

**Assessing Financial Technology Readiness in Indian Banking: Workforce Adaptability,
Organisational Transformation, and Strategic Implementation**

***A REPORT SUBMITTED
TO
INDIAN INSTITUTE OF BANKING AND FINANCE
MUMBAI***

Submitted by

**Dr. Neha Chhabra Roy (Principal Investigator)
Dr. Sreeleakha P (Co-Principal Investigator)
Dr. Narayani Ramachandran (Co-Principal Investigator)**

**SVKM's Narsee Monjee Institute of Management Studies, Bangalore
Deemed to be University**

March, 2026

EXECUTIVE SUMMARY

The proposed research paper explores the degree of FinTech readiness in the Indian banking industry through a holistic, integrated analytical lens that examines both institutional (enabler-level) and behavioural (user-level) aspects. The main aim of the study is to examine banks' technological readiness and, at the same time, gauge employees' flexibility in the context of digital transformation. By doing so, the research fills a critical gap in the available literature, where technological infrastructure and human readiness are often discussed separately rather than as interdependent elements of digital adoption.

The four major research objectives of the study are (i) to identify and build indicators of FinTech preparedness using both theoretical and empirical literature, (ii) to categorise banks in various adaptability levels using sophisticated methods of analysis, (iii) to examine the underlying causes of different levels of preparedness, and (iv) to develop a dual-layered mitigation scheme to improve FinTech adoption within the banking ecosystem. To get these goals, the study uses a mixed method design, which uses a combination of primary and secondary data. The perceptions of the user level are measured on the theoretically based constructs of perceived usefulness, ease of use, digital literacy, and trust in technology with primary data, and enabler-level preparedness is measured on the indicators of IT infrastructure, investment in cybersecurity, regulatory congruence, and system quality with proxies of secondary data.

Fifteen banks were chosen to participate in the research and preparation was measured by two composite indices the User Preparedness Index (UPI) and the Enabler Preparedness Index (EPI). The results show a significant point of divergence between these two dimensions, and some of the banks show comparatively higher employee preparedness than institutional preparedness. This shows that, as much as the employees are ready and able to embrace FinTech innovations, organisational systems, infrastructure, and governance structures are mostly behind the curve thus limiting effective digital transformation.

The machine-learning-based classification of banks by adaptability level was used to reinforce the study's analytical rigor. The best predictive accuracy of the models tested has been shown to be 95% by the Random Forest algorithm, and the sensitivity is 100%, which means the algorithm is reliable when it comes to classifying highly adaptive and low adaptability banks. This category

served as the basis for further severity efforts, as important markers of preparedness faults were found within banks.

This paper also carries out a root cause analysis by associating the level-indicator deviations with behavioural and institutional constraints. These root causes were grounded in the available literature, contextualised for the banking sector, and further validated by industry players. The analysis notes that the major issues causing user-level limitations include a lack of clarity about technology benefits, low levels of digital literacy, a lack of trust, and perceived risk, whereas enabler-level limitations include legacy infrastructure, inadequate reskilling investments, incoherent cybersecurity frameworks, and poor regulatory alignment.

Based on these insights, the research will suggest specific mitigation measures at both enabler and user levels. Some of the institutional strategies encompass AI-driven reskilling, IT infrastructure, cybersecurity, and the implementation of a RegTech framework to support compliance and governance. At the user level, certification programs, peer learning, gamified training, and participation in FinTech innovation programs are suggested, as they help increase employees' adaptability. Notably, these mitigation measures are not generic but are tailored to the severity and root causes that have been established to each bank, which is practical and applicable.

To align with the ultimate research goal, the study develops a dual-layered conceptual mitigation framework that integrates behavioural and institutional interventions into a joint model. This framework stresses that the successful implementation of FinTech must be aligned with human potential and the technological system, but not with single gains in one of these areas. To further bring together the findings, a conclusion conceptual framework is provided, which demonstrates how indicators, severity level, root cause and mitigation strategy are interrelated, and hence the ecosystem of FinTech preparedness is displayed in a holistic picture.

In sum, the study is a valuable contribution to theoretical and practical insights into the topic, offering a structured, evidence-based, and practical solution to the problem of FinTech preparedness in the banking industry. It shows that sustainable digital transformation will be determined by reducing the mismatch between employees' adaptability and the institution's capabilities. The results of this study provide policymakers, banking institutions, and practitioners with useful information to develop more efficient strategies for coping with the dynamic environment of financial technology and building a robust, future-oriented banking system.

Acknowledgement

We express our sincere gratitude to the Indian Institute of Banking and Finance (IIBF) for providing us with the opportunity to undertake this research study titled “*Assessing Financial Technology Readiness in Indian Banking: Workforce Adaptability, Organisational Transformation, and Strategic Implementation.*” We deeply appreciate the Institute’s support and encouragement in enabling academic inquiry that contributes meaningfully to the evolving landscape of the banking sector.

We would like to acknowledge the financial support extended by IIBF for this project. The funding has enabled rigorous research, data analysis, and the development of insights to strengthen digital transformation and workforce readiness within the Indian banking ecosystem. We are especially thankful for the trust placed in us to explore a subject of critical importance to the industry. This study is a modest attempt to contribute to ongoing conversations around financial technology adoption, institutional preparedness, and human capital development in banking.

It gives us immense pleasure to express our heartfelt gratitude to all those who have inspired, encouraged, and supported us in successfully completing this research report. We extend our special thanks to Dr. K. Gangadharan, Director, Academics, IIBF, and the Research Advisory Committee for their invaluable guidance and support. Their efforts have been instrumental in the successful implementation of the IIBF macro research program, which has earned recognition for building a contemporary body of research-based knowledge and literature in the domain of banking and finance. We also express our gratitude to all survey participants for their time and responses, as well as to the anonymous reviewers of the initial project proposal and the Board members of IIBF for their constructive feedback and valuable suggestions for improvement. We are grateful to Dr. Kratika for her guidance and support, and to Ms. Anupama Bharadwaj for her assistance in coordinating with IIBF.

We would like to extend our sincere thanks to our student contributors, Joshith Reddy Gopidi and Nikhil Padgaonkar, for their valuable assistance in data collection, arrangement, analysis, and occasional coding support. We also thank the NMIMS Library team for providing access to library resources, data, and research papers, and the NMIMS Bangalore campus for facilitating the successful execution of this project. We further acknowledge the internal library

resource team and extend our thanks to the respondent bankers and senior officials who generously shared their insights and experiences.

We also extend our appreciation to all individuals, practitioners, and stakeholders who, directly or indirectly, contributed to this research through their inputs, perspectives, and support.

We hope that the findings and recommendations of this study will add value to policymakers, banking professionals, and researchers, and support the continued advancement of a resilient, inclusive, and technology-enabled banking sector in India.

Dr. Neha Chhabra Roy
Principal Investigator

Dr. Sreeleakha P
Co-Principal Investigator

Dr. Narayani Ramachandran
Co-Principal Investigator

TABLE OF CONTENTS

Abstract	11
1. Chapter 1.....	12
1.0 Introduction	12
1.1 Understanding Financial Technologies in the Banking Context	12
1.1.1 Pre-digital Banking (2000 -2010).....	13
1.1.2 Digital Banking (2010 – 2015).....	15
1.1.3 FinTech & AI (2016 – 2022).....	16
1.1.4 Future Banking (2023 – Present).....	18
1.1.5 Futuristic Financial Technologies and the Road Ahead	19
1.2 The changing job roles with changes in technology	19
1.2.1 Job roles during Pre-digital Banking Era (2000 -2010).....	19
1.2.2 Job roles in Digital Banking (2010–2015).....	21
1.2.3 Job roles in FinTech and AI Era (2016–2022).....	22
2. Chapter 2.....	28
Literature review	28
2.1 Background of the Study: Conceptualisations	28
2.2 Phase I- Technological Evolution and Skill Development, and Challenges in Banking Ecosystem.....	29
2.3 Phase -II: Indicators Identification for Technology Users and Technology Enablers (Input).....	32
2.4 Phase III- Categorising Adaptability and Identifying Key Parameters for Effective Technology Adoption	37
2.5 Root causes create variation in the Severity of Indicators	39
2.5.1 User perspective — Root causes of Low FinTech Readiness.....	39
2.5.2 Enabler Perspective - Root Causes of Low FinTech Readiness	40
2.6 Strategic Measures to Enhance Banks' and Employees' Readiness for Future Adoption	44
2.6.1 Mitigation Strategies from the User Perspective	44
2.6.2 Mitigation Strategies from the Enabler Perspective.....	45
3. Chapter 3.....	47
Research Methodology	47
3.1 Data - Primary Survey and Secondary Data	47
3.2 Objective 1- Identification of Technology Readiness Indicators	49
3.3 Objective 2(a): Banks Classification in adaptability groups from the User perspective-Secondary data Assessment	55
3.4 Objective 2(b): Classification Based on Primary Data (User Perspective)	59
3.5. Objective 3 & 4: Suggesting Mitigation Measures to Technology Users and Enablers backed by root causes and suggesting an integrative framework	60
4. Chapter 4.....	63
Banks Prioritisation and Indicators Severity Analysis Enabler centric Approach backed by secondary data	63
4.1 Descriptive Statistics of All Banks Data	64
4.2 Model comparison across banks	66
4.3 OOB error minimisation and mtry optimisation	68
4.4 Indicator's severity classification across banks using Random Forest Approach	68
4.5 Partial dependence across banks	70
4.6 Individual banks Indicators Severity analysis summary (DESCRIPTIVE, Correlation and model selection)....	71

4.7	Summarisation of selected banks' indicators, severity analysis, and bank broad dominant indicators exploration	82
5.	Chapter 5	87
	Bank classification and indicators severity analysis from the user perspective: application of Primary data	87
5.1	Cumulative bank-specific indicators normalised weight calculation	87
5.2	Bank-specific Indicators' classification	91
5.3	Preparedness Analysis of Banks based on Indicators classification	93
5.4	Primary data Banks Preparedness Index estimation	94
5.5	Comparison between primary and secondary data: index calculation and exploration of dominant indicators	100
5.6	Root cause mapping for banks based on EPI and UPI value	102
6.	Chapter 6	106
	Mitigation measures: discussions across banks	106
6.1	user-level mitigation strategies	106
6.1.1	Bank-specific Mitigation strategies	107
6.1.2	Dominant Indicators	118
6.1.3	Banking industry harmonized generic strategies to manage user level issues	119
6.2	Enabler-Level Mitigation Strategies	120
6.2.1	Mitigation plans suggested to each bank	120
6.2.2	Dominant Indicators	129
6.2.3	Banking sector aligned strategies to manage the Enabler level challenges	129
7.	Chapter 7	134
	Conclusion And Implications	134
7.1	Key Findings Of The Study	134
7.2	Policy Implications	136
7.3	Managerial Implications	136
7.4	Recommendation	137
7.5	Limitations Of The Study	138
7.6	Future Scope Of Work	138
7.7	Conclusion	139
8.	References	141
9.	Glossary	217
10.	Acronyms	219
11.	Project Completion Timeline (Gantt Chart)	223

TABLE OF TABLES

Table 2.1	Technology Preparedness of Indian banks - Employee and Bank Variables (Prepared by authors)	36
Table 2.2	Variables for Primary Data and Proxy for Secondary Data Generated for Parallel Analysis (Prepared by authors)	42
Table 2.3	Strategies used in the Past by Employees and Banks to enhance their Preparedness for Technology Enhancement (Prepared by authors)	46
Table 3.1	Suggested Driving Forces for Employees and Banks to Ensure Long-term AI/Tech adaptation (Prepared by authors)	50
Table 3.2	Bank wise responses collection for mid review	59
Table 3.3	Summary of Research Methodology – Presented based on Objectives (Prepared by author)	62
Table 4.1	Descriptive Statistics of Technology Readiness Indicators for all Listed Banks from 2020 to 2025 (Prepared by authors)	64
Table 4.2	Feature Correlation Matrix for all Listed Banks for the years 2020 to 2025 (Prepared by authors)	66
Table 4.3	Confusion Matrices and Metrics for Random Forest, SVM, and Neural Network on the Sector Broad Test Set from 2020 to 2025 (Prepared by authors)	67
Table 4.4	Severity Analysis of Indicators Across Selected Banks	69

Table 4.5 Random Forest Diagnostics Across Banks: Comparative Out of bag error, Accuracy, and False Positive Rate with Brief Correlation Context.....	72
Table 4.6 Individual Banks Summary of Selected EL and BL Indicators - Banks Classification into HAB and LAB - Preparedness Index Calculation and Prominent Indicators Identification	83
Table 4.7 Bank-wise Indicators Dominance Across Various Severity Classes	86
Table 5.1 Primary survey-based indicators classification	88
Table 5.2 All banks' Variables Severity Analysis and Ranking.....	90
Table 5.3 Summary of Primary Data Analysis Across Each Bank Individually and Summary of Responses	98
Table 5.4 Similar and Diverse Indicators from both Enabler and User Perspectives after Compiling Data of Primary and Secondary Data Analysis.....	101
Table 5.5 Integrated Banks wise Preparedness and root cause mapping.....	103
Table 6.1 Comprehensive Bank-wise FinTech Preparedness, Root Cause, and Mitigation Summary	132

TABLE OF FIGURES

Figure 1.1 Technology Evolution and Banking Sector Transformation.....	19
Figure 1.2 Evolution of Technology and Bank Job Roles (Prepared by authors).....	25
Figure 2.1 Banking Ecosystem Project Architecture	32
Figure 4.1 Summary of User-specific and Enabler-specific Indicators (Prepared by authors).....	63
Figure 4.2 OOB Error Minimisation and Tree Optimisation for RF.....	68
Figure 4.3 Random Forest Importance by Mean Decrease Accuracy and Mean Decrease Gini for all Banks, for 2020–2025.....	70
Figure 4.4 Partial Dependence of ARAA, IMPR, DTHE, ELAR, and IFR on TAP for all Banks, for years 2020–2025	71
Figure 4.5 Tech Preparedness Index Calculation Across Selected Banks (prepared by authors).....	84
Figure 5.1 All banks' Variables Severity Analysis comparative plot	89
Figure 5.2 . Normalised rating of Individual Indicators (prepared by authors).....	99
Figure 6.1 . Normalised rating of Individual Indicators (prepared by authors).....	131

TABLE OF ANNEXURES

ANNEXURE I.A Demographics and Background.....	155
ANNEXURE I.B Technology Readiness & Workforce Adaptability From Enabler And User Perspective.....	155
ANNEXURE I.C Strategies Implemented by Banks & Employees.....	156
ANNEXURE II.A Axis Bank-Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3	157
ANNEXURE II.B Axis Bank-Random Forest OOB error versus number of trees, 2020 Q1 to 2025.....	157
ANNEXURE II.C Random Forest-based prioritisation of indicators for Axis Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG).....	157
ANNEXURE II.D Axis Bank-Partial dependence of DFQ, DTHE, and ITII for Axis Bank, 2020 Q1 to 2025 Q3.....	158
ANNEXURE II.E Axis Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini, 2020 Q1 to 2025 Q3	158
ANNEXURE II.F Axis Bank – Variables Severity Analysis and Ranking.....	159
ANNEXURE II.G Axis Bank – Indicators Severity Analysis comparative plot.....	160
ANNEXURE III.A Bank of Baroda – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3	161
ANNEXURE III.B Bank of Baroda – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025.....	161
ANNEXURE III.C Bank of Baroda – Random Forest-based prioritisation of indicators for Bank of Baroda with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)	161
ANNEXURE III.D Bank of Baroda – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Bank of Baroda, 2020 Q1 to 2025 Q3.....	162
ANNEXURE III.E Bank of Baroda - Partial dependence of BATR and ITII, 2020 Q1 to 2025 Q3.....	162
ANNEXURE III.F Bank of Baroda – Variables Severity Analysis and Ranking	162
ANNEXURE III.G Bank of Baroda – Indicators Severity Analysis comparative plot	164
ANNEXURE IV.A Bank of Maharashtra – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3	165
ANNEXURE IV.B Bank of Maharashtra – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025	165
ANNEXURE IV.C Bank of Maharashtra – Random Forest-based prioritisation of indicators for Bank of Maharashtra with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)	165
ANNEXURE IV.D Bank of Maharashtra – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Bank of Maharashtra, 2020 Q1 to 2025 Q3	166
ANNEXURE IV.E Bank of Maharashtra - Partial dependence of CMD, 2020 Q1 to 2025 Q3.....	166
ANNEXURE IV.F Bank of Maharashtra – Variables Severity Analysis and Ranking.....	167
ANNEXURE IV.G Bank of Maharashtra – Indicators Severity Analysis comparative plot.....	168
ANNEXURE V.A DCB Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3.....	169
ANNEXURE V.B DCB Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025	169
ANNEXURE V.C DCB Bank – Random Forest-based prioritisation of indicators for DCB Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)	169
ANNEXURE V.D DCB Bank - Partial dependence of IMPR, 2020 Q1 to 2025 Q3.....	170

ANNEXURE V.E DCB Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Bank of Maharashtra, 2020 Q1 to 2025 Q3	170
ANNEXURE V.F DCB Bank – Variables Severity Analysis and Ranking.....	170
ANNEXURE V.G DCB Bank – Indicators Severity Analysis comparative plot	172
ANNEXURE VI.A HDFC Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3.....	173
ANNEXURE VI.B HDFC Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025.....	173
ANNEXURE VI.C HDFC Bank – Random Forest-based prioritisation of indicators for HDFC Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG).....	173
ANNEXURE VI.D HDFC Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for HDFC Bank, 2020 Q1 to 2025 Q3.....	174
ANNEXURE VI.E HDFC Bank - Partial dependence of IFR, 2020 Q1 to 2025 Q3.....	174
ANNEXURE VI.F HDFC Bank – Variables Severity Analysis and Ranking	174
ANNEXURE VI.G HDFC Bank – Indicators Severity Analysis comparative plot	176
ANNEXURE VII.A Indian Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3.....	177
ANNEXURE VII.B Indian Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025.....	177
ANNEXURE VII.C Indian Bank – Random Forest-based prioritisation of indicators for Indian Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG).....	177
ANNEXURE VII.D Indian Bank - Partial dependence of DTHE and CCRTU, 2020 Q1 to 2025 Q3.....	178
ANNEXURE VII.E Indian Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Indian Bank, 2020 Q1 to 2025 Q3.....	178
ANNEXURE VII.F Indian Bank – Variables Severity Analysis and Ranking	178
ANNEXURE VII.G Indian Bank – Indicators Severity Analysis comparative plot	180
ANNEXURE VIII.A ICICI Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3.....	181
ANNEXURE VIII.B ICICI Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025	181
ANNEXURE VIII.C ICICI Bank – Random Forest-based prioritisation of indicators for ICICI Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG).....	181
ANNEXURE VIII.D ICICI Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for ICICI Bank, 2020 Q1 to 2025 Q3.....	182
ANNEXURE VIII.E ICICI Bank - Partial dependence of DFQ and CCRTU, 2020 Q1 to 2025 Q3	182
ANNEXURE VIII.F ICICI Bank – Variables Severity Analysis and Ranking	182
ANNEXURE VIII.G ICICI Bank – Indicators Severity Analysis comparative plot	184
ANNEXURE IX.A IDFC Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3	185
ANNEXURE IX.B IDFC Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025	185
ANNEXURE IX.C IDFC Bank – Random Forest-based prioritisation of indicators for IDFC Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG).....	185
ANNEXURE IX.D IDFC Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for IDFC Bank, 2020 Q1 to 2025 Q3.....	186
ANNEXURE IX.E IDFC First Bank - Partial dependence of AIPCS, IFR, ELAR and IMPR, 2020 Q1 to 2025 Q3.....	186
ANNEXURE IX.F IDFC Bank – Variables Severity Analysis and Ranking.....	187
ANNEXURE IX.G IDFC Bank – Indicators Severity Analysis comparative plot.....	188
ANNEXURE X.A IndusInd Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3.....	189
ANNEXURE X.B IndusInd Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025	189
ANNEXURE X.C IndusInd Bank – Random Forest-based prioritisation of indicators for IndusInd Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)	189
ANNEXURE X.D IndusInd Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for IndusInd Bank, 2020 Q1 to 2025 Q3.....	190
ANNEXURE X.E IndusInd Bank - Partial dependence of CCRTU and CMD, 2020 Q1 to 2025 Q3.....	190
ANNEXURE X.F IndusInd Bank – Variables Severity Analysis and Ranking.....	190
ANNEXURE X.G IndusInd Bank – Indicators Severity Analysis comparative plot	192
ANNEXURE XI.A Indian Overseas Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3.....	193
ANNEXURE XI.B Indian Overseas Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025.....	193
ANNEXURE XI.C Indian Overseas Bank – Random Forest-based prioritisation of indicators for Indian Overseas Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)	193
ANNEXURE XI.D Indian Overseas Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Indian Overseas Bank, 2020 Q1 to 2025 Q3	194
ANNEXURE XI.E Indian Overseas Bank – Variables Severity Analysis and Ranking	195
ANNEXURE XI.F Indian Overseas Bank – Indicators Severity Analysis comparative plot	196
ANNEXURE XII.A Kotak Mahindra Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3	197
ANNEXURE XII.B Kotak Mahindra Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025.....	197
ANNEXURE XII.C Kotak Bank – Random Forest-based prioritisation of indicators for State Bank of India with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)	197
ANNEXURE XII.D Kotak Mahindra Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Kotak Mahindra Bank, 2020 Q1 to 2025 Q3.....	198

ANNEXURE XII.E Kotak Mahindra Bank - Partial dependence of DBU, 2020 Q1 to 2025 Q3	198
ANNEXURE XII.F Kotak Mahindra Bank – Variables Severity Analysis and Ranking	198
ANNEXURE XII.G Kotak Mahindra Bank – Indicators Severity Analysis comparative plot.....	200
ANNEXURE XIII.A State Bank of India – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3.....	201
ANNEXURE XIII.B State Bank of India – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025	201
ANNEXURE XIII.C State Bank of India – Random Forest-based prioritisation of indicators for State Bank of India with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)	201
ANNEXURE XIII.D State Bank of India – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for State Bank of India, 2020 Q1 to 2025 Q3	202
ANNEXURE XIII.E State Bank of India - Partial dependence of DFQ, DTHE, and IMPR, 2020 Q1 to 2025 Q3	202
ANNEXURE XIII.F State Bank of India – Variables Severity Analysis and Ranking.....	203
ANNEXURE XIII.G State Bank of India – Indicators Severity Analysis comparative plot.....	204
ANNEXURE XIV.A UCO Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025.....	205
ANNEXURE XIV.B UCO Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3	205
ANNEXURE XIV.C UCO Bank – Random Forest-based prioritisation of indicators for UCO Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG).....	205
ANNEXURE XIV.D UCO Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for UCO Bank, 2020 Q1 to 2025 Q3.....	206
ANNEXURE XIV.E UCO Bank - Partial dependence of DFQ, DTHE, and ITII, 2020 Q1 to 2025 Q3	206
ANNEXURE XIV.F UCO Bank – Variables Severity Analysis and Ranking	206
ANNEXURE XIV.G UCO Bank – Indicators Severity Analysis comparative plot.....	208
ANNEXURE XV.A Union Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025	209
ANNEXURE XV.B Union Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3	209
ANNEXURE XV.C Union Bank – Random Forest-based prioritisation of indicators for Union Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG).....	209
ANNEXURE XV.D Union Bank of India - Partial dependence of ITBCS, 2020 Q1 to 2025 Q3	210
ANNEXURE XV.E Union Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Union Bank, 2020 Q1 to 2025 Q3.....	210
ANNEXURE XV.F Union Bank – Variables Severity Analysis and Ranking	210
ANNEXURE XV.G Union Bank – Indicators Severity Analysis comparative plot	212
ANNEXURE XVI.A Yes Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3	213
ANNEXURE XVI.B Yes Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025	213
ANNEXURE XVI.C Yes Bank – Random Forest-based prioritisation of indicators for Yes Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)	213
ANNEXURE XVI.D Yes Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Yes Bank, 2020 Q1 to 2025 Q3.....	214
ANNEXURE XVI.E Yes Bank - Partial dependence of DFQ, DBU and BATR, 2020 Q1 to 2025 Q3	214
ANNEXURE XVI.F Yes Bank – Variables Severity Analysis and Ranking.....	215
ANNEXURE XVI.G Yes Bank – Indicators Severity Analysis comparative plot.....	216

ABSTRACT

Financial technology (Fintech) has significantly transformed the banking sector by creating new job roles, operational structures, and institutional preparedness. This study assesses how banks and their employees, particularly mid-level executives, adapt to these changes and prepare for technology-based job roles. The research addresses the broader impact of technological advancements on banking institutions, focusing on organisational readiness and employee skill adaptability. This study employs a hybrid of the Technology Acceptance Model (TAM), the Extended Technology Acceptance Model (ETAM), and the Unified Theory of Acceptance and Use of Technology (UTAUT) to analyse key determinants influencing financial technology adoption in banking operations. The study adopts both primary and secondary data analysis), where a machine learning-driven method, which deals with class imbalance issues, such as the Random Forest model (RF), Support Vector Machine (SVM), or Neural Networks (NN), will classify banks and employees based on their adaptability using secondary data. Primary data were collected through surveys of mid-level banking executives, and secondary data were analysed from financial institutions and regulatory reports to understand broader trends in financial technology adoption. The study reveals gaps in financial technology readiness among banks and their employees, highlighting skill gaps, infrastructure challenges, and regulatory constraints. Classifying banks based on adaptability, enablers, and the user side helped pinpoint areas requiring intervention. The findings provide actionable strategies for banks to enhance their infrastructure, cybersecurity frameworks, and employee reskilling programs, enabling a synchronised Fintech integration roadmap. It also offers policymakers a deeper understanding of regulatory adjustments required for Fintech-driven banking. Additionally, researchers can leverage the proposed Fintech adoption framework to explore workforce digital adaptation strategies in the banking sector.

KEYWORDS: FINTECH ADOPTION, BANKING, ENABLER (INSTITUTION) READINESS, USER (EMPLOYEE) READINESS, MACHINE LEARNING BASED CLASSIFICATION, OPERATIONAL EFFICIENCY

1. CHAPTER 1

1.0 INTRODUCTION

Financial technologies (FinTech) have become more important in the banking industry over the last thirty years. Technological progress has significantly improved the speed, accuracy, and efficiency of financial transactions and operational processes. Technological innovations have revolutionized the banking operations, and the earliest use of technology in banking was the introduction of Core Banking Solutions (CBS) in the 1990s, but the latest applications are real-time payments (Chhabra Roy & Prabhakaran, 2025), AI-driven fraud detection (Choithani et al., 2024), and blockchain-based settlements (Jing, Qin, Yao, Han, & Wang, 2024). Global financial institutions have been actively investing in such innovations to maintain operational effectiveness, cost reduction, and create a better customer experience. According to a McKinsey and Company study, financial institutions globally had invested more than \$500 billion in digital transformation projects over the last ten years (A. Agarwal, Singhal, & Thomas, 2021). By 2030, AI will save the banking industry \$1 trillion a year (PWC, 2019). Deloitte, (2023) report also indicates that 77 percent of banks already deployed AI in their work, especially in fraud detection, risk management and credit scoring.

1.1 UNDERSTANDING FINANCIAL TECHNOLOGIES IN THE BANKING CONTEXT

The financial services sector has drastically transformed from a manual branch-based banking system to digital services through the use of Financial Technologies (FinTech). According to the World Bank, FinTech is a digital innovation that contributes to financial intermediation, risk management, and access to financial services (Asif, Lodhi, Sarwar, & Ashfaq, 2024). This banking system's technological revolution has transformed the activities of financial institutions, providing value to customers, improving their client interaction, and reducing their risks. It has also helped in financial inclusion by reaching out to those who could not access the services before, especially the underbanked groups (S. Biswas, Carson, Chung, Singh, & Thomas, 2020). The revolution has made FinTech a mediator of financial operations, which makes transactions more efficient, serves the customer better, and offers access to a wider range of financial products. In this report, we define FinTech as a series of technologies used by banks in order to increase their ability to operate and provide services. The spectrum includes enabler-side technologies (including banks) as well as user-side technologies (end-users). The enabler-side technologies are robust IT infrastructure, cybersecurity, advanced core banking

systems, regulatory technologies, and service delivery mechanisms. Such technologies ensure that the banking operations are implemented with sufficient risk management systems and compliance requirements. Digital wallets, online interfaces, and mobile applications are some of the user-side technologies. They act as the main channel of communication with customers and also satisfy the needs of the customers through these technologies (Akinbowale, Klingelhöfer, & Zerihun, 2024).

Technology advancement and macroeconomic changes in the world have influenced the emergence of FinTech in India. We have identified four related stages of this evolution: (i) Pre-digital Banking, (ii) Digital Banking, (iii) FinTech & AI, and (iv) Future Banking. The progress started through the simple automation of financial processes, which paved the way for higher-level innovations. Gradually, data analytics and AI are slowly replacing human decision-making, allowing banks to provide more personalised financial services and risk management. Subsequent stages brought about open banking ecosystems, which have encouraged financial institutions to collaborate with third-party providers to create new products and services tailored to the consumer (Türk Kurtça & Demirci, 2022). This has seen the increased focus based on the provision of smooth customer experiences, through real-time access to financial services and information, which brings more transparency and trust to the financial industry.

Overall, FinTech is marked by the interaction between technology and finance that leads to the appearance of innovations that change the nature of banking. With the banking industry in India adapting to these changes, it is set to shape the future of financial services in India and overseas. The further technological development of FinTech is not only a technological shift but a radical redefinition of how financial institutions and their customers will interact, underscoring the necessity of cooperation, adaptability, and responsiveness in a complex financial landscape.

1.1.1 PRE-DIGITAL BANKING (2000 -2010)

The events of this phase were in line with the economic liberalisation policies in the 1990s. Increased competition, deregulation and emphasis on customer service drove major changes in this period. This dynamic nature caused banks to change their operations from branch-based to network-based. The most important was Core Banking Solutions (CBS), which helped banks centralise information and transactions. Through this, customers could access banking services at any branch at their convenience. All stakeholders accepted the CBS well and hence

established a more interconnected banking ecosystem. This project was initiated by the State Bank of India under the name of the SBI CBS Project. It was the largest centralised core processing project in the world at the time, across the entire chain of branches of SBI and its affiliate banks. The project was the conversion of 140 million accounts in 14600 domestic branches and affiliates. This project was initiated with the assistance of Tata Consultancy Services in 2002 and was completed by July 2008, with all branches being fully converted (Bhusan & Singh, 2023). The top privately owned banks, including ICICI Bank and HDFC Bank, have implemented this technology to facilitate real-time transactions to their customers. The introduction of Automated Teller Machines (ATMs), debit and credit cards were introduced together with CBS to enhance the customer experience. ATMs let customers withdraw their money without having to go to a bank clerk. Making payments through debit cards involves connecting the card to the bank account; they deduct the money directly, rather than a cash transaction. Credit cards give customers the opportunity to purchase the item and to settle the payments later. The Indian Banks Association further democratised the banking services by launching the Shared ATM Network Initiative (Swadhan) that enabled the customers to conduct transactions at any bank ATM. With these advancements, the international messaging system, the Society for Worldwide Interbank Financial Telecommunications (SWIFT) also came into place, which guarantees the safety and efficiency of money, securities, trade and treasury operations through a standardised code system (Madan Lal Bhasin, 2016). Financial crimes like money laundering, cyber crimes and terror money laundering were on the increase as the world continued to advance in the field of technology. This required verifying customer accounts. Therefore, the Know Your Customer (KYC) project was a compliance measure and legal obligation for banks to verify the identities of their customers and improve security. Electronic transfer systems were also another milestone in this period. High-value transactions were implemented using Real-Time Gross Settlement (RTGS), retail inter-bank fund transfers were done through the use of the National Electronic Funds Transfer (NEFT) and instant interbank transfers were implemented via the Immediate Payment Service (IMPS) during this period. This had to be done to remain in line with economic changes.

The advantages of CBS and electronic banking channels were numerous. Customers were able to have real-time access to their accounts, thus providing 24/7 convenience. In the case of banks, it led to lower transaction costs, better liquidity management, and retention of more customers. Banks can achieve better service delivery by ensuring their services are more

accessible and user-friendly to better meet the changing needs of their customers. This transition, however, was challenged. The cost of delivering CBS was prohibitive, particularly to small or resource-bound banks. Further, diffusion was restricted by a lack of digital literacy. ATM facilities were mainly located in cities, making them less accessible to the rural population. There were also cyber threats and uncontrolled data protection measures. In general, this step played a vital role in balancing operational efficiency and customer empowerment, laying the groundwork for future innovations in online and mobile banking. The stage required new employee skills to handle positions as the industry moved from manual to technological operations. This transition saw the employees gradually upskill themselves and succeed.

1.1.2 DIGITAL BANKING (2010 – 2015)

The years 2010 through 2015 represented a great breakthrough in the banking industry, which was brought about by the wide use of the internet and smartphones. Their growth was facilitated by the regulatory frameworks, and swift changes that were characterized by the internet were readily adapted by the banks. The banks provided all-inclusive internet banking, whereby customers could make their banking transactions over the internet via the web interface. These were services that involved payment of bills, checking their bank balance, transferring, and application of debit/credit cards. These steps also allowed customers to send money electronically and safely and efficiently. These modes were fast, 24-hour and suitable for high-value transactions, and this was what the customers loved since they did not have to carry physical cash to transfer funds.

As smartphones began to penetrate and their utilization was on the rise, banks used this as a platform to reach many customers by launching mobile banking apps and SMS messages. Security aspects (OTP and two-factor authentication) were applied to ensure that mobile transactions can be safe and trustworthy. Mobile banking applications such as Online SBI service by SBI, iMobile app by ICICI Bank and Net Banking platform by HDFC Bank have transformed the online banking services. Using the above new technologies, the expectations of customers on the banking services have been altered as they have been exposed to increased convenience, lessening delays in transactions and increased reliance on digital financing methods (Javaid, Haleem, Singh, Suman, & Khan, 2022). The KYC process became computerised. In the e-KYC process, the banks enter all documents and biometric information into the e-Aadhaar system to confirm the information and verify the bank account holder. On

the same note, the technology was applied to determine the credit repayment history of the customer. The automated credit scoring evaluates the creditworthiness of a borrower by applying both traditional and non-traditional methods, and with the aid of AI, assists in sanctioning loans (Sardana & Singhania, 2018).

Even where banks used these technologies in a bid to be efficient in operations and ensure customer satisfaction, there were challenges. The areas where the internet and smartphones penetrated were limited only to rural regions, and this also impacted the banking services. It has been found that several rural banks have not fully embraced digital technologies because of poor network connectivity. Several cybersecurity threats, such as identity theft, phishing, malware, ransomware, insider and Trojan attacks, have become a critical issue. According to a study by Deloitte (2023) on the topic of five ways banks can reduce the impact of a catastrophic cybersecurity event, in 2021, the number of ransomware attacks against banks increased by 1381%. Security lapses became a concern. Not all web interfaces were as user-friendly, and therefore, the elderly, less tech-savvy customers found them hard to use. The workers of these positions found it hard to adjust to the new skills that were needed within the banking sector since the sector needed specialized skills and financial expertise during this period.

1.1.3 FINTECH & AI (2016 – 2022)

The Digital India initiative by the Indian Government revolutionised the next phase by encouraging cashless transactions via the Unified Payments Interface (UPI). Having been introduced in 2016 by the National Payments Corporation of India (NPCI), UPI is an interoperable mobile-first, instant payment system that uses merchant QR Codes and virtual IDs. The program is taking center stage in digital payments in India and is known worldwide as a standard of real-time payments. At present, it boasts an enormous user base of 491 million people and 65 million merchants, becoming one of the successful FinTech integrations in the banking services (PwC, 2025). Other comparable projects include the Aadhaar-enabled Payment Systems (AePS) and RuPay cards, which have greatly increased financial inclusion in villages. The use of digital wallets, such as Google Pay, Paytm, and PhonePe, has only expanded the adoption of the cashless economy.

The other significant innovation during this period was the use of technology like AI chatbots, blockchain, open banking, and RegTech (Iddrisu, Yakubu, Yussif, & Issah, 2025). The pandemic provided the chance to engage with consumers online, and there is no turning back.

By employing the newest financial tools, such as AI and Machine Learning (ML), banks are discovering new ways of running their business. AI and ML will indeed be used to their maximum possible potential until the next technological breakthrough. The use of AI chatbots has transformed customer service and served as virtual assistants, leveraging Application Programming Interfaces (APIs) and Natural Language Processing (NLP) to respond to customer questions in real-time. With the use of Blockchain, the level of security and transparency has increased, because transactions are stored in decentralised, immutable registers. Open banking, where banks provide customer financial data to approved third parties at the customer's request, is another financial service, gradually gaining traction. This step can allow individual customer services, increased convenience, control and additional options. RegTech simplifies regulatory compliance with these innovations. It assists with threat monitoring and risk analysis too.

With these services, customers will be able to use their smartphones to make seamless cashless transactions, allowing millions of people to use this financial ecosystem. To remain in line with the market transformation, government-funded banks such as SBI have embraced the digital service YONO (You Only Need One), whose purpose is to offer e-commerce, banking, investments, and lifestyle services under one roof. Likewise, other private banks like HDFC, ICICI, Axis Bank, and others have partnered with FinTech startups to create tailored solutions to engage with customers, make payments and carry out other financial operations.

The banking service revolution that has been achieved through the integration of FinTech is incredible. FinTech helped bridge the financial services gap serving the unbanked regions, decreasing the digital divide and making India a global leader in real-time digital payment solutions (Chitimira & Ncube, 2021). To cope with this new shift in work, the new positions: AI and data analytics manager, RegTech, Compliance Manager, etc. were established to make sure these processes are implemented correctly. This required employees to be AI and ML savvy to manage this task. Not many banks have invested in upskilling development to train their employees. But the rate of digitisation in the sector was such that major challenges were also created. Growing digital fraud, data privacy problems and developing standardised cybersecurity norms are now urgent. Despite these advances, there was the digital divide.

Altogether, this stage was a paradigm shift in the banking industry, as non-collaborative approaches gave place to a collaborative one where banks, fintechs, governmental organizations, and technology vendors collaborate, developing the financial ecosystem. This

team spirit is essential to facilitate innovation, improve security, and encourage the further evolution of the Indian digital environment..

1.1.4 FUTURE BANKING (2023 – PRESENT)

The current period will be characterized by substantial transformations in the banking industry by implementing FinTech. In the services to customers, banks will employ Metaverse banking, DeFi, Smart Contracts, and Quantum computing to serve them. Banks are experimenting with how immersive experiences can be combined with technologies such as virtual and augmented reality, which enables customers to interact with avatars, transact banking business, and seek appropriate advice on their finances with legal advice through the Metaverse. They use the Metaverse to give virtual reality training to their employees. The other FinTech is DeFi (Decentralised Finance), a blockchain-based solution allowing peer-to-peer financial services that use blockchain without intermediaries (Das & Ganguly, 2024). In this case, the transactions are between two parties, which are public, they are registered in a public ledger, and hence are transparent. The prices are reduced, yet accessibility and control are higher.

Smart Contracts are likewise self-executing online agreements that use blockchain as a basis to enforce defined contractual terms automatically and therefore lessen the reliance on middlemen by banks. The innovations are used to process loans, insurance claims, trade securities and manage assets. Smart contracts are used to increase the automation, security and transparency of transactions thus reducing human error. Quantum Computing is another unrealised FinTech invention, which is in its infancy, as it allows banks to take advantage of accurate forecasting of risks, fraud detection, and optimum portfolios (Schwab Klaus, 2021). It is still an emerging technology that is not many banks adopt it.

On the whole, these developments indicate that India is becoming a data-driven banking system, which makes the country a digital financial service leader in the world. The emerging changes have improved on efficiency in operations, customer satisfaction and clarity in banking transactions. These technologies will make risk management predictable, where the banks will be able to determine the level of creditworthiness of customers and hence eliminate human influence in lending choices. These technologies, however, have their own challenges to the sector. Very multifaceted technologies may open the door to cyber threats and ethical issues. To be ahead of the technological changes, banks should invest in employee upskilling to remain on the par.

