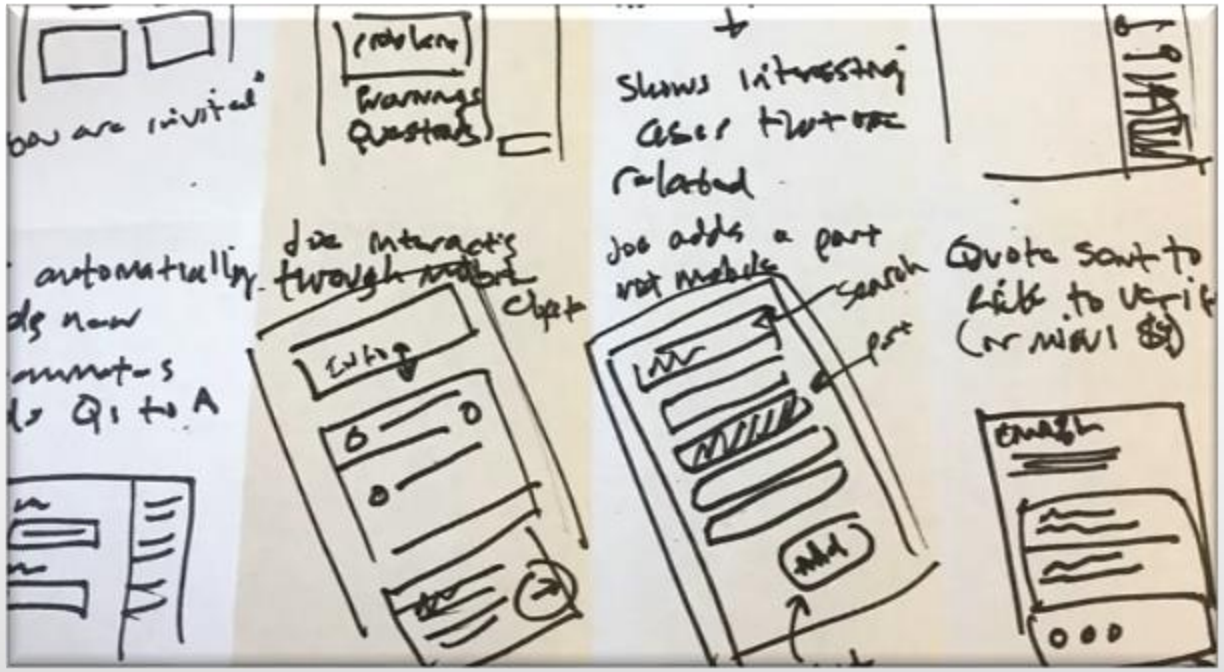


SILENT-NETWORK AUTHENTICATION FOR BILL PAYMENTS

CASE STUDY

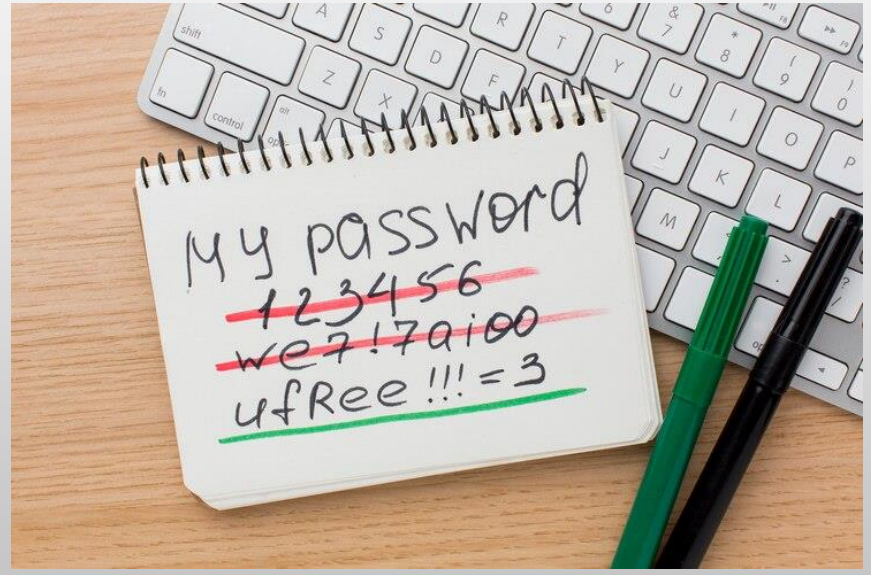
SAMEENA KHAN – SR. UX RESEARCH MANAGER

PROJECT OVERVIEW

Objective: Create a seamless, secure, and frictionless way for users to authenticate and make bill payments.

