structured guidance, and implements robust security measures to safeguard privileged accounts effectively in financial institutions (Memole-doodson, 2018b). Through the efficient use of PAM to guarantee adherence to contractual requirements for information security, legal requirements, regulatory systems, and corporate policies. Businesses can comply with compliance mandates, strengthen their security posture, and effectively handle privileged access by ISO standards (Purba & Soetomo, n.d.-b).furthermore the significance of documentation, audit trails, integration, and compatibility of PAM solutions with existing IT systems to effectively manage privileged access and meet compliance standards. PAM helps mitigate risks such as credential-based attacks and unauthorized access to critical systems. Furthermore, PAM systems offer scalability and flexibility, enhancing operational efficiency and productivity in managing complex IT environments. Prioritizing PAM can lead to enhanced security, regulatory compliance, accountability, and operational efficiency in cybersecurity

practices (Mr. Siddhesh Bhargude, 2023). however, the implementations of PAM should be successful to get the benefit. Nearly limitless access to privileged accounts across computer systems raises the possibility of a breach involving the most precious assets of a firm. (Walker, 2019).

Privileged Access Management tool used to manage privileged access and the risks associated with credential loss. It emphasizes the potential consequences of credential loss in terms of data security, effective strategies for preventing credential theft and managing privileged access within an organization. PAM projects fail due to the following key challenges such as incorrect focus on technical features, over-reliance on agent-based technology, insufficient integration of PAM components, and lack of governance and strategic alignment. By addressing these challenges and implementing best practices, the study seeks to help organizations improve the effectiveness of their PAM initiatives, enhance the security of privileged accounts, and mitigate risks associated with unauthorized access to sensitive data (Walker, 2019). Integrating the Identity Governance and Management Framework for privileged users in higher education, addressing the issues, and putting up a thorough plan to improve security and access control measures (Parveen et al., 2021). The importance of preventing insider attacks on privileged accounts within organizations. It emphasizes the risks associated with insider threats, including unauthorized access to sensitive data, data manipulation, system disruption, and compliance violations.

The best practices for managing and securing privileged accounts, such as limiting access, monitoring activity, implementing strong authentication, regularly changing passwords, segregating duties, conducting regular training, and implementing access controls. Organizations can lower their risk of insider attacks and safeguard their vital systems and data by using these best practices (Sindiren & Ciylan, 2018). The importance of implementing a comprehensive security

solution that focuses on analyzing and visualizing privilege access metrics from Windows Active Directory and Linux devices (Anwar, 2022). By ensuring that security measures are both technically sound and easy to use, incorporating usability factors into security evaluations can improve the overall security of software systems. Continuous refinement and improvement in heuristics, models, and tools are essential to enhance the usability evaluation process for security measures (Feth & Polst, 2019).

Table 2.1 Summary of Related Works

S.no	Author and Year	Study Title	Methods Used	Objective/ Purpose	Key Findings	Research Gap
1	Cobia A Winter 2-15-2019	Privileged Access Management	literature review	the study aims to guide organizations in implementing effective strategies to protect privileged accounts, mitigate risks, and maintain data security integrity in the face of evolving cyber threats.	The importance of ensuring the protection of credentials and effective management of privileged access to avoid security breaches.	There is a lack of comprehensive studies that connect the impact of organizational culture and employee behavior on the security of privileged accounts.

2	Sindiren E, Ciylan B (2018)	Privileged Account Management Approach for Preventing Insider Attacks	Combination of literature review, analysis of existing security practices, case studies,	The significance of implementing security measures such as limiting access, monitoring activities, providing training, enforcing policies, and integrating privileged account management into overall security strategies to mitigate the risks associated with insider attacks.	The critical role of privileged account management in mitigating insider threats and stresses the importance of comprehensive security measures to safeguard information systems from internal vulnerabilities.	a lack of effective frameworks and procedures tailored to monitor and manage privileged accounts, which are critical in preventing insider attacks.
3	Tirtadjaja W, Rana M, Shanmugam K *2021*	Managing High Privileged Accounts in IT Enterprise Enhanced Security	literature review	The aim is to reduce human errors in privilege assignment, increase security and efficiency, ensure user account compliance, enhance end-user productivity, and provide a realistic,	Managing high-privileged accounts across diverse systems within large IT organizations emphasizes the criticality of implementing consistent security measures and access controls.	The lack of accessible, detailed information on comparable systems presents a challenge for researchers and practitioners

		Infrastructure		practical, and cost-effective solution		looking to explore effective solutions in this domain.
4	Memoledoo dsonJ *(2018) (September)*	Privileged Account Management for the Financial Services Sector	Collaborative Approach	Overall, the study aims to equip financial organizations with the knowledge, tools, and strategies needed to effectively manage privileged accounts, enhance security posture, and mitigate risks associated with privileged access within the financial services sector.	PAM addresses specific sector requirements, leverages practical examples, assesses and mitigates risks, sets clear objectives, utilizes structured guidance, and implements robust security measures.	There is a need for further research on how to adapt PAM practices to these emerging technologies while maintaining security and compliance
5	Purba A, Soetomo M*2018*	Assessing Privileged	literature review	Ultimately, the study aims to provide insights and recommendations for organizations to	Through the efficient use of PAM to guarantee adherence to contractual requirements for information security,	There is a lack of comprehensive understanding and mapping of

		Access Management (PAM) using ISO 27001:2013 Control		leverage PAM solutions effectively in enhancing security, meeting compliance requirements, and managing privileged access in alignment with ISO standards.	legal requirements, regulatory systems, and corporate policies.	how PAM solutions can effectively address the controls specified in the ISO 27001:2013 standard.
6	Mr. Siddhesh Bhargude July 2023	Privileged Access Management Ensuring Security and Accountability	qualitative research	The study aims to highlight the importance of managing, securing, and limiting access to privileged accounts within organizations to reduce the risk of unauthorized access, misuse, or abuse.	The importance of Privileged Access Management in safeguarding organizations against security threats, ensuring compliance with regulations, improving accountability, mitigating risks, and enhancing operational efficiency in cybersecurity practices.	More research is needed on how user behaviour impacts the effectiveness of PAM and how to incorporate behavioural analytics into PAM strategies.
7	Walker Network	Why do PAM	literature review	The study on Privileged Access	The study aims to highlight key challenges	Many PAM initiatives are

	Security (2019) 2019(9) 15-18	projects fail?		Management (PAM) aims to identify common reasons why PAM projects fail to meet initial expectations and provide practical insights on how organizations can prevent these failures.	such as incorrect focus on technical features, over-reliance on agent-based technology, insufficient integration of PAM components, and lack of governance and strategic alignment.	approached in silos; research is needed to explore comprehensive frameworks that combine governance, policy, and technology.
8	Anwar W *(2022) (August 2021)*	Privilege Access Analysis Security Tool for Windows & Linux	literature review	This study emphasizes the importance of prioritizing data visualization and analysis to effectively manage privileged access within an organization.	The importance of implementing a comprehensive security solution that focuses on analysing and visualizing Privilege Access metrics from Windows Active Directory and Linux devices.	The lack of comprehensive baseline research for Privilege Access Analysis within the Identity and Access Management (IAM) domain in cybersecurity.

The practice of controlling access rights for people, accounts, and systems within an organization is known as privilege access management or PAM, and the researcher reviewed the literature on the subject. However, the researcher found a gap in the literature regarding the usability characteristics of PAM systems. Although there were some general studies on access management and system usability, there was not enough research on the usability challenges and considerations of PAM applications. Therefore, the researcher aims to conduct a study to explore the specific usability factors and dimensions that are crucial for effective and user-friendly PAM systems. This could involve evaluating existing PAM tools usage, gathering user feedback, and identifying key usability criteria that should be addressed to enhance the overall user experience and adoption of these security-focused access management technologies. By addressing this gap in the literature, the researcher hopes to provide a more comprehensive understanding of PAM system usability, which could help organizations implement more usable and effective access management controls to improve their overall security posture. In summary, the researcher recognized a lack of focused research on PAM usability and wants to conduct a study to explore this topic in more depth, to expand the knowledge base in this area of access management and information security.

2.7. Research Model and Hypothesis Development

The Unified Theory of Acceptance and Use of Technology (UTAUT) is a theoretical model that is widely recognized in the field of information systems research. It helps to understand and explain why users accept and adopt technology. The model provides a complete framework for studying the factors that influence an individual's intention to use a particular technology. The researcher used the UTAUT model for PAM usability by considering the following points.

General Applicability: The UTAUT model is not specific to any particular technology or industry, making it suitable for studying the acceptance and use of various technologies, including PAM

systems. It has been successfully applied in diverse contexts, such as e-commerce, healthcare, and banking. Therefore, it can be reasonably applied to examine PAM usability at CBE.

Comprehensive Framework: The UTAUT model incorporates several key factors that influence technology acceptance and use, including performance expectancy, effort expectancy, social influence, and facilitating conditions. These factors align with the core elements of PAM usability, such as user perception of system effectiveness, ease of use, the influence of colleagues and superiors, and available resources and support. Using the UTAUT model, the researcher can systematically investigate these factors and their impact on PAM usability.

Established Validity and Reliability: The UTAUT model has been widely tested and validated across numerous studies, providing evidence of its reliability and validity. It has demonstrated robustness in predicting and explaining user behavior towards technology adoption. By leveraging an established theoretical model, the researcher can enhance the credibility and accuracy of PAM usability findings.

Practical Implications: The UTAUT model offers practical implications by identifying influential factors that can guide the design and implementation of PAM systems to enhance usability. Using this model, the researcher can provide actionable recommendations to CBE based on the factors affecting PAM usability, promoting better user acceptance and system adoption.

In conclusion, the UTAUT theoretical model is appropriate for study on PAM usability in CBE due to its general applicability, comprehensive framework, established validity and reliability, potential for, and practical implications. Its utilization will provide a structured and well-established foundation for examining the factors influencing the acceptance and use of PAM systems.

2.7.1. The UTAUT Model and Extension

To examine the usability factors of privileged access management, a researcher conducted a thorough investigation of existing studies, frameworks, and models. However, a gap was found in the literature for the PAM system usability model. To fill this gap, the researcher extended the UTAUT model by incorporating three additional factors (error, security features, and audit reporting capabilities). By adopting Nielsen's usability models, literature review, international standards, and vendor-based standards to establish the relevance and importance of these constructs in the study of PAM usability factors.

Errors Handling: The error rate of the system should be minimal so that the user makes the least number of errors when using the system. If some errors are made, they should be recovered easily. Finally, catastrophic errors should be avoided. Users are often distracted from the task at hand, so prevent unconscious errors by offering suggestions, utilizing constraints, and being flexible.

Perceived Security: The ISO standards emphasize the importance of making Privileged Access Management (PAM) easy to use for effective implementation and compliance with information security requirements (Culot et al., 2021). To improve system security while maintaining usability, it's crucial to integrate security measures into the design of user interfaces from the very beginning. This emphasizes the need for a comprehensive approach that considers both security and usability aspects in application systems (Y. Wang & Rawal, 2017). Therefore, integrating security measures into the design of user interfaces from the initial stages is significant, and a holistic approach to security and usability is necessary in application systems. Achieving a balance between security and usability is crucial when implementing improvements. This strategy strives to establish a system that is both secure and user-friendly, enhancing security measures while ensuring maximum usability for end-users (Y. Wang & Rawal, 2017). Enhancing the usability of security

features can improve the overall security of health information in e-Health applications, reduce the risk of data breaches, and ensure the confidentiality, integrity, and availability of sensitive health data in Ethiopian health systems (Lessa & Etoribussi, 2023). Privileged Access Management in safeguarding organizations against security threats, ensuring compliance, and improving overall cybersecurity posture (Mr. Siddhesh Bhargude, 2023).