1.1.5 FUTURISTIC FINANCIAL TECHNOLOGIES AND THE ROAD AHEAD

On the one hand, the future of the Indian financial technology market is set to be highly transformed due to the presence of AI analytics, quantum computing, embedded finance, and Central Bank Digital Currencies (CBDCs). These advancements will open the doors to a new age of the Internet of Things (IoT) to automate payments, a rise in compliance with Regulatory Technology (RegTech), and an increase in eco-friendly banking by using Green FinTech (RBI, 2023). Nonetheless, banks should take care when venturing into such thrilling changes, taking into consideration data ethics, transparency of algorithms, and cyber resiliency. The laws will lead to constant changes to balance innovation and customer trust and systemic stability in the financial system (Albshaier, Almarri, & Hafizur Rahman, 2024).

The process of financial technologies implementation in India is not just a story of the technological progress, it is a significant learning process in the institutions. Banks have been shown to be constantly changing in tandem with the innovations and in their quest to balance between inclusivity and efficiency without compromising on security and the much needed human touch in an ever more automated world (Figure1.1)

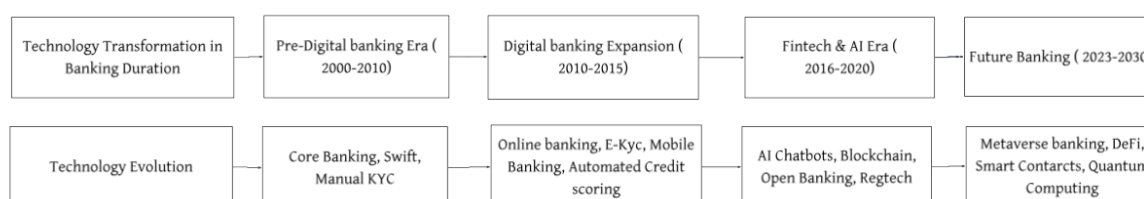


Figure 1.1 Technology Evolution and Banking Sector Transformation

1.2 THE CHANGING JOB ROLES WITH CHANGES IN TECHNOLOGY

1.2.1 JOB ROLES DURING PRE-DIGITAL BANKING ERA (2000 -2010)

With the economic liberalisation, a slow transition towards the bank environment being automated as opposed to manual operation had been observed between 2000 and 2010. There was a wider financial stability in India, growth of technology and competition because the industry was opened up to new reforms. Specifically, the implementation of the technological innovations like the CBS, KYC verification mechanisms and SWIFT was regarded as an innovation in the sphere of financial services.

Employees had their job descriptions changed as the banks began switching the manual operations into technology operated banks. The Branch Operations Manager, Risk and Compliance Officer, Customer Relationship Officer, and the supervisor of the process of transaction roles became more prominent. The Branch Operations Manager was in charge of the smooth running of the bank branch that would balance the compliance, operations and administrative duties of the bank. This has been a critical position because the banking industry was moving towards the end of paper, manual, and cumbersome operations into real time and technology and automated operations. They were previously applied manually in the management of fund transferring, keeping of ledgers and checking of customer information. Branch Operations Managers are needed in the new position to have knowledge in financial acumen, knowledge of banking software, and knowledge of banking regulations. In addition to these hard-technical competencies, operations managers ought to know how to handle teams, communicate effectively, be flexible, and problem-solve.

In the case of new technology, the norms of banking regulation have changed as well. Mishandling of human errors and fraudulent documents was also increasing due to the inability of the available workforce to manage the same. It came with the need to create new employment positions in this field. Risk and Compliance Officer took its role. They were obliged to comply with regulatory terms of the RBI because the number of human mistakes and fraudulent documents was increasing. They have responsibility to ensure that there are internal controls, routine audits and to raise red flags whenever there is a suspicion of activity. In order to resolve the challenges of the security breaches, Risk Officers must have a comprehension of regulatory and compliance requirements as they are the main connection between the operational branches and the regulators. During this process, they benefit the bank as they are the ones who can recognize the possible risks and prevent the occurrence of major fraud.

With more financial products being launched in the industry, Customer Relationship Officers played a critical role in the sector as the industry moved from a more bureaucratic and product-focused strategy to a customer-focused strategy. One of the strategies at this stage was the customer-oriented approach. The position was proactive, which guaranteed the preservation of long-term relationships with customers with the purpose to build trust and loyalty and offer a personalised banking experience. They were also expected to respond to all customer queries and identification of new customers, cross-selling other financial products like insurance and

mutual funds, and long term client retention. Customer Relationship Officers should possess a decent mix of financial and interpersonal skills, which are negotiation, communication, relationship-building, problem-solving, analytic thinking, and product knowledge. Effective Customer Relationship Officers were retained customers of the bank. The other job that was developed was that of the Transaction Processing Supervisors who helped in the back-office processes, such as clearing of cheques, issue of drafts, and also the reconciliation of accounts. This position was significant because it assisted in administration of day to day activities.

In general, at this stage, the banks concentrated on the reliability of their operations. Since the industry was gradually embracing the use of technology, this was a period that was under the control of the human labor force who depended on human precision and efficiency with regard to their operations to enable growth. The employees were instrumental in ensuring the stability of the sector because they upskilled themselves to comply with the new demands of the banking industry.

1.2.2 JOB ROLES IN DIGITAL BANKING (2010–2015)

The Digital Banking expansion phase was another major innovation in the banking industry that was propelled by the use of the internet. Banks were quick to embrace the change in the market by providing all-inclusive online banking services, such as bill payments, checking of balances, transferring funds and applying debit/credit cards. It allowed customers to do virtually everything with the bank without going to the branch. The most significant technologies that were applied in this phase were online banking systems, mobile applications, e-KYC, and automated credit scoring models. The Internet and Mobile Apps have increased availability, yet in ways that have been difficult to foresee. Having easy access to internet by everyone and banking services right at the touch of a button, this has brought up more fraudulent activities such as cyber threats and information theft by hackers. Digital fraud has been on the rise as never before. The threat of cybersecurity was the greatest. The novel functions of Digital Banking Officer and Cybersecurity and Fraud Analyst had to be considered in order to solve this issue (Willcocks, 2024). The Digital Banking Officers serve as a communicator between the customers and the technology and connect with the customers in digital wallets, mobile applications and internet banking. As the list of customers grew constantly, digital banking officers had to communicate with the customers online and apply data-oriented approaches to decision-making. Their expertise was in solving problems and analytical skills, and the knowledgeable inside the digital platforms and cybersecurity devices.

To address the challenges of cyber threats, the employment opportunities of Cybersecurity and Fraud Analyst positions exploded. Their duty was to track the differences in transactions, identify and eliminate cyber threats, and safeguard digital assets without tarnishing the reputation of the bank.

By introducing technology into its procedures, banking operations were extremely sensitive and dangerous. Banks became forced to deal with huge volume of customer information. Therefore, the e-KYC process was used to verify customer authenticity in order to secure the identity of the bank account holders. The e-KYC was also accurate, fast and efficient; the traditional KYC process was prone to errors. The move also aimed at deterring money laundering activities, especially when customers open counterfeit accounts. The e-KYC procedure guaranteed the database to be current, mistake free and safe. KYC and Anti-Money laundering Managers were charged with the responsibility of verifying that the accounts of customers were legitimate as well as preventing the chances of identity theft (Tsingou, 2018). The other major application of digital tools in banking was to apply data analytics, machine learning models and AI to determine the creditworthiness of the repayment behaviours of customers with the help of Automated Credit Scoring Models. These systems compared both conventional and non-conventional sources of data in order to make real-time decisions regarding the financial credibility of customers.

During this stage, the job descriptions were Digital Banking Officer, Cybersecurity and Fraud Analyst, KYC and Anti-Money laundering Manager, with the necessary digital, financial, and analytical skills. The fast development of the technology implied that a number of workers could not cope with it. The industry quickly went online, and employees needed to be retrained to have new skills and competencies. Digital platforms, however, were not embraced by all employees who feared that they would be mismatched with their tasks, although they were used to working manually and on paper. To adjust to new technology platforms, banks began several training initiatives to reskill their workers.

1.2.3 JOB ROLES IN FINTECH AND AI ERA (2016–2022)

The third stage involved the introduction of deep-tech interventions such as introductions of the Machine Learning (ML) algorithms, Open Banking (Jin et al., 2021), RegTech, Artificial Intelligence and Blockchain. It offered tailored customer service, enhanced risk management and enhanced security. Such innovations, based on AI and necessitating new interdisciplinary

roles, integrating finance, technology, and analytics, shook the job profiles in Indian banking to a considerable degree. The banks required AI & Data Analytics Managers to interpret and convert data into actionable insights, as well as introduce AI/ML solutions to promote strategic growth (Choithani et al., 2024). Equally, the design, implementation, and maintenance of systems based on blockchain needed Blockchain and Digital Payments Officers. Their role is to come up with the integrated digital payment structures, implement smart contracts, develop decentralised applications and apply cryptographic measures to combat cyber threats. The RegTech (Regulatory Technology) Compliance Officers apply technology to automate the regulatory compliance processes. Simple, routine processes should be automated to allow people to concentrate on the strategic responsibilities of the bank. They track and evaluate the changing laws and how they affect the bank and enforce that the bank adheres to all regulations and legal obligations.

During this step, AI and Data Analytics Managers, Blockchain and Digital Payments Officers, and RegTech (Regulatory technology) Compliance Officers, all occupied in the area of efficiency, were transferred to the realm of intelligence - decision-making became predictive, personalised, and imbued with data security. The AI/Data Analytics Managers control data gathering, data analysis, interpretation, and implementation of AI/ML models in the financial environment. These positions demanded a good command of SQL, programming languages, financial modelling, big data technologies, cloud platforms and data visualisation tools. In the banking industry, blockchains revolutionized the world of digital payments. Therefore, a new position of Blockchain and Digital Payments Officers was designed to exploit and further innovate financial products under this technology. They were masters of mingling their strategic and operational duties. This position was responsible to integrate, operate and implement electronic payment systems using distributed ledger technology. Their technical capabilities are blockchain architecture, cybersecurity, and basic cryptography. As mentioned earlier, with the growing application of technology, new opportunities have arisen to vigilantly protect the banking sector. Therefore, tougher regulatory standards were implemented and RegTech Compliance Officers had to monitor compliance with government regulations. On the whole, the technical skills that a banking occupation demanded in this stage were more integrated and of equal significance as their functional skills. The skill sets and competencies of employees grew exponentially as the banks changed with technology.

1.2.4. Job roles in Future Banking Era (2023–2030)

The banking industry is currently looking at Metaverse, DeFi, Smart Contracts, and Quantum computing. During this stage, the banking industry is considering new avenues to provide its clientele with the immersive banking experiences, peer-to-peer finances, and online agreements with the support of smart contracts. New occupations like Cybersecurity Governance Officer, AI Governance Officer, Quantum Computing Specialist, and DeFi Risk Manager are new. The AI Governance Officers are the ones who will offer strategic guidance in AI projects, align AI governance with the IT systems of the bank, and what risks AI will present to the bank. This job will be essential in executing AI policies across the bank. There is an increased cybersecurity threat. The India Cyber Threat Report, (2025) indicates that the BFSI sector is targeted the most, and then there are healthcare and hospitality. India registered 369 million malware detections in 2025. This demonstrates the necessity of a Cybersecurity Governance Officer in the nation. They are tasked with ensuring strategies and policies regarding cyber risks and compliance. The position guarantees defense against cyber attacks on the sensitive information and online assets of the bank. They also have a role in training and educating their stakeholders on ways of defending themselves against any type of cyberattack. As the number of positions requiring this kind of role increases, banks are investing in training and upskilling their current employees to assume this role.

A DeFi Risk Manager recognises, evaluates, and addresses risks in the decentralised finance, such as smart contract vulnerabilities, liquidity crises, market volatility, and regulatory uncertainty. Some of the strategies they use include due diligence, using analytics to track real-time protocols, stress testing, and cooperating with development and compliance departments to control the risk and maintain the viability of the protocol. They aim to safeguard the assets and capital efficiency within the uncertain DeFi ecosystem. Professionalism in the field of blockchain, code programming, such as Python, software, and others, such as Dune Analytics, are essential to evaluate the risks on-chain and vulnerabilities of smart contracts. The Specialists of quantum computers are people specialized in the creation of quantum algorithms to address some intricate problems. They must also have advanced programming, as well as mastery of quantum mechanics and advanced mathematics.

In the diverse new job roles required today, workers need cross-disciplinary functional skills and more sophisticated capabilities, including AI/ML technologies, regulatory compliance, technology, and business knowledge. Fintech innovations have also posed some challenging issues to the banking industry such as relying too much on AI, regulatory, and trust with

automated systems. Therefore, new positions, including Cybersecurity Governance Officer, AI Governance Officer, Quantum Computing Specialist, and DeFi Risk Manager, are being requested. Such positions demand technologically and financially savvy professionals who are able to balance innovativeness and risk avoidance with the implementation of new governance structures. Altogether, throughout these four periods, the evolution of the Indian banking job role shows a definite change: - To data-driven decision-making and not the manual accountability; - To digital-centered customer communication and no longer the branch-based one; and - To ethical and algorithmic accountability rather than transaction security.

Every new wave of technological development required new skills, be it the control of core banking or of AI systems and digital ecosystems (Asif et al., 2024). The shift also highlights a two way dependency that is the technology would not operate without expert human governance and the employees would have to keep changing to stay afloat. With the transition of the banking industry towards AI-driven, decentralised systems, the human component no longer participates in processing but leads by design, interpreting, and establishing trust (Nallakaruppan, Balusamy, Shri, Malathi, & Bhattacharyya, 2024). (Figure 1.2)

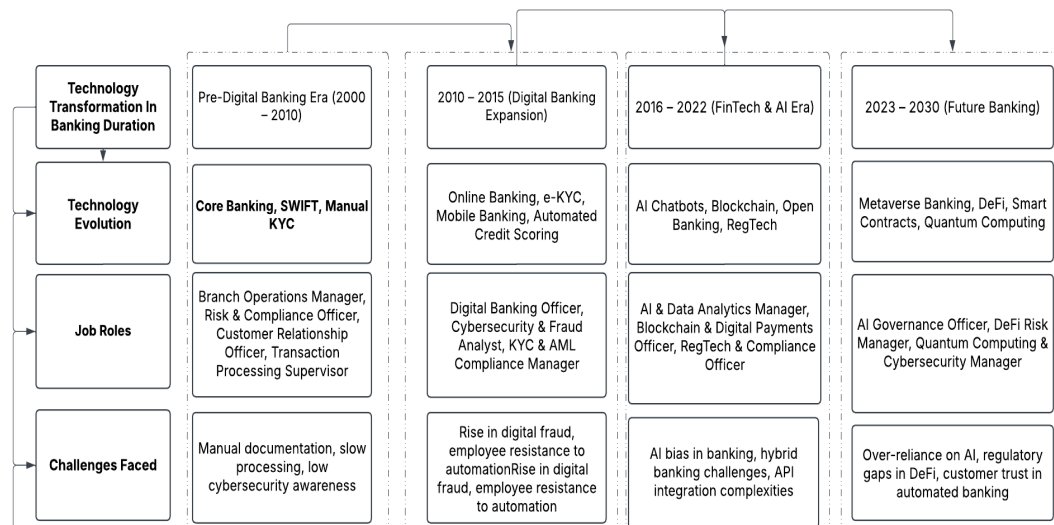


Figure 1.2 Evolution of Technology and Bank Job Roles (Prepared by authors)

These technological advances have resulted in tremendous gains but they have not been easily implemented. The example of successful cases, like the use of tech-based risk assessment models by (Lyu, 2025) has seen the time of loan processing cut by 80%. The HSBC blockchain cross-border settlements cut transaction time to several minutes (Mertzanis, 2023), which proves the power of digital transformation. The examples of the TSB Bank IT migration crisis in 2018 that left millions of customers without access to their accounts (Vasudevan, 2022) and the failure of

AI/tech-based fraud detection at Wells Fargo in 2021 that has created thousands of false fraud alerts (Welch, 2023), however, demonstrate the dangers of unmanaged technological change.

The adoption of digital technologies in the Indian banking sector has grown faster with the rise of digital transactions that have increased by more than 76 percent over the past five years (RBI, 2023). This has been further boosted by government programs like the Unified Payments Interface (UPI), Aadhaar-enabled banking and regulatory pressures to go cashless. Nevertheless, the issue of workforce preparedness is still a challenge. FICCI (2023) indicates that 60 percent of banking professionals believe that they are undertrained to deal with tech-driven automation and that a third of banks have a formal reskilling program. Moreover, almost a half of the employees are unwilling to adopt technologies because they are afraid to lose their jobs and not because they are not sure about the chances of upskilling (Aziz Baker, 2025). These issues and regulatory intricacies and cybersecurity issues form loopholes that make the successful incorporation of emerging technologies in the Indian banking activities difficult (Bank for International Settlements, 2021). The operational restructuring cannot be done at a catch-up because financial institutions cannot afford to be left behind in the competitive banking industry and due to the lightning speed of the technological advancements. They need to create a strategic framework that would include the incorporation of the new technologies in their operations maximising the efficiency and reducing the disruption. The study has relied on a four-stage process to assess the willingness of banks to use technology: (1) the challenges of job roles brought about by the advent of new technology, (2) the readiness of the employees and the institutions to the new technologies, (3) the strategic steps that the banks and the employees need to undertake to become more tech-friendly, and (4) the assimilation of all the stages into a systematic sequence.

To fill such gaps, a systematic way of assessing the preparedness at the institutional (technology enablers) and workforce (technology users) level is necessary in order to develop E-U fintech readiness system. The main research question of this work is the following: How can banks enhance their operational preparedness to incorporate emerging and new technologies into their Ecosystem? This study uses the empirical data collection approach and machine learning analysis to evaluate the preparedness of Indian banks and employees working in tech-related jobs systematically.

In particular, the paper aims to

1. To understand the major forces that affect the implementation of FinTech and emergent technologies between the technology users (employees) and technology enablers (banking institutions).

2. To categorize the level of adaptability of banks in regard to technology users and enablers.
3. To propose specific mitigation options to increase FinTech preparedness by relying on empirical classification.
4. To create a dual-layer FinTech integration framework to support both technology users and the enablers.

Through realization of these aims, the study provides meaningful ideas as to how banks can take the initiative to reformulate their operational systems to remain competitive, effective, and technologically flexible in the era of unending digitalization..

2. CHAPTER 2

LITERATURE REVIEW

The main theme of this chapter is the background of the last chapter, wherein the basis of technological innovation in banking industry and the rising challenges were analyzed. On that note, it has developed a theoretical framework that has been built by the authors, who have examined the relevant literature using the right themes. The research is carried out in a total of five themes, which include Technological Evolution and Skill Development, Challenges in the Banking Ecosystem, Indicators Identification of Technology Users and Enablers, Categorising Adaptability and Identifying Key Parameters towards effective Technology Adoption and the root causes that help in creating diversity in the severity of indicators of both enablers and users. Lastly, the chapter deals with the mitigation strategies. Thus, the chapter mostly preconditions basing the foundation by determining the gaps in the current system and discussing the ways on how they can be addressed in the future. The specifics of the sub-sections are given.

2.1 BACKGROUND OF THE STUDY: CONCEPTUALISATIONS

A four-stage process is to be evaluated to determine whether or not the banks are ready to adopt technologies. Stage one focuses on technological development and its role in job positions (Adel, ElBakary, ElDahshan, & Salah, 2022), where the use of high-tech technologies such as artificial intelligence and blockchain involves her knowledge (Javaid et al., 2022). System readiness is evaluated in stage two based on the readiness of employees as well as the ability of an institution to adopt new technologies (Belias, Koustelios, Vairaktarakis, & Sdrolias, 2015). This step is meant to determine the most important things that affect employee acceptance and to classify them based on adaptability. Third, the preparedness is measured by analyzing the intentions of the employees and banks to implement new technologies (Zhang, Du, & Zhang, 2022). It also demonstrates the mediating variable of the institutional preparedness and the idea that the implementation of technologies does not entirely rely on the workforce ability, but on the preparedness of the banking systems (A. Das & Das, 2023). The institutional preparedness of a bank is also determined by the identification of factors that lead towards technological preparedness and ranking the factors with respect to their capability to adjust to emergent innovations. The fourth stage is where the weaknesses of current structures are pinpointed and strategic solutions applicable in action to enhance workforce preparedness and institutional flexibility. A number of practical examples highlight the impacts of deploying

banking technologies that are operationally unprepared. Through this systematic method, the research will offer an in-depth approaches to comprehending the technological readiness of the banks, crucial factors that influence technology adoption and strategies to be implemented by policies in order to improve efficiency in its operations. (Figure 2.1)

2.2 PHASE I- TECHNOLOGICAL EVOLUTION AND SKILL DEVELOPMENT, AND CHALLENGES IN BANKING ECOSYSTEM

In recent 30 years, the world of banking has experienced the outburst of technological innovations which transformed the character of work (Imran, Maqbool, & Shafique, 2014) and redefined the role of middle-level managers (Kesavaraj, Azariah, Raja, & Priya, 2014). These managers are the backbone of banking organisations between strategic decision making processes and on ground implementation. As technology improved, the changes of manual labor to work done by machines and artificial intelligence programs have altered work characteristics (Das & Ganguly, 2024), and new abilities have to be created and other job roles have to be born (Talero & Gaudette, 1995). Despite the major positive impact of these innovations on the operational efficiency, financial inclusion, and customer service, they have brought the challenges of workforce restructuring, regulation issues, cybersecurity, and skills gaps (Manyika et al., 2017; Schwab Klaus, 2021). To cope with these challenges, the financial institutions will have to undertake appropriate measures to ensure that the transition is smooth. Conversely, the employees have had to constantly change with the emerging technologies in order to be effective in a more digital banking setup.

Middle-level professionals in banking business performed transaction processing, risk assessment, and customer complaint resolution between 2000-2010 and the majority of banking transactions were performed manually (Midiwo, 2016). The Branch Operations Managers, Risk & Compliance Officers, Customer Relationship Officer, and Transaction Processing Supervisor were among the most urgent job roles during this era as they all had to deal with financial statement analysis, paper-based Know Your Customer (KYC) checks, and regulatory compliance (Ammirato, Sofo, Felicetti, & Raso, 2019). Manual documentation and inefficiency in the verification of transactions was one of the largest challenges banks had to deal with. In the absence of automated tracking systems, the processes were slow, could easily be misplaced by humans, and costly to maintain. The anti-fraud strategies were more proactive, i.e., they required workers to manually scan transactions to find any evidence of a fraudulent act (Arntz, Gregory, & Zierahn, 2017). Cybersecurity issues were not that sensitive and fraud cases remained unnoticed because they had no surveillance technology (Frey & Osborne,

2017). The workloads came about using the paper-based workflows, which led to customer dissatisfaction and slow delivery of services (Bessembinder, H; Lemmon, 2002). However, there were few expectations put on workers to acquire technical skills other than general financial knowledge and as a result, they were unprepared towards the digital revolution that came to pass.

The second wave of change began in the period between 2010 and 2015 when financial institutions began using online and mobile banking systems to improve service delivery by automating their operations, preventing financial fraud, and conducting improved Know Your Customer (KYC) (Albshaier et al., 2024). Digital Banking Officers, Cybersecurity and Fraud Analysts, KYC and Anti-Money laundering (AML) Compliance Managers, the new occupational titles revealed the necessity of the industry to obtain professionals with experience in the field of security risks and adherence to regulatory standards in a dynamic digital context (N.C. Roy & Basu, 2021). This transformation was however tainted with a number of problems. The growth of digital fraud by an exponentially increasing number was one of the largest challenges since cybercriminals took advantage of the loopholes in the new digitalised financial structures (Manyika, S. Lund, M. Singer, O. White, 2016). The rise in cases of identity theft, phishing activities, and unauthorised transactions have become an issue of concern to the financial institutions, and therefore, there was an urgent necessity to seek the services of professionals possessing knowledge in fraud prevention. Moreover, the workers, especially those who were accustomed to working in the conventional banking sector, were not willing to embrace the use of digital tools, resulting in a disruption of the workflow (Bughin, Seong, Manyika, Chui, & Joshi, 2018). The middle management struggled to make a smooth transition between manual and digital platform because employees had to be trained in cybersecurity awareness, information technology cooperation, and data analytics (Schwab & Zahidi, 2020). Most banks lacked formal upskilling schemes, and as a result, it delayed the digital transformation and brought about inefficiencies in the organizing of operations.

The period between 2016 and 2022 saw the start of the integration of AI, blockchain and predictive analytics into the core operations of banks. AI-based fraud detection, blockchain-based payment services, and RegTech improved the speed of operations and accuracy of compliance (Bessen, 2019). New job titles like AI and Data Analytics Manager, Blockchain Officer and RegTech Compliance Analyst were essential. Yet, such a fast change provoked the doubt of algorithmic bias in decision-making, particularly in credit rating and fraud alerts (Dery, Sebastian, & van der Meulen, 2017). The regulatory regulations grew, which pressured the middle-level professionals. Workflow inconsistency was formed due to integration of

hybrid banking models of marrying legacy systems and digital platforms. Managers were also supposed to be efficient in their operations and coordinate various compliance models and customer care requirements. The association of FinTech also made matters more complicated, with banks being obliged to supervise third-party APIs of data safety, regulations and cross-border risk (Hunt, Prince, Dixon-Fyle, & Yee, 2018). Consequently, the employees had to acquire cybersecurity standards, API protocols, and real-time compliance mechanisms, which raised the pressure on the need to engage in constant learning and organisational support.

The next step in change between 2023 and 2030 will be fuelled by tech-governance, DeFi, and quantum computing. Continuous pressuring of banking will be implemented through fully autonomous AI-based financial services, DeFi ecosystems outside of the banking paradigm and development of quantum computing cryptography. The new roles to be created that will be essential in regulating such emerging technologies include AI Governance Officers, DeFi Risk Managers, and Quantum Computing and Cybersecurity Managers (Montagnani, Najjar, & Davola, 2024). Nevertheless, the overreliance of technology in risk examination, credit screening and fraud detection could pose transparency and responsibility challenges, and this may necessitate professionals with expertise in tech-auditing and regulation enforcement (Vandezande, 2024). Additional challenges are also presented by DeFi because the use of decentralised financial ecosystems is not regulated by banks. The blockchain banking requires banks to develop new risk management frameworks to deal with smart contract threats, AML compliance, and security of transactions. Mid-managers have to learn how to regulate the financial system without centralisation, use cryptographic security, and develop risk avoidance mechanisms (Fard, Roper, & Hess, 2016). The greater application of quantum computing in banking and cybersecurity will also necessitate employees to be familiar with quantum encryption methods and new and improved cybersecurity systems to protect financial against emerging threats. (Figure 2.1)

In this evolving context, the FinTech readiness of both technology enablers and users must be systematically assessed. As this study emphasises, workforce adaptability and organisational preparedness are not isolated; they are deeply interconnected. Therefore, understanding how institutions and individuals co-evolve with technology is critical for shaping the future of digital banking in India..

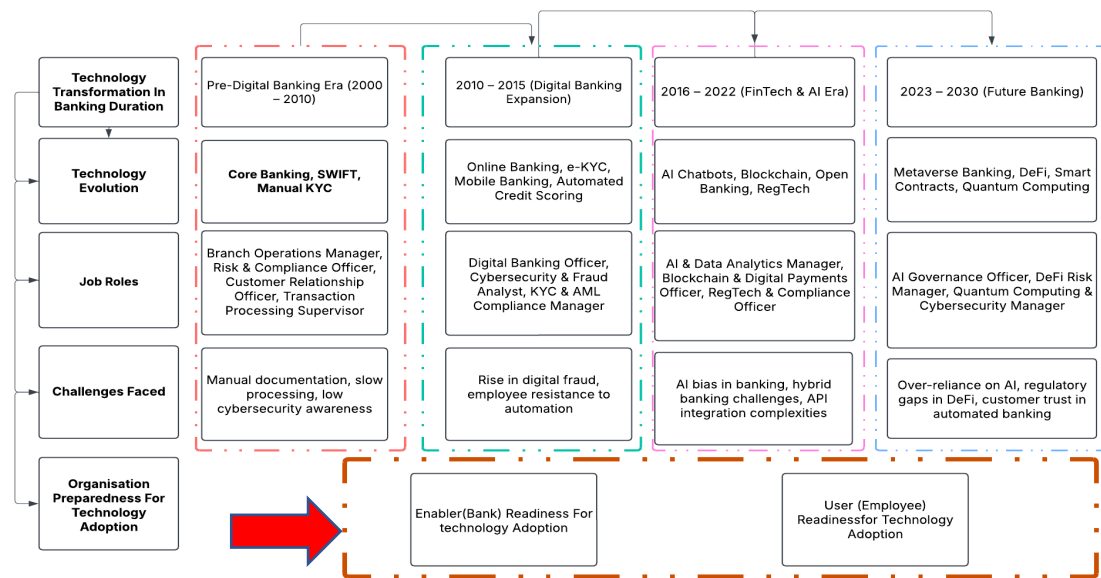


Figure 2.1 Banking Ecosystem Project Architecture

2.3 PHASE -II: INDICATORS IDENTIFICATION FOR TECHNOLOGY USERS AND TECHNOLOGY ENABLERS (INPUT)

The adoption of advanced financial technologies is not only a problem to the employees but also a problem to banks. Technology will always keep changing, but the banks and the employees cannot stand still since they should be adaptable and vigilant to maintain the competitive advantage. A number of driving forces affect the capacity of the two parties to integrate and use technology. The obstacles to fintech preparedness should be examined systematically to know what prevents banks to implement emerging technologies and why employees find it hard to follow suit. Throughout the impending technological change, it is not something that can be considered optional by financial institutions. Rather, they should take initiative to overcome the constraints that hinder a smooth adoption. A way of solving these challenges is to first unravel the factors that determine technology readiness both through the eyes of the employee and the bank.

There should be a systematic framework to harness the willingness of the financial institutions and their labor. Banks are technology enablers who invest in automation, cybersecurity, and compliance with regulations whereas employees are technology users. Evaluation of the preparedness of both sides will help the banks to make sure that the adoption of Tech-based decision-making, the integration of DeFi, and quantum security of information is properly integrated into financial services without disrupting the operations of the firms. According to

previous studies, the most prominent challenges include lack of skills in technology literacy among workers (Venkatesh, Thong, & Xu, 2016), attitude to automation because of job insecurity (Frey & Osborne, 2017), technical security issues in the activities of tech-powered banks (Taddeo & Floridi, 2018), and legal restrictions on the growth of technology and DeFi (Arner, Barberis, & Buckley, 2016). These aspects give rise to systematized assessment of technological preparedness to facilitate workforce change. We simultaneously obtain employee (technology user) and institutional (technology enabler) views, which are typically absent in the literature.

A number of theoretical frameworks have been used in previous research to evaluate the preparedness of the banks and employees to adopt new technology. The Technology-Organisation-Environment (TOE) Model (Arpaci, Yardimci, Ozkan, & Turetken, 2012) measures the alignment of technological, organisational, and environment by the financial institutions towards digital transformation. The concept of the adoption by banks as an institution of new technologies is explained by the Diffusion of innovation (DOI) Theory (García-Avilés, 2020) which is described by the perceived benefits and institutional culture in an incremental manner. Technology adoption behaviours have been greatly assessed using Technology Acceptance Model (TAM) (Davis, G.B., & Olson, 1985). Extended TAM is based on both employee and organisational factors, which is why it was applied to the introduction of technology and automation (Stewart & Jürjens, 2018a). The ETAM model evaluates the employee preparedness through determining the factors affecting the adoption of technology. It is also the bank-readiness; organisational enablers, including cybersecurity investments, infrastructure, and adherence to regulatory guidelines are considered (Jing et al., 2024). Also, it looks at the influence of the preparedness of a bank regarding employee adoption behaviour with reference to training, compliance initiatives, and risk mitigation. The Unified Theory of Acceptance and Use of Technology (UTAUT) (Jinger et al., 2023) discusses the influence of employee behaviour on the use of technology as affected by the performance expectations, social influence, and enabling conditions. Although these models are helpful, they fail to explain the readiness of both employees and banks in the situation of technology adoption. Attitudes, beliefs and behavioural intentions towards technology adoption have always been measured using the Technology Acceptance Model (TAM), Extended Technology Acceptance Model (ETAM), and other models. Though these models have been effective in analysing the user readiness, they do not take into account the organisational or systemic enablers. Conversely, such models as the Unified Theory of Acceptance and Use of Technology

(UTAUT) focus more on organisational readiness, infrastructure, and facilitating conditions, but do not pay much attention to individual behaviour. In order to assess the level of FinTech preparedness amongst the Indian banking industry both at institutional and employee levels, a composite theoretical framework is followed, which integrates variables in TAM, ETAM and UTAUT. A mixed method enables the simultaneous evaluation of behavioural, infrastructure, cultural and strategic variables. By doing so, the dynamics of employee adoption, as well as institutional enablers are both analysed in-depth. A combination of these views would help to gain a better picture on technology readiness.

The first stage of the research is used to establish a set of variables that can be applied to gauge FinTech preparedness in the Indian banking industry. These variables can be categorized into two broad areas in order to show the dual-layer approach that is taken in the study: individual-level indicators that consist of technology users (employees) and enabler-level indicators that consist of technology enablers (banks and institutions). The recognition is based on the theoretically developed models, such as the Technology Acceptance Model (TAM), TAM2, the Unified Theory of Acceptance and Use of Technology (UTAUT), and the Socio-Technical Systems theory. A selection of variables is made using the empirically relevant variables, the theoretical significance of variables, and variables in the data. (Discussed in Table 1)

The initial set of variables at User level is under the core beliefs, especially those explained by the TAM. This encompasses Perceived Usefulness (PU) - the conviction that employee job performance is enhanced by technology-based banking tools - that defines the willingness of the employees to take up the tools (Tahar, Riyadh, Sofyani, & Purnomo, 2020). The second variable is Perceived Ease of Use (PEOU) is the perceived ease of using technology and is a determinant of adoption because it removes reluctance (Walczuch, Lemmink, & Streukens, 2007). These opinions create the psychological base of the early adoption of FinTech solutions.

The second group in the category of individual-level indicators consists of the Personal Capabilities cluster, which is an operational and skill-related facilitator of technology adoption. The variables, in this case, are - Technology Self- Efficacy (TSE), which embodies the confidence of the employees in the usage of digital platforms and reflects training requirements (Alnoor, Al-Abrow, Abdullah, & Abbas, 2020); Digital Literacy (DL), the possibility to navigate and operate digital applications, that influences the daily operations and flexibility (Rovira-Garcia, Juan, Sanz, & Gonzalez-Casado, 2015); and Digital Readiness (DR), the willingness to use innovative banking

The third group of variables are included in the cluster of Risk and Trust factors that include psychological and behavioural obstacles to adoption. Perceived risk (PR) is the worry of losing a job, and data security that prevents openness to change (Gurung, Luo, & Raja, 2008). The Trust in Technology (TT) is defined as the confidence of the employees in digital decision-making systems (Dai, Duan, & Zhang, 2020), whereas the Cybersecurity Awareness (CSA) can be described as the presence of the knowledge of the threats and mitigation measures, thus contributing to the increase of the trust and safe usage (Georgiadou, Mouzakitis, Bounas, & Askounis, 2022). Anxiety of automation and effects on employment continuity is measured by Job Security Concerns (JSC) based on (Frey & Osborne, 2017)

Facilitating Conditions is the second enabler construct cluster, outlined by UTAUT. This incorporates the Facilitating Conditions (FC), which implies the availability of supportive infrastructure, resources, and training systems to support the use of technology (Uddin, Mollah, & Ali, 2020). The Employee Reskilling Investment (ERI) summarizes the amount of budget used to take care of the needs of workforce transformation, upskilling, and developing confidence (Jinger et al., 2023). The other important criterion is AI Infrastructure Readiness (AIR), which is an indicator of how the legacy systems have been modernised to facilitate AI applications (Nortje & Grobbelaar, 2020).

The last enabler group is Governance and Compliance Factors that are essential in the controlled world of banking. Regulatory Alignment (RAI) evaluates the bank's compliance with legal and regulatory technology standards, helping build trust in adoption and avert risk (Arner, Zetzsche, Buckley, & Kirkwood, 2024). Cybersecurity Investment (CSI) quantifies investment in securing digital systems, enhancing the risk of breaches and making it more resilient (Novelli, Taddeo, & Floridi, 2024). Every variable is accompanied by a measurable proxy, which can be obtained either via secondary databases (RBI reports, NPCI, NASSCOMS, TRAI, NSSO, CERT-IN, and other bank disclosures) so as to assure that the study will have access to credible and structured data to apply not only statistical analysis but also machine learning models to the obtained data. All these indicators of user- and enabler-level constitute the empirical foundation of categorizing the levels of adaptability, constructing the indices of readiness, and suggesting the strategic interventions during the subsequent stages of the research (Table 2.1).

Table 2.1 Technology Preparedness of Indian banks - Employee and Bank Variables (Prepared by authors)

LEVEL	CONSTRUCT CLUSTER	VARIABLE	DEFINITION	JUSTIFICATION	REFERENCE
USER-LEVEL INDICATORS (USER)	Core Beliefs (TAM)	Perceived Usefulness (PU)	Belief that Technology-driven banking tools will enhance job performance.	Determines employee willingness to adopt Technology-based tools for efficiency.	(Tahar et al., 2020)
		Perceived Ease of Use (PEOU)	Perception that Technology-based technology is user-friendly.	Affects adoption rates by reducing the reluctance toward technology.	(Walczuch et al., 2007)
	Personal Capabilities	Technology Self-Efficacy (TSE)	Employees' confidence in using Technology-based banking platforms.	Determines skill gaps and training needs in financial operations.	(Sappri, Baharudin, & Raman, 2016)
		Digital Literacy (DL)	Ability to work efficiently with digital applications.	Necessary for effectively navigating digital banking tools.	(Chen et al., 2020)
		Digital Readiness (DR)	Preparedness for banking innovations involving technology.	Measures adaptability to digital transformations.	(Gurung et al., 2008)
	Risk & Trust Indicators	Perceived Risk (PR)	Concerns about job displacement and data insecurity.	Addresses psychological barriers to adoption.	(Georgiadou et al., 2022)
		Trust in Technology (TT)	Confidence in digital decision-making systems.	Affects willingness to use or rely on AI-based systems.	(Alnoor et al., 2020)
		Cybersecurity Awareness (CSA)	Knowledge of threats and mitigation in tech-enabled systems.	Enhances trust and risk management capacity.	(Nasution, Rusnandi, Qodariah, Arnita, & Windasari, 2018)
		Job Security Concerns (JSC)	Fear of automation replacing job roles.	Causes resistance to adoption due to employment anxiety.	(Cetindamar, Abedin, & Shirahada, 2021)
	Socio-technical Alignment	Human-AI Collaboration (HAC)	Willingness to collaborate with AI systems.	Reflects openness to tech-assisted roles and evolving work culture.	(Frey & Osborne, 2017)
ENABLER-LEVEL INDICATORS	System Characteristics (TAM2)	System Quality (SQ)	Performance and reliability of digital platforms.	Affects perceived usefulness and actual usage.	(Fedele, Punzi, & Tramacere, 2024)
	Compatibility/Image (TAM2)	Human-AI Collaboration (IHAC)	Repeated for system alignment lens.	Also represents how well AI integrates into job roles.	(Nortje & Grobbelaar, 2020)
	Facilitating Conditions (UTAUT)	Facilitating Conditions (FC)	Availability of resources, training, and support.	Enables smoother adoption and actual use.	(Arner et al., 2024)
		Employee Reskilling Investment (ERI)	Investment in workforce upskilling.	Helps bridge digital skill gaps and builds confidence.	(Taddeo & Floridi, 2018)
		AI Infrastructure Readiness (AIR)	Bank's tech infrastructure and readiness for AI.	Determines backend support for front-end tech implementation.	(Venkatesh et al., 2016)
		Regulatory Alignment (RAI)	Alignment with legal and data compliance norms.	Builds trust and reduces regulatory risk in adoption.	(Ali & Osmanaj, 2020)
		Cybersecurity Investment (CSI)	Strategic investments in fraud detection and digital safety.	Reduces perceived risk and increases trust in digital systems.	(Tahar et al., 2020)

With the fast technological growth in the banking sector, it is no longer adequate that the banks and the employees act in isolation when it comes to the adoption of technology. It is necessary to have a coordinated strategy with both organisations developing to successfully integrate Fintech, DeFi, and quantum computing (M. M. Rahman, Elshamly, ur Rehman, Jameel, & Hameed, 2023). Automation opposition, training shortage, security risks in cyberspace, and legal obstacles should be addressed in a systematic manner (Chhabra Roy & Prabhakaran, 2025). The digital transformation can be proactively tackled by banks through the use of a well-organized framework, which would not leave employees behind but would implement the tech-based banking services effectively and safely.