Expected user outcomes: Seamless Experience. Robust Security. Improved User Satisfaction.

Business goals: Improve user retention and satisfaction. Enhance timely bill payments.



RESEARCH GOALS

- **Identify key pain points** in the current authentication process.
- **Test user perceptions** of trust, privacy, and usability in silent network authentication.
- **Measure the impact** on user retention and completion rates for bill payments.

OVERARCHING RESEARCH QUESTIONS

1. **What are the key user pain points in current bill payment authentication, and what systemic or design flaws drive these challenges?**
   (Focus: pain points, root causes, user experience gaps)
2. **How do user perceptions of trust, privacy, and usability differ between silent network authentication and traditional methods, and what factors shape these perceptions?**
   (Focus: comparative evaluation, trust dynamics, behavioral drivers)
3. **What is the measurable impact of silent network authentication on user retention and payment completion rates, and what mechanisms explain this impact?**
   (Focus: behavioral outcomes, friction reduction, business metrics)

RESEARCH METHODOLOGY

- **Secondary Research**
  -  **Industry Trends**
  -  **Competitive Analysis**
  -  **Internal Data**
    -  Call Support Logs
    -  User Feedback

Primary Research

Qualitative & Quantitative Methods

- User Interviews
- Diary Studies
- Concept Testing
- Usability & A/B Tests

CONCEPT PROTOTYPE : SILENT AUTHENTICATION

KEY FINDINGS IN USER AUTHENTICATION

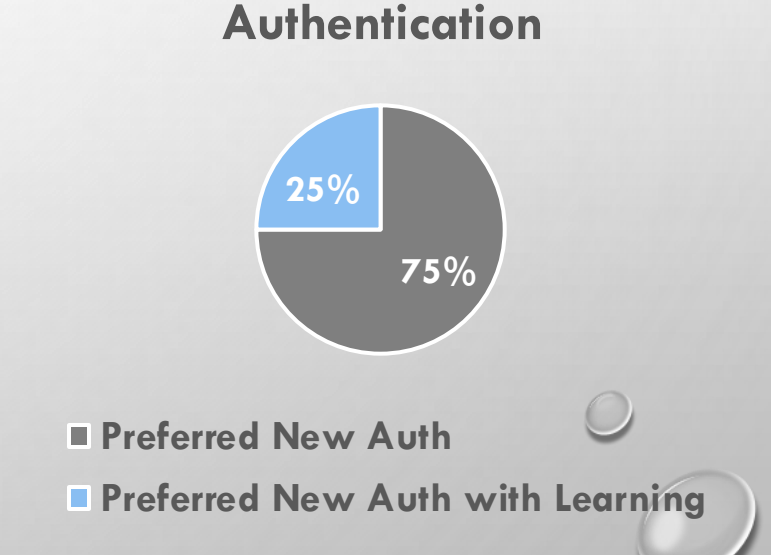
- **Password fatigue** and frequent **authentication failures** causing high user drop-off rates (87%)
- **Privacy concerns** surrounding passive data collection (36%)
- Need for a **scalable solution** for bill payment authentication (93%)

KEY INSIGHTS

Perceive (Streamlined Authentication): Users favored methods that balanced security with convenience, seeking a frictionless experience.