Audit Reporting Capabilities: Privileged access management, monitoring and auditing play a crucial role in detecting suspicious behavior and unauthorized access. Organizations should closely monitor and audit privileged account activities to track usage patterns and identify any unusual or potentially malicious actions (Sindiren & Ciylan, 2018). By keeping a watchful eye on privileged account usage, organization can proactively detect and respond to insider threats ,thereby enhancing their overall security posture. Audit Reporting Capabilities characteristics of PAM are the international standards, vendor-based standards, and the main feature of the PAM system which is the reason the researcher added the UTAUT model to investigate the PAM usability factor to the study.

Hypothesis Development

Usability considerations play a crucial role in the success of a privileged access management system in CBE. The model developed by integrating various models, standards, and literature reviews, highlights the four fundamental constructs of the UTAUT model Performance Expectancy, Effort Expectancy, Social Influence, And Facilitating Condition. This model also added new constructs for error handling, perceived security features, and audit reporting capabilities to ensure the effective usability of the PAM system at CBE.

1. Performance Expectancy: This construct represents the degree to which an individual believes that using the PAM system will help them to attain in job performance. It is influenced by perceived by usefulness, extrinsic motivation, job fit, and outcome expectations It is widely agreed that employee performance is a critical indicator of a firm's success. ("Roles of Expectancy on Employee Engagement and Job Performance," 2019).

H1: Users' perception of system performance positively influences their intention to use the PAM system.

2. Effort Expectancy: This construct represents the degree of ease associated with use of the PAM system. It is influenced by perceived ease of use and complexity.

H2: Higher perceived ease of use reduces the effort required and increases users' intention to use the PAM system.

3. Social Influence: This construct represents the degree to which an individual perceives that important others believe they should use the new system. It is influenced by subjective norms, social factors, and image. Social influence impacts consumer upgrade decisions. Well-connected adopters have a stronger influence on first-time adoption, while upgraders with higher homophily have a stronger influence on upgrade adoption (D. Wang et al., 2019).

H3: Peer recommendations and social influence positively affect users' intention to use the PAM system.

4. **Facilitating Condition:** This construct represents the degree to which an individual believes that an organization and technical infrastructure exist to support the use of the system. It is influenced by perceived behavioral control, facilitating conditions, and compatibility. The

adoption and diffusion of standards in Information Infrastructures necessitate a complex coordination of actors, which includes individuals, organizations, and institutions, along with their respective work practices and organizational behavior. These actors must work together to establish institutional arrangements that can support the successful diffusion and adoption of standards, that can ultimately shape the behavior of the organization (D. Wang et al., 2019).

H4: Adequate resources and support available positively impact users' intention to use the PAM system.

5. Errors Handling:

Minimizing errors is essential for PAM success. Errors such as misconfigurations, accidental privilege escalations, or unauthorized access attempts can lead to security vulnerabilities and potential system failures. By reducing errors through clear system prompts, validation mechanisms, and error prevention measures, the overall effectiveness and success of PAM can be improved.

H5: The effective management of error handling positively enhances user intention to use the PAM system.

6. Perceived Security:

Privileged access management effectively monitors and controls access to critical internal systems, networks, and data, offering benefits and best practices for modern cybersecurity (Mr. Siddhesh Bhargude, 2023). Robust security features are crucial for PAM's success. Strong authentication mechanisms, encryption, secure session management, and privilege elevation controls protect against unauthorized access and privilege misuse. Effective security features minimize the risk of

data breaches, insider threats, and unauthorized access attempts, ensuring the integrity and confidentiality of sensitive information.

H6: A positive perception of robust security features enhances users' intention to use the PAM system.

7. Audit and reporting capabilities:

Comprehensive audit and reporting capabilities are critical for PAM's success. These features enable organizations to monitor privileged activities, track access events, generate compliance reports, and detect anomalous behaviors. Auditing and monitoring approaches are critical for access control in database systems (Omotunde & Ahmed, 2023). Effective audit and reporting mechanisms provide visibility into privileged access activities, support compliance requirements, and aid in incident response and forensic investigations.

H7: Effective audit and reporting features positively influence users' intention to use the PAM system.

Additionally, the UTAUT model suggest that the relationship between these core constructs and the intention to use and actual use of PAM system may be moderated by factors such as user demographics (e.g., age, gender), experience with the system, and voluntariness of use. By grounding the PAM usability research in the well-established UTAUT framework, the study aims to provide a robust and comprehensive understanding of the determinants of PAM system acceptance and usage, which can inform the design and implementation of a more user-friendly and effective access management solution.

Formulating hypotheses for each of these variables and their potential impact on PAM success is crucial. It's worth noting that hypotheses can be further refined based on the specific research

objectives, as well as the measures used to assess PAM usability success. These hypotheses should be testable through data collection and analysis methods that evaluate the relationship between the independent variables and dependent variable. Using these hypotheses as a starting point can help explore the connections between the independent variables and user intentions in the context of the PAM system being studied. The hypotheses suggest that the usability factors and support mechanisms associated with these independent variables will have a positive impact on the overall success of the PAM system in the CBE. Therefore, improvements or enhancements made in each independent variable are more likely to lead to positive outcomes in PAM success.

H8: Behavioral Intention Use Will Have a Positive Influence on PAM System Usability Success.

2.7.2. Proposed Conceptual Framework for PAM System Usability

The UTAUT theoretical model was utilized as the guiding framework for the study of PAM system usability. The UTAUT model provides a comprehensive approach to understanding the key factors that influence an individual's intention to use and their actual usage of a technological system. By grounding the PAM usability research in the well-established UTAUT framework, the study aims to provide a robust and comprehensive understanding of the key determinants of PAM system acceptance and usage, which can inform the design and implementation of more user-friendly and effective access management solution. As mentioned earlier in the literature review, different system usability models are amongst the most widely used models to evaluate information system usability some of them are adopted for the constructs of the PAM conceptual framework. These considerations will provide valuable insights into the success and usability of a PAM system within CBE. The UTAUT model's four fundamental constructs were tailored to the context of PAM system usability. This involved integrating performance expectancy, effort expectancy, social

influence, facilitating condition, with error handling, perceived security and audit reporting capabilities from literature to study the usability of PAM system.

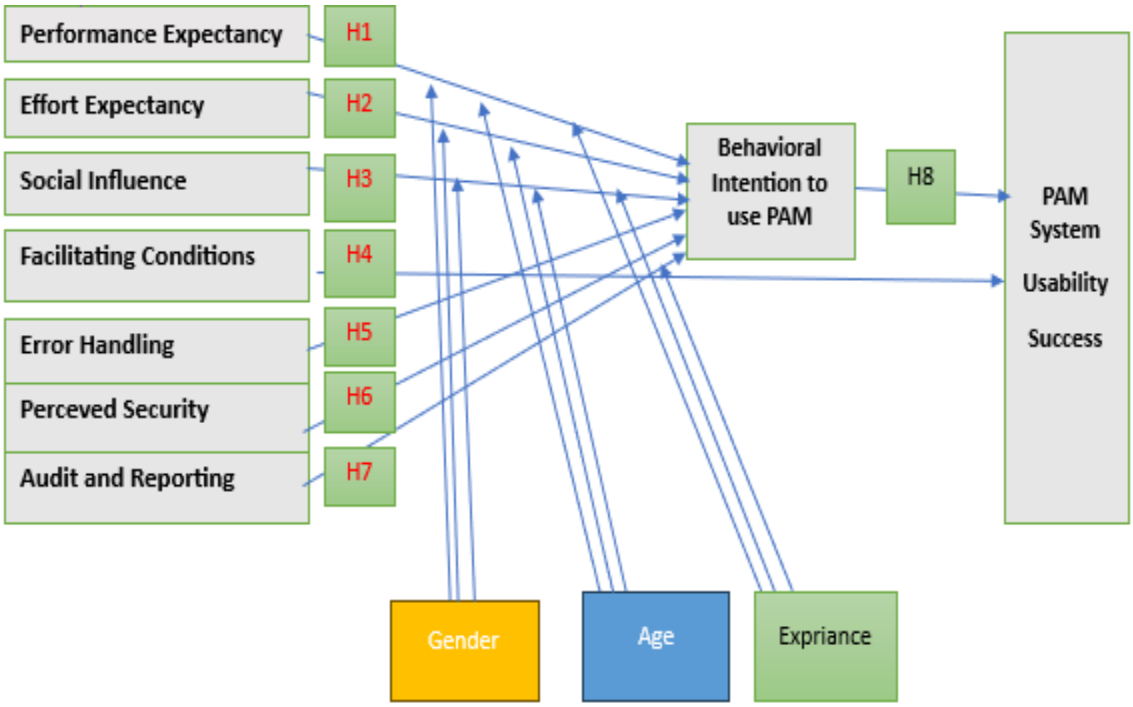

Figure 2.6. Conceptual Framework of PAM Usability Model

Adopted from (Venkatesh et al., 2003)

2.8. Chapter Summary

The literature review chapter provides a comprehensive analysis of existing research, theories, and findings related to privileged access management and its usability. The primary focus of this chapter is to establish the theoretical and empirical foundation that supports the need for and relevance of conducting a usability study on PAM solutions. The chapter begins by defining PAM and outlining its importance in securing sensitive data and critical systems within organizations critically evaluates existing usability studies and frameworks that have been applied in the context of PAM or related security solutions. By drawing on established usability principles and best practices, the review aims to identify gaps and opportunities for enhancing the user experience of PAM tools. Moreover, the chapter discusses theoretical models and frameworks, such as

The Unified Theory of Acceptance and Use of Technology (UTAUT) and their applicability in understanding user acceptance and adoption of PAM solutions. The literature review concludes by synthesizing the key findings and insights from the existing body of knowledge, emphasizing the significance of addressing PAM usability challenges and the potential benefits of improved user experience in PAM deployment.

CHAPTER III

Research Design and Methodology

3. Introduction

The research design and methodology section of a study is crucial in outlining the overall approach and strategy that will be employed to address the research questions or objectives. It serves as a roadmap for the research process, detailing how data will be collected, analyzed, and interpreted to draw meaningful conclusions. This section also provides insights into the rationale behind the chosen research design, highlighting its appropriateness and relevance to the study at hand.

In this chapter, we will investigate the details of the research explain the research methodology used to identify the factors that affect the usability of PAM raised in the research question, and propose a solution to bridge the gap through the design and methodology adopted for this study The researcher discuss the research paradigm, approach, design, data collection methods, sampling techniques, and data analysis procedures employed to achieve the research goals. By presenting a comprehensive overview of the research design and methodology, the researcher aims to provide a clear and structured framework for conducting the study effectively and rigorously.

3.1.Research Design

For the research topic Enhancing Usability of Privileged Access Management (PAM) Systems: A Case Study of Implementation Strategies at the Commercial Bank of Ethiopia (CBE) a mixed-method research design was employed. Data collection involved the distribution of questionnaires to gather quantitative insights on user experiences with the PAM system. Additionally, interviews were conducted to collect qualitative data, allowing for a deeper exploration of user perceptions and preferences regarding PAM system usability.