2.4 PHASE III- CATEGORISING ADAPTABILITY AND IDENTIFYING KEY PARAMETERS FOR EFFECTIVE TECHNOLOGY ADOPTION

Evaluating the technological readiness will be important in the process of enabling banks and employees to optimise their acculturation to technology and financial innovations. Although previous research papers have measured multiple consequences of technology implementation like the acceptance level, the improvement of the employee performance, the effectiveness of risk mitigation, the outcome of compliance, these indicators tend to measure individual aspects of the digital transformation. Despite the insights they are valuable, they never give a complete picture of how banks and employees as entities will adjust to the changes in technology and also do not help to classify the institutions or individuals in terms of their ability to adjust to the changes in the future. The aim is to determine which banks are more capable of adapting to new technologies and which employees are highly or lowly adaptable in the use of technologies. Through the creation of organized lists of adaptivity, financial institutions would be able to design their strategies of digital transformation proactively instead of merely reacting to operational inefficiencies as they occur.

This categorization will have a number of advantages to banks. To start with, highly adaptable banks could be a core benchmarking institution and could offer a good insight as to best practices to be adopted, investment in the digital infrastructure, and workforce training strategies. Conversely, those banks that prove to be less adaptable can receive specific intervention measures, such as more advanced reskilling, more refined regulatory frameworks, and improved cybersecurity infrastructure, to assist in closing the digital gap. Under this strategy, a systematic map will be provided to banks to enhance their operational resilience during the era of technological changes.

In the workforce management, it is essential to differentiate the flexibility of employees to enable banks to distinguish employees who are more open to technological change and those who struggle to integrate workflow based on technological changes in their daily activities. High adaptable workers can become useful change agents within the company, enhance the transfer of knowledge, coach their colleagues, help them to avoid digital surprises. On the other hand, the less adaptable employees should be offered employee-specific training programs and upskilling sessions as well as formal career advancement plans, which will help them keep up with the current technological change. This business strategy will help reduce workforce alienation, as it will make sure that the process of digitalization will augment the workforce and not displace it.

The research sorts banks and employees and the main parameters that motivate the adaptability are identified. Though a particular bank or staff member can demonstrate different degrees of adaptation, it is important to know the signs which lead to such categories. There are parameters that will define the capability of a bank or employee to embrace technology without any problems. It is crucial to identify these parameters, as it allows financial institutions to identify certain areas of weaknesses in their tech adoption frameworks.

A bank can be faced with the issue of inflexibility not simply due to lack of interest but due to lack of cybersecurity investments, misaligned regulation, or aged information technology infrastructure. On the same note, an employee may not want to attain the use of technology not because he or she does not want to but because of the lack of digital skills, the absence of the exposure to technology in making decisions or the fear of losing the job. Mapping these regulatory indicators can be used to determine that there are certain areas where a bank should intervene and as a result, it is able to ensure that the right challenges are addressed by the right solutions.

The main goal of this classification based outcome measure is to provide a formulaic approach to the integration of technologies in banks. This study will allow banks to develop customized interventions to close their adaptability gaps rather than using a one-size-fits-all approach. This is to make sure that the financial institutions are not just embracing new technologies just because it is innovative but rather they are integrating them into their operations and workforce frameworks in a way that will bring about long term sustainability.

Finally, the technological development will keep on increasing and banks will need to adjust to such changes. Nevertheless, not every bank or its employees has the same degree of preparedness with regard to facing FinTech disruptions. To increase digital transformation efforts, financial institutions can create specific approaches that improve their digital transformation path by classifying adaptability and determining key contributing indicators. This classification driven solution will be of a good resource to financial institutions. It will enable them to mitigate certain weaknesses, develop systematic strategies of incorporating FinTech, and streamline the transformation of workforce to maintain order in operations and a regulatory environment in a digital environment.

2.5 ROOT CAUSES CREATE VARIATION IN THE SEVERITY OF INDICATORS

2.5.1 USER PERSPECTIVE — ROOT CAUSES OF LOW FINTECH READINESS

Psychological, skill, and trust are factors that influence the adoption of FinTech by employees in banks, as they either adopt it, use it, or champion the new technologies. Low perceived usefulness and ease of use, poor technology self-efficacy, unequal digital literacy, low digital readiness, perceived risk concerns, low trust in automation, poor cybersecurity awareness, job security anxieties, and challenges in working with AI systems are also key employee-side root causes. The variables of the TAM/UTAUT theories are these factors, and perceived usefulness and ease of use are the main antecedents of the technology adoption (Davis, G.B., & Olson, 1985).

We have found that the skills gap and self-efficacy of employees are severe. Senior employees and those in the branches are found to have low digital fluency and inadequate exposure to hands-on practice platforms (Udayakumar, Joshi, Boomiga, & Sugumar, 2023). The major causes of this are a lack of systemic training and structured upskilling programs (Vellinga et al., 2001). In cases where employees are not properly trained, and they are not assured that they can use new technologies, it is difficult to adapt. Psychological risks have also slowed the use of technology, such as fear of data abuse, responsibility, and loss of a job. There were system outages or hacks, and, therefore, the trust towards technology and readiness to use it decreases among employees (Guha & Indurkar, 2020). Unless the employees clearly observe the productivity improvements, or the interfaces are complicated to them, interchangeability to technology is higher (Ismail & Haq, 2024; Uddin et al., 2020).

On the institutional (bank) side, several of the same problems are organisational in nature. Disconnected IT systems and legacy complications create a friction phenomenon and are not

user-friendly at a scale (Alawida, Omolara, Abiodun, & Al-Rajab, 2022; Said, J., Bakri, H.H.M. and Karim, 2015). The inadequate investment in reskilling programs and ongoing digital learning ecosystems limits the self-efficacy of the employees and the potential of the bank to redeploy the workers to digital-related jobs (Narsimha et al., 2022). Poor governance of cybersecurity, insufficient budgets on protective infrastructure, and missing incident response strategies are all valid concerns of information security and exposure to fraud (Neha Chhabra Roy, 2024; Vajjhala & Venu Gopal Rao, 2021). Lastly, the lack of explicit AI regulation and unified human-AI systems of work creates ambiguity of operations and regulatory risk (Malgieri, 2019; Sari & Celik, 2021). Therefore, the interaction between employee and bank factors occurs. The lack of institutional preparedness decreases staff preparedness and trust. In the meantime, workplace anxieties and low digital skills are helping to sustain institutional change, making the institutional change a vicious cycle.

2.5.2 ENABLER PERSPECTIVE - ROOT CAUSES OF LOW FINTECH READINESS

In the enabler or institutional approach, the underlying causes of the low FinTech preparedness rates among the Indian banking institutions can be broadly grouped into infrastructure, governance, investment, and general ecosystem maturity. The organisational ability to digitalise is impaired by systemic limitations, which have direct impacts on the technology infrastructure and the flexibility of the human resources. There are a number of important obstacles to institutional technology adoption. The structural inefficiencies associated with frequent system downtime, poor scalability, and the presence of both outdated and newer systems decrease technological flexibility and agility. Outdated core systems continue to be used by many banks that are not easily upgraded to the modular upgrades and API integrations necessary to implement FinTech solutions, which are important in a faster fashion, including open banking, real-time payments, and AI analytics (Farrugia, Zerafa, Cini, Kuasney, & Livori, 2021; Garcia-Segura, 2024). This technical momentum does not only slow innovation, it makes more expensive to combine systems that face the customers and those that support the back end. The other important weakness is the absence of well-developed human-AI collaboration models. There is a lack of institutional policies that determine the ways in which the employees approach automated systems and regulate the algorithms. This absence of regulation causes regulators and employees to be unsure of the dependability and responsibility of AI decision-making. Lack of transparent audit trails and human-in-the-loop system exposes institutions to compliance failures as well as human opposition to automation (Aizenman, Ito, & Pasricha, 2022).

It is common in branches of smaller towns and semi-urban areas to have little IT support, poor vendor management, and a poor maintenance culture (Akinbowale, Klingelhöfer, & Zerihun, 2022; Coy, Lambert, & Miller, 2016). These, particularly in regional branches, also lead to uneven FinTech preparedness and imbalance in service levels and fragmented technology experience across the range of the operational network of the bank. The gap generates operational bottlenecks and weakens the faith of customers in online channels. The other reason that limits the digital transformation is underinvestment in employee reskilling and cybersecurity infrastructure. Most banks have not established learning and continuous upskilling channels, and do not have allocated sufficient funds to this process, which causes technology stagnation within the workforce (Chhabra Roy & Prabhakaran, 2023; Chhabra Roy, 2020). On the same note, insufficient funding for cybersecurity solutions exposes institutions to insider-based fraud and external cyberattacks. Empirical data points to the fact that these weaknesses are enhanced by the lack of a consistent cyber awareness campaign and institutionalised incident response exercises (Masum & Parker, 2020).

With the fast development of the regulatory guidance (particularly the Reserve Bank of India (RBI), the National Payments Corporation of India (NPCI) and the Securities and Exchange Board of India (SEBI), compliance has become an ever-changing goal. Lots of institutions are unable to understand and apply them because of their disjointed compliance frameworks and ineffective coordination of legal and technology (Aizenman et al., 2022; Zharova & Lloyd, 2018). Regulatory anomalies also contribute to the physical hindrance in the technology preparedness of banks. Lastly, the organisational culture and strategic digital roadmap weaknesses can be found. Most banks do not have well-defined ROI frameworks or internal communication systems to link technology investments to business value, despite the large-scale transformation projects (Schwab Klaus, 2021). Lack of collective aims and digital metrics based on performance prevents the congruence between the vision of the leadership and operational performance. Such institutional inadequacies not only restrict technological capacity but also erode trust and flexibility of employees (Table 2.2). The table below will summarise the key root causes found in the literature and align them with the FinTech readiness indicators applied in the study. These root causes provided a standard for further mitigation planning.

Table 2.2 Variables for Primary Data and Proxy for Secondary Data Generated for Parallel Analysis (Prepared by authors)

Primary Data Results – User Perspective						Secondary Data Results – Enabler Perspective			
	Level	Variable	Var. Abbr.	Root Cause for indicators Severity (Employees)	Root Cause – High Severity (Banks)	Suggested Proxy Indicator	Proxy Abbr.	Root Cause – High Severity (Employees) 2	Root Cause – High Severity (Banks) 2
1	User-Level	Perceived Usefulness	PU	Lack of clarity on the benefits of new technology; resistance due to perceived workload increase (A. Das & Das, 2023; Dootson, Beatson, & Drennan, 2016)	Inadequate communication of tech benefits; weak alignment between technology goals and business outcomes (Ferreira & Sandner, 2021)	Adoption Rate of FinTech/AI Applications	ARAA	Low perceived personal benefit from digital tools (Sivapragasam, Agüero, & de Silva, 2011)	Lack of ROI measurement on technology outcomes (N.C. Roy & Vishwanathan, 2018b)
2		Perceived Ease of Use	PEOU	Complexity of systems; poor UI/UX; insufficient hands-on support (Montagnani et al., 2024)	Legacy systems and non-integrated platforms causing process friction (Wang, Asif, Shahzad, & Ashfaq, 2024)	Customer Complaint Ratio on Tech Use	CCRTU	Lack of user training (Carminati, Caron, Maggi, Epifani, & Zanero, 2015)	Outdated software integration (Ksieniewicz, Woźniak, Cyganek, Kasprzak, & Walkowiak, 2019)
3		Technology Self-Efficacy	TSE	Low confidence in using AI/FinTech tools; fear of making errors (Fedele et al., 2024)	Inadequate digital up-skilling programs (Kshetri, 2005)	Digital Training Hours per Employee	DTHE	Limited exposure to practice platforms (Pratt, Holtfreter, & Reisig, 2010)	Insufficient investment in digital learning ecosystems (Choithani et al., 2024)
4		Digital Literacy	DL	Lack of digital awareness or technical fluency among older employees (Hacker, 2023)	Workforce heterogeneity and uneven training coverage (Roy & Vishwanathan, 2018)	Internet & Mobile Penetration Rates	IMPR	Low basic tech skills (Martinez, Viles, & G. Olaizola, 2021)	Uneven infrastructure between urban/rural branches (Shen, 2024)
5		Digital Readiness	DR	Lack of motivation to use new systems; dependency on manual processes (Nasution et al., 2018)	Fragmented IT systems, absence of digital culture (Shaikh, R. Glavee-Geo, 2017)	% Digital Banking Usage	DBU	Skill mismatch (Zinchenko, Pervichko, & Akatova, 2014)	Absence of strategic digital roadmap (Button, Hock, Shepherd, & Gilmour, 2023)
6		Perceived Risk	PR	Fear of data misuse, privacy invasion, or job loss (Belhouchette, Berkane, & Belhadeh, 2019)	Weak cybersecurity governance and unclear accountability (S. Agarwal, Ghosh, Ruan, & Zhang, 2024)	Incidence of Fraud Reports	IFR	Anxiety over data exposure (Guo, Habich-Sobiegallo, & Kostka, 2023)	Lack of real-time fraud monitoring (Carminati et al., 2015)
7		Trust in Technology	TT	Low trust due to system failures or poor past experiences (Madan L Bhasin, 2016)	Data breach history; absence of robust AI explainability frameworks (Singh, Mehtre, & Sangeetha, 2022)	% Customer Migration to Digital Channels	CMD	Scepticism toward automation (Narsimha et al., 2022)	Low transparency in algorithmic decisions (Madan Lal Bhasin, 2016)
8		Cybersecurity Awareness	CSA	Limited awareness of phishing, ransomware, or cyber hygiene (Sivapragasam et al., 2011)	Inadequate investment in cybersecurity training and internal drills (Choithani et al., 2024)	Cybersecurity Training Coverage	CTC	Poor threat perception (Siregar & Tenoyo, 2015)	Gaps in incident response planning (Lodhia & Mitchell, 2022)

9		Job Security Concerns	JSC	Fear of automation-induced redundancy (Fuchs, Nguyen, Nguyen, & Schaeck, 2023)	Workforce downsizing linked to tech modernisation (Das & Ganguly, 2024)	Employee Layoff/Automation Ratios	ELAR	Low sense of career continuity (Donald, Baruch, & Ashleigh, 2023)	Cost-cutting pressures due to digital transition (Olmo, Saiz, & Azofra, 2021)
10		Human-AI Collaboration	HAC	Difficulty adapting to AI-enabled decision systems (Adewumi & Akinyelu, 2017; Kanchan, Patibanda, & Gorti, n.d.)	Lack of frameworks integrating AI and human workflows ((Malgieri, 2019)	Ratio of Tech-Supported Job Roles	RTSR	Confusion over task delegation between AI and human inputs (Dunphy, 2024)	Unclear AI governance models (M. J. Rahman & Zirur, 2023)
11	Enabler-Level	System Quality	SQ	Repetitive errors or lags reduce trust in digital systems (Chhabra Roy & Prabhakaran, 2024)	Frequent downtime, poor scalability ((Jenab & Moslehpour, 2016)	Downtime Frequency per Quarter	DFQ	Low confidence in system reliability (Tsai & Su, 2021)	Under-investment in infrastructure redundancy (Stewart & Jürjens, 2018b)
12		Human-AI Collaboration (Inst.)	IHAC	Resistance to automated supervision tools (Halima Oluwabunmi Bello, Courage Idemudia, & Toluwalase Vanessa Iyelolu, 2024)	Lack of AI-human integration policies (Montagnani et al., 2024)	Ratio of Tech-Supported Job Roles	RTSR	Unclear task boundaries (Bonilla, Blanco, Zarza, & Alarcón-Padilla, 2022)	Unstandardized AI policy frameworks (Sunrise & Elizabeth, 2019)
13		Facilitating Conditions	FC	Limited IT support and troubleshooting accessibility (van Daalen, 2023)	Poor IT infrastructure and maintenance culture (Morais & Khaled, 2017)	IT Infrastructure Index	ITII	Lack of peer tech support (Gaur, 2020)	Fragmented vendor management (Wang et al., 2024)
14		Employee Reskilling Investment	ERI	Lack of structured learning pathways (Chhabra Roy & Prabhakaran, 2023b)	Absence of budget prioritization for skill renewal (Bhargava et al., 2021)	% Budget Allocated to Tech Reskilling	BATR	Skill stagnation (Mukhopadhyay, Chatterjee, Bagchi, Kirs, & Shukla, 2019)	Budgetary constraints or competing financial priorities (Moschella & Tsingou, 2013)
15		Tech Infrastructure Readiness	AIR	Lack of access to modern tools; reliance on outdated systems (Mantelero, 2014)	Dependence on legacy systems; delayed migration (Wang et al., 2024)	% Legacy Systems Migrated to Tech-Ready Infra	LSMARI	Perception of outdatedness (Bajwa, Ahmad, Mahmud, & Bajwa, 2023)	Integration delays and compatibility issues ((von Grafenstein, Jakobi, & Stevens, 2022)
16		Regulatory Alignment	RAI	Confusion over compliance requirements; lack of awareness of digital policies (Lacey, Goode, Pawada, & Gibson, 2020)	Delays in adapting to RBI, SEBI, and NPCI digital guidelines (Eric & Richard, 2019)	Tech Policy Compliance Score	AIPCS	Ambiguity on digital ethics (Martinez et al., 2021)	Fragmented compliance structure (Masum & Parker, 2020)s
17		Cybersecurity Investment	CSI	Lack of employee access to security tools or awareness programs (Wang et al., 2024)	Budget shortfall for cybersecurity infrastructure (A. Das & Das, 2023)	% IT Budget for Cybersecurity	ITBCS	Insufficient protection literacy (Allen, 2024)	Underfunded cybersecurity measures (Bajwa et al., 2023)

2.6 STRATEGIC MEASURES TO ENHANCE BANKS' AND EMPLOYEES' READINESS FOR FUTURE ADOPTION

Measuring technological preparedness cannot be complete without establishing strategic actions that financial institutions and their staff can implement to bolster preparedness to bank using technology and the new financial technologies. In the past, the banks and their employees have proposed different strategies of adapting to the digital transformation, such as upskilling, changes in regulations, modernisation of infrastructure, and governing policies. Using the wisdom of these strategies that have been adopted in the past, it is possible to identify what has worked, the current pitfalls, and new actions that must be implemented to facilitate the smooth adaptation of innovations in the future. Many financial institutions have tried different strategic plots to deal with the threats of FinTech, digital banking and automation. Table 2 below provides the main actions taken by the banks and employees in the past, with their respective implications with regard to technological preparedness.

2.6.1 MITIGATION STRATEGIES FROM THE USER PERSPECTIVE

On the side of the user, user-oriented interventions should strive to create trust, trust in computer transformation, and reliance. One of the beginning steps is the design and delivery of role-based and practical training programs. Programs comprising structured learning with simulated learning interventions and scenario-based laboratories can improve technology self-efficacy and decrease fear of errors (Alnoor et al., 2020). Measures of outcomes may be in the form of proxy measures, including Digital Training Hours per Employee (DTHE), and also through observed task performance improvement. The establishment of psychological safety and career continuity routes is also important. The risk of being replaced can be lowered by upskilling guarantees, reskilling scholarships, and internal mobility programs, which help the employee to move into digital jobs (Eric & Richard, 2019). The question of developing trust in technology is about transparency, explainable AI (XAI) schemes, writing down the logic of algorithms and spreading the concept across all levels of employees to relieve scepticism. Lastly, scheduled cyber hygiene trainings and mock exercises can significantly contribute to cybersecurity awareness and, thus, decrease insider threats and enhance employee awareness (Chhabra Roy & Prabhakaran, 2023b; Roy & Viswanathan, 2020).

To increase perceived usefulness, effective communication and co-creation are also required. Pilot projects, feedback loops, and change design, which involve employees, would contribute to aligning the adoption of technology with both daily reality and perceived value and ownership. Perceived ease of use can be further enhanced by simplifying the digital interfaces, maintaining constant assistance through UX/UI optimisation and fast response help desks (Bajwa et al., 2023).

2.6.2 MITIGATION STRATEGIES FROM THE ENABLER PERSPECTIVE

There should be institutional-level strategic, technical, and governance interventions to boost FinTech readiness. The most urgent need is the modernisation of the basic infrastructure. Banks need to shift to API-first, cloud-portable systems by migrating high-impact legacy systems (e.g., the LSMARI proxy) to make sure that they are modularly scaled and can exchange data with other systems (Nawari & Ravindran, 2019; Rohit, Arun, Sushil, & Rajni, 2018). At the same time, organizations are supposed to implement an effective system of AI and data governance. These must provide transparency, accountability and ethical AI practice policies, backed by audit trails and human oversight procedures (Mangala & Kumari, 2017). Regulatory sandboxes will allow safe experimentation with emerging FinTech models.

Institutionalisation of reskilling investment should be done by having special learning budgets and competency frameworks. Continuous digital learning must be a percentage of HR or IT budgets, and the outcomes of this measure have to be measurable in terms of performance and career advancement. Cybersecurity is an investment and not a cost of operation. It is possible to increase the cybersecurity (ITBCS proxy) portion of the IT budget, accompanied by red-teaming exercises and regional incident-response playbooks, which can greatly increase resilience (Chhabra Roy & Prabhakaran, 2024).

Moreover, it is essential to enhance the enabling environment and vendor management. Unity in the quality of the infrastructure in different regions can be achieved through standardised procurement, explicit Service Level Agreements (SLAs), and an active approach to vendor risk assessment (Aizenman et al., 2022; Coy et al., 2016). Lastly, digital ROI and outcome-based metrics should be integrated into strategic planning, and the institutions should tie the digital adoption rates and the frequencies of downtime (ARAA, DBU, DFQ) to KPIs of leadership. This forms the basis of making technology decisions based on business value and accountability (Masum & Parker, 2020) (Table 2.3)

Table 2.3 Strategies used in the Past by Employees and Banks to enhance their Preparedness for Technology Enhancement
(Prepared by authors)

Strategy Domains	Strategy	Description	Impact on Readiness	Reference
Strategies Implemented by Enablers	AI-Driven Reskilling Programs	Banks introduced AI training and data analytics programs to equip employees with future-ready skills.	Increased AI literacy and reduced workforce resistance to automation.	(Subramanian, Riya, & Rajendran, 2024)
	RegTech Compliance Frameworks	Adoption of AI-based regulatory technology (RegTech) to ensure seamless compliance and governance.	Improved regulatory alignment for AI-based banking operations.	(Ryan, Crane, & Brennan, 2020)
	Cybersecurity & Risk Mitigation Measures	Investment in AI-based fraud detection, multi-layered authentication, and quantum encryption.	Strengthened data security and reduced financial cyber threats.	(Bentley, Stephenson, Toscas, & Zhu, 2020)
	IT Infrastructure Upgradation	Replacement of legacy banking systems with cloud computing, open APIs, and AI-based data processing.	Improved adaptability for AI-driven banking operations.	(Dahiya & Mathew, 2016)
	Human-AI Collaboration Policies	Formulation of internal policies that promote AI-human collaboration instead of workforce replacement.	Reduced employee fear of job displacement and encouraged AI integration.	(Fragiadakis, Diou, Kousiouris, & Nikolaidou, 2024)
	DeFi Risk Management Strategies	Development of specialised DeFi risk assessment and compliance models.	Enhanced preparedness for the adoption of decentralised finance (DeFi).	(Jensen & Ross, 2020)
Strategies Implemented by Users	Technology Certification Programs	Employees pursued specialised AI, FinTech, and blockchain certifications.	Improved competency in handling AI-powered banking tools.	(Randall & Zirkle, 2005)
	Peer Learning & Mentoring	Internal knowledge-sharing sessions and AI-driven mentoring initiatives.	Accelerated AI adaptation through workplace collaboration.	(Stone, Cooper, & Cant, 2013)
	Gamified AI Training Models	Use of interactive learning platforms and AI simulations for skill enhancement.	Increased employee engagement in AI skill acquisition.	(Suresh Babu & Dhakshina Moorthy, 2024)
	Participation in FinTech & AI Bootcamps	Employees engaged in FinTech hackathons and AI-driven innovation challenges.	Strengthened digital readiness and problem-solving skills.	(Almansour, 2023)
	Regulatory & Compliance Upskilling	Training in AI ethics, cybersecurity compliance, and regulatory frameworks.	Enhanced understanding of AI governance in banking.	(Nwokediegwu et al., 2024)

These historical strategies have enabled banks and employees to navigate past digital transformations, ensuring they remain competitive and well-prepared for the evolving financial landscape. However, as the complexity of AI-driven automation, decentralised finance (DeFi), and quantum computing security grows, it is essential to implement additional measures to ensure comprehensive readiness for future technological advancements.

3. CHAPTER 3

RESEARCH METHODOLOGY

This research will examine multiple dimensions of enabler (banks') and user (employees') readiness for Tech-driven job roles, evaluating institutional preparedness and workforce adaptability. The study will employ empirical data collection, expert interviews, and machine learning-based analytical methods to assess the impact of emerging technologies on banking operations and the workforce, thereby evaluating their preparedness. A structured framework will be followed to analyse technology readiness from both the enabler and user perspectives, thereby suggesting strategic measures for tech adoption.

3.1 DATA - PRIMARY SURVEY AND SECONDARY DATA

The growing integration of Fintech, digital automation, and cybersecurity into banking operations requires a thorough assessment of the adaptability of enablers and users. This research adopts a mixed-methods approach, combining primary and secondary data to evaluate FinTech readiness in the banking system from user (employee) and enabler (organisational) perspectives. Primary data will be collected to gain insights into employees' beliefs, skills, and behavioural responses to technology adoption, as well as organisational preparedness for large-scale digital transformation in finance. The sample will comprise 15 public and private sector banks actively adopting financial technology, accounting for nearly 78% of technology expenditure over the past five years. Target banks include BoM, BoB, UCO, ICICI, CBI, Kotak, Union, IOB, IndusInd, SBI, IB, HDFC, IDBI, Axis, and DCB. Data will be sourced from middle-level banking professionals—managers, risk officers, compliance specialists, technology innovators, digital leaders, technology officers, Fintech experts, and CTOs—with 2–15 years of experience. These professionals hold pivotal roles affected by digital restructuring. Data collection will utilise a semi-structured questionnaire (dummy annexure -I) distributed through various modes: email, online video interviews (Zoom/Teams), phone calls, face-to-face meetings, and focus group discussions. The structured questionnaire used in this study comprises three key sections. Part A captures respondent demographics and job-related details such as designation, experience, and department. Part B assesses fintech and technology readiness using a series of items mapped to key constructs at both the user and enabler levels (e.g., perceived usefulness, digital literacy, system quality, infrastructure). Part C explores strategic and behavioural responses to digital transformation. All items in Parts B and C are assessed using a 5-point Likert scale ranging from Strongly Disagree (1) to Strongly Agree (5).

The detailed questionnaire is enclosed in the annexure. Approximately 30-50 officials per bank will be surveyed, since the people involved in such a domain may be limited, and we will try to authenticate the responses only from relevant people who have witnessed several technological transformations. Respondents will be selected from technology-driven metropolitan and Tier-1 cities such as Delhi, Mumbai, Bengaluru, Kolkata, Chennai, Hyderabad, Lucknow, Pune, Ahmedabad, and Kanpur. A non-probabilistic purposive sampling method will focus on professionals directly engaged in tech-enabled operations and digital restructuring.

The authors believed that collecting responses from users alone might yield a biased perspective; thus, they also relied on secondary data to validate it from an enabler (bank) perspective. Secondary data will supplement primary findings and help validate proxy indicators for user and enabler readiness. The authors chose only proxy indicators that are suitable for the variables listed in Table 3 and that are available in the public domain. The hypothetical proxies and data collection will be challenging; the authors ignored them. These proxies will be sourced from reputable entities such as the Reserve Bank of India (RBI), NASSCOM, IBA, IDRBT, NPCI, DSCI, banks' investor presentations, and industry reports and research databases. Detailed proxy secondary indicators are discussed in Section 3.2 for each identified variable. Notably, annual secondary data for each selected bank will be gathered from 2020 to 2025. In the context of studying fintech innovation and technology readiness in Indian banks, the chosen five-year period from 2020 to 2025 is critical. This timeframe captures the accelerated digital transformation driven by the COVID-19 pandemic, regulatory push, and rising fintech collaborations. While the ideal plan is to collect quarterly or monthly data to capture finer trends, such granular data may not be uniformly available across banks. In such cases, annual data will be used. To address potential limitations, a normalisation process will be applied to extrapolate intra-year trends, given that the pace of fintech adoption typically progresses incrementally within a financial year, making annual data a reasonable and practical proxy. This temporal data collection will enable the study to capture digital acceleration before and after COVID-19, as well as emerging trends in technology adoption and digital risk management. By triangulating structured primary data with institutionally verified secondary data, the research aims to deliver evidence-based insights into user readiness, organisational strategy, and the digital transformation journey of Indian banks.

2.2 OBJECTIVE 1- IDENTIFICATION OF TECHNOLOGY READINESS INDICATORS

To identify key indicators influencing the adoption of emerging technologies among Technology Users (employees) and Technology Enablers (banking institutions). In both domains, prominent indicators are selected and identified based on foundational technology adoption theories such as the Technology Acceptance Model (TAM), the Extended TAM, and the Unified Theory of Acceptance and Use of Technology (UTAUT) (as discussed in section 3.2). To ensure the empirical validation of each conceptual variable, a measurable and reliable proxy indicator is assigned to each selected variable, corresponding secondary data sources are identified, and a few sources from which data are collected are also highlighted in Table 3. This facilitates both data triangulation and contextual validation across selected Indian banks. The proxies are aligned with national datasets, regulatory disclosures, industry reports, and institutional dashboards. The entire set of indicators and their proxies, along with sources, is highlighted in Table 3.1.

Table 3.1 Suggested Driving Forces for Employees and Banks to Ensure Long-term AI/Tech adaptation (Prepared by authors)

Level	Variable	Var. Abbr.	Suggested Proxy Indicator	Proxy Abbr.	Secondary Data Source	Information
User Level	Perceived Usefulness	PU	Adoption Rate of Fintech/AI Applications	ARAA	RBI Reports, Bank Fintech/AI/IT Usage Reports	Kotak Mahindra Bank - More than 90% of retail loan decisions in FY25 were handled by Kotak's proprietary AI/ML models, which reduced gross NPA formation by 18% from the previous year. Generative AI was used for customer query resolution, risk, and compliance. (Annual report of Kotak Bank) Yes Bank: YES ROBOT, the Microsoft Azure-powered AI banking chatbot, launched as the first always-on, conversational AI... NLP, ML models, and predictive analytics... YES Bank deployed analytics for SME/retail loan segmentation, marketing, and acquisition
	Perceived Ease of Use	PEOU	Customer Complaint Ratio on Tech Use	CCRT U	RBI Ombudsman, Consumer Complaints Database	Customer grievances filed with the Reserve Bank of India's (RBI) Ombudsman Offices saw a marginal increase in FY25, reaching 2.96 lakh complaints, up from 2.93 lakh in the previous fiscal year, according to the RBI's annual report released on May 29. Common customer issues pertained to loans and advances, as well as digital banking products, areas that remain particularly vulnerable to customer dissatisfaction. The RBI attributed the steady rise in complaint volumes to growing consumer awareness and outreach. During the year, the central bank conducted 47 town hall meetings and 239 awareness programmes, specifically targeting user groups such as students, senior citizens, and women. RBI Governor Sanjay Malhotra specifically called out that AI and technology could help address consumer complaints, especially those arising from digital interfaces like ATM failures, erroneous charges, or mis-selling via digital banking
	Technology Self-Efficacy	TSE	Digital Training Hours per Employee	DTHE	Bank CSR/HRD Reports, Skill India Dashboard	Kotak Mahindra Bank (FY 2023–24) - Average total training hours per employee: 41.0 hours, composed of ~21.0 hours of classroom training and ~20.0 hours via digital Learning Management System (LMS). This includes both functional and digital topics, though there is no separate breakdown just for digital-specific training. The indicator is certified by Price Waterhouse Chartered Accountants LLP. Source - https://www.valueresearchonline.com/stories/1269AC46-20F8-4CEB-A434-DE7A35818195/news-announcement/?utm_ Yes Bank (FY 2023–24) Total training hours per employee: 19.81 lakh hours across the bank, averaging about 14,73,312 hours delivered to 76,030 employees, which equates to roughly 26 hours per employee. Only 8% of programs were online, suggesting digital/digital-leaning content was relatively limited relative to total training hours. Source - https://www.scribd.com/document/871140826/CB-Sustainability-Report-2023-24-Digital-Version?utm_ Market Data Report 2025 by Gitnux (HR in the Banking Industry) This source estimates about 20 training hours per employee annually, directly in banking institutions—well below recommended levels—while noting that banks typically allocate approximately 2.5% of payroll to training and development
	Digital Literacy	DL	Internet & Mobile Penetration Rates	IMPR	TRAI, IAMA, Census, NSSO	1. As of April 2024, overall internet penetration in India stood at ~55.3%, which is below the global average, with stark rural–urban disparities: urban internet subscriptions per 100 population exceeded rural by over 2x. Just 9.9% of rural households had a computer compared to 32.4% in urban areas. Source - https://economictimes.indiatimes.com/industry/banking/finance/banking/digital-tech-adoption-has-improved-efficiency-of-banks-increased-competition-on-sector-rbi-rcf-report/articleshow/112102722.cms?utm_ 2. The Reserve Bank of India (RBI) has said its digital payments index (DPI) increased 4.45% to 465.33 in September 2024, up from 445.5 in March 2024. The rise in RBI-DPI was propelled by a stronger payment infrastructure and enhanced transaction efficiency across the country. The RBI has been publishing the digital payments index (DPI) since 2021, keeping March 2018 as a base. Source -

					https://www.fortuneindia.com/macro/rbis-digital-payments-index-rises-445as-of-september-2024/120225?utm_
Digital Readiness	DR	Digital Banking Usage (% of Total Transactions)	DBU	RBI Digital Payment Reports, NPCI	Kotak - 163% growth in UPI transaction volume from Mobile Banking App (Q4FY24 vs Q4FY23). source - https://www.kotak.com/content/dam/Kotak/investor-relation/Financial-Result/Annual-Reports/FY-2024/kotak-mahindra-bank/Error-Clarification-Integrated-Annual-Report-2023-24.pdf Bank of Baroda - WhatsApp Banking users grew from 6.16 lakh to 14.04 lakh; transactions increased from 47.8 lakh to 207.5 lakh in FY22. Source - Source: Annual Report 2021–22
Perceived Risk	PR	Incidence of Fraud Reports	IFR	NCRB, CERT-IN, RBI Annual Reports	1. Yes Bank - No fraud or data loss incidents reported under Section 143(12) of Companies Act for 2021. 2. In FY24, India witnessed a sharp surge in cyber-fraud related to banking transactions, with the number of reported cases rising almost fourfold—from 75,809 cases in FY23 to 2,92,743 cases in FY24. The total monetary loss also spiked significantly, from ₹421.4 crore to ₹2,054.6 crore. H-value frauds (involving ₹1 lakh or more) rose dramatically from 6,699 cases to 29,082 cases over the same period. Maharashtra accounted for over 25% of the total losses, followed by Tamil Nadu with around 23%. Private sector banks were disproportionately affected, with Kotak Mahindra Bank, Axis Bank, HDFC Bank, ICICI Bank, and SBI together responsible for 62% of the total fraud value and 53% of the total cases. This alarming rise is attributed to the rapid growth of digital payments—rising from 162 crore in 2012–13 to over 14,700 crores by February 2024—outpacing the general population’s awareness and digital literacy, making users more vulnerable to phishing, impersonation, and AI-powered scams. Source - https://www.thehindu.com/data/cyber-fraud-in-banking-transactions-surges-in-fy24-data/article68813626.ece
Trust in Technology	TT	% Customer Migration to Digital Channels	CMD	Bank Annual Reports, RBI Payment System Data	Within five years, 44% of banks expect more than 50% of their deposits to be mobilised online. About 33% of banks expect more than 50% of their lending to be processed digitally by the same time frame. Source - https://bfsi.economictimes.indiatimes.com/news/policy/digital-set-to-grab-lions-share-of-bank-deposits-and-credit-disbursals-says-rbi-survey/112233212?utm_
Cybersecurity Awareness	CSA	Cybersecurity Training Coverage	CTC	CERT-IN, RBI, Bank Internal Reports	RBI’s Master Direction on IT Governance, Risk, Controls & Assurance Practices (effective April 1, 2024) mandates formal cybersecurity governance, including regular training for employees, customer awareness, and supervisory involvement by the board and CISOs. HDFC Bank In FY 2024, HDFC Bank conducted over 16,000 virtual fraud awareness sessions across India, covering more than 200,000 participants, including staff, customers, and various community segments. A dedicated session attended by over 5,000 employees in June 2024 focused on digital fraud tactics and safe banking practices, led by a former Mumbai Police Commissioner Media Bulletins. The bank routinely observes a monthly “Cyber Jagrookta Diwas”—in-training workshops for branch staff to promote safe digital usage. SBI deployed a mix of micro-learning tools and hybrid digital options, including podcasts, virtual case-study forums, gamified quizzes, and internal webinars, with reach of 110,000–111,000 unique users during FY 2023. A Digital Leadership Programme covered 386 senior officials through a classroom module at ISB Hyderabad, focusing on risk awareness and digital safety practices. Institution-wide compliance coaching interventions were rolled out in 638 branches, emphasizing risk culture and cybersecurity awareness.
Job Security Concerns	JSC	Employee Layoff/Automation Ratios	ELAR	Bank HRD Reports, NSSO Employment Survey	Automation and AI adoption have significantly shrunk middle-tier support roles: The officer-to-support staff ratio shifted from 50:50 in FY 11 to 74:26 in FY 23, signalling a sharp decline in clerical and routine jobs Reserve Bank of India. Source - https://timesofindia.indiatimes.com/business/india-business/digital-push-is-driving-out-mid-level-banking-staff-rbi/amp_articles/112121208.cms?utm_H turnover rates—exceeding 30% in private banks during FY 23—reflect restructuring and job displacement due to digital transformation Source - https://timesofindia.indiatimes.com/business/india-business/digital-push-is-driving-out-mid-level-banking-staff-rbi/amp_articles/112121208.cms?utm_