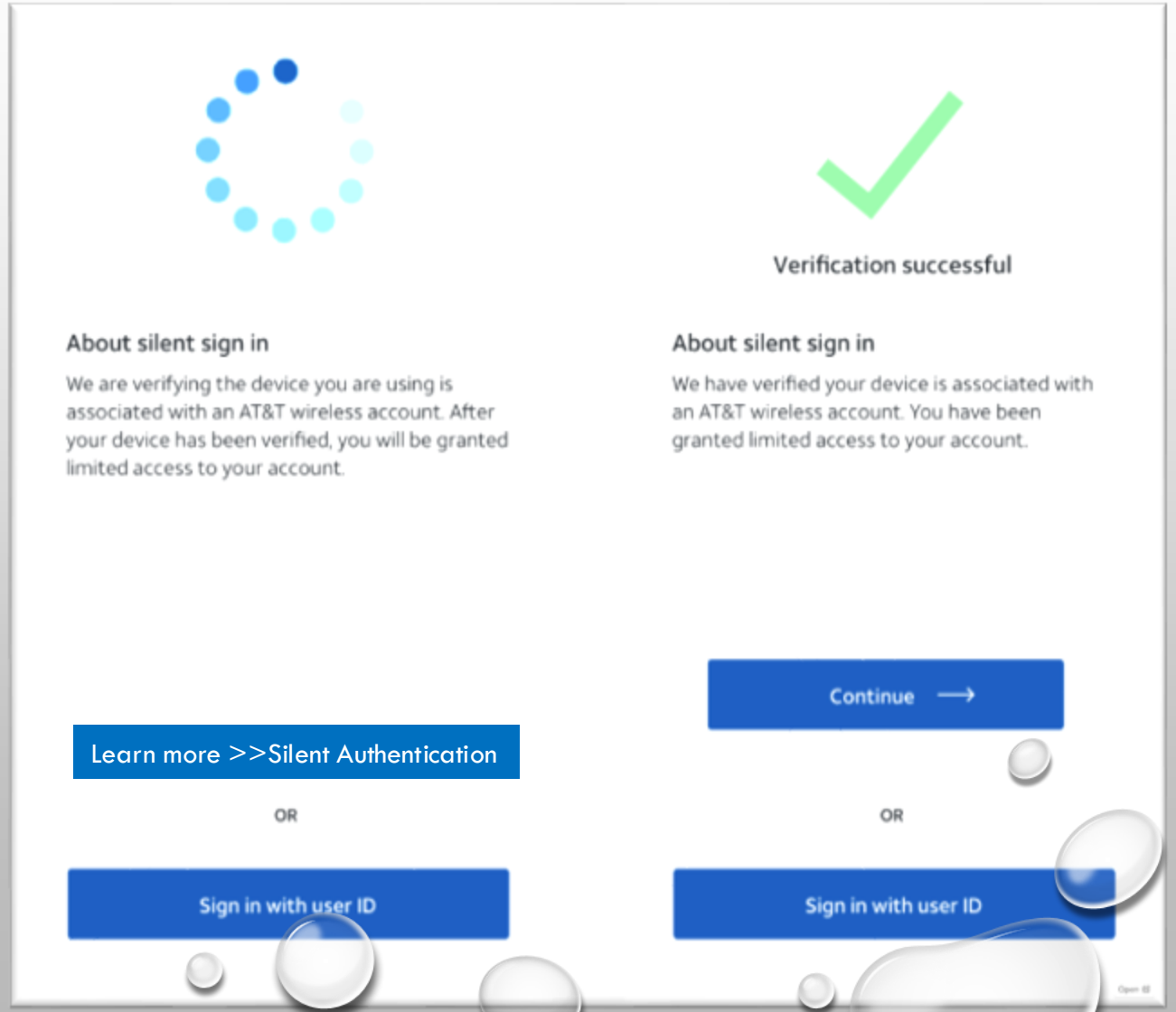
Feel (Security Perception): Users perceived passive identification with OTC as secure and unobtrusive.

Want (Enhanced Security): Users desired stronger silent security plus an additional authentication layer for bill payments.

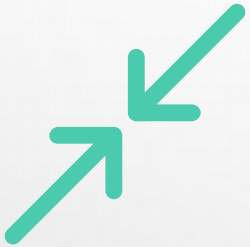


RECOMMENDED ENHANCEMENTS

- **Passive identification:** Display network and device sign-in to reassure users that authentication is happening seamlessly.
- **OTC:** implement one-time code for additional verification.
- **User education:** inform users about the benefits and security of the new authentication process.



USER & BUSINESS IMPACTS



Reduced Friction
Lowered user drop-off rates during payments.