The quantitative data obtained from the questionnaires was analyzed using logistic regression analysis. This statistical technique enabled the identification of factors influencing user satisfaction and usability within the PAM system. On the other hand, the qualitative data gathered from the interviews underwent thematic analysis. By systematically organizing and interpreting the interview responses, key themes and patterns related to PAM system usability were extracted, providing valuable qualitative insights into user needs and challenges.

Overall, the research design and methodology employed in this study aimed to triangulate quantitative and qualitative data to gain a comprehensive understanding of the usability issues surrounding PAM systems within the selected organization. The combination of questionnaires and interviews, along with logistic regression and thematic analysis, allowed for a holistic investigation of user experiences and the development of tailored implementation strategies to enhance the usability of PAM systems.

3.2. Research Methodology:

The research methodology for studying PAM usability is a mixed approach of quantitative and qualitative methods. When researching a PAM system's usability, the researcher prefers to use a mixed-methods approach because it allows one to comprehensively understand the topic by combining quantitative and qualitative data. Using both data types, the researcher can capture numerical insights about system performance and user success rates while exploring users' experiences, challenges, and suggestions through qualitative data. The triangulation of multiple data sources enhances the validity of the findings, and the complementarity of quantitative and qualitative data provides a more holistic view of the PAM usability issues. Additionally, the mixed-methods approach allows for exploration and explanation, practical implications for system improvement, and flexibility in adapting the research design based on emerging insights.

3.3. Population and Sampling Methods

3.3.1. Quantitative Sampling

The appropriate sample size should be determined to ensure high-quality research and to prevent the wastage of resources. (Adhikari, 2021). Obtaining an appropriate sample size is crucial for survey researchers as it affects the accuracy, cost, and time required for obtaining a sample estimate. Despite its importance, obtaining a good estimate of the population variance is challenging, and a lack of knowledge of sampling theory can hinder researchers from obtaining an appropriate sample in survey research. (Adam, 2020).

To conduct a study, defining the target population is important. This could be a specific group of people, such as PAM users or administrators. To select a representative sample from this population, various sampling techniques are there. For this particular research, the researcher focused on CBE, one of Ethiopia's largest banks. CBE has almost 246 privileged IT users across headquarters this is the size of the population. To ensure a fair selection process, the researcher used the probability sampling method and randomly selected all of the IT users from CBE's headquarters in Addis Ababa. This sample size is considered adequate to achieve statistical significance and allow for the findings' generalizability. There are various formulas used for computing sample size. one of the most prominent formulas used is Yamane's formula. n=N/(1+N(e)2.

To calculate the sample size (n) using the formula n=N/(1+N(e)2, where N represents the population size and represents the desired margin of error, The total number of PAM users in CBE is 246. A sample of 150 employees will be selected using a 95% level of confidence and 5% margin error according to Yamane’s (1967) formula.

3.3.2. Qualitative Sampling

The researcher intends to employ purposive and judgmental sampling, which are non-probability sampling techniques. In qualitative research, the size of the sample does not necessarily imply significance (Barbour, 2022). In this specific case, the aim is to gather the PAM administrators and information security managers who have an understanding of PAM systems to obtain a diverse range of perspectives. When selecting participants, accessibility, willingness to participate, and relevance to the research objectives should be taken into account. Theoretical sampling is a qualitative method that allows researchers to select participants based on their unique experiences and knowledge, rather than relying on a predetermined number of participants (Barbour, 2022). The qualitative methodology will utilize a team consisting of three PAM experts and two security managerial position. This diverse group will offer a comprehensive and reasonable approach to the research, resulting in precise and insightful findings. The team comprises domain experts who possess both strategic and technical expertise and understanding of PAM systems in details.

3.4. Data Collection Methods

The process of obtaining pertinent information to support research aims is known as data collection, and it is a crucial component of research. It is achieved through various methods such as observation, where researchers observe and record data from a particular phenomenon, interviews, where researchers engage with individuals to obtain first-hand information, questionnaires, where respondents provide answers to pre-determined questions, and database access, where researchers extract information from existing data repositories. These methods enable researchers to obtain accurate and reliable data, which is crucial for making informed decisions in research (Mazhar, 2021).

3.4.1. Quantitative Data Collection Methods:

Data collection through questionnaires is a popular method in large surveys. Questionnaires consist of a set of questions that respondents are asked to answer and return. This method is widely used by researchers, organizations, and governments (Mazhar, 2021). Quantitative data collection involves using questionnaires to gather numerical data from the user of the privileged access management system through Google Forms. This is done by adopting a set of standardized questions that address the research goals and inquiries. The questionnaire will cover various aspects of PAM usability, such as performance expectancy, effort expectancy, social influence, facilitating conditions, with error handling, perceived security, and audit reporting capabilities. A pilot test was conducted with a small sample of participants to confirm the validity of the questions. Methods such as Cronbach's alpha were utilized to assess the questionnaire's internal consistency. The construct validity of the questionnaire needs to be evaluated, through factor analysis or other validation methods. Finally, the survey should be given to a representative sample of PAM users.

3.4.1.1. Instrument Development

Table 3.1: Research Construct and their Items

#	**Performance Expectancy:**	
1	Using the PAM system increases my productivity.	
2	The PAM system helps me accomplish critical tasks efficiently.	
3	I believe that the PAM system enhances my job performance.	Adopted from (Venkatesh et al., 2003)
4	The PAM system improves my ability to manage privileged access effectively.	
	Effort Expectancy:	Adopted from (Venkatesh et al., 2003)
5	Interacting with the PAM system is easy.	
6	Learning how to use the PAM system was simple for me.	
7	It is easy for me to navigate through the PAM system features.	
8	Using the PAM system requires minimal effort on my part.	
	Social Influence:	

9	My colleagues encourage me to use the PAM system.	Adopted from (Venkatesh et al., 2003)
10	Managers in my organization emphasize the importance of using the PAM system.	
11	I feel supported by my peers in adopting the PAM system.	
12	The organizational culture promotes the use of the PAM system.	
	Facilitating Condition:	Adopted from (Venkatesh et al., 2003)
13	I can access the necessary resources to use the PAM system effectively.	
14	The technical support for the PAM system is readily available when needed.	
15	The organization provides adequate training on how to use the PAM system.	
16	I have the tool and equipment to fully use the PAM system.	
	Errors Handling:	Adopted from Jakob Nielsen model
17	I have the opportunity to improve my skills when using the PAM system.	

18	Error messages displayed by the PAM system are clear and easy to understand.	
19	The PAM system effectively handles user input errors.	
20	The PAM system effectively handles errors and provides appropriate recovery mechanisms	
	Perceived Security:	Adopted from Protection Motivation Theory (PMT) model
21	The PAM system provides robust password management features.	
22	I feel confident in the security measures implemented by the PAM system.	
23	The PAM system effectively controls access to sensitive information.	
24	I believe that the PAM system enhances the overall security posture of our organization.	
	Audit and Reporting Capabilities:	Control, Compliance, and Audit (CCA) model
25	The PAM system provides detailed audit logs of privileged access activities.	
26	The system can easily generate reports on privileged access usage.	

27	The audit and reporting features of the PAM system help in information system policy compliance adherence.	
28	I believe the audit and reporting capabilities of the PAM system to be valuable for security monitoring.	
	Behavioral Intention to Use	Adopted from (Venkatesh et al, 2003)
29	I am likely to rely on a PAM system for controlling access privileges.	
30	I plan to use a PAM system regularly to manage access privileges.	
31	I intend to continue using the PAM software in the future.	

3.4.2. Qualitative Data Collection Methods

Gathering comprehensive and in-depth information about PAM usability through techniques like interviews is known as qualitative data collection. Interviews involve direct communication with respondents to gather information this method can be structured, unstructured, or semi-structured, depending on the level of pre-defined questions and flexibility in the conversation (Mazhar, 2021).

3.5. Data Analysis

The process of collecting data is crucial to research as it provides the foundation for analysis and interpretation. Researchers rely on the data collected to identify patterns, trends, relationships, and insights that help them better understand the research problem at hand (Mazhar, 2021). With this information, they can draw meaningful conclusions and make informed decisions that can lead to advancements in their field of study. Without proper data collection, analysis and interpretation would be incomplete and unreliable, hindering progress and innovation (Mazhar, 2021).

3.5.1 Quantitative Analysis:

Analyses the quantitative data using appropriate statistical techniques. This may include descriptive statistics and inferential statistics, such as hypothesis testing, regression analysis, and analysis of variance (ANOVA), to draw conclusions and determine significant differences or relationships between variables. Utilize statistical software packages to facilitate data analysis and ensure accuracy. By following these steps, effectively collect quantitative data on PAM usability through surveys or questionnaires. The resulting data will provide numerical insights into various aspects of PAM usability, allowing for statistical analysis and quantitative comparisons.

3.5.2. Qualitative Data Analysis:

The quantitative data analysis will be thematic and involves identifying and analyzing recurring patterns, themes, or categories within the qualitative data. Analyze the qualitative data using appropriate qualitative analysis techniques. This may involve approaches such as thematic analysis, to meet the research objectives and the nature of the data. Identify and code key themes, patterns, or categories that emerge from the data. Finally, perform deductive analysis to come up with the existing model theory.

3.6. Integration and Interpretation:

The researcher can identify common themes and insights by comparing and contrasting the results from various data sources. Lastly, the findings should be interpreted in the context of the research objectives and questions to obtain a comprehensive understanding of PAM usability.

3.7. Validity and Reliability

The researcher used for validity and reliability of the data collection for both quantitative survey and qualitative interview questions adopted from the UTAUT model Adopted from (Venkatesh et al., 2003) and Adopted from the Jakob Nielsen model. By collecting data systematically and following established protocols, researchers can ensure the validity and reliability of their findings. Proper data collection methods help in minimizing bias and errors, leading to more accurate results (Mazhar, 2021). Validity and reliability are important considerations in mixed research methods, which combine qualitative and quantitative approaches. validity and reliability are essential concepts, but they are understood and applied differently in each tradition:

- **Validity:**

Validity refers to the extent to which a research study accurately measures or reflects the concept or phenomenon it intends to study. In Mixed research, validity can be addressed in the following ways. Quantitative research aims to measure what it intends to measure, and the validity of a study refers to how well it achieves that goal. Validity can come in different forms, such as internal or external validity, face validity, content validity, and criterion validity. On the other hand, validity in qualitative research focuses on the research's credibility, trustworthiness, dependability, transparency, and transferability, rather than its fit with reality. The emphasis is on ensuring the evidence and research findings are trustworthy and reliable. (Nha, 2021).

- **Reliability:**

Reliability refers to the consistency and stability of research findings or measures. In mixed research, ensuring reliability is involved. Reliability is important in research, referring to the consistency of instruments, procedures, and results. In quantitative research, it means consistency of data obtained through measurement instruments. In contrast, in qualitative research, reliability is replaced by terms like dependability or consistency. Qualitative research aims to enhance dependability through strategies like triangulation, member checks, audit trails, and respondent validation. Understanding these differences is crucial for researchers to apply validity and reliability criteria effectively (Nha, 2021).