	Human-AI Collaborati on	HAC	Ratio of tech-supported Job Roles	RTSR	Bank HR Tech Adoption Reports	1, The Tech-related keyword frequency in private sector banks' annual reports rose nearly six-fold in FY 2022-23 compared to FY 2015-16; for public sector banks, it increased more than three-fold in the same period. 2. The study also found that banks with larger asset sizes and stronger capital ratios (CRAR) exhibited significantly Her AI adoption scores, suggesting that more resource-rich banks are leading the shift toward AI technologies
Enabl er Level	System Quality	SQ	Downtime Frequency per Quarter	DFQ	Bank IT/Infra Audit Reports	BOB: "IT uptime maintained above 99.9% across core services." HDFC: "They Themaintained 99.94% uptime, supporting H transaction volumes and a secure digital infrastructure."
	Human-AI Collaborati on (rep.)	IHAC	Ratio of Tech supported Job Roles	RTSR	Bank IT/Infra Audit Reports	Kotak 2025: More than 400 digital and engineering professionals were hired in FY25, bringing technology roles to 21% of the bank's white-collar workforce Over 2,800 staff undertook AI/ML upskilling programs in FY25, achieving an 83% certification rate. https://economictimes.indiatimes.com/industry/banking/finance/banking/kotak-mahindra-bank-plans-to-hire-400-engineers-to-ramp-up-tech-transition/articleshow/109945197.cms https://www.kotak.com/content/dam/Kotak/investor-relation/Financial-Result/Annual-Reports/FY-2025/kotak-mahindra-bank/Kotak-Managements-Discussion-and-Analysis_FY-2024-25.pdf
	Facilitating Conditions	FC	IT Infrastructure Index	ITII	MeitY, NITI Aayog	Bank of Baroda - 70% of enterprise workloads were virtualized and over 1,200 branches transitioned to cloud-enabled infra (FY21 Annual Report).
	Employee Reskilling Investment	ERI	% Budget Allocated to Tech Reskilling	BATR	Annual Reports, HR Disclosures	The RBI also surveyed bank respondents in November 2024 and found that cloud and AI/ML were the top emerging technologies adopted, chiefly in customer service, risk management, and KYC functions. Yet, banks still allocated less than 10% of their IT budget to emerging tech, and over 80% had outsourced these implementations. Source - https://www.business-standard.com/technology/tech-news/cloud-ai-ml-top-emerging-techs-adopted-by-indian-banks-reveals-rbi-survey-124123000947_1.html?utm_
	Tech Infrastructu re Readiness	AIR	% Legacy Systems Migrated to Tech-ready Infra	LSMA RI	CIO/CTO Disclosures, IDC/NASSCO M Insights	75% of the virtual servers in the total server base at the Bank https://www.kotak.com/content/dam/Kotak/investor-relation/Financial-Result/Annual-Reports/FY-2025/kotak-mahindra-bank/Kotak-Managements-Discussion-and-Analysis_FY-2024-25.pdf Bank of Baroda 2021: 70% of enterprise workloads were virtualized and over 1,200 branches were transitioned to cloud-enabled infrastructure environments (Bank of Baroda Annual Report)
	Regulatory Alignment	RAI	Tech Policy Compliance Score	AIPCS	RBI/NITI AI Policy, Bank Compliance Reports	Kotak Mahindra Bank- Information systems are ISO 27001 certified, and we conduct regular third-party security evaluations to ensure their robustness https://www.bsigroup.com/en-IN/products-and-services/assessment-and-certification/validation-and-verification/client-directory-profile/KOTAK_-0047299142-002
	Cybersecuri ty Investment	CSI	% IT Budget for Cybersecurity	ITBCS	CERT-IN, Bank Audit Reports, PwC/KPMG Sector Studies	HDFC Bank spends 6-7 per cent of its overall expenses on technology-related aspects every year. https://economictimes.indiatimes.com/industry/banking/finance/banking/hdfc-bank-says-6-7-pc-of-overall-

At the user level, the variable Perceived Usefulness (PU)—which captures employees’ belief that technology enhances job performance—is validated through the Adoption Rate of tech Applications (ARTA). This proxy can be derived from RBI’s IT usage disclosures and internal bank IT implementation reports. Perceived Ease of Use (PEOU), which reflects how user-friendly banking technologies are perceived, is linked with the Customer Complaint Ratio on Tech Use (CCRTU). This is sourced from the RBI Ombudsman database and consumer grievance portals, which regularly track and publish trends in complaints related to digital channels. Technology Self-Efficacy (TSE), measuring confidence in using banking platforms, is operationalised through Digital Training Hours per Employee (DTHE), available from bank-level HRD or CSR disclosures or consolidated in the Skill India Dashboard. For Digital Literacy (DL), which assesses the ability to navigate digital tools, the proxy is Internet and Mobile Penetration Rates (IMPR), drawn from TRAI, IAMAI, Census, and NSSO digital inclusion surveys. The broader construct Digital Readiness (DR)—indicating preparedness for transformation—is measured using Digital Banking Usage (DBU) as a percentage of total transactions, with data extractable from RBI Digital Payment Reports and NPCI dashboards. In the category of Risk and Trust Indicators, Perceived Risk (PR) is reflected by the Incidence of Fraud Reports (IFR), which are publicly available via CERT-IN, RBI Annual Fraud Reports, and NCRB databases. Trust in Technology (TT), which gauges confidence in digital decision-making, is proxied by the % of Customer Migration to Digital Channels (CMD)—accessible through bank annual reports and RBI Payment System statistics. Cybersecurity Awareness (CSA) is assessed through Cybersecurity Training Coverage (CTC), data for which is often found in bank-level training disclosures, internal audits, and CERT-IN compliance assessments. Job Security Concerns (JSC), which indicate resistance due to automation anxiety, are validated using Employee Layoff/Automation Ratios (ELAR), measurable via NSSO Employment Surveys, and bank HR department records. Lastly, the user-level variable Human-AI Collaboration (HAC), which reflects openness to working with tech-assisted systems, is validated through the Ratio of tech-Supported Job Roles (RTSR). This can be traced in Bank HR reports, tech adoption disclosures, or industry HR benchmarking studies conducted by NASSCOM and sector councils. At the enabler level, System Quality (SQ)—a core TAM2 variable denoting the performance and reliability of digital platforms—is proxied by Downtime Frequency per Quarter (DFQ). These figures are generally recorded in internal IT audit reports and bank infrastructure dashboards. The enabler-side view of Human-AI Collaboration (IHAC) is again validated via IRTSR, aligning with its dual relevance across users and systems. Under the Facilitating Conditions cluster, Facilitating Conditions (FC)—which indicate the availability

of institutional support such as training and resources—are measured using the IT Infrastructure Index (ITII). This data is publicly available through MeitY reports, NITI Aayog e-readiness indices, and industry infrastructure disclosures. Employee Reskilling Investment (ERI) is validated through the % Budget Allocated to Tech Reskilling (BATR), which is available in bank annual reports, HR disclosures, and strategic transformation documents. Similarly, Tech Infrastructure Readiness (TIR) is captured through the % of Legacy Systems Migrated to AI-ready Infrastructure (LSMARI), retrievable from CIO/CTO disclosures, NASSCOM AI readiness surveys, and industry digital maturity benchmarks. In the Governance and Compliance Indicators, Regulatory Alignment (RAI) is assessed via the AI Policy Compliance Score (AIPCS), reflecting the bank's adherence to RBI/NITI digital guidelines and internal compliance audits. These scores can be constructed using policy disclosures and AI ethics frameworks published in RBI Circulars or institutional digital governance reports. Finally, Cybersecurity Investment (CSI) is proxied by the % IT Budget for Cybersecurity (ITBCS), a figure typically disclosed in bank cybersecurity audits, PwC/KPMG banking sector studies, and public financial filings. Through this proxy-based design, the study ensures that all indicators are not only conceptually robust but also empirically traceable and grounded in the Indian banking ecosystem. This dual validation—drawing from both theoretical models and observable data—lays the foundation for further classification, pattern analysis, and model testing in subsequent phases.

The study focuses on both behavioural and structural dimensions of adoption; gathering data through both primary and secondary sources is deemed essential. The primary data will be collected using surveys and Focused Group Discussions (FGDs) with professionals from the banking and financial technology sectors. A semi-closed questionnaire will be used to ensure consistency while also allowing for context-rich responses. Secondary data were collected for each variable by selecting one close and meaningful proxy indicator from relevant databases and institutional sources. These proxies reflect the operational or measurable equivalent of the constructs identified from the literature, ensuring real-world relevance. For convenience and transparency, secondary data has already been compiled for a few major banks and stored in a separate Excel file, which will be shared with this submission via email.

3.3 OBJECTIVE 2(A): BANKS CLASSIFICATION IN ADAPTABILITY GROUPS FROM THE USER PERSPECTIVE-SECONDARY DATA ASSESSMENT

To achieve the second objective—classifying banks based on their tech adaptability from an enabler standpoint—the study adopts a comprehensive secondary data-driven methodology. For each enabler variable, a suitable proxy indicator is identified to realistically and reliably reflect the variable's operationalisation. These proxies, summarised in Table 3, were collected from Data for five financial years (2019–20 to 2024–25). When only quarterly or monthly data is available, interpolation will be performed using mean and standard deviation-based spreading to generate annualised monthly data and ensure consistency across years. Furthermore, the indicators are passed to a machine learning algorithm, which classifies them into various groups using Equations 3.1 –3.3.

$$TAP = f(\text{user Readiness, enabler Readiness}) \text{-----Eq (3.1)}$$

$$TAP = f(\text{core belief; personal capabilities; Risk and trust; Socio} \\ \text{-- technical alignment; system characteristics; Compatibility; Facilitating Conditions}) \\ \text{-----Eq(3.2)}$$

$$TAP = f(PU; PEOU; TSE; DR; PR; TT; CSA; JSC; HAC; SQ; IHAC; FC; ERI; AIR; RAI; CSI) \text{---(3.2)(a)}$$

$$TAP = f(ARAA; CCRT; DTHE; IMPR; DBU; IFR; CMD; CTC; ELAR; RTSR; DFQ; ERTSR; ITII; BATR; LSMARI; AIPCS; ITBCS) \text{---(3.2)} \\ \text{(b)}$$

$$TAP = \alpha + \beta_1 * ARAA + \beta_2 * CCRT + \beta_3 * DTHE + \beta_4 * IMPR + \beta_5 * DBU + \beta_6 * IFR + \beta_7 * CMD + \beta_8 * CTC + \beta_9 * \\ ELAR + \beta_{10} * RTSR + \beta_{11} * DFQ + \beta_{12} * ERTSR + \beta_{13} * ITII + \beta_{14} * BATR + \beta_{15} * LSMARI + \beta_{16} * AIPCS + \\ \beta_{17} * ITBCS \text{-----Eq (3.3)}$$

The dependent variable, banks' technological adaptability (TAP), a Fintech/Tech Investment Flag, is used as the binary dependent variable. This indicator captures whether a bank has shown strategic commitment to digital transformation through investments in emerging technologies (e.g., AI, cloud, blockchain, cybersecurity) or partnerships with fintech firms. Data is sourced from secondary public disclosures—annual reports, investor presentations, press releases, and digital transformation updates—further validated using databases like Bloomberg, Tracxn, and Crunchbase for the period 2020–2025. A threshold-based rule classified banks as tech-adaptable (1) if they met any of the following: (i) investment $\geq$ INR 100 crore in digital initiatives, (ii) ≥ 2 fintech partnerships, or (iii) reported migration to cloud or AI-based systems. Banks not meeting these criteria are marked as non-adaptable (0). This binary transformation enabled integration into a supervised machine learning classification model. However, further for independent

variables, proxy data is considered as passed on in the previous equation, as mentioned earlier. The data is passed through a machine learning algorithm.

A growing body of literature explores the application of machine learning techniques to detect and predict technology preparedness. Ku, Chen, and Chiu (2007) propose a novel preparedness index approach based on machine learning techniques, including random forest, artificial neural networks, and support vector machines. Several machine-learning techniques have been used to evaluate tech readiness, including logistic regression, decision trees, neural networks, and support vector machines. Fanai and Abbasimehr (2023) propose combining convolutional neural networks and long short-term memory networks to detect technology preparedness for digital transformation adoption. Adewumi and Akinyelu (2017) analyse network traffic data for technology readiness using unsupervised learning algorithms, including clustering and anomaly detection. Awoyemi, Adetunmbi, and Oluwadare (2017) investigate machine learning techniques for detecting the evolution of mobile payment systems, such as logistic regression, decision trees, and random forests. Several methods exist for predicting and prioritising (Baesens, Höppner, & Verdonck, 2021; Balakrishnan, Khan, & Arabnia, 2020a; Deilami & Kamruzzaman, 2017; Roy & Prabhakaran, 2022), but the easiest, fastest, and most accurate methods are recommended. An assessment of TPI presents unique challenges: a low false-positive rate is essential for successful prediction (Ben-Asher & Gonzalez, 2015). Reducing the false-positive rate when dealing with technology-readiness indicator assessment data is challenging. False-positive rates can affect business continuity, as incorrectly imposing technology on employees can bring work to a halt and lower employee morale; sometimes, the new way of imposing technology in banks is not always accurate (Li, Zhang, Masum, Shahriar, & Haddad, 2020). These issues must be addressed carefully. The RF method will be applied to prioritise and predict technology-prepared indicators due to similar specific characteristics of organisations, such as banks' readiness, including class imbalance, unstructured data, and multicollinearity (Li et al., 2020; Mustapha, 2018; Saravanan, Kannan, & Thangaraj, 2012).

RF as a tool is the best option for handling H-dimensional data (Balakrishnan, Khan, & Arabnia, 2020b). It is individually associated with TPI and reduces class imbalance problems and uncertainty with tech imposition events. It possesses several characteristics of ensemble learning that make it a versatile approach. The data will be split into two proportions before being processed into the supervised algorithm (training and test data in the proportion of 80:20. The

most appropriate model will be selected based on accuracy.¹, true positive rate² (TPR), true negative rate³ (TNR), false-positive rate⁴ (FPR), false-negative rate⁵ (FNR), sensitivity⁶, and specificity⁷. Specify whether the RF model best fits the provided data (details in Section 4.4). Using RF, the importance of indicators is predicted and prioritised. The prominence of the indicator in terms of impact can be captured. The data is arranged and processed to prioritise technology preparedness indicators, providing more accurate and reliable results to inform the prioritisation and prediction of the importance of tech preparedness indicators as high, medium, and low.

RF method can classify TPIs with their level of adaptability using Variable Importance Measures (VIMs) and display TPIs with the Hest predictive power. It can also predict the importance of future indicators by constructing the regression model. The classification stage involves grouping similar indicators at the ends of decision tree branches and then grouping similar trees to gauge the adaptability of the indicator. In this process, several group trees or models are made via randomly changing inputs and the best model is selected using an Out of Bag (OOB) error. OOB errors are used to prioritise and choose among all generated models. The Her the error, the less reliable the model. Later, the model depicts Mean Decline Accuracy (MDA)⁸ and Decline Gini coefficients (DGC)⁹ values to project the importance of each derived indicator. The importance (VIM) is measured by considering MDA/DGC values and is divided by the OOB estimations. This way, the derived values are ranked, and unimportant indicators are removed from the model until only significant indicators remain. Once the importance of indicators is Hlighted, it is categorised as H, medium, or low adaptability. Authors classify the adaptability of banks by considering each indicator's MDA/ DGC values and comparing them with the average MDA/ DGC values (average MDA/ DGC across all TPI). H-adaptability indicators are

¹ How precisely the measured value or findings reflect the real or the original values

² True Positive Rate refers to the proportion of those with the condition who received a positive result

³ TNR ratio of true negative and total negative is an effective measure to assess the rate at which non-fraud events are detected through the model - it should be high

⁴ FPR is an effective measure to assess the rate at which the non-fraud events are detected as fraud through the model; the ratio of the false-positive and total negative should be low since non-indicators are identified as indicators which affect the efficiency of the bank

⁵ FNR is an effective measure to assess the rate at which fraud events are not detected through the model - riskier for the banks if ignored, since the ratio of false-negative and totally positive should be low for an effective model

⁶ The proportion of affected individuals with a positive test result

⁷ The Specificity is the True Negative Rate and refers to the percentage of people without the condition who received a negative result on this test

⁸ The mean decrease in accuracy - is a method of computing the feature importance on permuted out-of-bag (OOB) samples.

⁹ Gini importance (or mean decrease impurity), is a set of Decision Trees, with a set of internal nodes and leaves in each. An internal node is used to divide the data into two separate sets with similar responses.

derived values more than double the average value, medium indicators have values higher than average, and low indicators have values lower than average (equation 3.4).

In the RF process, after indicator prioritisation, the most severe indicators involve a partial plot and show an individual impact between each indicator and TAP. It may detect the impact weight potential of each indicator on TAP. RF analysis will be conducted to assess the adaptability of indicators. Further, significant and consistent indicators will be investigated to minimise their impact. Once the major indicators have been identified and the model has been validated, mitigation measures are recommended. The prediction model is based on accuracy, True Positive rate (TPR), True Negative rate (TNR), False Positive rate (FPR), False-negative rate (FNR), sensitivity, specificity, and detection rate. The entire study will be conducted using Python scripts in Google Colab to fit regression models, perform RF classification, compute MDA & DGC values, and Generate Partial plots. If values are more than double the average in both MDA and MDG cases, we call the variable H (H); if both MDA and MDG values are less than double the average but greater than average, we call it medium; and if values fall below average, then we call the indicators Low adaptable indicator.

$$TAP = F(HIGH_{cf}, MEDIUM_{cf}, LOW_{cf}) \text{-----Eq (3.4)}$$

After preparing the indicators under L, M and H adaptable categories, a Preparedness Index will be computed for each bank. The number of H, M, and L values will be counted for each bank. These are then used to compute a weighted average preparedness index (PI) using equation (3.5)

$$Preparedness\ index(PI) = \frac{3 * H + 2 * M + 1 * L}{Total\ indicators} \dots \dots \dots (3.5)$$

This score is then normalised across all banks to bring comparability, and banks are plotted on a distribution curve. Using a slope change In this method, thresholds are identified to split the PI into two categories: High Adaptability Banks (HAB) and Low Adaptability Banks (LAB). Now, for HAB and LAB classification, for each bank, the average preparedness index is calculated using an averaging approach that combines all banks' data and estimates the average PI for all banks, known as the average PI (API). A bank is classified as HAB when the API is compared with its PI value; if the PI of the bank is > API, then we call the bank under the highly adaptable category (HAB), or else we call the bank under the low adaptable category (LAB). This systematic, data-centric approach ensures robust classification of banks into tech adaptability segments based on Enabler's perspective, validated secondary data proxies, highlights prime

indicators contributing to adaptability mismatches, and sets the stage for identifying institution-specific interventions and sector-wide policy directions.

3.4 OBJECTIVE 2(B): CLASSIFICATION BASED ON PRIMARY DATA (USER PERSPECTIVE)

To assess banks' employee-level adaptability to technology, a primary data survey is conducted to capture users' perspectives on technology adaptability. This phase focuses on classifying banks based on the preparedness of their internal workforce—an essential user-side perspective for assessing tech readiness. A structured questionnaire-based survey is administered among employees across selected banks. A target of 30–50 respondents per bank is set to ensure representativeness, including operational-level staff and managerial personnel to mitigate bias and reflect a balanced organisational view. Currently in mid-review stage the respondents are collected from each bank though initially planned were 30 but up to mid review stage, the responses which came out are summarised in table below, where we found few banks has more representation i.e., ICICI banks, HDFC banks, Axis bank etc. the reason for more representation is that we run associated programs with the respective banks however few banks we found less representation i.e., union banks, bank of Maharashtra etc. but since it is a mid-review we are still trying to get some more responses. We will make sure by the final review that the complete bank's bare minimum responses will be collected, and again the analysis will be performed. Overall, across 15 banks, the responses we collected till mid review, while we are submitting a report, are 511. (Table 3.2)

Table 3.2 Bank wise responses collection for mid review

BANK	RESPONSES
AXIS	30
INDIAN BANK	30
ICICI	88
BOB	30
HDFC	33
INDIAN OVERSEAS BANK	30
IDBI	30
KOTAK	30
INDUSIND	30
DCB	30
SBI	30
YES	30
UCO	30
UNION	30
BOMH	30

To classify indicators into HAB and LAB category the authors focused solely on employee survey responses for each indicator. Average weights were calculated accordingly, across two domains, each containing ten and seven indicators respectively. For scoring, equal weights ($\frac{1}{2}$

each) are given to both domains. Within each domain, the total score is equally divided among sub-indicators (e.g., if 10 indicators exist under user readiness, each carries a weight of 0.05; if six indicators exist under enabler readiness, each carries ≈ 0.083). The weights were estimated using Equation 3.3. The subsequent classification of indicators into HAB and LAB categories was based on comparing normalized indicator weights (W_n) with the average weights (A_w) of a domain: $W_n = A_w IR_i$ ----- (3.6) If $W_n > A_w$, then the indicator is classified as H, M and L again using the same policy if the indicator weight is more than $2 \cdot A_w$ we call it H indicator but if indicator weight is in between $A_w < W_n < 2A_w$ we called indicator moderate or else it is treated as Low. this way every indicator is classified as H, M and L categories. further authors applied the same approach for all banks and then later like Eq 3.5 the banks are classified into HAB and LAB category after counting the H, M and L indicators and placing them in equation 3.5, this way EPI's are being calculated. further if specific banks EPI is greater than average EPI thus banks were classified as HAB else we classify them in LAB category. this way using primary data authors have classified banks again into HAB and LAB category. using LAB and HAB classifications using both EPI and UPI authors compared the banks preparedness is high at which side whether it is high from both EPI and UPI or any one area or it is low in both sides this way authors compared both ways banks and found similar and dissimilar banks.

3.5. OBJECTIVE 3 & 4: SUGGESTING MITIGATION MEASURES TO TECHNOLOGY USERS AND ENABLERS BACKED BY ROOT CAUSES AND SUGGESTING AN INTEGRATIVE FRAMEWORK

Building upon the dual-layer classification of adaptability from both secondary (HAB/LAB) and primary data (HAB/LAB), Objective 3 identifies root causes of low adaptability and suggests targeted mitigation measures for both technology enablers and users. Here, the authors explored the root causes of the variation in the severity of that indicator role, which were extracted from the literature review in section 2.5. Further, the severity and root causes are used together. Authors proposed a dual-layer mitigation measure where each low-category indicator is treated as highly severe, as it contributes less to preparedness. Further, using the root cause linked to each low indicator associated with banks, the root cause is mapped. further using banks severity level and prominent root causes the mitigation measure are suggested. The classifications provide a structured lens offering a clear understanding of their strengths and weaknesses across strategic, infrastructural, and behavioural dimensions. For each bank, the indicators most responsible for low adaptability—linked to leadership commitment, investment priorities, regulatory alignment, or employee-level skills and behavioural readiness—are systematically

traced back to earlier analyses. This ensures that mitigation measures are evidence-based and context-specific rather than generic recommendations.

The mitigation strategies are developed with a dual orientation both severity and root causes and those directed at technology enablers, i.e, leadership teams, IT departments, and regulatory authorities, and those directed at technology users, primarily bank employees and operational staff. this way enablers, the emphasis is on strengthening digital infrastructure, improving governance, and aligning policies with technological imperatives, whereas users, focus lies in upgrading skills, fostering a culture of digital acceptance, and building behavioural readiness for AI-driven banking transformation. Importantly, these recommendations draw upon best practices from High performing banks (HAB), which serve as benchmarks that LAB institutions can adapt. To ensure practicality and contextual relevance, the proposed measures are validated through focus group discussions (FGDs) and consultations with banking experts, enabling iterative refinement based on practitioner insights. The FGD was mostly planned as per annex I but on occasions few open ended questions were also asked.

finally, Objective 4 then synthesises these insights into a Dual-Layer Integrated Tech Adaptability Framework that captures enabler- and user-side perspectives. The framework integrates three key components: identification of adaptability indicators, classification of banks across both perspectives, Enabler and User (HAB/LAB), and bank-specific mitigation measures addressing root causes of low adaptability. By combining quantitative classification with qualitative validation, the framework ensures both analytical rigour and practical applicability. The outcome is a holistic, stakeholder-oriented model that provides actionable pathways for Indian banks to enhance their readiness for digital transformation, ensuring alignment between leadership strategies, infrastructural enablers, and employee adaptability. After synthesising the detailed processes across all objectives, the overall research methodology is summarised in the table below, Highlighting objectives, data sources, variables, methods, outcomes, and linkages to subsequent stages (Table 3.3)

Table 3.3 Summary of Research Methodology – Presented based on Objectives (Prepared by author)

Objective	Data Source	IVs / DVs	Method / Approach	Outcome / Derived Indicator	Linkage to Next Stage
Objective 1: Identification of indicators (User & Enabler side)	Literature review, expert consultation, regulatory reports	Not applicable (exploratory stage)	Thematic review & expert validation	Finalised set of User Readiness Indicators (URI) and Enabler Readiness Indicators (ERI)	Provides input variables for classification models in Obj. 2a & 2b
Objective 2(a): Classification using secondary data (Bank perspective)	Annual reports, investor presentations, press releases, Bloomberg, Tracxn, Crunchbase (2020–2025)	DV: TAP (Tech Adaptability Flag, binary 0/1) IVs: Proxy data – Tech investments ($\geq$ ₹100 Cr), fintech partnerships, AI/Cloud adoption, etc.	Binary classification model; supervised ML algorithm	Bank-level classification: HAB, MAB, LAB (H/M/Low Adaptable Banks – Enabler side) using PI	Root cause tracing for enabler gaps (feeds Obj. 3)
Objective 2(b): Classification using primary data (User perspective)	Structured employee survey (30–50 respondents per bank; staff & managers)	DV: Weighted Adaptability Score (0–100%) IVs: User readiness indicators (skills, behaviour, motivation) & Enabler readiness indicators (infrastructure, perception)	Weighted scoring, domain-wise normalisation, adaptability zone rules (>67% H, 33–67% M, <33% L)	User-based classification: HAB, LAB (Hly/Mly/Least Adaptable from user perspective)	Root cause tracing for user gaps (feeds Obj. 3)
Objective 3: Suggesting mitigation measures	Outputs from Obj. 2a & 2b, FGDs, peer benchmarking	DV: Adaptability Category (HAB/LAB & HAB//LAB) IVs: Root cause indicators traced from URI & ERI	Comparative analysis; FGD validation; peer best practice benchmarking	Bank-specific mitigation measures (indicator-linked, dual-layer: user + enabler)	Direct input for Obj. 4 (framework design)
Objective 4: Development of an Integrative Framework	Synthesised results from Obj. 1–3	IVs & DVs combined from all prior stages	Framework integration (quantitative + qualitative synthesis)	Dual-Layer Integrated Tech Adaptability Framework (DITAF) covering both users & enablers	Final output of the study

4. CHAPTER 4

BANKS PRIORITISATION AND INDICATORS SEVERITY ANALYSIS ENABLER CENTRIC APPROACH BACKED BY SECONDARY DATA

Following the collection of data, the authors first undertook the secondary data analysis, which indicates the enabler (bank-side perspective) of how adaptability is observable in individual banks in their search of secondary data. As banks post secondary data it presents a distinct image of the bank outlook. In doing so, the data as stated was gathered considering all 17 proxies in table 2.1 and also considering all the chosen 15 banks, depending on the present trend in annual report data between 2021-2025 as addressed in section (3.1). Moreover, the project will classify the banks into separate readiness groups to assess their readiness to changes that are brought about by the advent of fintech. The typology will be determined by technological flexibility, the level of the workforce skills, and the institutional preparedness. The banks and employees under lower adaptability categories will be suggested to be trained more on technology and to be improved in infrastructure and policy interventions in structured ways. This will make sure to use the best resources that are available to avoid wastage and simplify the process of integrating FinTech. As an example, Tech adoption strategies based on the similar classification have been effectively applied to the fintech sector of Singapore and to the European banking industry. These papers have shown that specific Technology training initiatives and policy changes led to Fintech literacy, operational efficiency, and regulatory compliance. With the aid of these success stories, the current study will deliver bank- and employee-specific strategies that will assist in a seamless digital transformation. The results of the proposed study are represented with the help of the data obtained with all 15 banks, and summarized cumulatively, as shown below. The project is supported by a certain set of variables, and the corresponding proxy variables have been named (Figure 4.1).

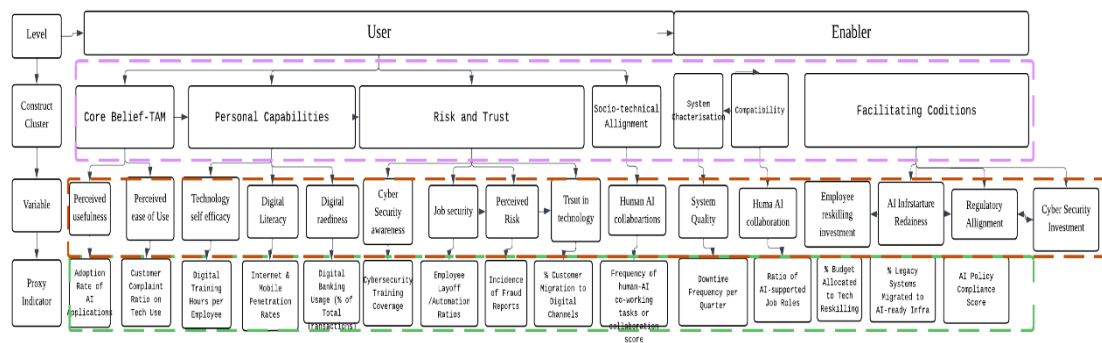


Figure 4.1 Summary of User-specific and Enabler-specific Indicators (Prepared by authors)

Once the information in both the secondary sources is obtained, the first step to classify banks by technology adaptability is done with the help of machine learning. Table 5 presents the input data set and the classification rules. Random Forest model has been found to be the best and therefore, it is chosen to analyze it further based on its performance in the metrics.

4.1 DESCRIPTIVE STATISTICS OF ALL BANKS DATA

The nature of the variables have been analysed first with a table of correlations and descriptive statistics before proceeding to the study on RF.1 Already, following cumulative banks, all the things have been exposed in detail: in the tables 4.1 and 4.2. The same is conducted later to each bank and reported in this report in annexures. As it looks into descriptive authors in the exploration of that panel of Axis, BOB, BOMH, DCB, HDFC, IB, ICICI, IDFC, IndusInd, IOB, Kotak, SBI, UCO, Union and Yes Bank, from 2020 to 2025, Annual summaries show consistent gains in front-end adoption, and continuing dispersion in back-end readiness and exposure. Table 4.1 summarised the descriptive statistics that show a summary of operational and behavioural patterns of 96 observations each indicator. The findings demonstrate significant heterogeneity as the high-variance factors like ITIII (mean = 2213.85; SD = 2342.84; max = 11844) and BATR (mean = 121.59; SD = 125.96; max = 670) have a high variability in the variable of technology investments and borrowing-related activities across banks. On the contrary, the parameters of stability generated by the system, such as CTC (mean = 0.757; SD = 0.134), LSMARI (mean = 0.862; SD = 0.132), and RAISR (mean = 0.171; SD = 0.081) exhibit narrower dispersion, which is also indicative of constant operational thresholds. Customer and channel performance measures/ statistics , including IMPR (mean = 81.64; SD = 11.61) and CMD (mean = 83.57; SD = 13.65), demonstrate moderate variability, but risk-linked measures, including IFR (mean = 95.396; SD = 63.121; max = 250), demonstrate oligopolar but irregular exposures. Such measures as DFQ (mean = 29.21; SD = 3.55) and ELAR (mean = 3.205; SD = 0.996) are relatively constant. On the whole, the large min-max paths and the different standard deviations reflect the behavioural differences by institutions implying different operational performance, liquidity statuses, risk aversity and capabilities in different banks due to technology.

Table 4.1 . Descriptive Statistics of Technology Readiness Indicators for all Listed Banks from 2020 to 2025 (Prepared by authors)

Statistic	count	mean	std	min	max
ARAA	96	0.531	0.249	0	0.95
CCRTU	96	5.906	9.661	0	91
DTHE	96	41.75	13.253	5	70

IMPR	96	81.635	11.607	48	97
DBU	96	87.585	12.14	19.25	99
IFR	96	95.396	63.121	10	250
CMD	96	83.565	13.648	19.25	99
CTC	96	0.757	0.134	0.43	1
ELAR	96	3.205	0.996	0	4.577
RAISR	96	0.171	0.081	0.01	0.4
DFQ	96	29.213	3.548	19.543	34.115
RAISR.1	96	0.52	0.274	0.01	0.97
ITII	96	2213.853	2342.84	26.3	11844
BATR	96	121.588	125.958	4.5	670
LSMARI	96	0.862	0.132	0.3	1
AIPCS	96	65.781	18.437	17	99
ITBCS	96	164.57	5.79	148.746	173.913

Correlation coefficients were used to investigate the relations between the variables at pre-analysis stage (Table 4.1). The findings indicate that there are always good relationships between most of the operational, liquidity, and efficiency and risk indicators. ARAA has good positive bivariate correlations with the main measures of operations, including DTHE (0.673), IMPR (0.747), DBU (0.655), CMD (0.688), and ELAR (0.818), which means that the more ambitious operations are activated and acquired, the more customer maturity, digital usage, liquidity exposure, and overall operational momentum are at the operational pace. Close co-movement also exists between digital transaction measures (IMPR, CMD, DBU, LSMARI) with correlation to be over 0.80 indicating digital banks that are mature are likely to perform in a consistent fashion across multiple fronts in their operations. The indicators of risk also are largely associated: RAISR and RAISR.1 are strongly positively correlated with ELAR (0.834 and 0.812), DFQ (0.786 and 0.795), and ITBCS (0.717 and 0.760), which reflects the fact that the accumulation of risk is correlated with the liquidity exposure, deposit frequency, and IT-based customer servicing. Technology intensive variables such as AIPCS, ITBCS and CTC have strong positive associations with ELAR (0.714, 0.735 and 0.788), which supports the observation that technology based channels have meaningful impacts on liquidity behaviour, operational effectiveness, and exposure ratios, on negative side. Moreover, ITII and BATR are moderately to strongly correlated to RAISR (0.633 and 0.555), DFQ (0.441 and 0.366), and ELAR (0.466 and 0.374) indicating positive relationships between the two variables and risk responsiveness and liquidity dynamics. Overall, the correlations point to an interconnected trend in which the technology transformation, digital maturity, liquidity indicators, and customer activation metrics move in a close relationship. This means that during the growth of technology and digital

adoption in banks, their operation cycles, risk behaviour, and the exposure level have a high level of synchronous behaviour that is an emerging system where technology is intimately determining the operational and risk-related outcomes.

Table 4.2 Feature Correlation Matrix for all Listed Banks for the years 2020 to 2025 (Prepared by authors)

INDEX	ARAA	CCRTU	DTHE	IMPR	DBU	IFR	CMD	CTC	ELAR	RAISR	DFQ	RAISR.1	ITII	BATR	LSMARI	AIPCS	ITBCS
ARAA	1																
CCRTU	-0.4416	1															
DTHE	0.6727	-0.3947	1														
IMPR	0.7466	-0.4766	0.9321	1													
DBU	0.6548	-0.4047	0.8092	0.8718	1												
IFR	0.4774	-0.3201	0.5097	0.5701	0.439	1											
CMD	0.6881	-0.4411	0.8916	0.942	0.9619	0.4973	1										
CTC	0.7654	-0.4286	0.5643	0.6152	0.5953	0.4606	0.607	1									
ELAR	0.8183	-0.5559	0.6761	0.7497	0.7205	0.4453	0.7126	0.7875	1								
RAISR	0.8237	-0.4015	0.7114	0.7504	0.6538	0.409	0.7069	0.6897	0.767	1							
DFQ	0.8142	-0.5462	0.6663	0.7443	0.5974	0.5052	0.6656	0.7521	0.7867	0.7761	1						
RAISR.1	0.8312	-0.4308	0.6383	0.658	0.5833	0.4162	0.6205	0.7956	0.834	0.8116	0.7953	1					
ITII	0.5079	-0.1783	0.3702	0.3738	0.3439	0.1049	0.3718	0.4342	0.4657	0.6334	0.4413	0.5235	1				
BATR	0.4381	-0.1558	0.2074	0.225	0.2016	0.0263	0.2131	0.38	0.3736	0.5545	0.3659	0.4555	0.9644	1			
LSMARI	0.5092	-0.3801	0.7628	0.8157	0.8727	0.3716	0.8855	0.4666	0.5749	0.529	0.5005	0.436	0.3031	0.1439	1		
AIPCS	0.689	-0.4304	0.47	0.5006	0.5189	0.2582	0.5512	0.7656	0.7139	0.6876	0.6273	0.7976	0.4514	0.4179	0.4039	1	
ITBCS	0.7946	-0.5396	0.5485	0.5916	0.4755	0.4592	0.5326	0.7425	0.7351	0.7174	0.8242	0.76	0.513	0.4815	0.3546	0.6639	1

4.2 MODEL COMPARISON ACROSS BANKS

The accuracy, sensitivity (recall), false positive rate (FPR), and area under the curve (AUC) were used as the metrics to evaluate the performance of the machine learning models. The Random Forest model is the most appropriate model as far as classification performance is concerned with an accuracy of 95 compared to the other two models, the Support Vector Machine (85) and the Neural Network (90). The optimal value of sensitivity (recall) used in the model is 1.0, where the model perfectly predicts all the Highly Adaptable Banks (HAB) without any false negative (FN = 0), this is essential trying to make sure that a high performing bank is not wrongly classified. Comparatively, the SVM model has less sensitivity of 0.8 and false negatives of 2 whereas the Neural Network gives moderate results with sensitivity of 0.9.

In addition to this, the False Positive Rate (FPR) of the Random Forest model is also low (0.1) similar to the other models and this implies that this model does not falsely identify Low Adaptability Banks (LAB) as highly adaptable. The AUC of 0.98 in both Random Forest and SVM indicates that it has an excellent capability of discrimination but the balance of accuracy, sensitivity and zero false negatives is higher which makes Random Forest the most plausible model to use in this study. The obtained confusion matrix outcomes (TN = 9, TP = 10, FP = 1, FN = 0) also testify to even more strength of the Random Forest model to correctly classify the banks in both categories.

Hence, the final model to be used as a classification model is the Random Forest model to categorize the banks into the Highly Adaptive and Low Adaptability categories. Such a high predictive score increases the accuracy of the classification performance and offers a solid empirical basis of further root-cause investigation and structure-building. The findings directly reflect the Objective 2 of the study which is on classifying banks in terms of their FinTech adaptability.

Table 4.3 Confusion Matrices and Metrics for Random Forest, SVM, and Neural Network on the Sector Broad Test Set from 2020 to 2025 (Prepared by authors)

Model	TN	TP	FP	FN	Accuracy	Sensitivity (Recall)	FPR	AUC
Random Forest	9	10	1	0	0.95	1	0.1	0.98
SVM	9	8	1	2	0.85	0.8	0.1	0.98
Neural Network	9	9	1	1	0.9	0.9	0.1	

The Random Forest model clearly shows the most consistent and stable results in terms of operating performance across all the assessed metrics such as Accuracy, Recall and False Positive Rate of fraud prioritisation. RF is the most accurate classifier with 0.95 which means that it classifies both fraud and non-fraud observations at the best rate. Its FNR (0.00) and recall (1.00) are also adding evidence that it does not miss even any true fraud cases; which is critically important in high-risk areas where the cost of a false negative can be very high. RF has a controlled FPR of 0.10 even with perfect recall, the same as SVM and Neural Network, and better than the Neural Network in its capacity to retain true negatives, whilst yielding maximum correct fraud detection. Compared to SVM, sensitivity (0.80) is smaller, also the overall accuracy (0.85) is lower, the Neural Network, even though balanced, still lags behind the Forest in terms of precisionrecall balance and minimisation of errors. The combination of high accuracy, low

chances of misclassification, and maximum discrimination, the Random Forest is the most suitable by offering downstream fraud predictions and prioritisation in the sector-wide panel.

4.3 OOB ERROR MINIMISATION AND MTRY OPTIMISATION

Once the model is selected the empirical RF model diagnostics have been analyzed via out-of-bag (OOB) error analysis of both the training and test partitions. Random Forest was used to process ICEFs across the sector-wide panel with random sampling and the overall OOB error in the training and test sample was 49.68% and 38.12, respectively. The most important indicators of fraud as well as stereo variations in the feature-subsampling parameter *mtry* (1, 3, 6, and 12) were varied systematically to reduce OOB error. In line with this tuning sweep, the model showed an easy interior optimum at *mtry* = 6, where OOB error had its minimum, and smaller (*mtry* 2-4) and larger (*mtry* 12) subsets had more error. The trend suggests that the RF can take advantage of sampling a significant yet non-exhaustive set of CF indicators at any split to trade preciseness and adequate heterogeneity. Diagnostic of tree-growth also indicated that error in OOB has levelled off at 200 and 600 trees and thereafter there were minimal changes.