Enhanced Security
Increased user confidence through dual-layer authentication.

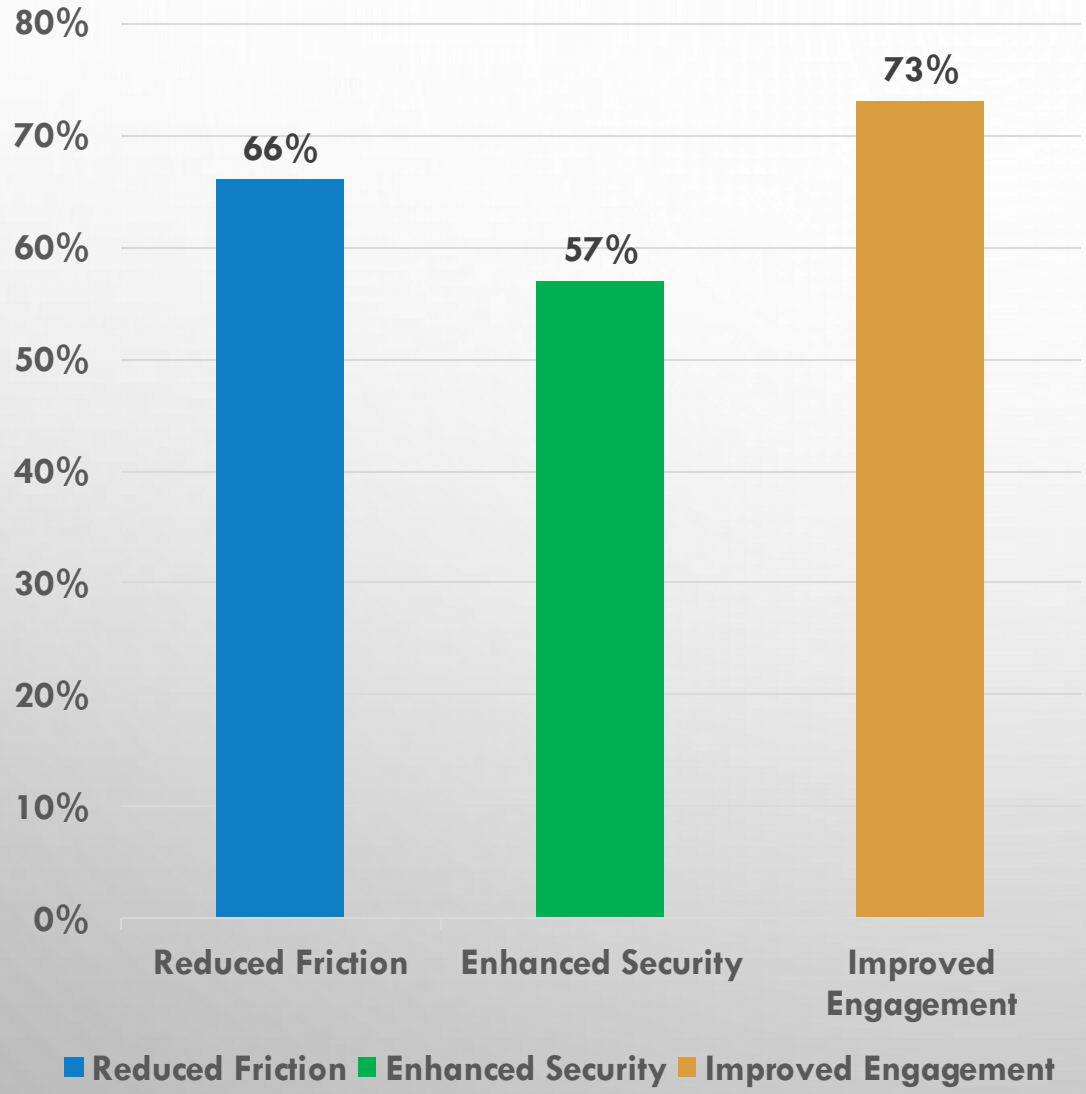
Improved Engagement
Boosted user satisfaction and retention rates.

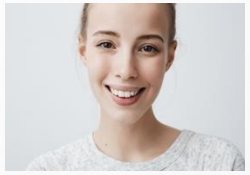
"Secure yet seamless..."