3.8. Chapter Summary

In this chapter concerning research design and methodology for a mixed approach, the emphasis lies on the integration of qualitative and quantitative methods to attain a holistic comprehension of the research problem. The chapter underscores the significance of selecting a suitable research design that harmonizes with the research objectives and questions. This chapter presents a thorough outline of research design and methodology for a mixed approach, which combines qualitative and quantitative techniques to foster a more profound understanding of the research problem underscoring the importance of combining qualitative and quantitative methods to reinforce the rigor and validity of research findings.

CHAPTER IV

Data Analysis and Discussion

4.1. Introduction

The main objective of this research is to answer the research question by examining the factors influencing the usability of privileged access management systems at CBE. The research used a mixed-method design, which involved gathering both quantitative and qualitative data. The quantitative component involved a structured questionnaire developed to measure the constructs of The Unified Theory Of Acceptance And Use Of Technology (UTAUT), as well as additional factors such as perceived security features, error handling, and audit and reporting capabilities. The questionnaire items were carefully selected from validated scales in the literature and rigorously pre-tested to ensure clarity and relevance. A sample of 150 PAM system users within the Commercial Bank of Ethiopia provided their responses on a 5-point Likert scale questionnaire.

To complement the quantitative data, the researchers also conducted interview questions with three PAM experts and two security managers within CBE. The interview protocol was designed to explore the in-depth perspectives and experiences of these experts, covering topics such as key usability factors, implementation challenges, and best practices for improving PAM system acceptance and usage. The interviews were audio-recorded, transcribed verbatim, and lasted approximately 45 minutes on average.

The study utilized a mixed-method approach to gather both quantitative and qualitative insights. This allowed for a comprehensive understanding of the factors affecting the usability of the PAM system within the organization, leveraging the strengths of each data collection and analysis technique.

4.2. Quantitative Data Analysis

The quantitative data analysis involved demographic analysis to describe the characteristics of the survey respondents. Assessment of the reliability and validity of the measurement scales and hypothesis testing were conducted using appropriate statistical techniques, such as regression analysis to assess the relationships between the UTAUT and additional factors, and users' intention to use the PAM system.

The overall fit and explanatory power of the UTAUT model was evaluated to determine its suitability in impacting PAM system usability.

Reliability Analysis

Table 4.1. Cronbach's Alpha Result

Reliability Statistics	
Cronbach's Alpha	N of Items
.925	31

Results

Cronbach's alpha reliability analysis shows Performance Expectancy=0.82, Effort Expectancy=0.89, Social Influence=0.77, Facilitating Conditions=0.90, Errors Handling=0.88, Perceived Security =0.88, Audit and reporting capabilities, =0.88, Behavioural Intention to Use PAM=0.80. The result indicates that all measurements are reliable.

4.2.1. Demographic Analysis

Demographic analysis was performed to describe the characteristics of the survey respondents.

Descriptive Statistics:

1. Gender

Table 4.2. Respondents' frequency per Gender

Gender					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	108	72.0	72.0	72.0
	Female	42	28.0	28.0	100.0
	Total	150	100.0	100.0	

2. Age

Table 4.3. Respondents frequency per Age

Age					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	25-34	120	80.0	80.0	80.0
	35-44	26	17.3	17.3	97.3
	45-54	3	2.0	2.0	99.3
	55-64	1	.7	.7	100.0
	Total	150	100.0	100.0	

3. Education Level

Table 4.4. Respondents' frequency per Education Level

Education Level					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Degree	94	62.7	62.7	62.7
	MSc/MA	56	37.3	37.3	100.0
	Total	150	100.0	100.0	

4. Work Experience

Table 4.5. Respondents frequency per Work Experience

Work Experience					
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Less than 1year	2	1.3	1.3	1.3
	1-3 years	69	46.0	46.0	47.3
	3-5 years	13	8.7	8.7	56.0
	5-10 years	39	26.0	26.0	82.0
	More than 10 years	27	18.0	18.0	100.0
	Total	150	100.0	100.0	

Frequencies provide the frequency distributions and percentages for each demographic variable (e.g., gender, age group, educational level, and work experience).

4.2.2. Hypothesis Testing

Regression Analysis

Regression analysis was used in conjunction with other statistical approaches to evaluate the hypothesis testing on the UTAUT and other contracts, specifically regarding users' intention to use the PAM system.

Model Summary:

Table 4.6 Model Summary

Model Summary									
Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Change Statistics				
					R Square Change	F Change	df1	df2	Sig. F Change
1	.638[a]	.407	.378	.502	.407	13.921	7	142	.000
a. Predictors: (Constant), FC, EH, PE, SI, PS, AR, EE									

Analyze the R-squared (R^2) value, which shows how much of the variance in the independent variables (UTAUT components) is explained by the dependent variable (intention to use). A better model fit is indicated by a larger R2 value, which ranges from 0 to 1.

The predictor variables of performance expectancy, effort expectancy, social influence, enabling conditions, error handling, perceived security, and audit reporting capabilities that affect PAM usability were regressed on the dependent variable, behavioral intention to use the PAM system.

The seven parameters under research have a significant impact on behavioral intention to use the PAM system, as indicated by the independent variables' significant prediction of behavioral intention to use the system (P-value < 0.05). The model explains 40.7% of the variance in behavioral intention to utilize the PAM system, according to the R square =.407 data.

ANOVA

Table 4.7. ANOVA

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	24.593	7	3.513	13.921	.000[b]
	Residual	35.837	142	.252		
	Total	60.430	149			

a. Dependent Variable: BIUPAM

b. Predictors: (Constant), FC, EH, PE, SI, PS, AR, EE

An ANOVA test to assess the regression model's overall statistical significance. The ANOVA table will provide the F-statistic and its associated p-value, indicating whether the model as a whole significantly predicts the dependent variable. The p-value is 0.000 less than the chosen significance level of 0.05, The researcher can conclude that the model significantly explains the intention to use the PAM system.

1. Performance expectancy

Table 4.9. Performance Expectancy Variable Hypothesis Testing

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	4.280	1	4.280	11.281	.001[b]
	Residual	56.151	148	.379		
	Total	60.430	149			
a. Dependent Variable: BIUPAM						
b. Predictors: (Constant), PE						

Hypothesis H1: Users' perception of system performance positively influences their intention to use the PAM system.

The findings show that this hypothesis was supported, with a substantial and favorable impact on users' intention to utilize the PAM system, with the P-value of 0.001 < 0.05. This result is consistent with the UTAUT model's Performance Expectancy construct, which predicts that users are more inclined to use a system if they think it would enable them to accomplish their goals and perform better at work. It follows that the perception of the PAM system's value and its capacity to increase user productivity and efficiency play a pivotal role in motivating user adoption and intention to utilize the system.

2. Effort Expectancy

Table 4.10. Effort Expectancy *Variable Hypothesis Testing*

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	13.185	1	13.185	41.303	.000[b]
	Residual	47.245	148	.319		
	Total	60.430	149			
a. Dependent Variable: BIUPAM						
b. Predictors: (Constant), EE						

Hypothesis H2: Higher perceived ease of use reduces the effort required and increases users' intention to use the PAM system.

The findings validate the hypothesis that the perceived ease of use of the PAM system favorably increases users' intention to employ it, as indicated by the P-value of 0.000 < 0.05. The results align with the UTAUT model's Effort Expectancy construct, which posits that users are inclined to utilize a system more frequently if they believe it to be simple to learn and operate. It follows that factors like the PAM system's usability, intuitiveness, and ease of use are crucial for encouraging user adoption and sustained use.

3. Social Influence

Table 4.11. Social Influence Variable Hypothesis Testing

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	6.431	1	6.431	17.626	.000[b]
	Residual	53.999	148	.365		
	Total	60.430	149			
a. Dependent Variable: BIUPAM						
b. Predictors: (Constant), SI						

Hypothesis H3: Peer recommendation and social influence positively affect users' intention to use the PAM system.

The results show that the P-value, which is 0.000 < 0.05, supported the hypothesis. indicating that users' intentions to use the PAM system are positively impacted by social influence, such as peer endorsements and organizational standards. This finding aligns with the Social Influence construct in the UTAUT model, which highlights the role of social factors in shaping individual technology adoption decisions. The implication is that fostering a positive social environment, where peers and organizational leaders encourage and support the use of the PAM system, can contribute to its overall adoption and acceptance.

4. Facilitating Conditions

Table 4.12. Facilitating Conditions Variable Hypothesis Testing

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	7.141	1	7.141	19.832	.000[b]
	Residual	53.290	148	.360		
	Total	60.430	149			
a. Dependent Variable: BIUPAM						
b. Predictors: (Constant), FC						

Hypothesis H4: Adequate resources and support available positively impact users' intention to use the PAM system.

The findings show that the hypothesis was supported by the P-value of 0.000 < 0.05, indicating that users' intention to utilize the PAM system is positively influenced by the resources and support that are available. This result is consistent with the UTAUT model's Facilitating Conditions construct, which postulates that the availability of technical and organizational resources to enable system use can improve user adoption. The consequence is that potential obstacles can be addressed and more successful PAM system adoption and utilization can be enabled by giving users the required training, documentation, technical support, and resources.

5. Error Handling

Table 4.13 Error Handling Variable Hypothesis Testing

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	6.102	1	6.102	16.622	.000[b]
	Residual	54.329	148	.367		
	Total	60.430	149			
a. Dependent Variable: BIUPAM						
b. Predictors: (Constant), EH						

Hypothesis H5: The effective management of error handling positively enhances user intention to use the PAM system.

The results show that the hypothesis was supported by the P-value of 0.000 < 0.05, which suggests that efficient error handling in the PAM system increases users' propensity to use the system. By emphasizing the significance of error management and system reliability, which can improve overall usability, this finding expands on the UTAUT model.

6. Perceived Security

Table 4.14 Perceived Security Variable Hypothesis Testing

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	17.476	1	17.476	60.212	.000[b]
	Residual	42.955	148	.290		
	Total	60.430	149			
a. Dependent Variable: BIUPAM						
b. Predictors: (Constant), PS						

Hypothesis H6: A positive perception of robust security features enhances users' intention to use the PAM system.

The results show that the hypothesis was supported by the P-value of 0.000 < 0.05. This means that users' inclination to utilize the PAM system is increased when they perceive its security features to be strong. This conclusion adds this crucial component for PAM systems to the UTAUT paradigm and is consistent with the research on the significance of perceived security in technology adoption.

7. Audit And Reporting Capabilities

Table 4.15 Audit And Reporting Capabilities Variable Hypothesis Testing

ANOVA[a]						
Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	20.309	1	20.309	74.915	.000[b]
	Residual	40.122	148	.271		
	Total	60.430	149			
a. Dependent Variable: BIUPAM						
b. Predictors: (Constant), AR						

Hypothesis H7: Effective audit and reporting features positively influence users' intention to use the PAM system.

The findings show that the hypothesis was supported by the P-value of 0.000 < 0.05. This suggests that the PAM system's efficient audit and reporting capabilities have a positive impact on users' intention to utilize the system. The relevance of transparency, accountability, and compliance-related features—which are especially pertinent in privileged access management is incorporated into this discovery, expanding the UTAUT paradigm.

4.2.3. Hypothesis Result

The goal of the research is to determine how PAM usability is impacted by performance expectation, effort expectancy, social influence, enabling conditions, error management, perceived security, and audit and reporting capabilities.