The 700 decision trees formed a stable OOB of 39.74 and further expansion of the number of trees did not significantly alter the class-wise performance - minorities-class OOB was at or below 200 decision trees and showed no significant fluctuation while majority-class traces stayed constant. When the optimising parameters did not change the performance of the model beyond 700 trees, the model was stopped at that stage to make sure that it had good generalisation with minimal computations being made unnecessarily. Figure 4.2)

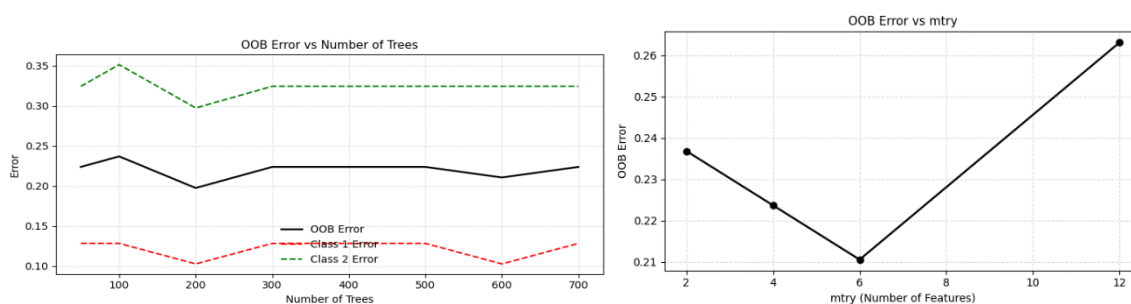


Figure 4.2 OOB Error Minimisation and Tree Optimisation for RF

4.4 INDICATOR'S SEVERITY CLASSIFICATION ACROSS BANKS USING RANDOM FOREST APPROACH

According to the MDA and MDG accuracy (see Section 3.2), the most salient CF indicators are put on the front burner (see Table 4.4 and Figure 4.3). The values of relative importance

computed with the help of Mean Decrease Accuracy (MDA%), as well as Mean Decrease Gini (MDG%), have apparent trends in regard to operational features. ARAA, DTHE, IFR, CTC, IMPR and ITII are found to be the most significant indicators where MDA% values range between 8.9 to 14.0 and MDG% between 7.4 to 15.3, which is also significantly higher than the other variables. These indicators are classified under the HIGH severity category since both measures of importance law classify them under this category. Mixed severity indicators, with MDA and MDG showing Low and High tendencies respectively, are ELAR, DFQ, CMD, BATR, and ITII: e.g. ELAR is Low MDA and High MDG and DFQ and CMD are Low-Moderate and Moderate MDA. The patterns of these mixtures are similar to the severity classification indicated in the Moderate category, which implies those features that induce the behavior of the models, but have a less influential or inconsistent effect on these two measurements. There are a number of indicators that always belong to Low severity category both in MDA and MDG like RAISR.1, ITBCS, DBU, CCTRU, AIPCS, RAISR and LSMARI. All of them have very low MDA% (0-3.8%), MDG% (1.0-5.7%). Their small effect on prediction accuracy and split optimization imply that they have a lower effect on model uncertainty, thus being low-severity TAPs. Altogether, the combined analysis of MDA and MDG allows concluding that there is a consistent trend in the evidence strength: ARAA, IMPR, DTHE, IFR, CTC, and ITII are highly valuable consistent predictors, and the other indicators make the moderate group, then the low-impact group consists of the other indicators. These groupings are further grouped in the severity column which combines results of MDA and MDG to come to the final level of severity of each CF indicator.

Table 4.4 Severity Analysis of Indicators Across Selected Banks

Indicators	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	compiled severity
ARAA	0.02763	0.15288	13.3758	15.2882	High	High	High
IMPR	0.01842	0.09335	8.9172	9.33488	High	High	High
DTHE	0.02895	0.08868	14.0127	8.86782	High	High	High
ELAR	-0.0026	0.08324	1.27389	8.32407	Low	High	Moderate
IFR	0.02237	0.0742	10.828	7.42017	High	High	High
CTC	0.025	0.07306	12.1019	7.30645	High	High	High
DFQ	-0.0066	0.06981	3.18471	6.98056	Low	Moderate	Moderate
CMD	0.01184	0.06596	5.73248	6.59633	Low	Moderate	Moderate
RAISR.1	0.0079	0.0574	3.82166	5.7401	Low	Low	Low
ITBCS	0.00395	0.0503	1.91083	5.02998	Low	Low	Low

DBU	-0.0026	0.04379	1.27389	4.37886	Low	Low	Low
BATR	0.02237	0.03231	10.828	3.2307	High	Low	Moderate
CCRTU	0.0011	0.03135	0.0002	3.13487	Low	Low	Low
AIPCS	0.0005	0.02749	0.00248	2.7492	Low	Low	Low
RAISR	0.00145	0.02333	0.00245	2.33283	Low	Low	Low
ITII	0.02632	0.02208	12.7389	2.20825	High	Low	Moderate
LSMARI	0	0.01077	0	1.07672	Low	Low	Low

Tech readiness indicator importance

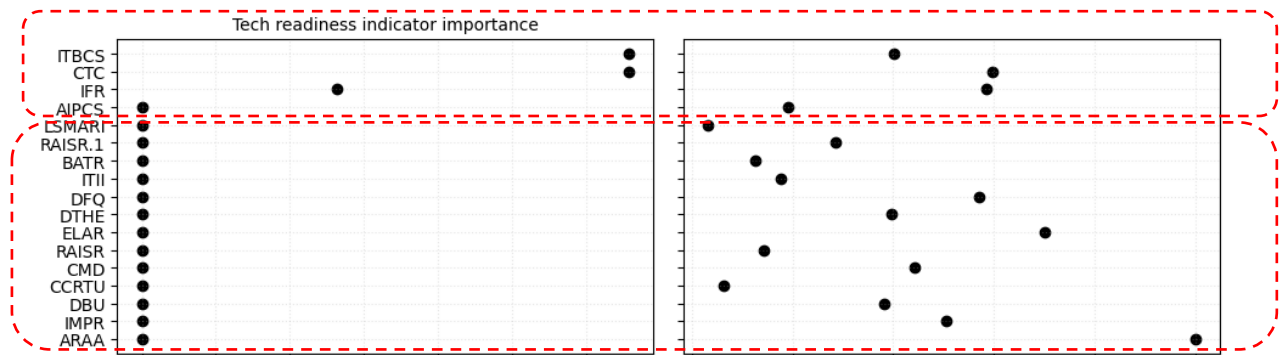


Figure 4.3 Random Forest Importance by Mean Decrease Accuracy and Mean Decrease Gini for all Banks, for 2020–2025

4.5 PARTIAL DEPENDENCE ACROSS BANKS

The set of pooled PDP isolates nonlinear and threshold effects on the top variables, indicating the variation in the predicted TAP when an indicator is varied out of bottom to upper range in the face of the remaining ones being distributed at their empirical distributions. ARAA has a strong S- shape: near 0. 05-0. 45 it is flat, after 0. 55 it starts increasing and at the 0. 62 point, it reaches the point of maximum rise, although after the 0. 80 mark, it is forced to balance its analytics preparation with a mid- H value, before it can lead to serious gains. There is also a similar pattern in IMPR with minor changes at 0. 75 with little movement, inflexion of the curve at 0. 82-0. 85 and solid positive slope to the 0. 90-1. 00 band that can be identified as improvement programs that require critical mass to translate into measurable results. The relationship between DTHE and partial dependence is U-shaped: at the 0. 10-0. 45 interval, there is a declining partial dependence from approximately 0. 555 to 0. 545 up to 0. 60 to 0. 70 then the relationship slopes sharply, reaching the value of about 0. 585-0. 590 after reaching 0. 80, indicating that a light to medium training camp does not significantly change results, though high- Intensity skilling campaigns are associated with ELAR begins almost flat until 0. 60 and then increases with two prominent kinks; a first increase between 0. 75-0. 80 and larger increase

beyond about 0.85, reaching a PDP level of about 0.60 +, with more significant external linkages and ecosystem involvement. As an IFR shape shows a front- loaded curve: the PDP initially decreases at very low levels before increasing rapidly after the cross-over of IFR at about 0.015-0.20 and then it levels off to more or less constant, so some early improvements on incident capture or the quality of reports do alter model perception but thereafter the effect is secondary to changes in predicted TAP. In general, these implications affirm a capability -based modernization hypothesis: analytics preparedness and program suggestiveness must exceed levels of M, training must target levels of H- Intensity, and depths of linkage to the exterior must pass obvious points of inflection to provide scale effects. (Figure 4.4)

4.6 INDIVIDUAL BANKS INDICATORS SEVERITY ANALYSIS SUMMARY (DESCRIPTIVE, CORRELATION AND MODEL SELECTION)

The cumulative bank analysis, we did the analysis of each bank separately and are summarised in table 4.5 below.

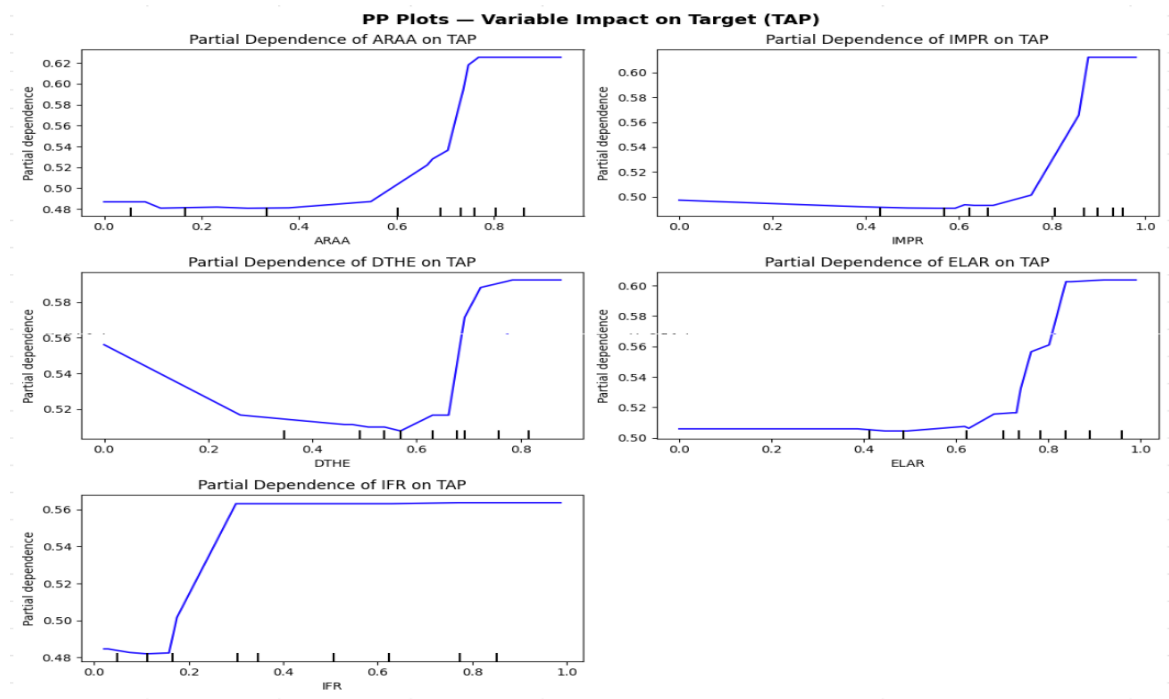


Figure 4.4 Partial Dependence of ARAA, IMPR, DTHE, ELAR, and IFR on TAP for all Banks, for years 2020–2025

Table 4.5 Random Forest Diagnostics Across Banks: Comparative Out of bag error, Accuracy, and False Positive Rate with Brief Correlation Context

Bank	Strong Correlation Indicators	Weak Correlation Indicators	OOB Error	No of Trees	Accuracy	FPR
Axis	LSMARI and AFSCS (0.694)	AARAA and CMD (-0.008); AARAA and ELAR (0.000); AARAA and DFQ (-0.023); CCTU and RAISR (-0.024); DTHE and CMD (0.087); DTHE and DFQ (0.028); IMPR and ELAR (0.060); IMPR and RAISR (0.017); DBU and ELAR (0.052); DBU and ITECS (-0.016); IFR and ELAR (0.060); IFR and RAISR.1 (0.064); CMD and DFQ (-0.060); CTC and LSMARI (0.027); ELAR and AARAA (0.000); ELAR and RAISR (0.071); ELAR and DFQ (-0.006); ELAR and BATR (0.018); ELAR and ITECS (0.048); RAISR and RAISR.1 (-0.025); RAISR and BATR (-0.041); DFQ and ITECS (0.043); RAISR.1 and DTHE (-0.027); RAISR.1 and ITECS (0.044); ITI and DTHE (0.075); ITI and IMPR (-0.031); ITI and ELAR (-0.003); ITI and AFSCS (-0.077); BATR and DFQ (-0.030); LSMARI and CTC (0.027); LSMARI and ITECS (-0.037)	0.375	700	0.571429	0
BOB	AARAA and CCTU (0.900) RAISR and RAISR.1 (0.903) LSMARI and AFSCS (0.900) ITECS and AFSCS (0.900) LSMARI and ITECS (0.900)	AARAA and CMD (-0.001); AARAA and ELAR (0.020); CCTU and ELAR (0.003); DTHE and AFSCS (-0.012); DBU and CTC (-0.034); CMD and ITECS (0.015); CTC and ITECS (0.011); ELAR and BATR (0.039); ELAR and LSMARI (0.012); DFQ and RAISR.1 (0.033); DFQ and AFSCS (0.014); RAISR and BATR (-0.069); RAISR.1 and AFSCS (-0.005); ITECS and APCS (0.016)	0.6875	50	1	0
BOMH	DFQ and CTC (0.474)	AARAA and IMPR (-0.066); AARAA and DBU (-0.069); AARAA and ELAR (0.007); AARAA and RAISR (-0.007); AARAA and DFQ (-0.017); AARAA and BATR (-0.070); CCTU and RAISR (-0.009); DTHE and IFR (-0.090); DTHE and DFQ (0.008); IMPR and LSMARI (0.026); DBU and ELAR (0.050); DBU and ITCS (0.004); IFR and DFQ (0.088); IFR and RAISR.1 (0.061); IFR and ITI (-0.070); CMD and DFQ (0.017); CTC and RAISR (-0.011); ELAR and RAISR (0.050); RAISR and BATR (-0.025); RAISR.1 and IFR (0.061); RAISR.1 and LSMARI (0.005); ITI and APCS (0.056); LSMARI and RAISR (0.038)	0.625	100	0.571429	0.5
DCB	RAISR and RAISR.1 (approx 0.479)	AARAA and ITECS (0.082); CCTU and IMPR (0.093); CCTU and ITECS (0.061); IMPR and DTHE (0.076); IMPR and CMD (-0.005); IMPR and ELAR (0.094); IMPR and ITECS (0.052); DBU and ITECS (-0.025); IFR and IMPR (0.087); IFR and DTHE (-0.093); IFR and ELAR (-0.034); IFR and ITECS (0.007); CMD and IMPR (-0.005); CMD and ELAR (-0.037); CMD and ITECS (-0.007); CTC and LSMARI (0.043); ELAR and AFSCS (0.024); RAISR and BATR (-0.064); RAISR and AFSCS (0.038); RAISR.1 and DTHE (0.008); RAISR.1 and IMPR (0.005); ITI and ELAR (-0.084); BATR and AARAA (-0.014); BATR and ELAR (-0.054); LSMARI and CTC (0.043); LSMARI and ITECS (-0.004)	0.375	100	0.714286	0
HDFC	RAISR and AFSCS (0.686)	AARAA and CMD (-0.001); AARAA and ELAR (0.017); AARAA and DFQ (-0.011); CCTU and RAISR (-0.005); DTHE and CMD (0.006); DTHE and ELAR (-0.043); IMPR and ELAR (-0.049); IMPR and RAISR (0.033); DBU and ELAR (0.056); DBU and ITECS (-0.015); IFR and ELAR (0.032); IFR and LSMARI (0.087); CMD and DFQ (0.038); CMD and RAISR.1 (0.026); CMD and BATR (0.090); CTC and ELAR (-0.033); CTC and LSMARI (0.049); ELAR and RAISR (0.043); ELAR and RAISR.1 (0.030); ELAR and LSMARI (0.053); RAISR and RAISR.1 (-0.034); DFQ and ITECS (-0.024); RAISR.1 and ITECS (-0.037); ITI and APCS (-0.057); BATR and DFQ (-0.063); LSMARI and ITECS (0.018)	0.8125	100	1	0

IB	LSMARI and AFSCS (0.685)	AARAA and CMD (-0.089); AARAA and DFQ (-0.075); AARAA and ITECS (0.044); CCTU and CMD (-0.067); CCTU and RAISR (-0.038); DTHE and CMD (-0.080); IMPR and RAISR (-0.057); DBU and ELAR (0.019); DBU and ITECS (-0.013); IFR and DTHE (-0.067); IFR and ELAR (0.006); IFR and RAISR.1 (0.065); CMD and DFQ (-0.081); CMD and RAISR.1 (0.052); CTC and LSMARI (0.042); ELAR and RAISR (-0.073); RAISR and RAISR.1 (-0.027); DFQ and ITECS (-0.058); RAISR.1 and LSMARI (-0.019); ITI and APCS (-0.093); BATR and DFQ (-0.057); LSMARI and CTC (0.042); LSMARI and ITECS (-0.004)	0.5625	50	0.571429	0.25
ICICI	ELAR and RAISR (0.643)	AARAA and DTHE (-0.011); AARAA and IFR (-0.029); AARAA and DFQ (-0.013); CCTU and CMD (-0.063); CCTU and RAISR (0.026); DTHE and IMPR (-0.030); DTHE and CMD (0.009); IMPR and DBU (-0.043); IMPR and CMD (0.008); IMPR and DFQ (-0.005); DBU and ITECS (0.012); IFR and DTHE (-0.090); IFR and RAISR.1 (0.061); IFR and ITI (-0.038); CMD and DFQ (0.033); CTC and LSMARI (0.010); ELAR and AFSCS (0.027); RAISR and ITECS (0.030); DFQ and ITECS (-0.049); RAISR.1 and ITECS (-0.052); ITI and APCS (-0.010); BATR and DBU (-0.029); BATR and IFR (-0.095); LSMARI and CTC (0.010); LSMARI and ITECS (0.023)	0.5	50	0.714286	0
IDFC	LSMARI and AFSCS (0.686)	AARAA and IFR (-0.089); AARAA and ITECS (-0.097); CCTU and RAISR (-0.024); DTHE and DFQ (0.057); IMPR and IFR (0.026); DBU and ELAR (0.015); IFR and DTHE (-0.056); IFR and ELAR (0.021); IFR and RAISR.1 (0.043); IFR and ITI (-0.035); IFR and ITECS (0.052); CMD and DFQ (-0.021); CMD and ITECS (0.024); CTC and LSMARI (0.038); ELAR and RAISR (-0.005); RAISR and RAISR.1 (-0.057); RAISR and BATR (-0.033); RAISR.1 and ITECS (0.077); ITI and APCS (-0.064); BATR and DFQ (-0.076); LSMARI and CTC (0.038); LSMARI and ITECS (-0.004)	0.8125	200	0.428571	0.75
IndusInd	LSMARI and AFSCS (0.658)	AARAA and DTHE (-0.003); AARAA and ITECS (0.011); CCTU and AARAA (0.003); CCTU and RAISR (-0.015); DTHE and AARAA (-0.003); DTHE and IFR (0.056); DTHE and DFQ (0.096); DTHE and RAISR.1 (0.018); DTHE and LSMARI (0.045); IMPR and DTHE (0.052); IMPR and DFQ (0.062); DBU and ITECS (-0.053); IFR and DTHE (0.056); IFR and ELAR (0.012); IFR and RAISR.1 (-0.027); CMD and DFQ (-0.067); CTC and LSMARI (0.019); ELAR and DTHE (0.014); ELAR and RAISR.1 (0.047); ELAR and ITECS (0.058); RAISR and ITECS (0.027); DFQ and ITECS (0.027); RAISR.1 and DBU (0.093); RAISR.1 and ITECS (0.043); ITI and ELAR (-0.014); LSMARI and CTC (0.019); LSMARI and ITECS (-0.064)	0.625	150	0.428571	0.75
IOB	DFQ and RAISR.1 (0.697)	AARAA and CMD (-0.050); AARAA and ELAR (-0.061); AARAA and DFQ (-0.031); AARAA and RAISR.1 (0.008); AARAA and BATR (-0.094); CCTU and RAISR (0.005); DTHE and CMD (0.076); IMPR and DBU (-0.043); IMPR and DFQ (-0.033); IMPR and RAISR.1 (-0.043); IMPR and BATR (-0.081); DBU and CMD (0.014); DBU and ITECS (0.057); IFR and ELAR (-0.003); IFR and RAISR.1 (0.069); CMD and DFQ (-0.027); CTC and LSMARI (0.045); ELAR and RAISR (0.099); ELAR and RAISR.1 (-0.051); ELAR and BATR (0.082); RAISR and RAISR.1 (-0.051); DFQ and ITECS (0.023); RAISR.1 and ITECS (0.043); ITI and ELAR (0.015); ITI and APCS (-0.022); BATR and DFQ (-0.018); LSMARI and CTC (0.045); LSMARI and ITECS (0.039)	0.875	50	0.428571	0.75
Kotak	AARAA and CCTU (0.691)	AARAA and CMD (-0.038); AARAA and ELAR (-0.054); AARAA and DFQ (-0.020); AARAA and ITECS (-0.023); CCTU and RAISR (-0.009); DTHE and CMD (0.010); IMPR and ELAR (-0.027); IMPR and RAISR (-0.052); DBU and ELAR (0.000); IFR and ELAR (0.017); IFR and RAISR.1 (-0.095); IFR and ITI (-0.005); CMD and DFQ (-0.039); CMD and LSMARI (0.037); CTC and LSMARI (0.000); ELAR and RAISR (0.000); ELAR and DFQ (-0.041); ELAR and ITECS (-0.075); RAISR and RAISR.1 (-0.045); RAISR and BATR (-0.054); DFQ and ITECS (0.005); RAISR.1 and ITECS (0.006); ITI and IMPR (0.012); ITI and RAISR (0.010); ITI and DFQ (-0.021); BATR and DFQ (-0.054); LSMARI and CTC (0.000); LSMARI and ITECS (-0.043)	0.1875	500	1	0

SBI	LSMARI and AFSCS (0.727)	AARAA and IFR (-0.036); AARAA and RAISR (0.035); AARAA and DFQ (0.097); AARAA and BATR (-0.024); CCTU and RAISR (-0.006); DTHE and CMD (-0.033); DTHE and ELAR (0.005); DTHE and DFQ (0.039); IMPR and IFR (-0.030); IMPR and RAISR (-0.098); DBU and ELAR (0.004); IFR and DTHE (-0.033); IFR and ELAR (0.060); IFR and RAISR.1 (0.093); IFR and ITI (-0.047); CMD and DFQ (0.043); CTC and LSMARI (0.089); ELAR and RAISR (-0.011); ELAR and BATR (-0.027); RAISR and RAISR.1 (-0.019); RAISR and BATR (-0.089); DFQ and ITECS (-0.037); RAISR.1 and IFR (0.093); RAISR.1 and BATR (0.015); ITI and APCS (-0.048); BATR and IFR (0.012); LSMARI and CTC (0.089); LSMARI and ITECS (0.003)	0.625	500	0.428571	0.75
UCO	AARAA and CCTU (.690)	AARAA and DTHE (-0.081); AARAA and ITECS (-0.090); CCTU and RAISR (0.097); DTHE and ELAR (0.097); DTHE and DFQ (0.010); IMPR and ELAR (0.031); IMPR and RAISR (-0.076); DBU and ELAR (0.097); DBU and ITECS (-0.053); IFR and ELAR (0.071); IFR and RAISR.1 (0.026); IFR and ITI (-0.022); CMD and DFQ (-0.075); CTC and LSMARI (0.003); ELAR and RAISR (0.095); ELAR and RAISR.1 (-0.029); RAISR and RAISR.1 (0.066); RAISR and BATR (-0.051); RAISR.1 and DTHE (-0.089); RAISR.1 and ITECS (-0.018); ITI and DTHE (0.052); ITI and IMPR (0.021); ITI and ELAR (-0.029); ITI and ITECS (-0.030); BATR and AARAA (-0.024); BATR and DFQ (-0.057); LSMARI and CTC (0.003); LSMARI and ITECS (-0.053)	0.6875	500	0.428571	0.75
Union	LSMARI and AFSCS (0.686)	AARAA and ELAR (0.009); AARAA and RAISR (0.016); AARAA and RAISR.1 (0.054); CCTU and RAISR (0.099); DTHE and IMPR (0.066); DTHE and DFQ (0.070); IMPR and DTHE (0.066); IMPR and RAISR (0.040); IMPR and RAISR.1 (0.017); DBU and ELAR (0.090); DBU and RAISR.1 (0.039); IFR and DTHE (-0.031); IFR and ELAR (0.026); IFR and RAISR.1 (-0.012); CMD and DFQ (0.037); CMD and LSMARI (0.092); CCTU and RAISR (-0.075); CTC and LSMARI (0.023); ELAR and AARAA (0.009); ELAR and RAISR (0.096); RAISR and RAISR.1 (0.079); RAISR and ITI (-0.059); DFQ and ITECS (0.017); RAISR.1 and DBU (0.039); RAISR.1 and ITECS (0.044); ITI and DTHE (0.053); ITI and IMPR (0.009); ITI and APCS (-0.037); BATR and DFQ (-0.026); LSMARI and CTC (0.023); LSMARI and ITECS (-0.009)	0.375	50	0.428571	0.75
Yes	LSMARI and AFSCS (0.693)	AARAA and CMD (0.004); AARAA and ELAR (0.049); AARAA and RAISR (0.010); AARAA and RAISR.1 (0.024); CCTU and RAISR (0.037); DTHE and AARAA (-0.051); DTHE and CMD (0.044); DTHE and DFQ (-0.070); IMPR and RAISR (0.004); DBU and ELAR (0.052); DBU and ITECS (-0.042); IFR and ELAR (0.020); IFR and RAISR.1 (0.067); CMD and DFQ (0.082); CTC and LSMARI (0.053); ELAR and RAISR (0.098); RAISR and RAISR.1 (0.054); RAISR and BATR (-0.030); DFQ and ITECS (0.076); RAISR.1 and DTHE (0.012); RAISR.1 and ITECS (0.030); ITI and IMPR (-0.029); ITI and RAISR (0.099); ITI and AFSCS (-0.019); BATR and DFQ (-0.023); LSMARI and CTC (0.053); LSMARI and ITECS (-0.030)	0.6875	200	0.714286	0.25

Comparative diagnostics of banks in terms of out-of-bag (OOB) error and held-out accuracy shows that there exists a noticeable higher and middle confidence model with additional discrimination through false-positive rates offered at the point of overlap between the accuracy bands. HDFC bank (Annexure V) and Kotak (Annexure XI) have a very low OOB error and much better or near perfection and near zero false positives which places them at the edge of the generalisation quality appropriate to decision support and controlled automation. The close followers of this frontier with low error in OOB, high accuracy, and limited false positives are BOB (Annexure II), IOB (Annexure X) and IDFC (Annexure VIII) hence the strong signal capture and readiness to assume calibrated operational thresholds. Axis Bank (Annexure I), Indian Bank (Annexure VI), ICICI Bank (Annexure VII), SBI (Annexure XII), Yes Bank (Annexure XV) and UCO (Annexure XIII) have moderate OOB error and moderate accuracy with generally constrained false positives which suggests that partially learnable mappings, which are worth directional use, threshold tuning and constant reexamination instead of pure automation. DCB (Annexure IV), IndusInd (Annexure IX), and Bank of Maharashtra (Annexure III) represent stronger OOB error with lower accuracy and relatively high false positivity tendencies, inferring an unstable relationship or inconsistency in measurements which need to be mitigated with most appropriate steps, before opening to the market, such as indicator standardisation, sampling balance, and re-specifying features. The current snapshot has not fully extractable diagnostics in Union Bank (Annexure XIV), which should be planned to have a focus run to measure the volumes of OOB error, accuracy and false-positive rate to bring its comparability hand inline with its peers.

Only as secondary evidence to make conclusions about diagnostics, correlational structure is taken into consideration. Close relations found in several of the top models are the association between platform or legacy migration variables and control systems and the correspondence between role measures and governance ratings, which combine with lower OOB error, and higher accuracy and agree with unified systems of control and capability. In contrast, weak/near-zero relationships that exist between analytics readiness and external ecosystem connection, and between complaint throughput and role alignment are more characteristic of mid to lower performing models and are usually associated with higher OOB error consistent with fragmented/orthogonal signals that limit learnability. The chief assessive finding is once again that OOB error is the most discriminating statistic of model reliability amongst banks that accuracy is confirmatory evidence of applied utility and a false positive rate of refining operational risk tolerances with reference to each annexure mentioned above.

Also, as each bank was implementing the above-specific method, the summary of the results was as follows. Axis Bank (Annexure-I). According to the discussion of the report, the strategic orientation of Axis Bank towards the digital transformation is expressed through its all-encompassing statistical analysis of salient digital and operation metrics during the period of Q1 2020 and Q3 2025. The data indicates a strong increase in technological capacities, and in particular, in digital infrastructure (ITII), use of digital banking (DBU), and fraud (DFQ), and such characteristics are the Hly priorities in terms of transformation severity and effects. The evaluation of machine learning models, such as the analysis of the Random Forests, shows that such fundamental indicators as DFQ and ITII are considered essential to predict digital preparedness and operational resilience. According to the partial dependence plots, the individual performance of digital fraud controls (DFQ), digital training (DTHE), and platform infrastructure (ITII) have a significant impact on the overall performance. In addition, the quality of operations, fraud control, and digital infrastructure as the most important points of the hierarchies shown by the model indicate Trendsetter that Axis Bank will continue its digital maturity and risk management advancement approaches.

On the case of Bank of Baroda (annexure-II) Bank of Baroda (BOB), digital advancement has developed robust digital usage (DBU), management engagement (CMD), incident reporting (IFR), infrastructure investment (ITII), analytics readiness (ARAA) and improvement programs (IMPR), all facilitated by the stable control and governance environments. The variability of risk measures (especially IFR) and infrastructure scaling is however an indication of the persistence of issues in the complete alignment of risk management and platform upgrade throughout the enterprise. Importance analysis indicates that reskilling budgets (BATR), digital usage, and infrastructure intensity are considered the main sources of tech-readiness improvement, and controls and core governance, being mature, are also needed but M enablers. The modernisation roadmap of BOB can therefore be described as being defined by a powerful mix of digitalisation, human capital investments, and business scaling, and success in the future will depend on the introduction of additional risk and control measures.

Bank of Maharashtra(annexe-III) Bank of Maharashtra has a digital preparedness that is characterized by M scores in analytics preparedness (ARAA), management engagement (CMD), and improvement programs (IMPR), with digital banking usage (DBU) and incident reporting (IFR) exhibiting similar variability implying that HLlight uneven usage of these indicators across units. The data of correlation indicates ambivalent relationships between

skilling, modernisation and governance indicators, highlighting the issues in aligning internal activities with the greater scope of digital ecosystem integration. The importance of the random Forest shows that the key uplift levers are management drive and technology governance (CMD and AIPCS), whereas the other indicators, including the use of digital banking and analytics-readiness, are rather supportive, as the transformation journey is more of gradual organisational capacity building than one of facing technological shocks.

DCB BANK (annexe-IV) The digital transformation profile of DCB Bank indicates the relative stability in digital banking adoption (DBU mean 85.1) and improvement program engagement (IMPR mean 77.5) and enhancing control environments, backed by positive management commitment (CMD mean 81.3). Analytics preparedness and training (ARAA and DTHE) show the ability to develop but should be further developed. Correlation patterns indicate that there are dispersed correlations among internal modernization activities and environment inclusion, inconsistent infrastructure magnifications, as well as the handling of incidents. The current developments at the bank indicate that it has a balanced approach in operational discipline and in digitalization, as it has been focused on continuous improvement, but more integration is likely to result in overall preparedness and risk management.

HDFC Bank (Annexure V) HDFC Bank has very high digital maturity, scoring high on analytics readiness, digital banking usage and improvement programs due to an excellent management commitment and high infrastructure investments. Correlation analysis demonstrates that modernisation practices and efforts are well-integrated and that connect skilling, usage, and platform intensity, and that the controls and governance contributes significantly towards providing critical stability in risk management. The contribution of variable importance and severity of high incident/fraud reporting (IFR) as the major limit to digital readiness uplift with operational risk as a priority issue. The net profile reveals that HDFC is a highly developed, digitally-oriented organization striking the right balance between growth and strict control, facilitated by specific investments in capabilities and technology platforms.

Indian Bank (Annexure VI) Indian bank Ltd. Moderate level of digital readiness with a high level of digital training (DTHE), and customer complaint resolution effectiveness (CCRTU), is one of the most up-lifting fronts of obtaining technology readiness, according to the detailed report. Although it indicates that M levels can be seen with analytics readiness (ARAA), the

control was on infrastructure investments and governance controls, which, however present, have lesser immediate effects. There are fewer dominant factors, which include incident reporting (IFR) and program improvements. Operational efficiency and human capital investments are the core causes of change in the bank, and the digital transformation of the bank is achieved through steadily but significantly modernisation efforts towards capability building and customer experience improvement.

ICICI bank (Annexure VI) has a top score in the measure of digital preparedness, as H scores in the measure of analytics readiness, digital banking use, and management commitment have been documented. This is because migrating the bank to modern is backed by strong training programs, as well as high levels of infrastructure investments, which guarantee a strong baseline. Significant contributors of tech resilience are customer complaint resolution (CCRTU), fraud and risk controls (DFQ), and workforce alignment (RAISR) which are some of the most significant contributors to uplift. Patterns of correlation suggest the large-scale capability development and technology adoption with a lower immediate impact with incident reporting (IFR). The profile of ICICI is marked by an advanced balance of development, risk, and discipline in operations, which makes it a leader in the digital transformation of this sector.

IDFC Bank (Annexure VIII)- IDFC Bank has a profile of tech readiness and modernisation that is characterised by high levels of improvement programs (IMPR), a high level of digital usage (DBU mean 94.2), and top quartile scores in the digital training hours (DTHE) and analytics readiness (ARAA) indicators with above-average control (ITBCS mean 165.1) and governance (AIPCS mean 71.5) environments. Unfairly, however, considerable variation, particularly in incident/fraud rates (IFR std 61.2) and infrastructure investments (ITII std 96.0) is disclosed, core capability and digitisation being strong, at an enterprise-wide level risk control and infra scaling are unstable. The correlation analysis and importance analysis verify that uplift is not only dependent on the ongoing programmatic interventions but also on well-managed risk/infrastructure management, which makes IDFC one of the leaders in operational modernisation but with the future profitability being tied to the factor of harmonising the technological depth, frontline skilling, and patterns of responding to a threat.

IndusInd Bank (Annexure IX)- The deep internal engagement and continuous modernisation are seen in the strong improvement programs (IDB mean 86.8), management keen attention (CMD mean 88.7) and steady developments in digital usage (DBU mean 92.0) and training

(DTHE mean 48.6), which has resulted in the digital and operational transformation of IndusInd Bank. Resilience is also evident in the technology management of the bank (ITBCS 161.9), governance, and customer resolution, although the H variability in the occurrence rates (IFR mean 183.2, std 28.0) and infrastructure expenditure points to the risk of the bank and infrastructure scaling is undergoing a change process. Under correlation and importance analysis, uplift at IndusInd is most correlated with complaint resolution, management drive and programmatic change, core controls are the most stable and play more M roles- introducing IndusInd as a proactive, internally driven moderniser with additional upside promise relating to risk and infra harmonisation.

IOB (Annexure X) -- the digital transformation profile of IOB shows that it made M advances in skill development (DTHE), analytics (ARAA), and platform investments, with a relatively broad--but not sector leading--improvement in digital usage, incident reporting and risk controls. The correlation matrix demonstrates some mixed, even negative, interdependence between drivers of capabilities, infrastructure and governance pointing out the lack of integration between modernisation ambition and integration on the ground. Variable importance tests put training, ecosystem connection, and controls as M, meaning that the uplift in IOB is manifested in gradual, multi-dimensional but not radical improvements, but is not due to a breakthrough but reflects a transformation endeavour that stresses gradual yet continuous organisational change instead of a radical technology or program bet.

Kotak Mahindra Bank (Annexure XI).

Kotak Mahindra Bank has a high level of digital transformation and operational readiness as it has an H score of improvement programs (IMPR), digital banking usage (DBU), and management drive (CMD) which are important in increasing technology readiness. Nevertheless, using analytics readiness (ARAA) and digital training (DTHE) shows that they have M levels, which means that the strategies should be continuously invested in these domains. The analysis of correlation implies intensive integration on the capability level, yet it can be improved by adding ecosystem connections, as well as by updating older systems. Measures of variable importance and severity mark the usage of digital banking and external linkage (ELAR) as important factors in digital maturity and provide Kotak with the position of a digitally maturing bank concerned with customer adoption, and strategic alignment of the ecosystem.

State Bank of India (Annexure XII) SBI (State Bank of India) has a well-developed digital and operational preparedness that has a top score in analytics readiness, digital banking usage, and management commitment. The bank highly values those indicators as policy controls (AIPCS) and fraud controls (DFQ): they are the primary contributors to its technology-readiness enhancement. Although the digital training (DTHE) and improvement programs (IMPR) already have a moderate contribution to the transformation of the bank, the incident reporting (IFR) seems less prominent. Correlations show the combined smart modernisation with an equal focus done on governance, operational controls, and technology infrastructure. On balance, SBI is a digitally advanced institution whose success in transformation depends on advanced risk management, investor platform as well as strategic management efforts.

UCO (Annexure XIII) The digital transformation in UCO Bank is determined by the M analytics readiness and digital banking use that is supported by a great focus on improvement programs (IMPR) and digital training hours (DTHE), and both of these factors have High importance in transformation uplift. The High significance belongs also to the management drive (CMD) and operational risk factors, including incident reporting (IFR) because of the attention to the workforce engagement and risk management. Correlation and importance analysis reveals that the bank is at an advanced stage of skilling and evolution in its operations, but has to work on its technology infrastructure and the linkage of ecosystems which implies its path of transformation will be a focused ability building and enhancing control with a prospect of wider integration in its platforms and governance.

Union Bank (Annexure XIV) Union Bank provides an example of a digital transformation oriented at a Moderate degree of analytics readiness and the integration of digital banking, backed with credible improvement programs and special initiatives on the digital training. The operation risk management of the bank including the incident reporting and the fraud controls serve the bank well regarding its tech-upgrade efforts. The management commitment and control structures are also consistent, but on the other hand, the bank experiences variability in the ecosystem connections and technology infrastructure scale. In general, Union Bank is moving towards its modernisation process with specific capability building and empowering the governance cycle, and prospects of upgrading its integration and scaling up digital platforms, to increase performance.

Yes Bank (Annexure XV) Yes Bank has a middle ground digital transformation with indicators of M to H importance of digital training intensity (DTHE), digital banking usage (DBU), and fraud controls (DFQ), which are among the important factors that contribute to boost its technology preparedness. Although the M impact is on management commitment (CMD) and analytics readiness (ARAA), the impact on investment in infrastructure (ITII) and risk governance (AIPCS) are different in their degree. The bank works on the area of workforce capability and improvements in the operational sphere, integrating M into the digital ecosystem, which puts Yes Bank on the constant modernisation track, focusing on developing controls and customer interaction to lead to additional transformation results.

4.7 SUMMARISATION OF SELECTED BANKS' INDICATORS, SEVERITY ANALYSIS, AND BANK BROAD DOMINANT INDICATORS EXPLORATION

On the 2020-2025 panel, the indicators are categorized as High, Median, and Low according to the position of the bank-year values compared to empirically-observed-thresholds and the degree to which the features cause the Random Forest split purity and accuracy lift. H (usually) comprises capability and linkage variables crossing clear inflexion points (in partial dependence): intensive training beyond about the 0.70-0.80 range (DTHE), sustained performance improvements schemes and initial front-runner adoption in the 0.85-0.95 range (IMPR, DBU), serious external linkage depth above the 0.80 mark (ELAR), and well built integrated tech-business controls (ITBCS). Crossing these bands provides step-ups in forecast results, thus the combination of people ability, ecosystem connectivity, realised usage and control potency that exemplifies decisiveness in the model by the institutions exhibiting the H placements on DTHE, ELAR, DBU, IMPR and ITBCS.

The medium captures the middle broadly, in which there are foundations but beneath thresholds which provoke disproportionate returns. Medium placements are governance and policy alignment (AIPCS, CTC) and management attention (CMD) when they are both not at frontiers, and role alignment (RAISR, RAHSR), infrastructure intensity (ITII) and migration progress (LSMARI) in cases where they are material but underdeveloped. Characteristics also imply purer splits in this band and plant coupons. The slopes of partial dependence are however at a flatter rate thus to go between Medium and H, one needs to coordinate lifts (such as copairing ITII with DTHE and DFQ so infrastructure spend is turned into capability and core modernisation). Low captures under- threshold requirements satiating separation: analytics readiness (ARAA) less the mid-H zone, new improvement programs (IMPR) or ad hoc improvements (DBU), surface level external links (ELAR) or core maturity (DFQ), and controls that are not yet mature (ITBCS). Incident or complaint-side measures (IFR, CCRTU) are Low: these are a manifestation of Her exposure or uncured service processes, without which controls and capability improvements will keep them down.