"Where else can we use this..."

"Love it, but only after I understand it is secure..."

USER & BUSINESS IMPACTS





"Silent authentication should become mainstream for transactions that are safe but still require security."

"I can pay my bill without any hassle—this is a game-changer!"

LONG-TERM STRATEGIC VISION

Future CX

Passive, continuous authentication with risks-based AI/ML intervention

Password-less device & network auth → Physical biometrics → Behavioral biometrics

Risk-based auth
Data Intelligence
Behavioral Biometrics

Physical Biometrics

Current CX

Authentication using passwords, secret answers

- Eliminate passwords that cause customer friction
- Fast follow silent-network authentication with physical & behavioral biometrics

APPENDIX

RESEARCH BRIEF FOR USER INTERVIEWS

Objective: the objective of the user interviews is to gather qualitative insights into participants' authentication preferences, security concerns, and transactional behaviors, particularly in the context of secure transactions such as bill payments. The interviews aim to explore the challenges associated with traditional login credentials and users' openness to alternative authentication mechanisms, including silent network authentication.

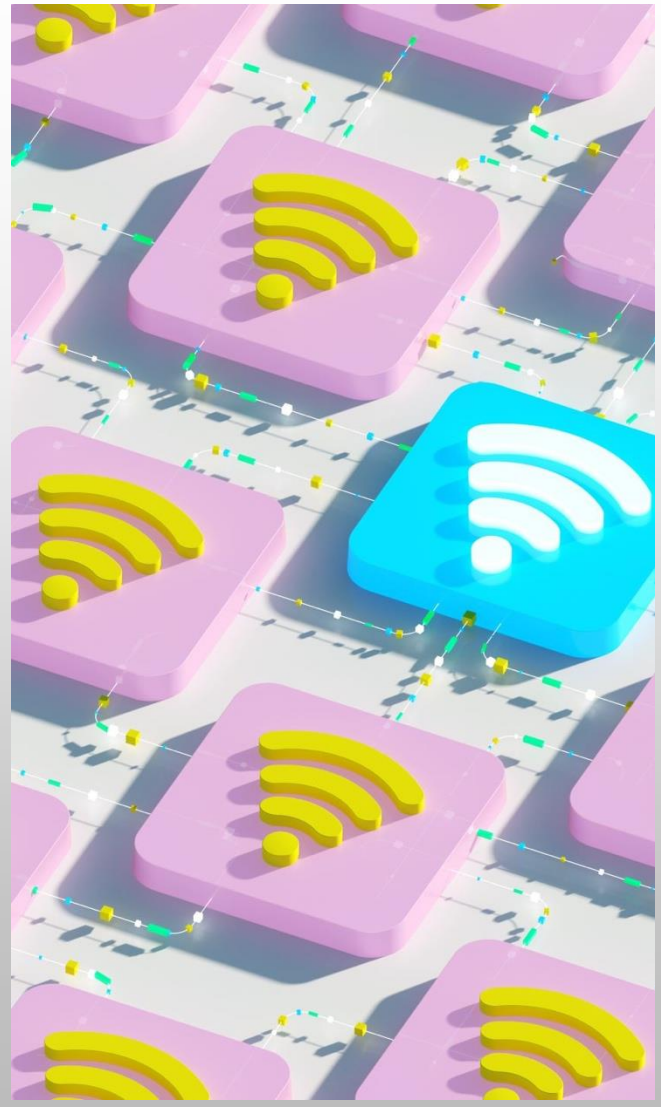
Participant profile:

- Age: 18-65 years
- Demographics: diverse backgrounds (gender, ethnicity, occupation)
- Technology proficiency: varied levels (from novice to expert)
- Usage patterns: regular users of online payment platforms for bill payments

PASSIVE AUTHENTICATION COMPONENTS

KEY ELEMENTS

- **Network identification:** Uses network signals (example: wi-fi) to identify and authenticate the user in the background.
- **Device identification:** Leverages device fingerprints (example: device id) to confirm the user's identity without active input.