The following hypotheses were proposed.

H1: Users' perception of system performance positively influences their intention to use the PAM system.

H2: Higher perceived ease of use reduces the effort required and increases users' intention to use the PAM system.

H3: Peer recommendation and social influence positively affect users' intention to use the PAM system.

H4: Adequate resources and support available positively impact users' intention to use the PAM system.

H5: The effective management of error handling positively enhances users' intention to use the PAM system.

H6: A positive perception of robust security features enhances users' intention to use the PAM system.

H7: Effective audit and reporting features positively influence users' intention to use the PAM system.

Table 4.16 All Hypothesis Testing Results

Hypothesis	Regression weight	F	P-value	Results
H1	PE→ BIUPAM	11.281	**0.001***	Supported
H2	EE→ BIUPAM	41.303	**0.000***	Supported
H3	SI→ BIUPAM	17.626	**0.000***	Supported
H4	FC→ BIUPAM	19.832	**0.000***	Supported
H5	EH→ BIUPAM	16.622	**0.000***	Supported
H6	PS→ BIUPAM	62.212	**0.000***	Supported
H7	AR→ BIUPAM	74.915	**0.000***	Supported

*Note: *P<0.05 PE stands for performance expectancy; EE for effort expectancy; BIUPAM for intention to use the PAM; FC for facilitating conditions; EH for error handling; PS for perceived security; AR for audit reporting capabilities.*

The hypothesis testing, H1 evaluates whether performance expectancy significantly and positively influences intention to use the PAM system. The results revealed that performance expectancy significantly and positively impacts intention to use the PAM system P=0.001. Hence H1 was supported. H2 evaluates whether the intention to utilize the PAM system is significantly and favorably influenced by effort expectancy. The findings showed that the intention to use the PAM system is strongly and favorably impacted by effort expectancy P=0.000. H2 was therefore supported.

H3 evaluates whether the intention to utilize the PAM system is significantly and favourable influenced by social influence. The findings showed that the intention to utilize the PAM system is strongly and favourable impacted by social influence P=0.000. H3 was therefore accepted. H4 evaluates if the intention to utilize the PAM system is significantly and favourable influenced by error handling. The findings showed that the intention to utilize the PAM system is positively and strongly impacted by mistake handling P=0.000. H4 was therefore supported. H5 evaluates if the intention to utilize the PAM system is considerably and favourable influenced by facilitating situations. The findings showed that the intention to use the PAM system is strongly and favourable impacted by facilitating conditions P=0.000. H5 was therefore accepted. H6 evaluates if the intention to utilize the PAM system is significantly and favourable influenced by perceived security. The findings showed that the intention to utilize the PAM system is positively and strongly impacted by perceived security P=0.000. H6 was therefore accepted. H7 evaluates if the ability to report on audits has a significant and positive impact on users' intentions to utilize the PAM system. The findings showed that the intention to use the PAM system is positively and strongly impacted by audit reporting capabilities P=0.000. H7 was therefore accepted.

4.2.4. Model Evaluation

Comparison with Existing Literature

The overall fit and explanatory power of the UTAUT theoretical model extended the additional constructs in predicting user intention to use the PAM system. The core UTAUT constructs (Performance Expectancy, Effort Expectancy, Social Influence, and Facilitating Conditions) have been widely validated in the UTAUT literature as influential factors in technology adoption and usage intention. The study's findings supporting hypotheses H1-H4 are consistent with the established UTAUT framework and its application in various technology domains.

Extension of UTAUT in PAM Context:

The addition of error handling, perceived security, and audit and reporting capabilities as extended factors (H5-H7) is an important contribution to the UTAUT literature, particularly in the context of privileged access management (PAM) systems. Previous UTAUT studies in other technology domains may not have emphasized these system-specific features, highlighting the need to tailor the UTAUT model to the unique requirements of PAM systems.

Expansion of PAM Usability Factors:

The study identified some of the extended factors, and the study's comprehensive model and empirical validation provide a more holistic understanding of the multifaceted nature of PAM system usability. Including audit and reporting capabilities, error handling and perceived security as a distinct factor extends the existing literature, recognizing the unique requirements and concerns associated with privileged access management.

Methodological Approach:

The quantitative survey method employed in the study aligns with the common research approach in UTAUT and technology acceptance literature, allowing for the statistical testing of the proposed hypotheses. The methodological approach complements the existing body of PAM usability research, which may have utilized different methods, such as qualitative explorations, to gain a deeper understanding of the phenomenon. Overall, the study findings provide a valuable contribution to the literature by extending the UTAUT framework to the specific context of PAM system usability, highlighting the importance of system-specific factors in addition to the core UTAUT constructs. This comprehensive understanding can inform the design, implementation, and evaluation of PAM systems to enhance the overall usability and user acceptance within CBE.

4.3. Qualitative Data Analysis:

Qualitative methodology uses data collected through the interviews. The purpose of the interviews was to gather the projections of the PAM experts and security managers staff of CBE to give feedback on factors impacting the usability of PAM.

4.3.1. Thematic Analysis of Interviews

Thematic analysis was employed to identify the key themes emerging from the interview data. The interview transcripts were systematically coded, and the codes were organized into broader themes that reflected the key factors influencing PAM system usability. After that, the qualitative and quantitative data were combined to give a more thorough grasp of the research problem. The emerging themes were then supported by a portion from the interviews.

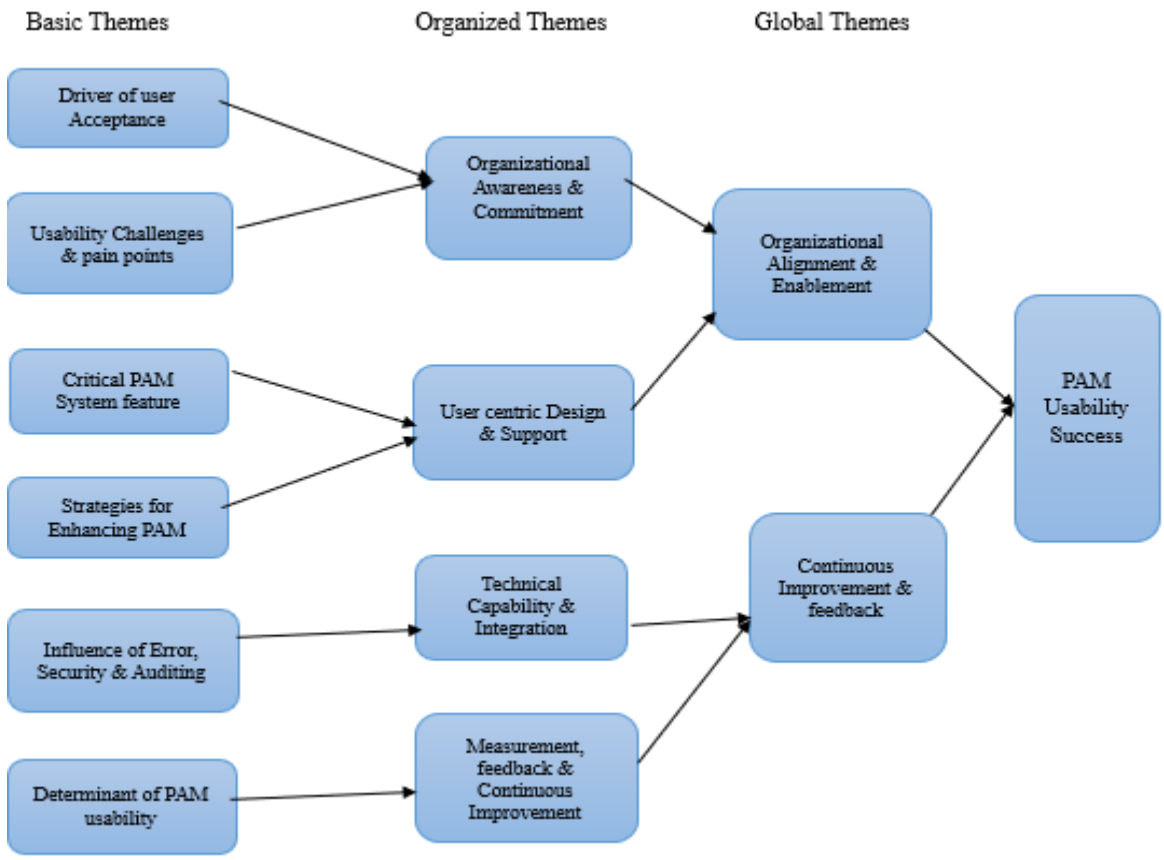

Fig. 4.1. Thematic Illustration: Major Factors for PAM System Usability Success.

Adopted from the Fit-Viability Model (Liang, 2007).

A. Themes Narration

In the qualitative data analysis of privileged access management system usability research, several key themes have emerged from interview transcriptions. The following are some key themes the researcher suggests focusing on for the qualitative data analysis that are filtered from interview transcription.

The drivers influencing user acceptance and adoption of PAM systems include management awareness and cybersecurity knowledge, users understanding the importance of PAM, quality of training available for PAM systems users, vendor support, and encouragement from management

towards the PAM supporting team. Additionally, usability challenges and pain points revolve around concerns about password compromise that will occur due to the unavailability of multifactor authentication and security perceived complexity of PAM systems, integration issues impacting established workflows, and user resistance to change. Organizational and contextual factors such as organizational culture, IT governance policies, and varying technical expertise among end-users also play a role in PAM adoption. Further, critical PAM system features and functionalities that enhance usability include user-friendly interface design, streamlined password management, session isolation, privileged threat analytics, and continuous monitoring. Strategies recommended for enhancing PAM system usability encompass comprehensive training programs, user-centred design with continuous feedback, dedicated user support, and visibility into user activity through reporting features. Error handling, security, and auditing aspects emphasize timely support for user requests, the effectiveness of security awareness training, and self-service reporting for transparency around access. Other determinants of PAM usability success involve top-down management support, ongoing user awareness and education initiatives, system stability with fast response times, and incentivizing and recognizing the efforts of the PAM team.

B. Organization of Themes

By focusing qualitative analysis on these key themes, be able to gather rich insights that complement the researcher's quantitative findings and provide a well-rounded perspective on PAM system usability research and emerging the following global themes.

1. Organizational Awareness and Commitment: This theme emphasizes how important organizational commitment and leadership are to the uptake and success of PAM systems. Factors like management's cybersecurity knowledge, recognition of PAM's value, and willingness to invest in training and supporting the PAM team are key to overcoming resistance and promoting user

acceptance. Organizational Culture and Governance also underscore the significance of the broader organizational context in shaping PAM usability and user acceptance. The existing corporate culture, IT governance frameworks, and the ability to navigate user resistance to change can all be important to adopting and successfully implementing the PAM system.

2. User-Centric Design and Support: This theme focuses on ensuring that the PAM system design and implementation prioritize the needs and experiences of end-users. By creating an accessible and streamlined user experience, addressing security fears, and offering thorough training and support, organizations can foster greater user acceptance and adoption of the PAM system.

3. Technical Capabilities and Integration: This theme emphasizes the importance of the technical capabilities and performance of the PAM system itself. Factors like system reliability, seamless integration with other enterprise systems, and the availability of advanced security features can all contribute to user satisfaction and continued usage of the PAM solution.