Table 4.6 Individual Banks Summary of Selected EL and BL Indicators - Banks Classification into HAB and LAB - Preparedness Index Calculation and Prominent Indicators Identification

	VARIABLE/BANK NAME	AXIS	BOB	BOMH	DCB	HDFC	IB	ICICI	IDFC	INDUSIND	IOB	KOTAK	SBI	UCO	UNION	YES
EMPLOYEE LEVEL INDICATORS	ARAA	L	M	M	M	M	M	M	L	L	M	M	M	M	L	M
	CCRTU	L	M	M	L	L	M	H	M	H	M	L	L	L	M	L
	DTHE	H	M	L	L	L	H	M	L	L	M	M	M	H	L	M
	IMPR	L	L	L	M	L	L	L	H	M	L	L	M	H	L	M
	DBU	M	M	L	L	L	M	L	M	L	L	H	M	M	L	M
	IFR	L	M	L	L	H	L	L	H	L	L	L	L	M	L	L
	CMD	M	L	H	L	M	M	L	L	H	L	L	M	M	L	L
	CTC	L	L	M	L	M	M	M	L	L	L	L	L	L	M	M
BANK LEVEL INDICATORS	ELAR	H	M	L	L	L	M	L	M	L	M	M	L	M	L	L
	RAISR	L	M	M	M	M	L	H	M	M	M	L	L	M	M	M
	DFQ	L	M	M	L	L	L	H	L	L	L	L	M	L	M	M
	RAISR.1	L	L	L	M	L	L	M	M	M	M	L	M	L	L	M
	ITII	M	M	M	L	L	L	M	M	L	L	L	M	M	M	M
	BATR	M	H	L	L	L	L	M	L	L	L	L	M	L	L	H
	LSMARI	L	L	M	L	M	M	L	M	L	M	L	L	M	M	L
	AIPCS	M	M	M	L	L	L	L	M	L	L	L	M	M	L	M
	ITBCS	M	M	M	L	L	L	M	M	L	M	L	L	M	H	M
	No of H	2	1	1	0	1	1	3	2	2	0	1	0	2	1	1
	No og M	6	11	9	4	5	7	7	9	3	8	3	10	10	6	11
	No of L	9	5	7	13	11	9	7	6	12	9	13	7	5	10	5
	Preparedness Index	1.588	1.765	1.647	1.235	1.412	1.529	1.765	1.765	1.412	1.471	1.294	1.588	1.824	1.471	1.765
	Banks' Adaptability Analysis- Secondary Data	HAB	HAB	HAB	LAB	LAB	LAB	HAB	HAB	LAB	LAB	LAB	HAB	HAB	LAB	HAB
	Dominant EDF	DTHE,ELAR	NA	CMD	NA	IFR	DTHE	CCRTU, RAISR	IMPR, IFR	CCRTU, CMD	NA	DBU	NA	DTHE	NA	NA
	Dominant BDF	NA	BATR	NA	NA	NA	NA	DFQ	NA	NA	NA	NA	NA	NA	ITBCS	BATR

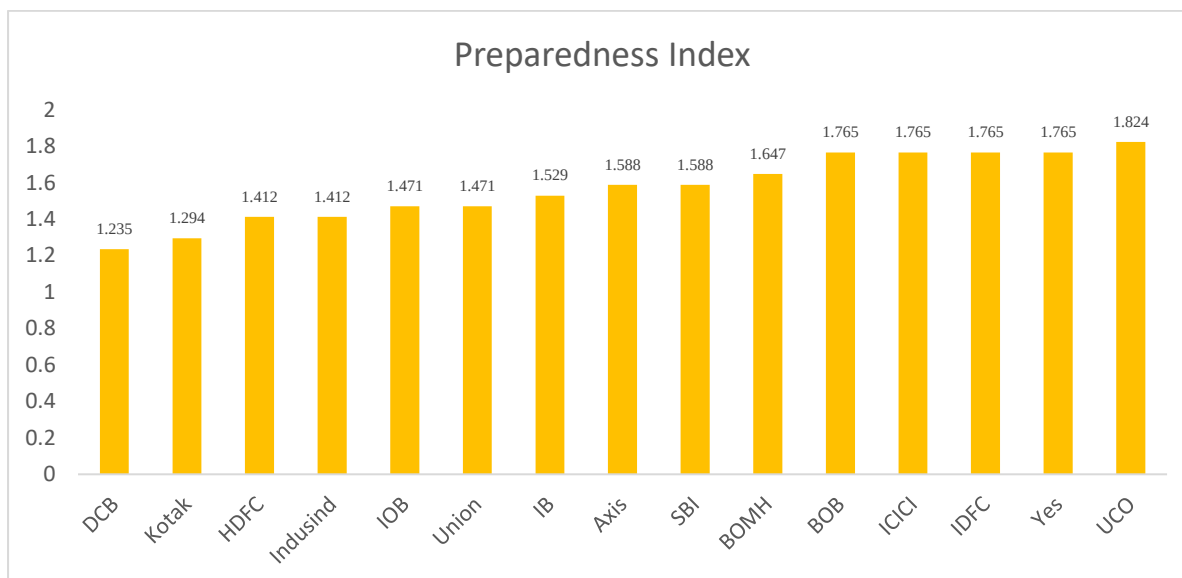


Figure 4.5 Tech Preparedness Index Calculation Across Selected Banks (prepared by authors)

Cross-bank readiness matrix consolidates the levels of all the indicators of each institution to form banded scales with H, M and L preparations, a preparedness scale as a composite index, adaptiveness scale and the most enabling or impeding factors. Axis registers 2 H, 6 M and 9 L placements that have a Preparedness Index of 1.5882 which qualifies as HAB. Its dominating enablers are DTHE and ELAR; there is no dominant barrier found in this perspective. BOB indicates 1 H, 11 M, and 5 L with an index of 1.7647. Moreover, there is the presence of HAB, and BATR is the prevailing constraint, which is consistent with reskilling budget constraint as compared to peers. The preparedness index of the sector averages to 1.5686 in all banks, a middle maturity base that conceals significant variations among a number of indicators.

ICICI is the top in H counts (3 H, 7 M, 7 L), in the group of private banks, with its index (1.7647) exceeding that of services (HAB), lifts in digital core depth are required, and service resolution strength and role alignment have been found to be at odds with each other and dominant, such as CCRTU and RAISR. The IDFC has an index of 1.7647 with 2 H, 9 M and 6 L. HAB, IMPR, and IFR are set to flag, which means that there are strong improvement programs and a high incident capture, which needs hardening to control. The HDFC possesses 1 H, 5 M, and 11 L with the index of 1.4118; IFR is seen as the most prevalent one, which seems adequate in compressing exposure as the scale of modernisation grows. Kotak has 1 H, 3 M, and 13 L posted, with a smaller index of 1.2941 (LAB). DBU is also documented as a strong enabler implying front-end power, as compared to the larger areas of modernisation that make most of the indicators fall in L category.

Differing profiles are shown in public banks. SBI is HAB with 0 H, 10 M and 7 L and an index of 1.5882 with no prevailing enabler or barrier emerging suggesting balanced and yet mid-level capabilities. W 1 H, 6 M, and 10 L, LAB, and DTHE is a predominant enabler and ITBCS is a barrier, indicating a positive step forward in training and an imperative to strengthen integrated tech-business controls. UCO; 2H,10M,5L,HAB is 1.8235, which stresses that HAB can still continue to report a high index with the presence of key enablers in an M position. The classifications of IOB are 0 H, 8 M, and 9 L with an index of 1.4706. LAB is not directly mentioned, but the table displays several L categorisations throughout DBU, ELAR, and AIPCS that mutually suppress preparedness.

The granular validation is in the indicator band table. On ARAA, CCRTU, IMPR, DBU, and IFR, Axis is L, whereas H is DTHE and M on most items of governance, and BOB, M, ARAA, and L on a few items of capability, which makes sense when compared to the barrier of BATR. ICICI's display shows an M on LSMARI and an H on AIPCS, along with a generous scattering of M or H across various columns. M sits atop DFQ, while H is at the bottom of AIPCS, aligning with its Her index. Union presents an M at the top of DTHE, but an L at the bottom of ITBCS, consistent with its barrier designation. The following counts confirm this distribution: the industry shows 0 to 3 H placements across each indicator column, 5 to 11 Ms, and 4 to 11 Ls. Hs are relatively scarce in CCRTU, IMPR, and IFR, whereas ELAR, DFQ, and AIPCS feature more Ms, suggesting these areas are most amenable to transforming Ls to Ms or Ms to Hs.

The Bank and theme can be used to target implications of action. HAB banks having indices above 1.70 (e.g. BOB 1.7647, ICICI 1.7647, IDFC 1.7647, Yes 1.7647) are to lock in the governance depth by increasing the ITBCS and AIPCS bands of B to H and speeding up the DFQ where it manifests as an obstacle and retain their advantage. LABs around 1.41-1.53 (HDFC 1.4118, IndusInd 1.4118, IB 1.5294) gain the most when DTHE and IMPR are brought to M and ELAR is raised above M, and according to the sector models, this gives step-wise improvements in the predicted outcomes with a level of threshold crossed. Where IFR is the barrier (HDFC, IDFC) then control stronger with analytics prepared (ARAA) to decrease variability induced by incidents. (Table 4.7). The matrix thus functions as a bank-specific modernisation playbook, translating cross-sectional evidence into ranked interventions. (Table 4.7)

Table 4.7 Bank-wise Indicators Dominance Across Various Severity Classes

Name of Bank	Low	Medium	High
Axis	ARAA, CCRTU, IMPR, IFR, CTC, RAISR, DFQ, RAISR.1, LSMARI	DBU, CMD, ITII, BATR, AIPCS, ITBCS	DTHE, ELAR
BOB	IMPR, CMD, CTC, RAISR.1, LSMARI	ARAA, CCRTU, DTHE, DBU, IFR, ELAR, RAISR, DFQ, ITII, AIPCS, ITBCS	BATR
BOMH	DTHE, IMPR, DBU, IFR, ELAR, RAISR.1, BATR	ARAA, CCRTU, CTC, RAISR, DFQ, ITII, LSMARI, AIPCS, ITBCS	CMD
DCB	CCRTU, DTHE, DBU, IFR, CMD, CTC, ELAR, DFQ, ITII, BATR, LSMARI, AIPCS, ITBCS	ARAA, IMPR, RAISR, RAISR.1	
HDFC	CCRTU, DTHE, IMPR, DBU, ELAR, DFQ, RAISR.1, ITII, BATR, AIPCS, ITBCS	ARAA, CMD, CTC, RAISR, LSMARI	IFR
IB	IMPR, IFR, RAISR, DFQ, RAISR.1, ITII, BATR, AIPCS, ITBCS	ARAA, CCRTU, DBU, CMD, CTC, ELAR, LSMARI	DTHE
ICICI	IMPR, DBU, IFR, CMD, ELAR, LSMARI, AIPCS	ARAA, DTHE, CTC, RAISR.1, ITII, BATR, ITBCS	CCRTU, RAISR, DFQ
IDFC	ARAA, DTHE, CMD, CTC, DFQ, BATR	CCRTU, DBU, ELAR, RAISR, RAISR.1, ITII, LSMARI, AIPCS, ITBCS	IMPR, IFR
Indusind	ARAA, DTHE, DBU, IFR, CTC, ELAR, DFQ, ITII, BATR, LSMARI, AIPCS, ITBCS	IMPR, RAISR, RAISR.1	CCRTU, CMD
IOB	IMPR, DBU, IFR, CMD, CTC, DFQ, ITII, BATR, AIPCS	ARAA, CCRTU, DTHE, ELAR, RAISR, RAISR.1, LSMARI, ITBCS	
Kotak	CCRTU, IMPR, IFR, CMD, CTC, RAISR, DFQ, RAISR.1, ITII, BATR, LSMARI, AIPCS, ITBCS	ARAA, DTHE, ELAR	DBU
SBI	CCRTU, IFR, CTC, ELAR, RAISR, LSMARI, ITBCS	ARAA, DTHE, IMPR, DBU, CMD, DFQ, RAISR.1, ITII, BATR, AIPCS	
UCO	CCRTU, CTC, DFQ, RAISR.1, BATR	ARAA, DBU, IFR, CMD, ELAR, RAISR, ITII, LSMARI, AIPCS, ITBCS	DTHE, IMPR
Union	ARAA, DTHE, IMPR, DBU, IFR, CMD, ELAR, RAISR.1, BATR, AIPCS	CCRTU, CTC, RAISR, DFQ, ITII, LSMARI	ITBCS
Yes	CCRTU, IFR, CMD, ELAR, LSMARI	ARAA, DTHE, IMPR, DBU, CTC, RAISR, DFQ, RAISR.1, ITII, AIPCS, ITBCS	BATR

To conclude, an analysis of preparedness index of all the banks in terms of secondary data sources indicated that DCB, Kotak, HDFC, Indian Bank, and State Bank of India are the least adaptive ones. Nevertheless, the remaining banks that will require additional adaptability modifications include bank of Baroda, ICICI, Indusind, State Bank of India and UCO. These were Enabler perspective responses, although one can do some analysis through the employee perspective as well these responses simply will not be sufficient without secondary data analysis. This should also be supported by primary response. To confirm this, the research shifted straight to evaluating the employee angle, as discussed in the following chapter.

5. CHAPTER 5

BANK CLASSIFICATION AND INDICATORS SEVERITY ANALYSIS FROM THE USER PERSPECTIVE: APPLICATION OF PRIMARY DATA

Though the analysis of the secondary data has given in-valuable background concerning the bank-level behavioural patterns as well as the operational indicators and the dynamic in relation to fraud, this information remains inadequate to classify the motivation of CF drivers completely. Secondary data suggests merely the institutional standpoint, but it is also the frontline staff behaviour, operational practice and experience-sharing that is extremely important in terms of conspiracy of multiple fraud formation, detection and reduction. Therefore, a transition to primary data analysis becomes necessary to capture the human-centric dimension of fraud risk that bank-level datasets cannot fully represent. As explained in Section 3.3, data were gathered through a structured primary survey by gathering the responses of the employees working in all the 15 banks involved. In total, 258 responses were gathered and processed using a normalised analytical approach, enabling the consolidation of respondent perceptions into comparable scales across institutions. These normalised and cumulative primary insights form the basis of the subsequent analysis, and the results are presented below.

5.1 CUMULATIVE BANK-SPECIFIC INDICATORS NORMALISED WEIGHT CALCULATION

While primary data analysis was conducted as described in Section 3.4, the overall bank data analysis highlights key variables within the Core Beliefs (TAM) theme and shows their normalized impact values. Perceived Usefulness (PU) has a normalized impact of 7.11 percent, compared to Perceived Ease of Use (PEOU) at 6.53 percent. PU is most affected in this category and has total domain weight of 13.64% with weighted average of 6.82, which puts it in the zone of Low Impact (LI) having a High severity. In Core Beliefs (TAM) theme, PU is the key variable, then PEOU, where both of them are rated highly in severity reflecting their quite important weight in influencing beliefs. Digital Readiness (DR) is leading the Personal Capabilities theme with a rate of 4.23 percent, Digital literacy (DL) has 4.13 percent and Technological Self-Efficacy with 3.80 percent. The total weight of this domain is equal to 12.16% and the weighted average is equal to 4.05, which is classified as Low Impact (LI), and DR, DL has high-severity influences and TSE has a lesser effect. In the Risk and Trust Indicators theme, Trust in Technology (TT) exerts the most influence at 3.31 percent, followed by Perceived Risk (PR) at 3.16 percent, Cybersecurity Awareness (CSA) at 3.02 percent, and Job Security Concerns (JSC) at 2.84%. It has the total weight of 12.32 with a weighted average

of 3.08 in the Low Impact (LI) zone, with all variables of high severity which is critical impact on behavior regardless of low impact magnitude. The primary theme variable, Human-AI Collaboration (HAC) representing the Sociotechnical Alignment theme has a dynamic effect of 11.93 percentage, and the overall weight of the domain and the overall mean is also 11.93 percent, making it a Low Impact (LI) with a Moderate severity of the variable, as it is strong but has a balanced effect on integrating the human and AI systems. System Quality (SQ) is most influential factor as it had the greatest impact on the topic (17.64 percent) in the System Characteristics (TAM2) theme and occupies the High Impact (HI) section with indispensability of the printed matter in the system performance. Human-AI Collaboration (IHAC) dominates the Compatibility and Usage (TAM2) domain, with a normalized result of 15.81 percent and a severity of High Impact (HI), which displays the significance of this behavior and interaction part. Cybersecurity Investment (CSI), Facilitating Conditions (FC), Regulatory Alignment (RAI), Employee Reskilling Investment (ERI), and AI Infrastructure Readiness (AIR) rank first, second, third and fourth with an impact of 3.53 percent, 3.45 percent, 3.19 percent, and 3.15 percent, respectively in the Facilitating Conditions (UTAUT) theme. The overall weight of this domain is 16.49 and weighted average is 3.30 which is high impact (HI). CSI and FC are extremely severity aspects whereas ERI, AIR, and RAI are intermediately cochanneling effects. Overall, System Quality (SQ) and Human–AI Collaboration (HAC/IHAC) are the main impact drivers, both in high-impact zones. Conversely, core beliefs and risk factors, despite their critical importance (high severity), operate mainly within lower impact zones. This indicates that while behavioral and perceptual factors shape adoption, system efficiency and human–AI integration are the primary determinants of overall impact and success.

Table 5.1 Primary survey-based indicators classification

CORE THEME	VARIABLE	ABBREVIAT ION	N O OF 1' S	N O OF 2' S	N O OF 3' S	N O OF 4' S	NO OF 5'S	WEIGHT ED SUM	WEIGHTE D AVERAGE	IMPAC T RATIN G	WA* IR	NORMALISE D IMPACT	
CORE BELIEFS (TAM)	Perceived Usefulness (PU)	PU	9	19	20	11	6	347	2306	4.5127	0.0625 00	0.282 045	7.11%
	Perceived Ease of Use (PEOU)	PEOU	4	14	82	21	3	198	2120	4.1487	0.0625 00	0.259 295	6.53%
PERSONAL CAPABILITIES	Technology Self- Efficacy (TSE)	TSE	26	58	13 8	15 2	137	1849	3.6184	0.0416 67	0.150 766	3.80%	
	Digital Literacy (DL)	DL	12	20	10 2	23 2	145	2011	3.9354	0.0416 67	0.163 976	4.13%	
	Digital Readiness (DR)	DR	10	29	82	20 7	183	2057	4.0254	0.0416 67	0.167 727	4.23%	
RISK & TRUST INDICATORS	Perceived Risk (PR)	PR	13	21	95	20 2	180	2048	4.0078	0.0312 50	0.125 245	3.16%	
	Trust in Technology (TT)	TT	6	11	70	21 2	212	2146	4.1996	0.0312 50	0.131 238	3.31%	

SYSTEM CHARACTERISTICS (TAM2)	SOCIOTECHNICAL ALIGNMENT	Cybersecurity Awareness (CSA)	CSA	17	53	10	16	174	1959	3.8337	0.031250	0.119802	3.02%
		Job Security Concerns (JSC)	JSC	29	68	11	15	140	1842	3.6047	0.031250	0.112647	2.84%
		Human-AI Collaboration (HAC)	HAC	16	36	13	18	143	1936	3.7886	0.125000	0.473581	11.93%
		System Quality (SQ)	SQ	2	12	65	23	197	2146	4.1996	0.166667	0.699935	17.64%
	COMPATIBILITY/IMAGE (TAM2)	Human-AI Collaboration (IHAC)	IHAC	14	50	11	18	141	1924	3.7652	0.166667	0.627528	15.81%
		Facilitating Conditions (FC)	FC	4	8	91	23	171	2096	4.1018	0.033333	0.136725	3.45%
		Employee Reskilling Investment (ERI)	ERI	18	40	13	16	157	1936	3.7886	0.033333	0.126288	3.18%
		AI Infrastructure Readiness (AIR)	AIR	9	35	15	17	129	1917	3.7515	0.033333	0.125049	3.15%
		Regulatory Alignment (RAI)	RAI	21	41	11	18	153	1938	3.7926	0.033333	0.126419	3.19%
		Cybersecurity Investment (CSI)	CSI	7	11	76	19	221	2146	4.1996	0.033333	0.139987	3.53%
											3.968253		
	FACILITATING CONDITIONS (UTAUT)												

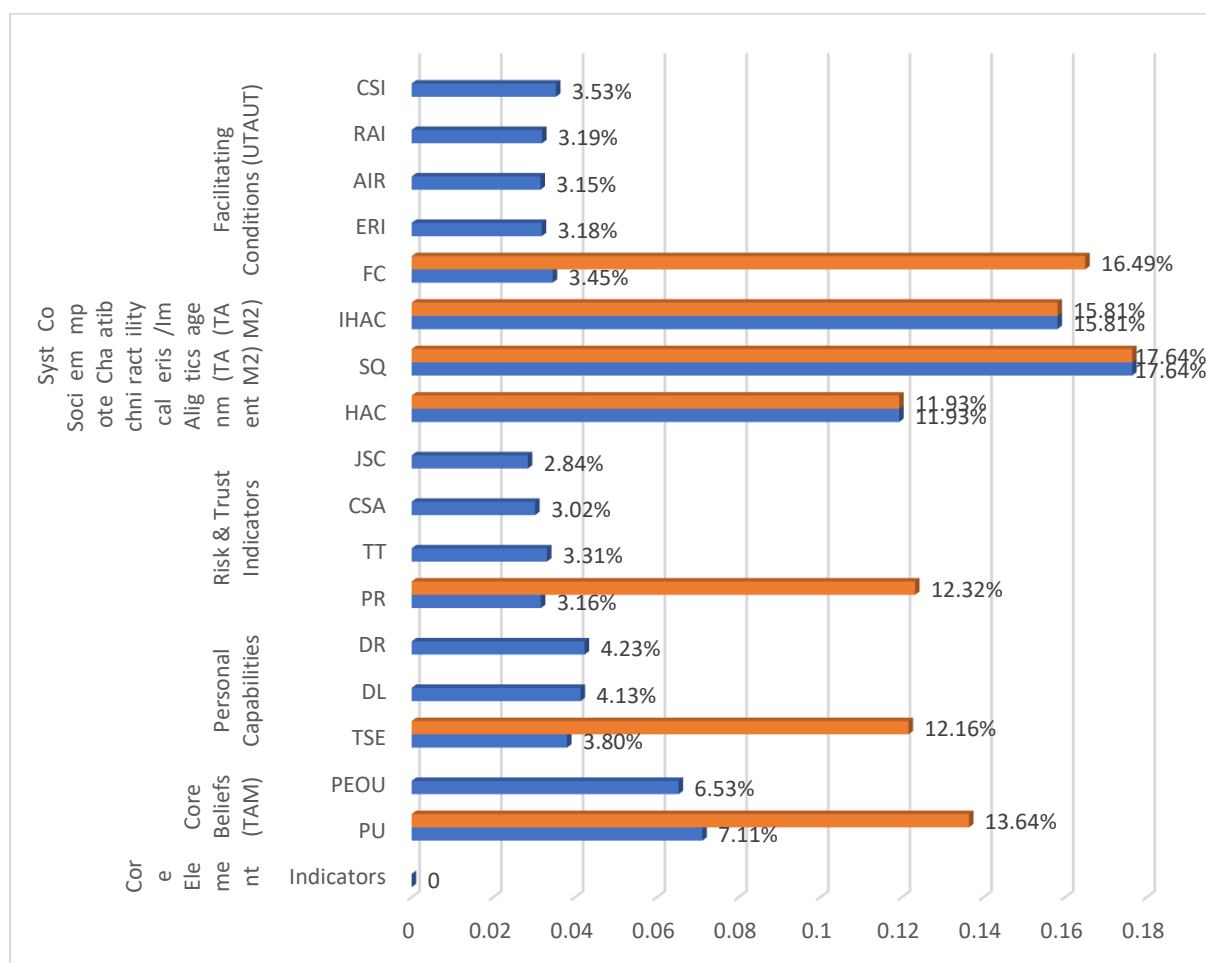


Figure 5.1 All banks' Variables Severity Analysis comparative plot

Table 5.2 All banks' Variables Severity Analysis and Ranking

Core Element	Variable Abbreviation	Normalised Impact	Aggregate weight of the subdomain	Weighted average	Zonal Impact	Level of severity
Core Beliefs (TAM)	PU	7.11%				H
	PEOU	6.53%	13.64%	6.82%	LI	H
Personal Capabilities	TSE	3.80%				L
	DL	4.13%			LI	H
Risk & Trust Indicators	DR	4.23%	12.16%	4.05%	LI	H
	PR	3.16%				H
	TT	3.31%			LI	H
	CSA	3.02%			LI	H
Sociotechnical Alignment System	JSC	2.84%	12.32%	3.08%		H
	HAC	11.93%	11.93%	11.93%	LI	M
Characteristics (TAM2)	SQ	17.64%	17.64%	17.64%	HI	M
	IHAC	15.81%	15.81%	15.81%	HI	M
Compatibility/Image (TAM2)	FC	3.45%				H
	ERI	3.18%				H
Facilitating Conditions (UTAUT)	AIR	3.15%				H
	RAI	3.19%			HI	H
	CSI	3.53%	16.49%	3.30%	LI	H
			14.29%	8.95%		

Core Beliefs domain entails high-severity items such as Perceived Usefulness (PU), which is a normalized 7.11 impact, and Perceived Ease of Use (PEOU), which is 6.53, which places PU as the strongest factor that is affecting belief formation. This domain has none of the Moderate-severity factors and does not have any of the Low-severity factors. The high-severity variables in Personal Capabilities are Digital Readiness (DR) with 4.23% and Digital Literacy (DL) with 4.13% both highlighting the role of preparedness and capability in the adoption of technology. This core element has no Moderate-severe factors. Technology Self-Efficacy (TSE) has Low-severity (3.80) which is less significant than DR and DL. As part of the Risk and Trust Indicators element, factors with high severity include Trust in Technology (TT) with a score of 3.31%, Perceived Risk (PR) with a score of 3.16, Cybersecurity awareness (CSA) with a score of 3.02, and Job security concerns (JSC) with a score of 2.84, meaning that trust and security concerns have a critical impact on user behavior. In this domain, there are no Low- and Moderate-severity factors. This core element has no high-severity factors. The only Moderate-severity factor is Human–AI Collaboration (HAC) at 11.93%, which plays a significant role in aligning human processes with AI systems. There are no Low-severity

variables in this category. System Characteristics contain one key Moderate-severity factor: System Quality (SQ) with a high numerical impact of 17.64%, though classified as moderate in severity. There are no high- or low-severity variables in this core element. This domain includes one Moderate-severity factor, IHAC, which has a substantial normalized impact of 15.81%. The high-severity factors in the Facilitating Conditions domain include Facilitating Conditions (FC) at 3.45%, Cybersecurity Investment (CSI) at 3.53%, Employee Reskilling Investment (ERI) at 3.18%, AI Infrastructure Readiness (AIR) at 3.15%, and Regulatory Alignment (RAI) at 3.19%, highlighting their influence on adoption readiness. There are no Moderate- or Low-severity factors in this category.

5.2 BANK-SPECIFIC INDICATORS' CLASSIFICATION

Across the banks listed, each institution exhibits a distinct distribution of indicators across the Low (L), Medium (M), and High (H) categories. Axis Bank shows wide dispersion, with many indicators, such as ARAA, CCRTU, IMPR, IFR, CTC, RAISR, DFQ, RAHSR, and LSMARI, falling into the Low category. A thick cluster of DBU, CMD, ITII, BATR, AIPCS and ITBCS occupies the medium category, with only two DTHE and ELAR put under the high category. This is indicative of a dualistic but risk-averse profile. Bank of Baroda (BOB) allocates most indicators, i.e., IMPR, CMD, CTC, RAHSR and LSMARI, to the Low category. A broader set is assigned to the Medium category, including ARAA, CCRTU, DTHE, DBU, IFR, ELAR, RAISR, DFQ, ITII, AIPCS, and ITBCS. Only BATR appears in the High category, indicating a moderate concentration in mid-level indicators. Bank of Maharashtra (BOMH) places many indicators in the Low category, such as DTHE, IMPR, DBU, IFR, ELAR, and RAHSR, with several others in the Medium category. CMD appears alone in the High category, suggesting a narrower high-risk profile. DCB Bank shows an extensive Low category, including CCRTU, DTHE, DBU, IMPR, CTC, ELAR, DFQ, ITII, BATR, and LSMARI. ARAA, IMPR and RAISR.1 are included under Medium category and none of the indicators are regarded as High.

Low indicators in HDFC bank include CCRTU, DTHE, IMPR, DBU, ELAR, DFQ, RAISR.1, ITII as well as BATR. The Medium category contains ARAA, CMD, CTC, RAISR, IFR, and LSMARI. No indicators are assigned to the High category. Indian Bank (IB) places many indicators in the Low category, including IMPR, IFR, RAISR, DFQ, RAISR.1, and ITII. Under Medium falls a set of three comprising of ARAA, CCRTU, DBU, CMD, CTC, ELAR, and LSMARI. The only indicator of the High category is DTHE. There are Low indicators of which

ICICI Bank classifies IMPR, DBU, IFR, CMD, ELAR, LSMARI, and AIPCS. There is a good number of entrants in the Medium category, such as DTHE, CTC, and RAHSR, ITII, BATR, and ITBCS. CCRTU, RAISR and DFQ belong under the High category. ICICI Bank categorises several indicators as Low, including IMPR, DBU, IFR, CMD, ELAR, LSMARI, and AIPCS. A substantial group appears in the Medium category, including DTHE, CTC, and RAHSR, ITII, BATR, and ITBCS. CCRTU, RAISR, and DFQ are placed in the High category. IDFC Bank has fewer Low indicators, i.e, ARAA, DTHE, CMD, CTC, DFQ, and BATR. A moderate set falls under the Medium category, including CCRTU, DBU, ELAR, and RAHSR, ITII, LSMARI, AIPCS, and ITBCS. The IMPR and IFR are marked as High.

IndusInd Bank has numerous indicators in the Low category and they are ARAA, D THE, D BU, IFR, CTC, ELAR, DFQ, ITII, BATR, LSMARI and AIPCS. Medium group encompasses IMPR, RAISR, and RAHSR whereas CCRTU and CMD are under High group. Indian Overseas Bank (IOB) disperses indicators in both categories where there is a large number of values in the Low category and a formidable Medium category where Indian AAA, CCRTU, DTHE, ELAR, RAISR, RAHSR, LSMARI, and ITBCS are found. No indicators are placed in the High category. Kotak Mahindra Bank places several indicators in the Low category, including CCRTU, IMPR, IFR, CMD, CTC, RAISR, DFQ, RAHSR, ITII, BATR, LSMARI, AIPCS, and ITBCS. The ARAA, DTHE and ELAR are the only indicators that fit in the Medium category and only DBU is indicated as High-severity. State Bank of India (SBI) shows a compact Low category and a medium-heavy cluster including ARAA, DTHE, DBU, CMD, DFQ, RAISR.1, ITII, BATR, and AIPCS. No indicators are classified as High. UCO Bank spans all three levels, with CCRTU, CTC, DFQ, RAHSR, and BATR in the Low category. A broader Medium set includes ARAA, DBU, IFR, CMD, ELAR, RAISR, ITII, LSMARI, AIPCS, and ITBCS. DTHE and IMPR fall into the High category. Union Bank and Yes Bank both have large Low categories, including ARAA, DTHE, IMPR, DBU, IFR, CMD, ELAR, and RAISR.1. They also feature substantial Medium groups. Union Bank assigns ITBCS to the High category, while Yes Bank assigns BATR and a few additional indicators to the High category. Both show a bifurcated classification structure with selective high-risk elements.

5.3 PREPAREDNESS ANALYSIS OF BANKS BASED ON INDICATORS CLASSIFICATION

Within the Core Beliefs (TAM) domain, the only High-severity factor is Perceived Usefulness (PU), with a normalised impact of 6.97 percent and standing out as the strongest determinant of belief formation. This domain does not contain any Moderate-severity factors. Low-severity factors are Perceived ease of use (PEOU), which makes graded at 6.56 percent and Technology self-efficacy (TSE), which falls at 3.95% and both of them are related to the formation of beliefs although to a lesser degree compared to PU. Under the Personal Capabilities domain, the High-severity elements are the Digital Risk (DR) with a 4.36 percent and Perceived Risk (PR) with a 3.09%, which means that the perception of the risk factors significantly contributes to the ability assessment of individuals. The latter domain contains no moderate-severe variables. The Low-severity factor is Digital Literacy (DL) at 4.10%, which, although numerically close to the risk indicators, is classified as having lower influence.

Trust (TT) and Cybersecurity Awareness (CSA) are High-severity factors in the Risk and Trust Indicators domain with 3.26 percent and 3.14 percent score respectively, indicating the central place of trust and security in the user behaviour pattern.. There are no Moderate-severity factors in this domain. The Low-severity factor is Job Security Concern (JSC) at 2.75 percent, which has the least influence within this category. The Sociotechnical Alignment core element does not contain any High-severity factors. Human-AI Collaboration (HAC) is the only Moderate-severity variable with a significant impact, 12.19 percent normalised. This means that it is applicable in determining the alignment between human processes and AI systems. Low-severity factors do not exist in this field. In the System Characteristics (TAM2) domain, the sole contributing variable is System Quality (SQ), classified as Moderate-severity with a substantial normalised impact of 17.43 percent. This domain does not include any High-severity or Low-severity indicators.

The Compatibility and Image (TAM2) domain also contains a single variable, IHAC (Image and Compatibility), which is identified as a Moderate-severity factor with a normalised impact of 15.98 percent. There are no High-severity or Low-severity variables in this domain. Within the Facilitating Conditions (UTAUT) domain, the High-severity factors include Facilitating Conditions (FC) at 3.39 percent and Customer Service Infrastructure (CSI) at 3.43 percent, both of which play a strong role in determining adoption readiness. There are no Moderate-severity variables in this domain. The Low-severity factors are Environmental Readiness (ERI)

at 3.08 percent, AI Readiness (AIR) at 3.13 percent, and Resource Availability (RAI) at 3.17 percent, each of which contributes modestly to the enabling conditions for system adoption.

5.4 PRIMARY DATA BANKS PREPAREDNESS INDEX ESTIMATION

1. Axis Bank – Axis Bank’s index of 5.33 is based on 6 High, 3 Medium, and 8 Low ratings and prominent employee-level indicators contributed as PU, PEOU, TSE, DL, PR, TT, CSA, and JSC are mostly low, showing limited readiness across skill, perception, and support functions. Though DR and HAC score Medium, it offers support; however, the high indicators are FC, ERI, AIR, and RAI, which indicate strong financial capacity and operational resilience. Since foundational employee parameters reduce overall preparedness and make the banks a LAB where dominant Employee indicators are PEOU, TT, CSA, and BLF, Axis Bank shows strong capital strength but poor employee-level readiness, resulting in a mid-range score and needs to be worked on these areas.

2. Bank of Baroda – EPI is 5.67 stems from 7 High, 3 Medium, and 7 Low indicators shows high-rated are DR, PR, TT, CSA, HAC, SQ, and FC, reflects strong technical and operational alignment. Low ratings in PU, PEOU, TSE, DL, and JSC weaken the employee side. Though bank-level performance shows mixed variation due to ERI and RAI are rated as high but AIR rated low makes the adaptability LAB. The dominant EDF includes PEOU, PR, TT, and BLF in ERI. Consistent bank-level strengths push the score upward despite employee-related weaknesses.

3. Bank of Maharashtra - Preparedness Index: 6.17, is among the best profiles, as it has 7 High, 6 Medium and only 4 Low ratings. Strong scores in PU, DR, PR, TT, CSA, HAC, and FC depict strong capability of preparation in major indicators of operation and behaviors. Well-rounded consistency is achieved by medium ratings in PEOU, TSE, SQ, IHAC, AIR, and JSC. Poor scores in DL, ERI and RAI are constrained. HAB is adaptable, and PEOU, PR, TT are the predominant EDF, as well as ERI is the dominant BLF. High and Medium ratings with little weaknesses features make a strong combination leading to high preparedness score.

4. DCB Bank - Preparedness Index: 6.33, as a result of 9 High, 3 Medium, and 3 Low ratings - a good profile. The scores of PU, PEOU, TSE, DR, PR, TT, HAC, SQ, and FC are high and demonstrate a high level of preparedness both at an employee and bank level. Median scores of DL, CSA and IHAC moderate maintaining performance. Risk is kept at a minimum by low

ratings only in JSC, AIR, and RAI. The level of adaptability is HAB, prevailing EDF is PU, DL, PR, TT, and dominance of BSF is RAI. The high-impact High scores are concentrated and DCB gets into the highest category.

5. HDFC bank - Preparedness Index: 5.33, is calculated on 6 High rating, 3 Medium, and 8 Low rating. Strong capabilities by the bank level are indicated by a high DR, PR, TT, CSA, HAC and FC. Nonetheless, low scores in the PU, PEOU, TSE, DL, JSC, ERI, AIR, and RAI bring the index to the downside. The middle zone is stabilized by medium scores in SQ, IHAC and RAI. Being highly institutionally robust and somewhat lacks certain homogenous employee level preparedness, HDFC is flexible with adaptable LAB, dominant EDF, PEOU, DR, TT, and BLF ERI.

6. Indian Bank - Preparedness Index: 6.33, at 9 High, 3 Medium and only 3 Low ratings. Good scores in PU, TSE, DL, PR, TT, CSA, HAC, SQ, and FC reveal high ability in the perception, training, and execution, and capital. Stability is rounded off by medium in PEOU, DR, and IHAC. The low scores are restricted to JSC, AIR and RAI. Adaptability LAB : the dominating EDF is PU, DL, PR and BLF is RAI. Its employee and bank-level ratings are strong, which places it on top of the performers.

7. ICICI Bank - Preparedness Index: 5.67, and is founded on 7 High, 3 Medium, and 7 Low ratings. Good operating performance is represented in highly rated parameters like PU, PR, TT, CSA, HAC, SQ and FC. PEUU, DR, and IHAC have moderate consistency in medium scores. Poor scores in TSE, DL, JSC, AIR, ERI, and RAI undermines the employee and technical base. LAB is dominant EDF PEOU, PR, TT and BLF AIR adaptable. The structure which is balanced and uneven creates a mid-high preparedness level.

8. IDFC Bank - Preparedness Index 5.83, IDFC gets 5.83 which is rated 7 High, 4 Medium, and 6 Low ratings. Core strength is created by high scores in PU, DR, PR, TT, CSA, HAC, and FC. Peers of PEOU, TSE, SQ, and IHAC have medium scores that favour stability. NEP has gaps in its skills and operations as demonstrated by low scores in DL, JSC, AIR, ERI, and RAI. The level of adaptability is HAB and EDF PU, DR, TT and BLF ERI. The score is explained by a strong base having moderate inconsistencies.

9. IndusInd bank - Preparedness Index: 5.83 is supported by 7 Higher, 4 Mediocre, and 6 Low ratings. Prices of PU, PR, TT, CSA, HAC, SQ, and FC are high, which indicate high preparedness of the core. In PEOU, DL, DR and IHAC, media are balanced in depth. Poor

scores in TSE, JSC, AIR, ERI, and RAI are indicators of gaps in capabilities. HAB, dominant EDF PU, PR, TT and BLF ERI is adaptive. This combination produces a stable but not the best preparedness.

10. Indian Overseas Bank - Preparedness Index: 5.67 with an index calculated based on 7 High, 4 Medium and 6 Low ratings. maximized PU, DL, PR, TT, CSA, HAC and FC reinforce the structure. PEOU, DR, SQ, and the IHAC have mediums whose operations are predictable. The lows of TSE, JSC, AIR, ERI, and RAI decrease the depth of overall capability. LAB, dominant EDF PU, PR, TT and BLF ERI all have adaptability. The bank has some stable strengths but significant weak points.