RESEARCH PROCESS

INTERVIEW STRUCTURE

1. **Introduction (5 minutes):**
   - Introduce the interviewer and establish rapport with the participant.
   - Provide an overview of the interview objectives and the importance of their participation.
2. **Authentication preferences (15 minutes):**
   - Explore participants' current authentication methods for online transactions, including bill payments.
   - Inquire about their experiences with traditional login credentials (username/password) and any associated challenges or frustrations.
   - Probe participants' attitudes towards alternative authentication mechanisms, such as silent network authentication and OTP factor authentication.
3. **Security concerns (10 minutes):**
   - Discuss participants' perceptions of security in online transactions, specifically in the context of bill payments.
   - Investigate any security-related incidents or concerns they have encountered in the past.
   - Gauge participants' willingness to adopt additional security measures, such as MFA, to enhance the security of their transactions.
4. **Transactional behaviors (15 minutes):**
   - Explore participants' typical transactional habits when paying bills online.
   - Inquire about the devices and networks they use for online transactions and any contextual factors that influence their authentication preferences.
   - Discuss the importance of security and convenience in their transactional experiences.
5. **Closing and thank you (5 minutes):**
   - Summarize key points discussed during the interview.
   - Thank the participant for their time and valuable insights.
   - Provide contact information for any follow-up questions or clarifications.

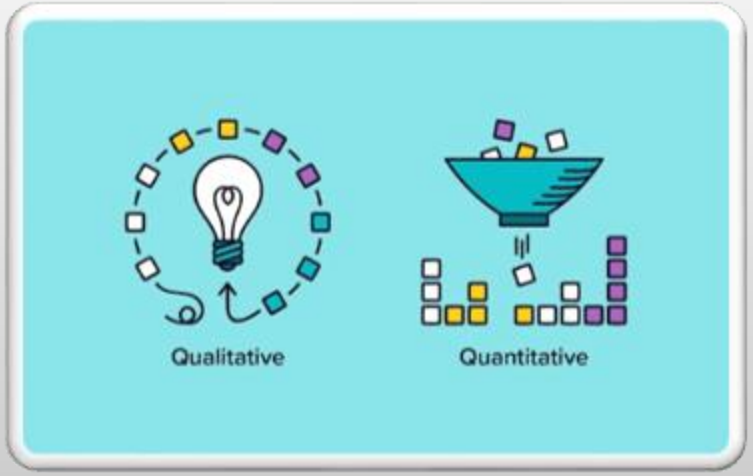
DATA ANALYSIS & SYNTHESIS

1. **Data cleaning & preparation:** ensure data quality and integrity through cleaning and transformation.
2. **Exploratory data analysis (EDA):** identify initial patterns, trends, and outliers visually and statistically.
3. **Hypothesis testing & modeling:** formulate hypotheses and develop models to test relationships and make predictions.
4. **Interpretation & synthesis:** interpret findings, draw conclusions, and generate insights for informed decision-making.

DATA ANALYSIS

1. **Qualitative data analysis**
   - **Transcribed and coded qualitative data** from user interviews, contextual inquiries, and prototype testing sessions.
   - Identified recurring **themes, patterns, and insights** related to user authentication preferences, security concerns, and transactional behaviors.
   - **Conducted thematic analysis to derive meaningful interpretations** and insights from the qualitative data.

2. **Quantitative data analysis**
   - **Collated and analyzed survey responses** to gather quantitative insights into user preferences, satisfaction levels, and security perceptions regarding authentication methods.
   - Generated summary statistics and visualizations to present key findings and facilitate data-driven decision-making.



DATA SYNTHESIS

1. **Synthesis of findings:**
   - Integrated qualitative and quantitative findings to develop a comprehensive understanding of user perspectives, security requirements, and usability considerations.
   - Identified commonalities and discrepancies across different data sources to triangulate findings and enhance the reliability of conclusions.
   - Synthesized key insights into actionable recommendations for optimizing authentication processes, enhancing security measures, and improving user experience in secure transactions.

2. **Iterative refinement:**
   - Engaged in iterative refinement of the analysis process, revisiting data sources and refining interpretations based on emerging insights and feedback.
   - Incorporated stakeholder input and expert perspectives to validate findings and ensure alignment with organizational goals and priorities.
   - Documented the analysis process and rationale behind key findings to maintain transparency and facilitate future research and decision-making processes.