4. Measurement, Feedback, and Continuous Improvement: This theme highlights the importance of ongoing monitoring, user engagement, and iterative improvement of the PAM system. By measuring the impact of PAM, actively asking user feedback, and providing users with visibility into their access activities, organizations can foster a sense of ownership and continuous enhancement of the PAM solution.

By organizing the key factors and themes into these four overarching areas, The researcher can build a comprehensive understanding of the critical elements that drive PAM system usability and user acceptance within the Commercial Bank of Ethiopia. This thematic analysis can then inform the researcher's research design, data collection, and the development of practical recommendations for improving PAM usability.

C. Global Themes

These two global themes, Organizational Alignment and Enablement and Continuous Improvement and Feedback highlight the critical importance of both the organizational and user-centric factors in driving successful PAM system usability and adoption.

4.3.2. Interpretation of the Findings

The overall findings emphasize the multifaceted nature of PAM system usability, encompassing The UTAUT theoretical framework, which proved to be a valuable model for understanding the key factors that influence PAM system usability, as the results demonstrate the relevance of the model's constructs (performance expectancy, effort expectancy, social influence, and facilitating conditions) in the PAM system context. In addition to UTAUT constructs, additional factors such as error handling, perceived security, and audit and reporting capabilities exist. The inclusion of these extended factors in the research model and the subsequent support for the related hypotheses suggest that a comprehensive understanding of PAM usability must consider both the user experience (as captured by the UTAUT constructs) and the system-specific features that address the unique requirements and concerns of privileged access management.

The importance of error handling highlights the need for PAM systems to provide reliable and user-friendly mechanisms for managing and recovering from errors, which can enhance user confidence and reduce the cognitive load associated with using the system. The emphasis on perceived security indicates that users' perception of the PAM system's ability to protect sensitive information and privileged access is a critical factor in driving user acceptance and intention to use the system. Addressing security concerns can foster trust and reduce user hesitation in adopting the PAM solution. The significance of audit and reporting features underscores the importance of

transparency, accountability, and compliance-related functionalities in PAM systems. Users are more likely to embrace the system if it provides the necessary tools for monitoring, auditing, and reporting on privileged access activities, which are crucial for regulatory and organizational requirements.

By triangulating the quantitative and qualitative findings, the research provides a comprehensive and robust understanding of the factors influencing PAM system usability and user acceptance. This combination of quantitative and qualitative data collection and analysis allowed for a robust and in-depth exploration of the research problem, providing both statistical evidence and contextual insights into the usability of the PAM system within the Commercial Bank of Ethiopia. To effectively triangulate the quantitative and qualitative findings from the privileged access management (PAM) system usability research. The researcher can consider the following:

4.3.3. Integration of Quantitative and Qualitative Findings

Convergence of Findings:

The quantitative findings indicate that factors such as performance expectancy, effort expectancy, social influence, facilitating conditions, error handling, perceived security, and audit and reporting capabilities significantly and positively impact users' intention to use the PAM system. The qualitative findings highlight the importance of continuous improvement and user feedback for maintaining the long-term effectiveness and user acceptance of the PAM system. These findings converge, suggesting that addressing the key factors identified in the quantitative analysis and establishing robust feedback mechanisms and iterative enhancements are crucial for driving PAM system adoption and usage.

Complementarity of Insights:

The quantitative data provides breadth and generalizability, identifying the factors influencing users' intention to use the PAM system. The qualitative data offers depth and context, emphasizing the need for continuous improvement and user feedback to ensure the PAM solution remains relevant and responsive to evolving user needs and security threats. When combined, the quantitative and qualitative results offer a more thorough knowledge of the elements influencing the PAM system's successful deployment and sustainability over the years.

Theoretical Triangulation:

This theoretical triangulation can strengthen the validity and reliability of the study's conclusions. The quantitative results can be validated using the Unified Theory of Acceptance and Use of Technology (UTAUT). Hypotheses H1–H4: The fundamental UTAUT constructs of Performance Expectancy, Effort Expectancy, Social Influence, and Facilitating Conditions constitute the foundation of these theories. The results demonstrate that these elements are relevant in affecting users' intention to utilize the PAM system and are consistent with the UTAUT theoretical framework. All of these assumptions were found to be supported. The qualitative findings can be understood in the perspective of the larger body of research on continuous improvement techniques and organizational user-centered design.

Implications for Practice:

To promote PAM system adoption and utilization, the combined findings advise enterprises to address the critical variables found in the quantitative analysis, such as performance expectancy, effort expectancy, and perceived security. Furthermore, as the qualitative findings make clear, creating feedback loops and ongoing improvement processes can help guarantee the PAM system's long-term viability and user acceptability

4.4. Discussion

The primary research questions guiding this study were, the following. What factors impact the usability of privileged access management systems at CBE? How can the usability of the PAM system be improved at CBE? The objective of the research is to examine the factors influencing the usability of privileged access management systems within the Commercial Bank of Ethiopia and explore strategies to enhance PAM usability.

The quantitative results show that users' intention to use the PAM system is considerably and favourable impacted by performance expectancy, effort expectancy, social influence, facilitating conditions, error management, perceived security, and audit and reporting capabilities. These findings are consistent with accepted theories and frameworks in the fields of user experience and technological acceptability, however additional support for the validity of the study may be necessary.

The qualitative findings complement the quantitative insights by emphasizing the importance of continuous improvement and user feedback loops. The data suggests that regularly measuring the impact of the PAM system, gathering user input, and incorporating it into iterative enhancements are crucial for ensuring the long-term effectiveness and user acceptance of the solution. This aligns with best practices in organizational change management and user-centred design. By triangulating the quantitative and qualitative data, the research provides a holistic perspective on the factors that drive PAM system adoption and usage. This integrated approach offers a deeper understanding of the interplay between technological, organizational, and user-centric elements, which is essential for developing effective strategies for implementing and sustaining privileged access management solutions usability.

Strategies for Improving PAM Usability:

The key strategies include streamlining access request and approval workflows, enhancing error handling and system feedback, delivering comprehensive training and user support, and integration with existing systems, effective PAM implementation requires seamless integration with other enterprise systems, such as identity management, IT service management, and business applications. The quality of these integrations can significantly impact the user experience and overall system usability. By simplifying access procedures, providing clear and informative error messages, offering robust training and support resources, and seamlessly integrating the PAM system with related business applications, the organization can significantly enhance the user experience and drive increased adoption.

Policy Briefings:

The following policy briefings are recommended to institutionalize a user-centric approach to PAM system design and usability:

User-Centric PAM System Design and Usability Policy: This policy mandates the adoption of user-centred design principles in the development and maintenance of the PAM system, establishes usability goals and KPIs and ensures that usability considerations are integrated throughout the system's lifecycle.

Continuous Usability Improvement and Feedback Policy: This policy implements a formal process for regularly gathering and analysis user feedback, allocating resources for usability testing and system improvements, and establishing feedback channels to address user concerns promptly.

PAM System Integration and Interoperability Policy: This policy mandates the integration of the PAM system with other enterprise applications and systems, defines technical and process standards for seamless data exchange and process integration, and aligns the PAM system's design

and implementation with the organization's overall information security and identity management strategies.

By implementing these strategies and policy briefings, CBE can significantly enhance the usability of its PAM system, addressing the key pain points identified through the mixed-methods research approach. This holistic approach to improving the user experience will drive increased user adoption, productivity, and satisfaction, ultimately contributing to the effective management and control of privileged access within Commercial Bank of Ethiopia. Overall, the findings highlight the need for a holistic approach to PAM system usability, considering both the user experience and the system-specific features that address the unique requirements and concerns of privileged access management.

CHAPTER V

Conclusion and Recommendations

5.1.Overview of the Study

This research study was conducted to investigate the key factors that impact the usability of the privileged access management (PAM) system at the Commercial Bank of Ethiopia. The study used a mixed-methods approach to obtain a thorough understanding of the usability challenges and user experience issues surrounding the PAM system deployment at CBE. It combined quantitative usability hypothesis testing with qualitative user interviews.

5.2 Discussion and Answering the Research Questions

The UTAUT has been widely adopted as a comprehensive theoretical framework for understanding and predicting the acceptance and use of various information technologies. Since its introduction in 2003, the UTAUT model has been extensively applied and validated across a diverse range of enterprise software systems, consumer technologies, and user contexts. Previous UTAUT-based studies have investigated the adoption and usage of systems such as enterprise resource planning (ERP) software, customer relationship management (CRM) tools, electronic health records, mobile banking applications, and a variety of other business and consumer technologies. These studies have consistently demonstrated the model's ability to explain a significant portion of the variance in users' behavioural intentions and actual usage behaviours. However, the current research represents one of the first efforts to empirically validate the UTAUT framework in the context of PAM systems. PAM solutions are a specialized category of enterprise software that are designed to secure, monitor, and control the access privileges of an organization's users, particularly those with elevated permissions and administrative rights.

The unique characteristics and security-critical nature of PAM systems differentiate them from the more general enterprise software applications that have been the focus of prior UTAUT-based studies. Factors such as the sensitive security and compliance requirements, the sensitive nature of privileged access, and the potential for significant business impact of misuse or breaches, may introduce additional usability considerations that are not necessarily captured by the core UTAUT constructs.

Quantitative Findings**:** The survey results provided empirical evidence supporting the applicability of the core UTAUT constructs and the extending of the UTAUT model to address the unique requirements of PAM systems in predicting user acceptance and usage of the PAM system at CBE. These findings indicate that users are more likely to accept and use the PAM system. By empirically investigating the applicability of UTAUT to the PAM domain, the current study contributes to the existing body of UTAUT research in several ways.

Extending The UTAUT Model's Generalizability: The results of this study show how adaptable the UTAUT framework is for understanding technological adoption and usability within the framework of a specialized, security-oriented enterprise system like PAM.

Identifying Context-Specific Usability Factors: The study goes beyond the high-level UTAUT constructs and uncovers additional usability dimensions that are particularly relevant to PAM systems, such as error handling, perceived security, and audit and reporting capabilities.

Providing practical insights for PAM system implementation: The qualitative analysis and proposed strategies for improving PAM usability offer valuable, user-centric insights that can guide organizations in the effective deployment and ongoing enhancement of their PAM solutions. By building upon the established UTAUT research and adapting the framework to the specific needs and challenges of PAM systems, the current study contributes to a more comprehensive

understanding of technology acceptance and usability in the PAM domain. This knowledge can inform both academic research and industry practice, supporting organizations in their efforts to enhance the user experience and drive the successful adoption of their PAM systems.

Qualitative Findings**:** The in-depth interviews provided additional contextual factors that can encouragement the usability of PAM system and address the second research question, which is how usability of PAM will be improved at CBE? a comprehensive set of strategies and policy briefings are proposed to improve the usability of the PAM system at CBE.

5.3.Recommendations for the Commercial Bank of Ethiopia

Based on the research findings, the following recommendations are proposed to enhance the usability of the PAM system at CBE.

Streamline access request and approval workflows**: -** By simplifying the processes for requesting and approving privileged access, users can navigate the system with ease. This involves creating user-friendly interfaces, reducing unnecessary steps, and providing clear guidelines on requesting and approving access. By doing so, CBE lowers the cognitive load on users and enhance task efficiency, leading to a smoother experience overall.

Enhance error handling and system feedback: -Implementing clear and informative error messages and system status updates is crucial in guiding users during task completion. These messages should not only notify users of errors but also offer guidance on how to resolve them. Providing real-time feedback on the status of tasks helps users stay informed and confident in their actions, ultimately improving their overall experience with the system.