11. Kotak Mahindra Bank - Preparedness Index: 5.50, is produced by 5 High, 4 Medium, and 8 Low ratings. Strong alignment is observed at bank level when there are highs in DR, PR, TT, HAC and FC. PEOU, DL, SQ, and IHAC have mediums that are partially stable. Poor insurances on PU, TSE, CSA, JSC, AIR, ERI, RAI degrade under and technical stability. Adaptability is LAB, dominant EDF TSE, TT, PR and BLF FC. The reason behind the mid-range preparedness is the high number of Low scores.

12. State Bank of India: Preparedness Index: 5.17, preparedness Index of 5.17 of SBI is the result of High, medium and Low 5, 4 and 9 ratings respectively- the highest number of Low ratings. Top scores on PR, TT, CSA, HAC, and FC demonstrate the bank level competence whereas poor employee-level competencies are reflected in Low score on PU, PEOU, TSE, DL, DR, JSC, AIR, ERI, and RAI. There is little offset in medium in SQ, IHAC, and RAI. In adaptability LAB, predominant EDF PU, PR, TT, and BLF ERI, the poor pervasive scores of SBI provide the worst preparedness.

13. UCO Bank - Preparedness Index: 6.33, is generated by 9 High, 3 Medium and 3 Low ratings. PU, DL, DR, PR, TT, CSA, HAC, SQ and FC represent the preparation of a wide scope. PEOU, TSE and IHAC have mediums that provide coherency. Limited Low ratings (JSC, AIR, RAI) make insignificant impression. The dominant EDF PU, DR, TT, and BLF ERI are adaptable. Among the best profiles of all the banks.

14. Union Bank - Preparedness Index: 5.33, which is the result of 6 High, 3 Medium, and 8 Low ratings. Strengths of DR, PR, TT, HAC, SQ, and FC. In PEOU, TSE and IHAC, mediums are added with moderate balance. Capacity failures are indicated by the lows in PU, DL, CSA,

JSC, AIR, ERI, RAI. The dominant EDF PU, DR, TT, and BLF ERI are adaptable. The asymmetric allocation makes the index moderate.

15. Yes Bank - Preparedness Index: 5.67, is a product of 6 high, 5 medium and 6 low ratings. Strong structural strength is demonstrated by highs in PU, DL, PR, TT, HAC and FC. PEOU, TSE, DR, CSA and IHAC mediums are operationally stable.. Low scores in JSC, SQ, AIR, ERI, and RAI reflect gaps in internal capability. With adaptability LAB, dominant EDF PU, PR, TT, and BLF ERI, the bank presents stable but imperfect preparedness.

Table 5.3 Summary of Primary Data Analysis Across Each Bank Individually and Summary of Responses

	Bank Name	Axis Bank	Bank of Baroda	Bank of Maharashtra	DCB Bank	HDFC Bank	Indian Bank	ICICI Bank	IDFC	Indusind Bank	Indian Overseas	Kotak Mahindra Bank	Satte Bank of India	UCO Bank	Union Bank	Yes
Employee Level	PU	L	H	L	H	L	H	H	H	H	H	H	H	H	H	M
	PEOU	H	L	H	L	H	L	L	L	L	L	L	L	L	L	M
Bank Level	TSE	L	L	M	L	L	L	L	M	M	H	L	L	L	L	L
	DL	L	L	M	H	L	H	H	H	H	L	M	H	H	H	L
	DR	H	H	M	H	H	H	H	L	L	H	H	M	H	L	H
	PR	L	H	H	H	L	H	L	H	H	H	L	L	H	L	H
	TT	H	L	H	H	H	H	H	H	H	H	H	H	H	H	H
	CSA	H	H	L	H	H	H	H	H	H	L	H	L	L	L	H
	JSC	L	L	L	L	L	L	L	L	L	L	L	L	H	H	L
	HAC	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
	SQ	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
	IHAC	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
	FC	H	H	H	H	H	L	H	H	H	H	H	H	H	H	H
	ERI	L	H	H	H	L	L	L	L	L	L	M	L	H	L	L
	AIR	L	L	H	L	L	H	L	L	L	L	M	L	L	L	L
	RAI	H	L	H	L	H	H	L	L	L	L	L	L	L	L	L
	ggdgm	L	H	L	H	L	H	H	H	H	H	L	H	H	H	H
	No of H	6.00	7.00	7.00	9.00	6.00	9.00	7.00	7.00	7.00	7.00	5.00	5.00	9.00	6.00	6.00
	No of M	3.00	3.00	6.00	3.00	3.00	3.00	3.00	4.00	4.00	3.00	6.00	4.00	3.00	3.00	5.00
	No of L	8.00	7.00	4.00	5.00	8.00	5.00	7.00	6.00	6.00	7.00	6.00	8.00	5.00	8.00	6.00
	Preparedness Index	5.33	5.67	6.17	6.33	5.33	6.33	5.67	5.83	5.83	5.67	5.50	5.17	6.33	5.33	5.67
	Adaptability level of banks	LAB	LAB	HAB	HAB	LAB	HAB	LAB	HAB	HAB	LAB	LAB	LAB	HAB	LAB	LAB
	Dominant EDF	PEOU TT CSA	PU DR PR CSA	PEOU PR TT	PU DL DR PR TT CSA	PEOU DR TT CSA	PU DL DR PR TT CSA	PU DL DR TT CSA	PU DL PR TT CSA	PU DL PR TT CSA	PU TSE DR PR TT	PU DL TT CSA	PU DL TT	PU DL DR PR TT JSC	PU DL TT JSC	DR PR TT CSA
	Dominant BLF	FC RAI	FC ERI ggdgm	FC ERI AIR RAI	FC ERI ggdgm	FC RAI	AIR RAI ggdgm	FC ggdgm	FC ggdgm	FC ggdgm	FC ggdgm	FC	FC ggdgm	FC ERI ggdgm	FC ggdgm	FC ggdgm

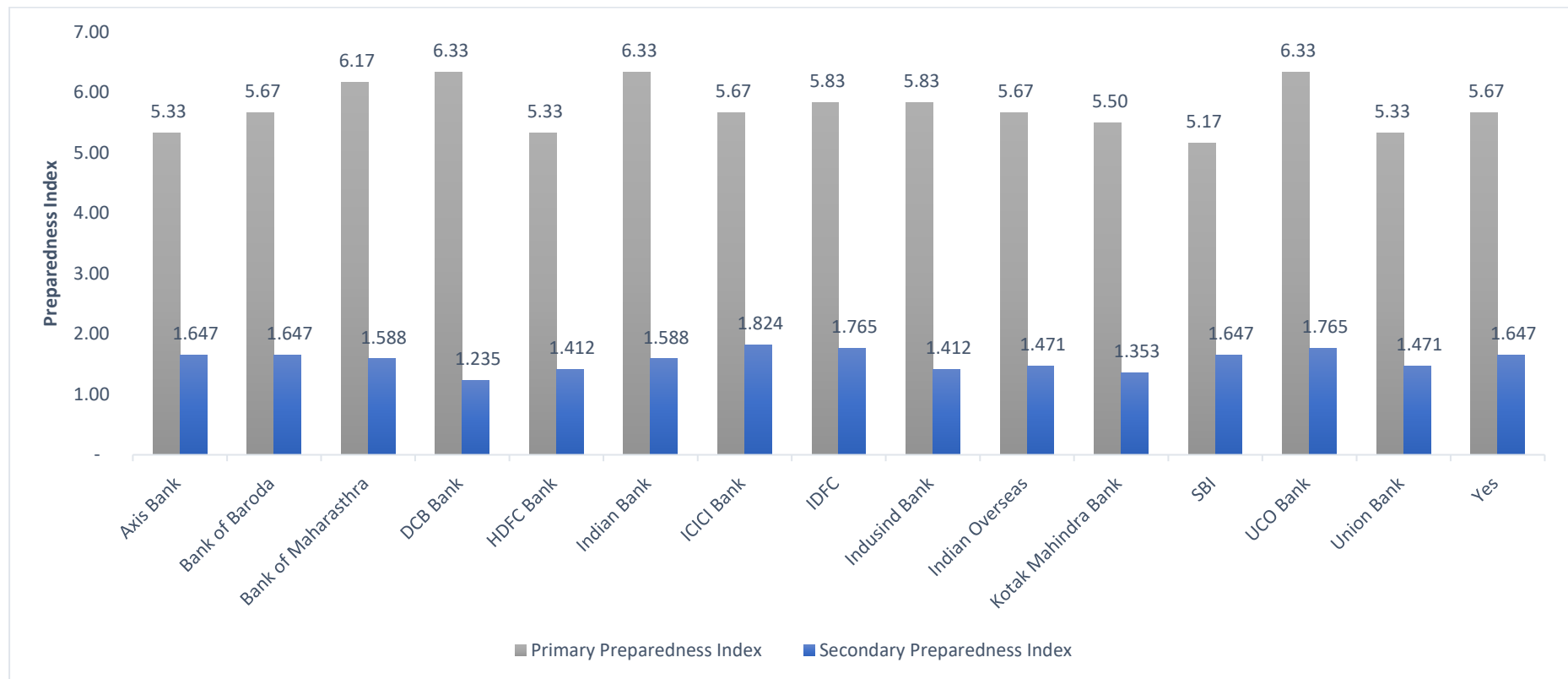


Figure 5.2 . Normalised rating of Individual Indicators (prepared by authors)

5.5 COMPARISON BETWEEN PRIMARY AND SECONDARY DATA: INDEX CALCULATION AND EXPLORATION OF DOMINANT INDICATORS

The relative comparison of both primary and secondary data provides an in-depth perspective on bank level preparedness because it has both bank level preparedness (enabler perspective) and employee level preparedness (user perspective). The Preparedness Index, which is calculated on the basis of secondary and primary data separately, reveals a clear-cut difference in institutional and employee adaptability. The EPI is quite low and well concentrated (around 1.23 to 1.82), meaning that banks do not distinguish themselves much in formal infrastructure, governance, and readiness on the system level. The majority of banks are classified as either HAB or LAB, which implies that basic structures for fintech readiness exist but high preparedness under an enabler perspective is still needs to be modifieds. In contrast the EPI values are much higher (approximately between 5. 17 and 6. 6.33), as the confidence of the employees, their ability to adapt, and their readiness to adopt the technologies are reflected. The binary classification using employee-based data reveals that again banks are categorised as HAB and LAB types and where some banks show high level of behavioral adaptability than structural preparedness. The large gap between the Index of Enabler Preparedness (1.23 to 1.82) and the Index of User Preparedness (5.17 to 6.33) can be seen as the adaptability in human behaviour and organizational change are developing at a different speed. Although the employees have quickly adjusted to the digital platform through exposure, training and the ease of use of the FinTech platforms, the institutional systems are still limited to work within the historical infrastructure, regulation-based compliance, and high-cost investments in technology, and found a discrepancy in investment made in technology and in the similar speed the infrastructure change or governance dynamism is not changed. This highlights the asymmetry between behavioural readiness and structural readiness. Moreover, the presence of multiple barriers around organisational inertia, risk aversion and fragmented and innovative digital strategies slower institutional adaptation, which increases the preparedness gap. The observation is not just a statistical phenomenon but a structural phenomenon that directly influences the quality of FinTech integration. This difference between the primary and secondary findings indicate a gap of readiness, as employees seem ready and flexible than the institute systems that enable them. This difference means that banks are already evolving user-level familiarity and acceptance, but enabler-side capabilities including infrastructure, integration, and governance mechanisms are not evolving equally fast. Besides, the joint analysis of Enabler- Level (EL) and Bank- Level (BL) measure can determine similar (S) and

different (D) trends in banks. The fact that similar indicators are apparent in both the perspectives implies that there is consistency in some aspects of preparedness, whereas the discrepancies indicate that banks have particular issues, strengths and weaknesses, and inequalities in growth across aspects. On the user (EL) level, the most prevalent indicators used repetitively are Perceived Usefulness (PU), Digital Literacy (DL), Trust (TT), Perceived Risk (PR), and Human-AI Collaboration (HAC), implying that the readiness to behave is mostly perception-driven, awareness-driven, and interaction with technology. At the enabler (BL) level, such prevailing pointers as System Quality (SQ), Human–AI Compatibility (IHAC), Employee Reskilling (ERI), AI Infrastructure Readiness (AIR), and Regulatory Alignment (RAI) highlight the role of system-level capability and institutional support systems in the overall preparedness. The variation of similar and different indicators between banks also underlines the point that preparedness is not universal; it depends on context-specific organization structure, level of technological maturity, and priorities of the strategy. The results of the combined analysis suggest that the preparedness of each bank depends on two essential aspects: Enabler-side preparedness (structural and institutional capabilities) and User-side preparedness (behavioral and adoption capabilities). Also, the analysis identifies major indicators of each bank that are major contributors to their preparedness levels. These pointers give a clear picture of whether a bank's preparedness is fuelled by greater infrastructure in technology, governance, or user adaptability. This suggests that the barriers that contribute the most to the overall criterion of FinTech adoption may not be the ones that have the highest statistical weight but instead the ones that are the most severe meaning that the banks have to address high-severity barriers like AI infrastructure readiness, employee reskilling, and regulatory alignment in order to realise meaningful digital transformation.

Table 5.4 Similar and Diverse Indicators from both Enabler and User Perspectives after Compiling Data of Primary and Secondary Data Analysis

		Axis Bank	Bank of Baroda	Bank of Maharashtra	DCB Bank	HDFC Bank	India n Bank	ICICI Bank	IDFC	Indus ind Bank	India n Overseas	Kotak Mahindra Bank	SBI	UCO Bank	Union Bank	Yes
Seco ndary	Preparedness Index	1.647	1.647	1.588	1.235	1.412	1.588	1.824	1.765	1.412	1.471	1.353	1.647	1.765	1.471	1.647
	Banks Adaptability analysis- Seco ndary Data	HAB	HAB	HAB	LAB	LAB	HAB	HAB	HAB	LAB	LAB	LAB	HAB	HAB	LAB	HAB

Primary	Preparedness Index	5.33	5.67	6.17	6.33	5.33	6.33	5.67	5.83	5.83	5.67	5.50	5.17	6.33	5.33	5.67
	Banks Adaptability analysis-Primary Data	LAB	LAB	HAB	HAB	LAB	HAB	LAB	HAB	HAB	LAB	LAB	LAB	HAB	LAB	LAB
	EL-Similar	PU, DL, PR	PEOU, TSE, DL, TTHAC	TT, JSC, HAC	PEOU, TSE, JSCHAC	TSE, DL, JSC, HAC	NA	PR, JSC	DL, PR, HAC	DR, TT, JSC, HAC	DL, CSA, HAC	PEOU, DR, PR	PEOU, DR, PR, CSA, JSC, HAC	PEOU, CSA, HAC	TSE, DR, PR, Hac	PU, JSC, HAC
	BL-Similar	Nil	SQ, ER, AIR	SQ, ER, RI	IHA, C, AI, R, RAI	ERI, GGD, GF	SQ, F, C, ER, I	IHA, C, R, AI	IHA, C, ER, I	IHA, C, ER, I, AI, R, RAI	IHA, C, ER, I, RAI	RAI, GGD, GF	SQ, I, HAC, AIR	NA	SQ, ER, RI, AIR, GGD, GF	IHA, C, AI, R
	EL-Different	PEOU, TSE, DR, PR, CSA, JSC, HAC	PU, DR, PR, CSA, JSC	PU, PEOU, TSE, DL, DR, PR, CSA	PU, DL, DR, PR, TT, CSA	PU, PEOU, DR, PR, TT, CSA	PU, PEOU, TSE, DL, DR, PR, TT, CSA	PU, PEOU, TSE, DL, DR, TT, CSA	PU, PEOU, TSE, DL, DR, TT, CSA	PU, PEOU, TSE, DL, DR, PR, TT, CSA	PU, PEOU, TSE, DL, DR, PR, TT, CSA	PU, TSE, DL, TT	PU, TSE, DL, TT	PU, TSE, DL, TT	PU, TSE, DL, TT	PEOU, TSE, DL, DR, PR, TT, CSA
	BL-Different	SQ, I, HAC, FC, ERI, AIR, RAI, GGD, GF	IHA, C, FC, RAI, GGD, GF	IHA, C, FC, ERI, AIR, RAI, GGD, GF	SQ, F, C, ER, I, GGD, GF	SQ, I, HAC, FC, AIR, RAI	SQ, IHA, C, AI, R, RAI, GGD, GF	SQ, FC, ERI, AIR, GGD, GF	SQ, F, C, AI, R, RAI, GGD, GF	SQ, F, C, AI, R, RAI, GGD, GF	SQ, F, C, AI, R, GGD, GF	SQ, I, HAC, FC, ERI, AIR	FC, ERI, AIR, GGD, GF	SQ, I, HAC, FC, ERI, AIR, RAI, GGD, GF	IHA, C, FC, AIR	SQ, F, C, ER, I, RAI, GGD, GF
		Axis Bank	Bank of Baroda	Bank of Maharashtra	DCB Bank	HDFC Bank	India Bank	ICICI Bank	IDFC	Indus Bank	India Overseas	Kotak Mahindra Bank	SBI	UCO Bank	Union Bank	Yes

5.6 ROOT CAUSE MAPPING FOR BANKS BASED ON EPI AND UPI VALUE

After identifying similar and dissimilar indicators across comparative analysis between banks, Table 5.5 gives an overall comparison of Enabler Preparedness Index (EPI) and the User Preparedness Index (UPI) of the selected banks, their top indicators, and the root causes. The root-cause mapping has been constructed in a systematic way depending upon the theoretical backgrounds presented in the literature review (Section 2.5) that identified major barriers to the adoption of FinTech behaviourally and institutionally. These underlying causal factors were further extended to the banking sector in line with the intensity of the indicators realised across banks. The relevance and contextual validity of the findings were also enhanced by checking the identified root causes through expert interactions with banking specialists, so that they are operational issues in the real world. the expert validation was not empirical in nature rather it was just validation was structural survey based nor interpretive. This integrated mapping enables one to see that the disparities in preparedness levels among institutional systems (EPI)

and employee adaptability (UPI) are caused by the underlying behavioral and infrastructural constraints. It also offers a systematic framework in connecting the indicator level deviations to the mitigation measures to be taken in order to improve the analytical and practical value of the study.

Table 5.5 Integrated Banks wise Preparedness and root cause mapping

Bank Name	EPI (Secondary)	UPI (Primary)	User Dominant Indicators	Enabler Dominant Indicators	User-Level Root Causes (Employees)	Enabler-Level Root Causes (Banks)
Axis Bank	1.647	5.33	ARAA, CCRTU, IMPR, IFR, CTC, RAISR	DFQ, RAHSR, LSMARI	Lack of clarity on benefits (PU), usability challenges (PEOU), gaps in digital literacy (DL, TSE), fraud concerns (PR)	Gaps in AI infrastructure (AIR), system downtime (SQ), partial regulatory alignment (RAI)
Bank of Baroda	1.647	5.67	IMPR, CMD, CTC	RAHSR, LSMARI	Low trust and awareness (TT, DL), system usability issues (PEOU)	Infrastructure delays (AIR), regulatory gaps (RAI)
Bank of Maharashtra	1.588	6.17	DTHE, IMPR, DBU, IFR, ELAR	RAHSR, BATR	Skill gaps (TSE, DL), perceived risk and job insecurity (PR, JSC)	Weak cybersecurity investment (CSI), governance gaps
DCB Bank	1.235	6.33	CCRTU, DTHE, DBU, IFR, CMD, CTC	DFQ, ITII, BATR, LSMARI, AIPCS, ITBCS	System complexity (PEOU), low training (TSE), trust deficit (TT, PR)	Infrastructure gaps (AIR), weak IT systems (FC), compliance gaps (RAI), low cybersecurity (CSI)
HDFC Bank	1.412	5.33	CCRTU, DTHE, IMPR, DBU, ELAR	DFQ, RAHSR, ITII, BATR, AIPCS, ITBCS	Skill mismatch (TSE, DL), job insecurity (JSC)	Legacy system issues (AIR), low reskilling (ERI), cybersecurity gaps
Indian Bank	1.588	6.33	IMPR, IFR, RAISR	DFQ, RAHSR, ITII, BATR, AIPCS, ITBCS	Usability challenges (PEOU), low confidence (TSE)	Weak IT support (FC), limited ERI, fragmented compliance
ICICI Bank	1.824	5.67	IMPR, DBU, CMD, ELAR	LSMARI, AIPCS	Job role concerns (JSC)	Need for ERI alignment, regulatory adaptation gaps
IDFC	1.765	5.83	ARAA, DTHE, CMD, CTC	DFQ, BATR	Low motivation and clarity (DR, PEOU)	Infrastructure scalability issues (AIR), ERI gaps
IndusInd Bank	1.412	5.83	ARAA, DTHE, DBU, IFR, CTC, ELAR	DFQ, ITII, BATR, LSMARI, AIPCS, ITBCS	Low confidence (TSE), risk concerns (PR), low readiness (DR)	Weak AIR, low ERI, compliance gaps
Indian Overseas	1.471	5.67	IMPR, DBU, IFR, CMD, CTC	DFQ, ITII, BATR, AIPCS	Low literacy (DL), cyber risk concerns (PR, CSA)	Weak IT infrastructure (FC), ERI gaps, delayed compliance
Kotak Mahindra Bank	1.353	5.50	CCRTU, IMPR, IFR, CMD, CTC, RAISR	DFQ, RAHSR, ITII, BATR, LSMARI, AIPCS, ITBCS	Trust deficit (TT), usability issues (PEOU), fraud concerns (PR)	Weak CSI governance, AIR gaps, unclear AI accountability
SBI	1.647	5.17	CCRTU, IFR, CTC, ELAR, RAISR	LSMARI, ITBCS	Fraud concerns and job insecurity (PR, JSC), usability gaps	Need for large-scale AIR transformation, cybersecurity strengthening
UCO Bank	1.765	6.33	CCRTU, CTC	DFQ, RAHSR, BATR	Low cybersecurity awareness (CSA), low confidence (TSE)	Moderate AIR gaps, ERI strengthening needed
Union Bank	1.471	5.33	ARAA, DTHE, IMPR, DBU, IFR, CMD, ELAR	RAHSR, BATR, AIPCS	Low motivation (DR), skill gaps (TSE), risk concerns (PR)	Weak ERI, fragmented compliance (RAI), AIR gaps
Yes Bank	1.647	5.67	CCRTU, IFR, CMD, ELAR	LSMARI	Job insecurity (JSC), trust issues (TT)	Infrastructure stabilisation (AIR), regulatory gaps (RAI)

The bank-wise assessment of indicator severities clearly shows a definitive and uniform trend of dual-layer causality, the interaction of both user-level (employee-driven) and enabler-level (bank-driven) factors merge to influence digital inefficiencies and risk exposure. In the majority of banks, the intensive indicators of user dominance (ARAA, IMPR, IFR, CTC, and CMD) represent the hidden limitations of behaviors and capabilities. They are the absence of clarity about the benefits of technologies (perceived usefulness), difficulty in use (perceived ease of use), technological illiteracy and technical self-efficacy gap, and increased risk with fraud and employment. As the example of Axis bank, HDFC bank and Indusind bank, there are multiple user level indicators that cluster up, which suggests that there are the problems of

skill mismatch, low confidence, and perceived risk, which means that workers are neither prepared nor matched to the current digital changes.

At the same time, the enabler-dominant indicators, which include DFQ, RAHSR, ITII, BATR, AIPCS, and ITBCS, point out structural and institutional bottlenecks in banks. They are mainly based on the lapses of AI infrastructure preparedness, feeble cybersecurity policies, splintered compliance approaches, system unavailability, and insufficient reskilling endeavors. Such enabler-level shortcomings are spread wider among banks like DCB Bank, Indian Overseas Bank and Union Bank and this means that technological and governance constraints in the back of operations are greatly limiting efficient operation. In relatively modern organizations such as HDFC bank and ICICI bank, the reality that the world is still limited by old technology and that the enterprise requires a superior correspondence between technological advancement and employee preparedness is an indication that the digital maturity is unevenly distributed.

The key observation made during this analysis is that user-level weaknesses cannot exist outside of enabler-level vulnerabilities i.e. the difficulty of using IT systems and lack of trust among employees is the natural result of simply having complex or unreliable systems, whereas the focus on fraud cases is compounded by the high level of inadequate cyber security practices. This interdependence is most noticeable in the case of such banks as Kotak Mahindra Bank and the State Bank of India, where the lack of trust and usability can be contrasted with insufficiencies in real-world governance of cybersecurity and necessities in computerized infrastructure transformations on the macrosystem level. In much the same vein, within banks like UCO Bank and IDFC Bank, it seems that the inefficiencies in the back end of being able to scale infrastructure and integrate enterprise risk is the cause of user-level insecurity and lack of motivation.

This dynamic can also be strengthened by the comparison between EPI (enabler performance index) and UPI (user performance index). Although UPI scores tend to be larger which implies more user-level constraints, they are usually based on or magnified by moderate yet critical gaps at the enabler level. This implies that the adoption issues in the banking sector that are digital are not only behavioural. Simply put, the results prove that digital transformation in banking is a socio-technical phenomenon, and the manner of behaviour by employees, institutional capacity, and technological infrastructure across the board shifts in unison.

On the whole, the findings are very empowering to the idea of a two-tier mitigation framework, since the only way toward effective risk mitigation and performance enhancement is to take action on both levels at once. Solving user-level concerns like training and awareness without fortifying the background infrastructure, cybersecurity and alignment of regulations would hardly have long-term results. On the other hand, technological underinvestments in regard to employee capacity building can result in underutilization as well as resistance. Thus, it is necessary to establish a comprehensive solution that would contain user-focused capacity-building, along with homeward technological and governance change to improve digital resilience and reduce the emerging risks in the banking sector.

Based on the root causes mapping as above, the following chapter will proceed to develop the analysis by transforming these identified constraints into particular mitigation strategies. In particular, Chapter 6 develops bank-specific mitigation planning frameworks, which are founded on the levels of the severity of indicators and their underlying root causes. Through alignment of mitigation measures with user level as well as enabler level shortcomings, the study helps in making the proposed actions specific to the situation as well as actionable. Thus, Chapter 6 will be a clear roadmap on how banks can overcome gaps in FinTech readiness and transition to strategic implementation after the diagnosis.

6. CHAPTER 6

MITIGATION MEASURES: DISCUSSIONS ACROSS BANKS

6.1 USER-LEVEL MITIGATION STRATEGIES

To overcome the low adaptability of the workforce to the digital transformation in banks, interventions that are consciously aimed at the creation of the user-level capabilities should replace technology-related ones. Recent research on FinTech and AI adoption has shown that the successful utilization of digital tools by users is not only determined by their access to technology but also by their ability to understand how they can optimize their work, minimize human error, and grow professionally (Venkatesh et al., 2016; World Economic Forum, 2023). Users may experience cognitive overload, reduced motivation, and a desire not to use digital initiatives when they perceive such initiatives as incongruent with their role requirements or not sufficiently contextualised, which in turn impairs the performance gains. Based on this, mitigation strategies at the user-level would need to focus on enhancing perceived usefulness and ease of use, and at the same time, alleviating uncertainty related to algorithmic decision-making, automation, and workflows supported by AI (Daultani, Dwivedi, & Pratap, 2021).

The opportunity to learn, practice, and reinforce skills through hands-on learning is a key factor in user adaptability. More recent research indicates that training strategies based on passive involvement or simply adhering to guidelines are not effective at instilling user trust in AI-based, data-intensive environments, particularly in such critical sectors as banking (OECD, 2021; World Bank Group, 2022). They require organised, but secure environments, such as simulations and practice platforms, where users can study digital systems and establish new workflows prior to their application in practice. These practical learning processes enhance self-confidence and digital literacy, which are critical in the continued use of a system and in enhancing productivity. Meanwhile, transparency in communicating shifting job expectations and new roles will reduce user anxiety, mitigate job insecurity, and foster a favorable attitude toward automation and human-AI cooperation (ILO, 2021; World Economic Forum, 2023).

At a larger organisational scale, the most effective user-level mitigation is backed by a digital culture that fosters learning, transparency, and trust. Empirical literature shows that people become trusting of advanced digital systems when the system logic, data governance, and accountability structures are well communicated, particularly in the context of AI-mediated decision-making (OECD, 2023). Equally, cybersecurity preparedness and responsible technology use are enhanced when behavioural relevance, real-world risk scenarios, and the consequences of decisions in user training focus on regulatory compliance (RBI, 2024). Together, these observations demonstrate that user readiness is not a static attribute but rather a dynamic capacity that is acquired during continuous learning, open

communication, and alignment between the digital systems and day-to-day work practices. This user-level foundation will enable banks to develop custom mitigation initiatives that transform digital investments into quantifiable returns in performance, sustained adoption, and organisational resilience.

6.1.1 BANK-SPECIFIC MITIGATION STRATEGIES.

A) Axis Bank

The issues related to the adoption of technology in Axis Bank are mainly influenced by the user-level concerns related to PU, TSE, DL, PR, and JSC. Although the bank has greatly invested in the digital platforms, workers tend to find it difficult to explicitly associate these platforms with the objective changes in the efficiency of tasks or better decision-making, which inhibits PU. The inconsistencies in DL across functions and demographic cohorts are an additional problem that undermines TSE especially in cases where AI-enabled tools are being made available without adequate contextualisation. High PR, in particular, on the issue of fraud responsibility, and continued JSC is a sign of insecurity concerning the attribution of errors, as well as the applicability of their tasks in an ever-more automated world. At enabler level, ERI and AIR constraints, coupled with disjointed digital investment (CSI) inhibit a steady capability building and consolidate disproportionate adoption experience.

To tackle them, Axis Bank needs to bring digital value to the working point. The connection between AI and FinTech tools explicitly recorded in terms of performance measurements, reduction of errors and professional growth, can strengthen PU and minimize ambivalence regarding accountability. TSE and DL may be developed gradually in the form of immersive learning environments, sandboxes, and simulation-based modules in which employees get an opportunity to experiment without the threat to operations. At the institutional level, AIR scaling using modular cloud architectures and ERI protection in long-term workforce planning will provide continuity in skillset development. JSC can also be reduced by enhancing governance related to the use of AI by making automation an enabler instead of a replacement for human functions (Alrahamneh, Murshed, & Alhalalmeh, 2026).

B) Bank of Baroda

The prevalent UDIs in Bank of Baroda, such as PEOU, TSE, DL, TT and JSC reveal a conflict between the operation complexity which could be observed in the past and the increasing demand on digitalization. Employees are often found to perceive digital systems as laborious instead of easing their burden, which makes them feel more complex and decreases PEOU. Assisted and scarce DL and exposure to digital tools undermine TSE and undermine TT, especially in case of system errors or delays. The problems are exacerbated by JSC, and automation efforts are typically presented without adequate guidance on the further direction of the positions (Cao & Song, 2025). On the enabler level,

the AIR and RAI-related constraints slow down experimentation and strengthen compliance-induced caution, postponing the stabilisation of digital workflows.

Development will be based on redesigning digital systems to capture real work practices rather than mere abstractions of the procedures. Simple interfaces, contextual guidance, and embedded learning tools can significantly reduce perceived effort and increase confidence in digital tools. Experts opine that DL and TT can be improved naturally by peer-learning techniques and obvious digital role models. Institutionally, a gradual change of AIR upgrades and active RAI (with the support of regulatory sandboxes and RegTech-coordinated compliance) will make it possible to create safe innovation spaces, and adoption may proceed without additional regulatory or operational risks (Iddrisu et al., 2025).

C) Bank of Maharashtra

The barriers to adoption in Bank of Maharashtra are mainly PU, CSA and JSC, which indicate that the institution is facing a challenge in integrating digital tools with performance expectation amidst increased sensitivity to cyber-risk. Low PU occurs when digital initiatives are positioned as compliance mandates, instead of productivity boosters. Weak CSA leads to a higher fear of personal liability in cases of fraud, which promotes conservative behaviour and manual overrides. JSC also contributes to resistance, since automation is commonly viewed as an indicator of workforce downsizing. Barriers at the enabler level- especially the low level of investment in cybersecurity (CSI) and diffuse governance decrease the scope and stability of the reskilling process.

The key to improvement is to rebrand technology as a support system, not a surveillance system. A simulated cybersecurity education that simulates actual operational threats can minimize anxiety that originated in CSA, as well as enhancing responsible digital conduct (Wai, 2024). Providing evidence on how automation can reduce errors and the mental burden can have a direct positive effect on PU and counter job-related fears. At the institutional level, by stabilising and augmenting the investments in cyber security with more transparent governance systems, the message concerning digital priorities and career sustainability may be consistently delivered.

D) DCB Bank

The combination of PEOU, TSE, and JSC on the user level and the reinforcement of the lack of weaknesses in AIR and RAI on the enabler level can largely explain the poor adoption of technology at DCB Bank. Regrettably, Low PEOU indicates that digital systems are viewed as too unintuitive, sometimes because of the discontinuous interfaces and missing integrations with the current workflows (Seyum, Wang, Zhang, & Wang, 2025). This has a direct effect of sabotaging TSE because employees are not confident driving systems, fixing exceptions and utilizing advanced features independently. Negative attitudes towards digital tools among employees are maintained with time through recurrent friction and the use of workarounds. Instead of viewing digitalisation as a chance to improve their

respective functions, they start to think that automation will result in more surveillance or the obsolescence of their skills, instead of perceiving it as a potential to increase their skills. These anxieties are heightened in organisations that have systems that are outdated and it may generate reliability and consistency problems, which does justify the experience of negative behaviours by employees. Simultaneously, due to the ambiguous guidelines concerning responsible artificial intelligence, particularly the accountability, audit, and compliance criteria, concerns about the personal and organisational risk emerge. The impossibility of this causes unwillingness to actively use technology and promote conservative practices, which decrease adoption rates.

To put an end to them, both levels of intervention are to be taken together. To enhance PEOU requires redesign based on the workflow, streamlined user experiences, and eradication of manual-digital processes in parallel, decreasing cognitive load and increasing perceived efficiency in that way. This implies that TSE needs role-specific and practice-focused learning, which goes through simulations and peer mentoring, where employees can safely experiment and develop mastery (Hidayat, Restiandi, & Sukresna, 2025). The circumstances causing distress in JSC may be addressed by clarifying the opportunities of role advancement in the future, connecting the technological adoption with role enrichments through transparent visualization, and aligning ERI with redeployment and promotion, instead of occasional education. On the enabler level, the stabilisation of AIR under the condition of phased modernisation, a modular upgrade and better interoperability of the systems will ensure the high reliability and the growth of user trust. Making RAI more clearly presented by internal guidelines, compliance playbooks, and regular regulatory communication will help to lessen the amount of uncertainty and legitimise the use of the tool, as well as motivate employees to approach digital systems in accordance with encouraged institutional priorities instead of personal risks.

E) HDFC Bank

The technology adoption issues of HDFC Bank are related to the synergistic effects of PU, TSE, DL, PR, and JSC on the user level, which are strengthened by the gaps in ERI, AIR, and CSI on the enabler level. Despite the perceived state of the bank as technologically advanced, uneven PU occurs when the employees fail to understand how new tools help increase efficiency of tasks or decision quality to a level that is above the established processes. The role and location differences in DL undermine TSE, especially when new digital tools are presented without the necessary contextualization making competitors stick to the bare minimum functionality or are even afraid of using systems. In a high-volume setting with mistakes that are very noticeable and with high ramifications, high PR is influenced by issues of accountability, data precision and customer facing, this type of PR affects the volume taking a center stage. All of these contribute to the increase in JSC since swifter automation and artificial intelligence-based decision-making are perceived not as role enlargement but as a symptom of role displacement (Premkumar & Arivazhagan, 2025). Poor and irregular ERI at the organisational level

reduces the richness and sustainability of skill development, and disproportionate AIR, notably in the fourth method of including legacy systems on new advanced platforms, gives rise to reliability issues that strengthen low PU and high PR. Based on experts' opinion, it is the perceived inadequacy of CSI that promotes even greater user anxiety over the possibility of data breaches and exposure to fraud, and, as a result, does not allow users to become comfortable with the system.

To intensify the adoption, it is necessary to rebrand a technology as something that enables clear performance and as a career strength. To improve PU, specific connection of digital tools with meaningful role outcomes is required with participation of role-specific use cases and success metrics which can be implemented into the daily workflows. Enhancing DL and TSE requires long-term ERI based on incremental, sequential learning via integration of initial (digital) and advanced (functional-specific) application coupled with on-job simulations and peer learning. PR and JSC might be facilitated by the open communication on accountability structures, error-management systems and clarity in reskilling-to-mobility pathways to cast automation as enhancement. At the enabler level, improving AIR through incremental modernisation and increased system integration will enhance reliability and user credibility and sustained CSI - combined with sustained, behaviourally based security awareness - will normalise secure digital behaviour (Al-Gasaymeh et al., 2024). These actions will together be able to stabilise confidence, create more perceived value, and make technology more rooted in daily banking practice.

F) Indian Bank

The pre-eminent UDIs of Indian Bank, PEOU, TSE, and JSC portray that the resistance of employees to technology is less common and rather how digital systems are felt in their day to day operations. Low PEOU indicates that platforms are seen as being complicated, discontinuous, or ill-matched with existing processes. This has a direct impact on TSE because their ability to try digital tools in the actual sense and gain guiding experiences to build confidence in utilizing such equipment alone cannot serve the employees. With time, the use of manual overrides, or peer support, strengthens a feeling that technology is an additional operating cost. This aversion of JSC is further encouraged by a feeling that many digital adoptions will have no correlation with obvious career advancement or job retention, which evokes fear that the automatization process will start to exceed reskilling sources. At enabler level, poor quality FC like unreliable IT support and slow responses curtail the powers of the bank to transition one-time adoption to long-term digital competence.

To enhance adoption, a stratified response is needed to support everyday user experience and institutional capability-building. At the user end, PEOU can be enhanced by re-engineering interfaces and processes implemented on real task flows, and by providing contextual help tools, guided walkthroughs, and just-in-time learning content integrated into systems. To develop TSE, Indian Bank ought to increase the experiential training based on sandbox settings, supervised pilot, and role specific

practice modules where employees could mishandle and learn through automaticity. To deal with JSC, there must be a clear connection between digital skills learning and internal mobility articulated pathways demonstrating how reskilling can be carried out to enrich a role rather than make it redundant. By enhancing the FC aspect at the bank level through properly staffed helpdesks, digital champions among employees, and clearly established procedures of escalating twists/turns, one can normalize technology usage to minimise frustration (Anagreh et al., 2024).

G) ICICI Bank

The outstanding UDIs of ICICI Bank, namely PEOU, TSE, PR, and JSC, portray tensions that are usually experienced in digitized advanced banks where the rate of innovation is high, yet there is uneven absorption by them. Though ICICI Bank deploys advanced tools, the PEOU issues arise whenever the employees are perceived to have a high level of complexity through the frequent upgrades, multi-layer interfaces, and parallel systems. This is a direct impact of TSE in that people find it difficult to match the shifting functionalities without an adequate time of practice and consolidation. High PR is especially relevant in contexts where AI-based decisions come into conflict with regulatory needs and customer-facing responsibility, and therefore employees need to be wary of using automated outputs. JSC is aggravated when the accelerated pace of automation and AI implementation are not externally accompanied by the systematic reskilling and role development, and employees consider digitalisation as a threat to their performance instead of career advancement. At the enabler level, there are pressures around ERI, AIR and RAI that signal difficulties in aligning talent investments, infrastructure preparedness and regulations with the aggressive innovation agenda of the bank.

It is necessary to re-align innovation delivery with employee assurance and institutional coherence to continue with adoption in such a context. At the user end, the enhancement of PEOU and TSE requires gradual, role-based onboarding scheme that delays the exposure to higher order functionality and incorporates a guided learning aspect in a live environment. An element of explainable AI, explanations of each decision, and documented override procedures will make PR much lower and allow the employees to be able to trust systems without being afraid of an undue level of responsibility. To JSC, it will be necessary to make reskilling opportunities transparent--connecting new digital skills to future tasks, within-company promotion, and performance-based pay. On the bank level, closer integration of ERI with product and innovation roadmaps results in the skill development being in line with the deployment and not behind it. Enhancing AIR by means of scalable, modular architectures can be used to ease operational friction when upgrading, and long-term RAI participation through regulatory sandboxes, automated compliance, and early consultation helps employees feel confident that the institutionally supported innovation will be operationally sound and regulatory (Truby, Brown, & Dahdal, 2020). All of this enables ICICI Bank to maintain its innovation advantage and enhance workforce flexibility and trust.