Provide comprehensive training and user support: - Developing robust training materials, user guides, and support resources is essential for empowering users to effectively navigate the PAM

system. Tailoring resources to provide to both novice and experienced users ensures that everyone can make the most of the system. Offering on-demand support further boosts user confidence and encourages efficient system usage.

Integrate the PAM system with other enterprise systems: - Exploring integration opportunities with related business applications can significantly enhance user workflows. By connecting the PAM system with enterprise resource planning (ERP) or IT service desk systems, users can enjoy seamless data flows and reduced duplication of efforts. This integration minimizes manual data entry and streamlines processes, ultimately improving overall productivity.

Establish a continuous usability improvement process: - Implementing regular usability testing and user feedback loops is key to identifying and addressing emerging usability concerns. By actively seeking feedback from users and conducting usability tests, CBE can proactively address issues and make iterative improvements to the system over time. This ongoing commitment to enhancing usability ensures that the PAM system remains user-centric and continues to meet user needs effectively.

By implementing the recommended improvements, the Commercial Bank of Ethiopia can enhance the overall usability of the PAM system, improve user productivity and satisfaction, and ensure the effective management and control of privileged access across the organization ultimately strengthening their cybersecurity posture and operational efficiency.

5.4. Research Contributions

The study makes several important contributions to the field of privileged access management and user experience research. The research investigates empirically validating the critical factors that impact the usability of privileged access management systems, offering a deep dive into the challenges and opportunities that shape user experiences. By showcasing the benefits of utilizing

a mixed-methods research approach, the study demonstrates how combining quantitative performance measures with qualitative user insights can drive informed decision-making for system enhancements. Furthermore, it provides valuable guidance for organizations, such as CBE, on effectively prioritizing and addressing usability concerns to boost user adoption rates and enhance satisfaction with PAM systems. Emphasizing the significance of incorporating user-centered design principles throughout the development and ongoing maintenance of enterprise security and access control solutions underscores the commitment to creating intuitive and user-friendly systems that align closely with users' needs and preferences.

5.5. Conclusion

In conclusion, all of the proposed hypotheses (H1–H7) in this study were supported, indicating that users' intention to use the privileged access management system is substantially influenced by factors such as performance expectancy, effort expectancy, social influence, facilitating conditions, error handling, perceived security, and audit and reporting capabilities. The core UTAUT constructs (H1-H4) were validated as significant factors in the context of PAM system usability, aligning with the established UTAUT framework. The additional factors of error handling (H5), perceived security (H6), and audit and reporting capabilities (H7) were identified as key determinants of PAM system usability, expanding on the UTAUT model to cater to the specific needs of PAM systems.

The insights gained from this research can assist organizations in creating and implementing PAM systems that better meet user expectations and requirements, thereby enhancing overall system usability and promoting user adoption. This study contributes to the growing body of knowledge on PAM system usability and sets the stage for future investigations into the variables affecting user acceptance and utilization of these crucial security solutions.

In summary, the study's findings offer valuable insights into the intricate aspects of PAM system usability, with practical implications for both researchers and practitioners in the field of privileged access management systems.

Based on studies conducted at the Commercial Bank of Ethiopia, it is recommended that future research focus on analysing system utilization to gain a comprehensive understanding of the privileged access management system's usability. Further exploration of different methodologies by organizations across various industries, such as telecommunications and private banking sectors, could lead to successful implementations and enhance overall information security in any company.

5.6. Limitation Of the Study

Although the privileged access management systems study provides insightful information, it's vital to recognize the following limitations. The specific setting or sample employed in the study, such as concentrating on a particular banking sector or organization, might have restricted the findings' generalizability. The breadth and depth of the research findings may also be greatly impacted by resource limitations, such as financial limitations, schedule restrictions, and restricted access to particular tools or technologies, like the Smart PLS tool, because of a lack of license.

References

Adam, A. M. (2020). Sample Size Determination in Survey Research. *Journal of Scientific Research and Reports*, 90–97. https://doi.org/10.9734/jsrr/2020/v26i530263

Adhikari, G. P. (2021). Scholars' Journal Calculating the Sample Size in Quantitative Studies. *Scholars' Journal*, *4*. https://www.nepjol.info/index.php/scholars

Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. *Future Internet*, *11*(3), 73.

Alruwies, M. H., Mishra, S., Abdul, M., & Alshehri, R. (2022). *Identity Governance Framework for Privileged Users*. *September 2021*. https://doi.org/10.32604/csse.2022.019355

Alruwies, M. H., Mishra, S., & AlShehri, M. A. R. (2022). Identity Governance Framework for Privileged Users. *Comput. Syst. Sci. Eng.*, *40*(3), 995–1005.

Ankele, R., Nahrgang, K., Stojanovic, B., & Badii, A. (2020). SoK: Cyber-Attack Taxonomy of Distributed Ledger-and Legacy Systems-based Financial Infrastructures. *Cryptology EPrint Archive*.

Anwar, W. (2022). *Privilege Access Analysis Security Tool for Windows & Linux*. *August 2021*. https://doi.org/10.13140/RG.2.2.33411.17448

Barbour, R. S. (2022). *Theoretical sampling*. SAGE Publications Ltd.

Baxter, R. S., & Martinez, C. S. (2020). *NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA THESIS ENHANCING IDENTITY AND ACCESS MANAGEMENT IN THE U.S. NAVY VIA MIGRATION TO MORE MODERN STANDARDS OF AUTHENTICATION*.

Bhuvaneswari, S., Keshav, N., & Hariharan, S. (2022). Multi-Image Cryptographic Based Two-Factor Authentication in Banking Systems and Services. *ECS Transactions*, *107*(1), 6075.

Cobia, A. (n.d.). *Privileged Access Management*. https://digitalcommons.lasalle.edu/ecf_capstones/34

Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: literature review and theory-based research agenda. *TQM Journal*, *33*(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202/FULL/PDF

Dhoot, A., Nazarov, A. N., & Koupaei, A. N. A. (2020). A security risk model for online banking system. *2020 Systems of Signals Generating and Processing in the Field of on Board Communications*, 1–4.

Dou, X., Yuan, Y., Cao, W., & Ouyang, P. (2020). *A Privilege Manage m ent Method of Centralized Manage m ent Syste m in the Co m puter Roo m*. 957–961.

Egwuche, O. S., Ganiyu, M., & Akeem, A. A. (2022). Assessing the Vulnerabilities of Internet Users to Cyber-Attacks using their Password Login Patterns. *2022 IEEE Nigeria 4th International Conference on Disruptive Technologies for Sustainable Development (NIGERCON)*, 1–4.

Ezza, H. A., Shokhnekh, A. V, Telyatnikova, V. S., & Mushketova, N. S. (2020). Quality parameters of information systems for business in the context of digital transformations. *E3S Web of Conferences*, *208*, 03059.

Fadillah, B. N., Khairani, D., & Rozy, N. F. (2020). MOBILE BANKING SYSTEM DEVELOPMENT USING NEAR FIELD COMMUNICATION TECHNOLOGY WITH ANDROID-BASED OPERATING SYSTEM (CASE STUDY: PT. BANK PANIN SYARIAH TBK). *Jurnal Teknik Informatika Vol*, *13*(1), 43.

Feth, D., & Polst, S. (2019). Heuristics and models for evaluating the usability of security measures. In *Proceedings of Mensch und Computer 2019* (pp. 275–285).

Gazzarata, G., Blobel, B., & Giacomini, M. (2017). *A Flexible Solu on for Privilege Management and Access Control in EHR Systems* (Vol. 13, Issue 1).

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2022). Detecting insider threat via a cyber-security culture framework. *Journal of Computer Information Systems*, *62*(4), 706–716.

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): analysis, trends, and usage in critical infrastructures. *Sensors*, *21*(14), 4759.

Grobler, M., Gaire, R., & Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, *4*. https://doi.org/10.3389/fdata.2021.583723

Haber, M. J., & Haber, M. J. (2020a). Privileged Access Management. *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations*, 151–171.

Haber, M. J., & Haber, M. J. (2020b). Privileged Account Management Implementation. *Privileged Attack Vectors: Building Effective Cyber-Defense Strategies to Protect Organizations*, 335–359.

Heale, R., & Noble, H. (2019). Integration of a theoretical framework into your research study. In *Evidence-Based Nursing* (Vol. 22, Issue 2, pp. 36–37). BMJ Publishing Group. https://doi.org/10.1136/ebnurs-2019-103077

Huh, J. H., Bobba, R. B., Markham, T., Nicol, D. M., Hull, J., Chernoguzov, A., Khurana, H., Staggs, K., & Huang, J. (2016). Next-generation access control for distributed control systems. *IEEE Internet Computing*, *20*(5), 28–37.

Jere. (2017). *Evaluating and designing network and information security solution for company in accordance to PCI DSS*.

Khajouei, R., & Farahani, F. (2020). A combination of two methods for evaluating the usability of a hospital information system. *BMC Medical Informatics and Decision Making*, *20*(1). https://doi.org/10.1186/s12911-020-1083-6

Lessa, L., & Etoribussi, A. G. (2023). *Usability of Security Mechanisms of E-Health Applications* (pp. 37–56). https://doi.org/10.4018/978-1-6684-6581-3.ch002

MAKING SENSE OF THEORETICAL FRAMEWORKS (1). (n.d.).

Mazhar, S. A. (2021). Methods of Data Collection: A Fundamental Tool of Research. *Journal of Integrated Community Health*, *10*(01), 6–10. https://doi.org/10.24321/2319.9113.202101

Memole-doodson, J. (2018a). *Privileged Account Management for the Financial Services Sector*. *September*, 2013.

Memole-doodson, J. (2018b). *Privileged Account Management for the Financial Services Sector*. *September*, 2013.

Mikhaylov, A. M., & Petrov, N. A. (2021). Features of Digital Transformation of Modern Banking Transactions. *Current Achievements, Challenges and Digital Chances of Knowledge Based Economy*, 673–681.

Mohamed, K. S. (2023). An Introduction to Deep Learning. In *Deep Learning-Powered Technologies: Autonomous Driving, Artificial Intelligence of Things (AIoT), Augmented Reality, 5G Communications and Beyond* (pp. 1–57). Springer.

Mohammed, I. A. (n.d.). *SYSTEMATIC REVIEW OF IDENTITY ACCESS MANAGEMENT IN INFORMATION SECURITY*.

Moustafa, A. A., Bello, A., & Maurushat, A. (2021). The Role of User Behaviour in Improving Cyber Security Management. *Frontiers in Psychology*, *12*, 561011. https://doi.org/10.3389/FPSYG.2021.561011/BIBTEX

Mr. Siddhesh Bhargude. (2023). Privileged Access Management: Ensuring Security and Accountability. *International Journal of Advanced Research in Science, Communication and Technology*, 647–651. https://doi.org/10.48175/ijarsct-12098

Omotunde, H., & Ahmed, M. (2023). A Comprehensive Review of Security Measures in Database Systems: Assessing Authentication, Access Control, and Beyond. *Mesopotamian Journal of CyberSecurity*, *2023*, 115–133.

Parveen, S., Ahmad, S., & Khan, M. A. (2021). Integration of Identity Governance and Management Framework within Universities for Privileged Users. *International Journal of Advanced Computer Science and Applications*, *12*(6), 555–562. https://doi.org/10.14569/IJACSA.2021.0120664

Pöhn, D., Seeber, S., Hanauer, T., Ziegler, J. A., & Schmitz, D. (2021). Towards Improving Identity and Access Management with the IdMSecMan Process Framework. *Proceedings of the 16th International Conference on Availability, Reliability and Security*, 1–10.

Purba, A., & Soetomo, M. (n.d.-a). Assessing Privileged Access Management (PAM) using ISO 27001:2013 Control. In *Management and Information Technology*. ACMIT.

Purba, A., & Soetomo, M. (n.d.-b). Assessing Privileged Access Management (PAM) using ISO 27001:2013 Control. In *Management and Information Technology*. ACMIT.

Rahalkar, S., & Rahalkar, S. (2019). Introduction to nmap. *Quick Start Guide to Penetration Testing: With NMAP, OpenVAS and Metasploit*, 1–45.

Rangraz Jeddi, F., Nabovati, E., Bigham, R., & Khajouei, R. (2020). Usability evaluation of a comprehensive national health information system: relationship of quality components to users' characteristics. *International Journal of Medical Informatics*, *133*. https://doi.org/10.1016/j.ijmedinf.2019.104026

Razikin, K., & Widodo, A. (2021). General Cybersecurity Maturity Assessment Model: Best Practice to Achieve Payment Card Industry-Data Security Standard (PCI-DSS) Compliance. *CommIT (Communication and Information Technology) Journal*, *15*(2), 91–104.

Roles of expectancy on employee engagement and Job performance. (2019). *Journal of Administrative and Business Studies*, *5*(2). https://doi.org/10.20474/jabs-5.2.3

Saeed, H. S., Abdul-Jabbar, S. S., Mohammed, S. G., Abed, E. A., & Ibrahem, H. S. (2020). Access Control Security Review: Concepts and Models. *Solid State Technology*, *63*(6), 6609–6629.

Sasipriya, S., Kumar, L. R. M., Krishnan, R. R., & Kumar, K. N. (2021). Intrusion Detection System in Web Applications (IDSWA). *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 311–314.

Sharma, L. R., Jha, S., Koirala, R., Aryal, U., & Bhattarai, T. (2023). Navigating the Research Landscape: A Guide to the Selection of the Right Research Design. *International Research Journal of MMC*, *4*(1), 64–78. https://doi.org/10.3126/irjmmc.v4i1.51863

Shekhar, P., Prince, M., Finelli, C., Demonbrun, M., & Waters, C. (2019). Integrating quantitative and qualitative research methods to examine student resistance to active learning. *European Journal of Engineering Education*, *44*(1–2), 6–18.

Sindiren, E., & Ciylan, B. (2018). Privileged Account Management Approach for Preventing Insider Attacks. In *IJCSNS International Journal of Computer Science and Network Security* (Vol. 18, Issue 1). https://www.researchgate.net/publication/341464060

Sindiren, E., & Ciylan, B. (2019a). Application model for privileged account access control system in enterprise networks. *Computers and Security*, *83*, 52–67. https://doi.org/10.1016/j.cose.2019.01.008

Sindiren, E., & Ciylan, B. (2019b). Application model for privileged account access control system in enterprise networks. *Computers and Security*, *83*, 52–67. https://doi.org/10.1016/j.cose.2019.01.008

Singh, C., Thakkar, R., & Warraich, J. (2023). IAM Identity Access Management—Importance in Maintaining Security Systems within Organizations. *European Journal of Engineering and Technology Research*, *8*(4), 30–38. https://doi.org/10.24018/ejeng.2023.8.4.3074

Steingartner, W., Galinec, D., & Kozina, A. (2021). Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry*, *13*(4), 597.

Teka, D., Dittrich, Y., & Kifle, M. (2016). Usability challenges in an ethiopian software development organization. *Proceedings - 9th International Workshop on Cooperative and Human Aspects of Software Engineering, CHASE 2016*, 114–120. https://doi.org/10.1145/2897586.2897604

Thombre, S. (2020). Freeware solution for preventing data leakage by insider for windows framework. *2020 International Conference on Computational Performance Evaluation (ComPE)*, 44–47.

Tirtadjaja, W., Rana, M. E., & Shanmugam, K. (2021). Managing High Privileged Accounts in IT Enterprise: Enhanced Security Infrastructure. *2021 International Conference on Data Analytics for Business and Industry (ICDABI)*, 655–660.

Tuononen, H. (2023). *Privileged access management model for a managed service provider*.

Walker, P. (2019). Why do PAM projects fail? *Network Security*, *2019*(9), 15–18.

Waltermire, K., Conroy, T., Harriston, M., Irrechukwu, C., Krishnan, N., Memole-Doodson, J., Nkrumah, B., Perper, H., Prince, S., & Wynne, D. (2018). *Privileged Account Management for the Financial Services Sector Volume B: Approach, Architecture, and Security Characteristics*. https://www.nccoe.nist.gov/.

Wang, D., Li, Z., & Xiao, B. (2019). Social influence in first-time and upgrade adoption. *Electronic Commerce Research and Applications*, *34*. https://doi.org/10.1016/j.elerap.2019.100834

Wang, Y., & Rawal, B. (2017). Usability meets security: a database case study. *Journal of Advanced Computer Science & Technology*, *6*(2), 33–39. https://doi.org/10.14419/jacst.v6i2.8425

Web Source

CyberArk PAS Configuration Notes (Architecture) - NETSEC (51sec.org)

Appendices

Appendix I. Survey Questionnaire

Performance Expectancy	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
Using the PAM system increases my productivity.					
The PAM system helps me accomplish critical tasks efficiently.					
I believe that the PAM system enhances my job performance.					
The PAM system improves my ability to manage privileged access effectively.					
Effort Expectancy:	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
Interacting with the PAM system is easy.					
Learning how to use the PAM system was simple for me.					
It is easy for me to navigate through the PAM system features.					
Using the PAM system requires minimal effort on my part.					
Social Influence:	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
My colleagues encourage me to use the PAM system.					
Managers in my organization emphasize the importance of using the PAM system.					

I feel supported by my peers in adopting the PAM system.					
The organizational culture promotes the use of the PAM system.					
Facilitating Condition:	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
I can access the necessary resources to use the PAM system effectively.					
The technical support for the PAM system is readily available when needed.					
The organization provides adequate training on how to use the PAM system.					
I have the tool and equipment to fully use the PAM system.					
Errors Handling:	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
I have the opportunity to improve my skills when using the PAM system.					
Error messages displayed by the PAM system are clear and easy to understand.					
The PAM system effectively handles user input errors.					
The PAM system effectively handles errors and provides appropriate recovery mechanisms					
Perceived Security:	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**

The PAM system provides robust password management features.					
I feel confident in the security measures implemented by the PAM system.					
The PAM system effectively controls access to sensitive information.					
I believe that the PAM system enhances the overall security posture of our organization.					
Audit and Reporting Capabilities:	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
The PAM system provides detailed audit logs of privileged access activities.					
The system can easily generate reports on privileged access usage.					
The audit and reporting features of the PAM system help in information system policy compliance adherence.					
I believe the audit and reporting capabilities of the PAM system to be valuable for security monitoring.					
Behavioral Intention to Use	**Strongly Disagree**	**Disagree**	**Neutral**	**Agree**	**Strongly Agree**
I am likely to rely on a PAM system for controlling access privileges.					

I plan to use a PAM system regularly to manage access privileges.					
I intend to continue using the PAM software in the future.					

Appendix II. Interview Question

Privileged Access Management System Usability Interview Question

These interview questions are intended to prompt participants to share their experiences, perceptions, challenges, and suggestions related to the usability of PAM. The questionnaire is adopted from the UTAUT model and tailored to the PAM system.

1) Interviewer Name …….
2) Interviewed Name……
3) Interview date and time ……...
4) Selected information system ……...
5) Organization: ……...
6) Gender: …….
7) Qualification of Education……
8) Position: ……...
9) Experience……...

Topic:	Privileged Access Management (PAM) System Usability
Purpose:	To find out how experts and IS security managers feel about the usability of the PAM system at CBE. The questions aim to encourage the interviewees to share their experiences, best practices, and recommendations to provide practical and actionable insights. The goal of these questions is to encourage the PAM experts to share their domain-specific insights and perspectives, which can then be used to identify potential extensions or adaptations to the core UTAUT model for the context of PAM usability research.

Check List

1.	Could you, please provide an overview of your experience and expertise in privilege access management systems (PAM)?
2.	What do you perceive as the key factors that influence user acceptance and adoption of PAM systems within CBE?
3.	In your experience, what are the unique challenges or pain points that users face when interacting with and utilizing of PAM solutions? How do these factors impact the overall success and effectiveness of the PAM system?
4.	Could you describe any organizational or contextual factors that you believe play a significant role in shaping PAM usability and user acceptance? For example, aspects related to corporate culture, IT governance policies, or the degree of user technical expertise.
5.	What specific features, functionalities, or design elements of PAM systems do you find most critical in driving user satisfaction and continued usage?
6.	Could you please share any effective strategies or best practices that you have used to improve the usability of PAM systems and encourage efficient privileged access management practices?
7.	rom your perspective, how important are factors like Error Handling, security concerns, and Audit and reporting capability in influencing user attitudes and behaviours towards PAM systems?
8	Based on your expertise, what advice would you give to CBE looking to improve their PAM usability practices and systems? Are there any additional factors that you consider crucial for the success of PAM usability, which you think could further enhance the usability of this enterprise access management area?

Appendix III. Letter of Support to Gather Data from CBE

Date: May 13,2024
Ref No. ST/SIS/087/2024/16

To: Commercial Bank of Ethiopia
Addis Ababa

Subject:- Student Fikru Afework Elyas

Dear Sir /Madam,

Student Fikru Afework Elyas (ID.No GSE/4378/14) is a graduate student at the School of Information Science, Addis Ababa University. He is currently conducting M.Sc. Thesis research under the title "Privileged Access Management (PAM) Usability."

I would like to thank you in advance for all the assistance that you would provide to the student.

With Regards

Dereje Teferi (PhD)
Head, School of Information Science

SCHOOL OF INFORMATION SCIENCE
ADDIS ABABA UNIVERSITY

Please write cooperation memo to Manager, Access Control Unit
14/05/24

Tel. +251-1-122-91-91 P.O.Box. 1176 Fax. +251-1-1239729

Appendix IV. Letter of Permission to Gather Data from CBE Staff.

የኢትዮጵያ ንግድ ባንክ
COMMERCIAL BANK OF ETHIOPIA
INTER DEPARTMENTAL MEMORANDUM

DATE ቀን	:	**May 14, 2024**
TO ለ	:	**Manager: Identity Access Management**
FROM ከ	:	**Team Leader: Training Operation and Logistics**
SUBJECT ጉዳዩ	:	**Request for Cooperation to Conduct Research**

Addis Ababa University College of Natural and Computational Sciences school of information science under its letter reference ST/SIS/087/2024/16 dated 13/05/2024 has requested our bank to assist **Fikru Afework (post graduate student)** to undertake his research paper under the title "**Privileged Access Management (PAM) usability .**

This is, therefore, to kindly request you to provide him the required assistance and cooperation without compromising confidentiality.

Best Regards,

Abera Tadesse