H) IDFC

The leading UDIs of IDFC (PEOU, DR, and JSC) indicate issues that lie not as much in the technical skill of the employees but in the manner the digital change is defined and embedded in the organisation. Although a high number of the employees have the minimum level of digital skills, the uneven DR is an indicator of uncertainties in priorities, the sequence in which digital initiatives are undertaken, and whether technology is used in line with the daily work routines. PEOU gets harmed when the systems are launched without the systematic accounts of purpose and the long-term direction because employees tend to see new tools as appendices instead of complementary system enablers. In these situations, JSC comes into the picture due to the interpretation of digital initiatives through the prism of role uncertainty, when future career opportunities, as well as the expectations of skills, are not well defined. The interplay between ERI, AIR, and RAI, at the enabler level determines whether digital intent will result into institutional learning. The lack of continuity in reskilling investments, changing infrastructure architecture and regulatory risk can all be employed to cool the pace and weaken employee faith.

Adoption in the context of IDFC needs to be strengthened through a conscious cultural and structural reinforcement with technical upgrades. The first step in improving DR is signalling by leaders and line managers is always to demonstrate the digital behaviours, explain how technology can be used to achieve strategic objectives, and to remind line managers of the importance of this by discussing performance (Hossain, Fernando, & Akter, 2025). The enhancement of PEOU can be done through the simplification of the workflow, providing contextual assistance to systems, and aligning digital KPIs with team-level goals to achieve usability as productivity and not compliance. To resolve JSC, the bank ought to clarify the future need in skills and role changes, which must be connected to actual career progressions and internal mobility. In the bank level, the sustained ERI, which is not a one-time training but a long-term competence investment will assist in the conversion of preparation to deployed competence. Small scale, incremental AIR investments can stabilise platforms, and permits the flexibility to scale new applications without interruption. Through focus group discussions, we infer that, ongoing RAI participation, automated compliance, and early regulatory consultation will additionally ensure innovation gets grounded to accepted governance limits and encourage the employees that digital change is meaningful and safe.

I) IndusInd Bank

Following change Some of the prevailing UDIs of IndusInd Bank PE O U, DR, JSC indicate a period of transitional ambiguity with digital initiatives on par with pilots to enterprise-wide implementation. Although most systems are quite accessible, the problem of unequal PEEU poses that interfaces and processes are not yet intuitive or contextualised enough to execute routine tasks. Loopholes in DR are an indicator of uncertainty on prioritisation, sequencing, and ownership of digital tools that makes employees use old practices even after the new systems are available. JSC also becomes intense in the

case of scaling automation that is not accompanied by clear communication on role development, skills applicability, and future employability. Coherence of ERI, reliability and scalability of AIR and the level of institutional confidence created by RAI, determine the effectiveness of the adoption at the enabler level. Little coordinated reskilling and signals, overlapping infrastructures and conservative regulatory interpretations combine to diminish consistency and retarding behavioural normalisation.

The answer to such challenges is the strengthening of user-level experience and bank-level systems. At user level, expansion of PEOU requires further incorporation of digital tools in their daily work, elimination of unnecessary manual processes and job aids and micro-learning to facilitate real-time utilization. The enhancements to the DR are strengthening the management through alignment of goals, reviews of routine performance based on the digital outcomes and adoption champions who make the usage a habit. To reduce JSC, the future role pathway, skill taxonomies, and internal mobility options need to be clearly articulated, which is an indicator of continuity and not displacement (Santoso et al., 2021). By practicing sustained ERI at the bank level, where capacity development relies on role-based learning, continuous learning will solidify the development of capability. Controlled, gradual AIR modernisation can guarantee stability of the system, as well as allowing gradual innovation and lowering anxiety of disruption. Continued RAI participation: by compliance-by-design and audit-ready architecture, and by going out of its way to talk to regulators, further institutionalisation of trust, digital initiatives will be able to scale with reliable and consistent performance.

J) Indian Overseas Bank

The prevailing UDIs in Indian Overseas Bank including PEU, DL, CSA, JSC, indicate gaps in structural and foundational capabilities other than resistance to change per se, and thus reduces the ability of the employees to navigate interfaces, interpret system prompts, and recover due to habitual errors, thus depressing PEOU and reinforcing reliance on manual processes. Perceived vulnerability to cyber threats, data breaches and transactional errors are also increased with weak CSA and risk aversion and avoidance behaviour are increased. Such fears are translated to high JSC since the employees associate digitisation to increased exposure and loss of control as opposed to empowerment. Constrained ERI at the enabler level limits the continuous skill reinforcement and legacy-heavy AIR environments at the enabler level discontinue the user experience and pose more cognitive load. Experimentation and adaptive learning are further inhibited by Conservative RAI which is usually a result of increased regulatory scrutiny in the banking sector of the public.

To bridge such gaps, a phase-based, confidence-building process that fulfills the readiness of the users and the capabilities of the organizations is necessary. At the user level, the reinforcement of DL must not be limited to classroom education, but must be expanded to include task-based and practical learning, peer mentoring, and role-specific digital playbooks, which also make everyday use far easier and enhance PEOU. By increasing awareness of cybersecurity practices by conducting practical drills,

simulating phishing attacks, and defining the unwanted consequences of events (incident-response), it is possible to turn fear into informed vigilance (Schreiber & Schreiber, 2024). To deal with JSC, clear communication in regard to continuity of the roles shall be addressed with internal mobility and promotion channels that are certification-based. At the bank level, ongoing ERI should focus on the continuous learning ecosystems instead of doing the episodic programmes, which ensure the skills are up to date as the systems change. Incremental AIR upgrades - oriented on simplification of the interface, system interoperability and reliability - can be gradual, bringing friction reduction without destabilizing the operations. Compliance-oriented innovation will be made possible by proactive RAI that is incorporated at an early stage of system design and rollout, and that can help to shift the usage paradigm of obligatory use to confident and routine digital use.

K) Kotak Mahindra Bank

PEOU, TSE, PR and JSC are some of the dominant UDIs of Kotak Mahindra Bank- and are used to indicate a context where employees have high performance expectations and low tolerance of system imperfections. Considering the fact that the bank is known to be technologically advanced, all slight disturbances, delays, or discrepancies in digital platforms will proportionately harm TSE and PEOU, which can be instantly repurposed into high PR. Accountability risks are perceived more acutely by employees when systems are front-office or high-value transactions and they are posed as being best-in-class. In the long run, such sensitivity contributes to JSC, where automation and decision making that involves AI presuppose the presence of more controls, more scrutiny, and uncertainty concerning the allocation of errors between humans and systems. RAI at the enabler level results in the ambiguity of the compliance boundaries, and disaggregated CSI undermines the understanding of the data ownership, model responsibility, and the further escalation of the advanced digital solutions, making it difficult to achieve consistent scaling of sophisticated solutions.

Maintaining trust in the high-expectation context is reliant on the reinforcement of experience reliability as well as the institutional assurance. At the user level, to make PEOU and TSE stronger, obsessive attention of the stability of the system, usable interfaces and quick failure and recovery mechanisms with the help of real-time notifications and open systems of error-solving processes can decrease the personal perceived risk. Accountability norms and decision overrides can be clearly defined to effectively reduce PR, and career story lines that make digital fluency relevant to both progress and impact can make JSC. On the bank-level, increased investment in CSI will be a factor that will boost trust in AI-enabled processes (Al-Dosari, Fetais, & Kucukvar, 2024). RAI engagement such as proactive and ongoing involvement, which are not adapted to a product design as post-hoc validation, can decrease product regulation vagueness and delay deployment. By ensuring the innovativeness speed matches the governance depth, the bank can maintain its digital lead, but the adoption process is

resilient, confident, and institutionally competent instead of easily losing its strength during the pressure.

L) State Bank of India

The unmatched scale, geographic dispersion, and workforce diversity of the bank is essential in enhancing the dominance of its UDIs of State Bank of India -PEOU, TSE, PR, CSA, JSC. The fact that the quality of infrastructure and exposure to users is different across the branches implies that PEOU is not spread evenly among employees, frequently exacerbating low TSE among those who have been exposed to digital environments sparingly. High PR and CSA are logical outcomes of the high transaction volumes and continuous exposure to the risk of fraud, phishing, and social-engineering that SBI faces, with even a single case getting broad internal coverage. These contribute to fear of making mistakes and being disciplined and as a result, cautious or avoidance behaviour. JSC is also supported by massive automation projects and centralisation projects, which under the absence of well-articulated role-shift projects, are perceived as menaces instead of facilitators. Within the enabler level, the disruption of ERI limits the richness and persistence of skill building, the imbalance in AIR maturity hinders sustained system execution, and the complexity of RAI requirements among the products and jurisdictions makes the process of coordinated rollout to be complicated.

As a major institution, SBI ought to concentrate on stability, reassurance, and inclusivity more than speed in risk management. We should make the interfaces normal but flexible, continuously support and train them, and make the common transactional processes easy to achieve better user experience and satisfaction. Cybersecurity awareness can be maintained without panic through regular training in the form of simulation, fraud exercises, and discussion of the real-world cases. Risk can also be minimized by having effective accountability and error control. We must establish observable routes to upskilling, linking digital skills to new or more advanced jobs rather than implying job loss, to fulfil the needs of the users to solve JSC. Experts opine that on an institutional level, CSA ought to be transformed not to one time training sessions but into long term workforce development programs that are associated with succession planning. The combination of a mixed approach where centralized systems are employed in the processes as well as the implementation of gradual upgrades will enhance user experience in various locations. Finally, engaging regulators during the initial stage and compliance internally will make SBI embrace digital solutions in a manner that is consistent, credible and trustworthy throughout the organization.

M) UCO Bank

The UDIs, which are the prevailing ones in UCO Bank such as PEOU, TSE, CSA, indicate that the issue of technology adoption is not as much subject to resistance as it is to a lack of exposure and opportunity to build confidence. Digital systems are often seen by the employees as being complex and unforgiving which has a direct impact on PEOU and inhibits TSE especially in operational and customer

facing positions where the cost of errors is felt to be high. The lack of knowledge about cyber threats and protection also increases anxiety, with the limited knowledge about the concept of cyber risks and protection driving the fear of participating in unintentional violations or being accountable due to fraud. The problems on the user level are compounded by the problems on the organizational level. A deficiency in the responsiveness and reliability of the system is a barrier to improvement, and an emphasis on the strict RAI compliance instead of experimentation with innovative ideas obstructs the learning process and the evolution of new practices.

To boost the pace of adoption the need to establish low-risk, confidence-building digital environment is necessary. At the user level, PEOU can be enhanced by more specific usability adjustments, such as simplified user interfaces, task-oriented processing, and vernacular or job-specific prompts, which can stimulate regular usage. Organized, practical education in the form of simulations, sandboxes, and instructed learning will slowly increase TSE, and employees will be able to experiment with no fear of actual ramification. CSA programs can be conducted regularly, as scenarios and are less prone to blame but rather to recognition and response to reduce cyber anxiety and develop practical vigilance. At the institutional level, the gradual yet steady AIR (technology infrastructure readiness) upgrades are necessary to maintain the stable performance and minimize the friction at the point of use. It is possible to align these investments with changing expectations of RAI (regulatory alignment), by introducing these investments in phases, internal auditing of them, and pilot testing informed by the regulators, to provide a safe space of experimentation whilst preserving trust. Combined, these solutions can enable UCO bank to move past its reserved use to assured and successful long-term digital interaction.

N) Union Bank

The predominant UDIs of Union Bank, such as PEOU, TSE, DR, PR, CSA, indicate the partially ready, but limited in terms of disparate confidence and increased risk perception, workforce. Although the digital tools have some baseline exposure, functions differ on PEOU, and thus systems are not always supportive of daily work. The lack of even-distribution of usability, coupled with little opportunity to become a master, hinders TSE, especially in job positions prone to legacy or where compliance is of high priority. Loopholes in DR are the uncertainty regarding the long-term digital orientation of the bank and the role of individual functions within this orientation. Simultaneously, high PR and CSA, which is caused by fraud issues, regulatory attention and more transparency of cyber incidents in the public banking ecosystem promote wary, and at times defensive, technology utilization. These dynamics at user level are influenced by enabler-level constraints: ERI is commonly diffused across wide cohorts, AIR upgrades are not uniformly handed out across functions and regions and strict RAI requirements may hamper iterative learning and innovation.

In a bid to effectively optimize adoption, one should make sure that there is congruency between readiness, capability, and assurance. At the user interface level, the process of reducing cognitive load

by redesigning workflows and the provision of contextual guidance in systems may directly improve PEOU and reinforce TSE by repetition and increased success. Reskilling programs can be integrated as digital, risk, and cybersecurity reskilling--to transform DR into an applied capability particularly in cases of visible leadership support and digital role modelling. Avoiding punitive information sharing on risk control measures, error management, and cyber security can minimise PR and normalise CSA as a collective responsibility and not an individual liability. On the institutional level, the strategic focus of ERI must be by roles that are most impacted by digital and regulatory change, and the learning outcomes would be evaluated to the performance indicators. The stability of the system can be improved in phases, in small steps, without reaching the full scope of the digital capabilities, which AIR currently does not have. Regulatory confidence can be established through proactive regulatory alignment based on internal compliance labs, pilot testing, and constant monitoring, which will not delay adoption. Collectively, all these can assist the Union bank in its transition between the cautious adoption of technology and other more stable and confident digital adoption.

O) Yes Bank

Yes Bank has three predominant UDIs of the TSE, DL, and JSC, which are strongly related to the recent phase of organisational stress and restructuring that has caused system, role and learning path disruptions. Minimized TSE is a result of skill disparities as well as recurrent alterations to platforms and procedures, thus restricting employees to mastery and self-confidence with course of time. The area of the DL gaps is more significant in non-core/support functions, where the exposure to newer digital and AI-enabled tools has been low, supporting the manifestation of manual workarounds. JSC is still relevant because the adoption of technology is usually considered through the prism of rationalisation and recovery, increased sensitivity to automation and job redundancy. At enabler level, the usefulness of ERI is limited whereby training is perceived to be corrective and not developmental and where advancing AIR and high RAI demands influence the speed and credibility of digital initiatives in the recovery phase.

To regain momentum, a digital narrative with people as its core will have to be based on consistency and growth. On a user level, structured, tiered learning pathways that combine general DL with role-specific digital and AI skills can slowly reconstruct TSE, particularly in the presence of guided practice contexts and guidance. The explicit expression of future-role typologies and internal mobility possibilities-clearly connected with reskilling milestones-can directly minimize JSC by reconsidering technology as one of the lenses to continuity and not displacement. Institutionally, persistent and secluded ERI ought to concentrate on key functions in connection with growth and conformance wherein ability results are noticeable. Friction can be minimised by accelerating AIR stabilisation by hybrid modernisation to restore confidence in core systems. Meanwhile, active RAI alignment, i.e. preemptive regulator involvement and internal compliance guarantee systems, may make innovation

activities legitimate. Combined, the following strategies can re-establish digital transformation as a core of restoring trust, creating workforce resilience, and creating long-term renewal at Yes Bank.

6.1.2 DOMINANT INDICATORS.

A high percentage of poor technology adoption as a result of PEOU (73%), TSE (73%), JSC (87%), AIR (80%), and RAI (73%) suggests an interconnected issue instead of individual areas of vulnerabilities. All these indicators reflect upon the extent to which employees feel that banks are being digitalized- in terms of the ease of engaging with customers, their reassurance in working with systems, perceived career security, institutional readiness to technology, and regulatory clarity. The fact they are predominant implies that the barriers to adoption lie less in the technological availability than in institutional-human failure.

PEOU stands out as a significant limitation since the banking technologies are becoming overlaid over the old processes as opposed to being substituted throughout. Systems will be cognitively demanding even with good functionality because of the use of many interfaces, compliance screens, exception handling workflows etc. The parallel, manual-digital processes in Indian banks, particularly, public sector and mid-sized banks of the private sector, further blur the concept of ease which reinforces the notion that technology adds effort, and does not subtract it. TSE is low in an environment that has an episodic digital exposure, role-agnostic, or excessively theoretical exposure. Several banks focus more on platform implementations than internalising skills, which leaves the employees familiar with systems but insufficient in troubleshooting, interpreting output, or how to recover when errors occur. Its existence is accelerated by the rapid implementation of AI and analytics, making opaque systems less controllable and masterful, which is the trend established in financial services digitisation across the globe (Aziz Baker, 2025). JSC being the dominant indicator indicates the presence of automation narrative that has exceeded promises of reskilling. Optimisation of costs, rationalisation of branches and artificial intelligence-driven efficiency communications, but without comparable redeployment models, generate fear that technology use is intensifying redundancy. It is especially sharp in clerical, operations as well as middle-level management where automation of tasks is most obvious and career-courses least re-defined.

Digital foundations were broken at the institutional level by weak AIR signals. This may be a case of banks becoming modernised in the front-end whilst core systems, data architecture and integration layers are partially modernised. The result of this mismatch is unstable performance, downtime and poor scalability which compromises the trust and confidence of the user. This feels as incomplete transformation to employees and makes them more resistant. Lastly, RAI prevails since banking technologies are highly regulated with their technologies and operations being subject to high regulation, but the requirements of regulation regarding AI, data use, and automation remain dynamic.

When internal control falls behind external control, the staff members feel an increased personal and organisational risk. Lack of clarity regarding accountability, auditability, and compliance will inhibit trial and error and active digital tool utilization

6.1.3 Banking industry harmonized generic strategies to manage user level issues.

he solution to PEOU is the change in the technology-focused design towards the workflow-focused design. Digitisation has seen leading banks around the world use process re-engineering before automation, which removes unnecessary steps before automation comes into play. Human-centred design methods, including co-creation with frontline staff, live environments usability testing, and constant simplification of the interface have demonstrated the ability to enhance perceived ease and continued use in a much greater manner. Another feature of progressive banks is the incorporation of contextual digital support (in-app prompts, guided workflows, conversational help) instead of the independent standalone training modules. This relies on experiential, role specific capability building to improve TSE. Best-practice institutions are out of the classroom or LMS-based training, and into simulation labs, sandboxes and supervised practice grounds, where employees can safely test out their experimental aspects. Tiered digital certification associated with role advancement, peer learning communities, and digital champions incorporated within business units have been found to be helpful in developing a sense of confidence and autonomy. Importantly, mastery is strengthened when the employees are not only rated on the results but also on the use of the technology. To mitigate JSC, it is necessary to re-conceptualize automation as augmentation, but not replacement. Successful banks clearly chart the future role structures indicating how future activities change instead of vanish. Harmonious redeployment opportunities, internal talent markets and ensured reskilling segments before the rollout of automation minimize fear and opposition. Across the world, the banks that publicly pledge not to forcefully lay off employees in the name of automating their systems in specified transition periods record relevant employee engagement with new technologies (Mehrotra, 2019).

Strengthening of AIR entails gradual, progressive modernisation as opposed to radical restructuring. By adopting hybrid clouds, API-based architectures, and the gradual replacement of core systems, banks can stabilise thier systems while still innovating. Ring-fenced infrastructure budgets, explicit dependency mapping, and resilience-by-design principles, which focus on uptime and scalability, are considered best practices. The reliability of digital tools increases the trust of employees when they see that the operational friction is minimized. RAI has to be dealt with by an active integration of regulation into the processes of innovation. Lead banks also have their own regulatory liaison and internal assurance staffs that breakdown changing guidelines into working process clarity in front of the staff. Reduced perceived compliance risk is achieved by explainable AI paradigms and transparent accountability matrices and a written human-in-the-loop controls (Villar & Khan, 2021). Participation

in regulatory sandboxes and early alignment with supervisory expectations legitimise experimentation and encourage confident adoption.

6.2 ENABLER-LEVEL MITIGATION STRATEGIES

To enhance the FinTech preparedness at the enabler-level, banks should stop their individual technology implementations and shift to systematic capability development at the infrastructure, governance, and strategic investment level. Recent findings of research on digital transformation suggest that the quality of systems, fragmented IT systems and the lack of enabling conditions tend to limit workforce flexibility and productivity, despite their positive attitude toward technology (OECD, 2023; World Economic Forum, 2023). These structural flaws directly translate into operation failures, user frustration and trust loss in the banking sector where reliability, compliance, and scalability are considered an absolute. Therefore, mitigation strategies at the enabler level should focus on the underlying requirements that can enable the digital tools to be internalised into the daily work processes instead of staying marginal or symbolic innovations.

Strategically, organisational readiness at the enabler level is determined by the congruency of the digital investments with transformation objectives on a long-term basis. In the literature on FinTech adoption, it is noted that such complementary assets as reskilling budgets, AI governance frameworks, and cybersecurity capabilities are often underfunded by banks, restricting the performance gains of high-technology infrastructure (OECD, 2023). The symptom of such misalignment is an indication of dynamic capability that is not well-developed within institutions. Thus, as a mitigation, banks need a modernization roadmap, investment planning, which is outcome-based and straightforward that is inclusive of digital capability metrics in enterprise performance management.

Further, governing the effectiveness of enabler-level preparedness is based on the effectiveness of regulatory alignment and risk governance. In highly regulated environments such as Indian banking, banks implement conservative policies or fragmented compliance protocols due to the uncertainty around AI accountability, data protection, and cyber risk (RBI, 2023; World Bank Group, 2022). Empirical studies also indicate that active regulatory participation, open policy guidelines, and long-term cybersecurity investment are not only minimizing the risk posed by institutions, but also serve as trust-building measures among employees and customers (World Economic Forum, 2023). Together, these observations highlight the fact that enabler-based mitigation is essentially about establishing stable, scalable, and reliable environments where employees can adjust, work and co-operate well with digital systems. By creating such enablers, the banks will be able to transform the technological progress into sustainable organisational performance and strategic resilience.

6.2.1 MITIGATION PLANS SUGGESTED TO EACH BANK.

A) Axis Bank

The major technology adoption issues that Axis Bank faces are mainly influenced by UDI including ARAA, CCRTU, IMPR, IFR, CTC, and RAISR. These indicators, when taken together, show that, as an employee, one is prone to unbalanced use of digital tools, low confidence in AI-enabled systems, and an increased perception of operational and cyber risk (Al-Dosari et al., 2024). The high number of fraud-related cases and complaints by customers, in addition to the increased cognitive and emotional load on the frontline staff members, puts the trust in new digital initiatives at the forefront of the service and undermines the learning-by-doing approach and slows the change in behaviour. The small number of positions that are supported by AI only limits the ability of the employees to internalise digital processes, thus making technology less central to daily operations and more peripheral to them. DFQ, RAISR, and LSMARI enhance these problems at the enabler level, making systems less reliable and perpetual and, consequently, diminishing the trust of employees and organisational preparedness to pursue globally scaled digital transformation.

Axis Bank should thus focus on moving away from fragmented, pilot-based experimentation towards the overall implementation of AI and FinTech solutions closely coupled with the fundamental banking processes and frontline operations. The introduction of AI-enhanced applications in credit evaluation, risk management, customer service, and compliance processes can greatly increase the level of exposure of employees to applications of AI and, consequently, promote experiential learning and enhance their perceptions of utility. To facilitate low ratios of customer complaints and related employee stress, the bank ought to institutionalise the user-centric design principles, with a structured form of employee-customer co-testing and an iterative feedback loop before the full rollouts. Migration of old systems must be in a phased manner (with the help of the robust cloud infrastructure, the redundancy mechanism and active monitoring) to minimize downtime and stabilize digital platforms (Gowda, 2021). To supplement these initiatives, regular and situation-based cybersecurity education, aligned with AI-based fraud detection and risk analytics, will help ease uncertainties, enhance trustworthiness in digital platforms, and sustain the use of technology. All these measures will allow Axis Bank to enhance the adaptability of the workforce and improve overall operational performance.

B) Bank of Baroda

The poor adoption of technologies within Bank of Baroda is mainly fuelled by UDI, such as low IMPR, CMD, and CTC, which, combined, restrict employees' daily interaction with the digital banking processes. Poor digital coverage - especially in semi-urban and rural operating environments - limits the opportunity to learn through repetitive digital observations, thereby strengthening the reliance on manual and branch-based workflows. This challenge is further worsened by limited customer movement that limits the amount of transactions that take place on the digital platforms, which reduces the familiarity and confidence of the employees with the FinTech systems. Employees are unclear about

fraud controls, data breaches, and compliance obligations due to insufficient cybersecurity training. These lead to psychological resistance to adopting digital technology. At the enabler level, RAISR and LSMARI represent a structural concentration of technological focus within IT or specialist teams, restricting organisation-wide exposure to digital and discouraging the spread of AI-based practices across the fundamental bank operations.

The proposed mitigation should focus on increasing digital exposure and addressing transition risks by adopting assisted-digital and hybrid models of service delivery. These models can slowly build customer adoption and, at the same time, introduce digital processes in the day-to-day activities, reinforcing learning-by-doing (Mahapatra & Singh, 2021). The bank needs to redefine job functions across operations, credit, and customer service so that AI and analytics can be incorporated beyond the technology departments and, hence, normalise human-AI interaction. The development of cybersecurity capabilities should be transitioned from periodic, compliance-based training to an ongoing, scenario-based programme that connects behavioural knowledge to immediate defences and fraud analytics to mitigate fear-based opposition. At the enabler level, the accelerated hybrid modernisation of legacy systems through gradual migration, cross-platform layers and minimal service disruption will stabilise the platforms and allow easier integration of FinTech solutions. In totality, these would build confidence in the workforce, reduce perceived risk, and enable the bank to be flexible to a long-term digital transformation.

C) Bank of Maharashtra

DTHE, IMPR, DBU, IFR and ELAR represent user-level issues in the Bank of Maharashtra. Combined, these signs indicate a workforce that is not well acquainted with digital work processes and lacks time to develop confidence in using technology frequently. The low intensity of training and limited volumes of digital transactions dilute task-technology fit, resulting in less competent and more reluctant employees. The high levels of fraud also add to the risk perception, which strengthens risky behaviour and impairs confidence in online platforms. The insecurity associated with automation further increases the difficulties as it fosters anxiety about role substitution and diminishes learning orientation and the desire to explore AI-enabled tools. At the enabler level, RAISR and BATR refer to the structural underinvestment in developing workforce capabilities and insufficient institutionalisation of human-AI collaboration at functional levels.

The Bank of Maharashtra's mitigation action should focus on introducing AI-powered, role-specific reskilling interventions into the overall HR and performance management framework. The interventions of training must go beyond generic digital literacy to real-world simulations, sandbox, and banking specifics, to enable employees to train in detecting fraud, digital customer servicing, and AI-aided decision-making in low-risk environments (A. Agarwal et al., 2021) This kind of experiential learning could reduce anxiety regarding fraud and improve self-efficacy and confidence in technology. To

overcome the problem of job insecurity, the bank must implement an augmentation-first approach to automation, explicitly stating that AI does not eliminate human jobs but instead supplements them, and providing explicit redistribution and internal career mobility opportunities. At the enabler level, it is necessary to allocate budgets for digital reskilling to indicate a long-term investment in the flexibility of the workforce (Kornelakis, Kirov, & Thill, 2022). Adding AI-enhanced positions to operations, compliance, and customer-facing functions will continue to civilise the customary use of digital work and contribute to long-term enhancement of flexibility and digital performance.

D) DCB Bank

The technology adoption limits of DCB Bank are strong on the user level, including CCRTU, DTHE, DBU, IFR, CMD, and CTC. Taken together, these signs indicate that workers are operating in unstable, high-friction digital spaces where systems are not seen as reliable and risky. Regular failures of customer-facing technology put additional work and emotional pressure on staff, which adds to the opposition to using digital tools instead of promoting the learning-by-doing concept. Poor training and cybersecurity awareness also erode confidence in the digital environment, and the poor migration of customers restricts employees from regular work with the digital flow. These user-level obstacles are supported by major enabler-level failures, such as high occurrence of system downtime, poor and disconnected IT infrastructure, insufficient investment in reskilling of workforce, slowness in adopting legacy systems, and regulatory and AI policy non-compliance, and limited cybersecurity resources (Willcocks, 2024). All these structural weaknesses undermine trust in technology and reduce the sustainability potential of the FinTech initiatives within the organisation.

To overcome them, a comprehensive reinforcement of the technological background and human resources is needed. The first concern should be modernisation of the main IT infrastructure with phases of cloud deployment, system backup, and active monitoring to minimise downtime and stabilize digital activities. Meanwhile, ongoing, role-specific digital training must be integrated into HR systems and assisted by AI-based learning analytics that can personalise skill growth and monitor proficiency throughout the course. Human-centred design and employee-customer co-testing can be used to redesign customer-facing platforms to reduce the number of complaints and the resulting employee stress levels by a significant margin. Based on experts' feedback, on the enabler level, the compliance automation supported by RegTech solutions will be necessary to facilitate the alignment of the digital initiatives with the changing regulatory demands and broader investments in cybersecurity. Further, enhanced threat detection solutions and scenario-based training are required to rebuild trust. Lastly, by developing effective AI governance structures that delimit responsibility, ethical usage, and human control, we will develop the institutional clarity needed to launch scalable FinTech adoption and enhance workforce adaptability.

E) HDFC Bank

Regardless of HDFC Bank being a digital leader, the trend of user-level indicators constitutes notable user adaptation strains in the workforce. Even in cases when the advanced systems are technically accessible, the cognitive strain and reserved involvement in using them present themselves along with CCRTU, DTHE, IMPR, DBU, and ELAR. Enabler-wise, the irregular nature of system downtimes, lack of scalability of infrastructure and the minimal expansion of AI-supported functions to more than limited functions diminish the trust of the employees in the system and the organisational purpose. Other pressures related to regulatory compliance needs and the growing need to enhance cybersecurity only make the adoption environment more complex due to perceived operational and accountability risks.

Enhancing the flexibility of the workforce in this situation will require repositioning digital implementation on employee experience and role clarification instead of the excessive spread of tools. Digital workflows can be streamlined, and the usability of interfaces can be enhanced to help directly cut complaint-induced cases of rework and alleviate the operational burden. Restructuring the human-AI collaboration models with a clear definition of areas of decisions, escalation strategies and responsibility may assist in rebranding AI as a performance-enhancing tool instead of a threat to employment survival. On the enabler level, ensuring the reliability of the system and confidence of the regulators requires long-term investment in scalable, AI-ready infrastructure and resilient cybersecurity architecture. It is also important to defend reskilling budgets via ring-fenced funding based on well-defined digital career routes (Donald et al., 2023). With consistent upskilling aligned with changing regulatory demands and new AI-capable functions, employees tend to be more proactive in interacting with digital systems, allowing the bank to convert its technological savvy into the consistent performance increase of its workforce.

F) Indian Bank

The technology adoption issues of Indian Bank are conditioned by user-dominant measures, including IMPR, IFR, and RAISR. These aspects reflect limited exposure to digital processes, increased risk perception, and lower possibilities for the employee to interact with AI-based systems. Frequent system downtime (DFQ), inadequate IT infrastructure (ITII), low reskilling investment (BATR), regulatory misalignment (AIPCS) and lack of investment in cybersecurity (ITBCS) further limit the ability to effectively use technology at the enabler level. The mitigation must aim to increase digital exposure by providing assisted-digital models that allow employees to slowly shift to positions that are technology-intensive. Enhancing the integration of AI-based job roles across functions will enhance experiential training and minimize reliance on the traditional process. At the enabler level, Indian Bank needs to focus on the modernisation of its IT infrastructure by using cloud and API-first systems, which would make the systems stable and scalable (N C Roy & Prabhakaran, 2023). At the same time, an AI-based reskilling program associated with role transformation must be integrated with the HR strategy. The

increased compliance structures and cybersecurity investment enforced by and through RegTech will decrease the perception of risk and establish long-term trust towards digital systems.

G) ICICI Bank

ICICI Bank's user-level inhibitors are discrete-level digital exposure (IMPR), asymmetric digital banking usage (DBU), customer migration barrier (CMD), and automation induced job-insecurity (ELAR). All these clues point to the idea that even with the existence of technologies, staff members might not be absorbed into the digital workflow fully, or they might feel threatened by automation. Low legacy system migration (LSMARI) and regulatory compliance issues (AIPCS) are at the enabler level, which impedes a smooth digital transformation. Mitigation must focus on achieving digital-first workflows across business functions and on having employees use digital platforms, not through parallel manual systems. By promoting customer migration by making the onboarding process easier and encouraging them to adopt the digital format with incentives, digital adoption will raise the overall rates of transactions and the level of familiarity of employees with the processes in the FinTech industry (Boustani, 2022) The necessity of the accelerated migration of legacy systems with the help of hybrid cloud strategies at the organisational level is vital to provide the possibilities of scaling. Enhancing RegTech-based compliance systems and AI governance frameworks will further align them with the changing regulatory requirements and increase the ability to trust technology-based operations.

H) IDFC First Bank

The indicators of user-dominance in IDFC First Bank are low FinTech/AI applications, insufficient training exposure, poor customer migration, and low coverage of cybersecurity training. These imply the lack of skills development and direct interaction with digital tools. In the enabler level, system reliability and workforce preparedness are decreased due to frequent downtime and low reskilling investment. The mitigation needs to focus on the shift of AI adoption at the pilot level to an enterprise-wide adoption, so that employees use the AI in normal working activities. To enhance self-efficacy and digital competence, continuous and role-specific digital training with the help of AI-generated learning platforms should be institutionalised. Experts opine that improving the resilience of the system by using cloud facilities and active monitoring will minimize the number of disruptions associated with downtimes. Also, the allocation of more funds towards reskilling and integrating cybersecurity awareness in the day-to-day operations will enhance the confidence and performance in the digital arena.

I) IndusInd Bank

IndusInd Bank is encountering several user-level issues, such as ARAA, DTHE, DBU, IFR, CTC, and ELAR. The combination of these points leads to a lack of capability and mental resistance to technology

use. These are worsened by system downtime, poor infrastructure, limited reskilling investment, legacy constraints, regulatory disconnect and insufficient cybersecurity investment, at the enabler level.

The mitigation should be holistic. At the user-level, the bank needs to introduce AI-based reskilling strategies, simulated learning, and guided career progression channels to minimize resistance and enhance competence (Willcocks, 2024). On the enabler level, end-to-end IT infrastructure modernisation, such as a cloud implementation and API connectivity, is necessary to stabilize systems. This will increase transparency and decrease unpredictability by enhancing AI governance and RegTech compliance mechanisms. At the same time, high-end investment in cybersecurity, such as AI-based fraud detection and multi-layered authentication, will reduce risks and increase confidence in online platforms.

J) Indian Overseas Bank

Indian Overseas Bank has IMPR, DBU, IFR, CMD, CTC as its most critical user level constraints. Such markers reveal low exposure to digital and high risk perceptions among employees. On the enabler level, DFQ, ITII, BATR, and AIPCS are additional barriers to digital transformation. The first step taken in mitigation is to make more areas digital by assisted banking models, especially those with lower coverage, so people can engage more with digital solutions, and more employees can be involved in digital operations. Digital migration will be quickened by improvement on customer onboarding and trust-building programs. The enabler level also has phased modernisation of infrastructure and cloud implementation as essential to enhance system reliability. It should be integrated with continuous reskilling programs based on AI and cybersecurity awareness training to enhance the adaptability of the workforce and decrease the perceived risk.

K) Kotak Mahindra Bank

CCRTU, IMPR, IFR, CMD, CTC, and RAISR are user-dominant indicators of Kotak Mahindra Bank. These indicate problems with usability, trust, and limited interaction between employees and AI systems. On the enabler level, readiness is further undermined by DFQ, ITII, BATR, LSMARI, AIPCS, and gaps in ITBCS. The mitigation should also aim at increasing the usability of the system by designing it with user-centred design and working through feedback loops, minimising the resistance to change through complaints (Andersen & Juelsrud, 2024). The expansion of AI-based positions in all business units will enhance workforce engagement with modern technologies. On the enabler level, there is a necessity for comprehensive IT modernisation, cloud-based infrastructure, and API ecosystems. RegTech solutions to strengthen cybersecurity structures and compliance regulations, and long-term reskilling, will guarantee the continuous establishment of digital capabilities.

L) State Bank of India (SBI)

The sheer size of SBI as an organisation also increases the effects of the user level barriers to technology uptake and daily performance. CCRTU, IFR, CTC, ELAR, RAISR are the dominant indicators of State Bank of India. The ongoing high customer complaint rates have shown that frontline employees are under strain and have to work with system inefficiencies amid a large and diverse customer base. The high rates of fraud and disparities in available cybersecurity training support the understanding of the perceived operational risk and ensure that employees are more cautious and less eager to be entirely dependent on digital channels. These issues are enhanced by job insecurity associated with automation, where clerical and operational workers feel threatened by digital transformation and not an opportunity. Meanwhile, the minimal diffusion of AI-assisted positions does not allow hands-on experience with more sophisticated tools, making learning-by-doing on large scales (Boustani, 2022). An enabler lens would create slow migration of old systems and limited IT budgets to support cybersecurity to undermine digital resilience, leading to unpredictable system performance and strengthening the mistrust of the new technologies.

To deal with these challenges needs a transformation strategy with a clear acknowledgement that SBI is large, that it has a public mandate, and a heterogeneous workforce. Core modernisation plan based on a hybrid cloud architecture can enable the bank to modernise its mission-critical systems in a gradual way without disrupting its operations across branches. Cybersecurity should be re-framed as a strategic pillar, not a support function. Board-level control, sophisticated artificial intelligence-driven threat thinking, and ongoing and scenario-based training that transforms security policies into daily behaviours should exist. It is also of vital importance to rebrand automation as a man-power expanding program. Anxiety can be mitigated through transparent communication on role redesign that is supported by well-organized reskilling and redeployment pathways that promote trust in the transformation agenda (Donald et al., 2023). As soon as employees observe clear progression paths into digitally enriched jobs and have access to stable and secure systems, large-scale adoption becomes a more viable option, even in an institution as complicated as SBI.

M) UCO Bank

The challenges associated with UCO Bank are predominantly related to the user level because of high complaint ratios and poor coverage of cybersecurity training which is a problem with usability and low risk awareness. System downtime, inadequate role integration, and minimal reskilling investment at the enabler level restrict the flexibility of the workforce. Mitigation must put priority in enhancing the reliability and usability of the system by upgrading infrastructure and testing it on users and reducing operational friction by employees. Continuous, behaviour-based training needs to be enhanced to increase cybersecurity capability. Increasing the number of functions being supported by AI will lead to better exposure to digital, and investing more in reskilling programs will boost employee confidence and performance in a technologically-enabled setting.

N) Union Bank of India

Union Bank displays a broad range of user-level issues, such as ARAA, DTHE, IMPR, DBU, IFR, CMD, and ELAR. All these are indicators of capability gaps and resistance towards digital transformation. Further inhibiting progress at the enabler level are limited RAHSR, BATR and AIPCS. Mitigation must take the form of holistic transformation. At the user level, the bank should offer reskilling programs that are continuous and AI driven, formal career progression, and effective communication about the automation effects to mitigate resistance. By providing incentives and easy digital interfaces, customer migration will be boosted to ensure the growth of digital transaction volumes and employee familiarity (Serrado, Pereira, Mira da Silva, & Scalabrin Bianchi, 2020). On the enabler level, integrating AI into job roles across functional areas, enhancing compliance frameworks through RegTech, and investing more in reskilling are needed to develop long-term organisational capacity and better FinTech preparedness.

O) Yes Bank

The technology adoption problems of Yes Bank are also intertwined with the fact that trust deficit remains a problem in the bank that influences both behaviour of employees and their relations with the customers. High customer complaints of digital services indicate that frontline employees are often facing friction with their systems, and its impact is undermining trust in the technology-facilitated processes. A high sensitivity on fraud risk also increases the alertness of the employees more so in a bank that has in the past been involved with reputational and financial stability problems. Minimal customer movement to digital channels restricts employee access to end-to-end digital processes strengthening reliance on manual processes or assisted processes. Meanwhile, the job insecurity that comes with automation provokes defensive sentiments toward the new technologies that cause employees to view FinTech ventures as cost-reduction measures instead of capacity-building measures (Aziz Baker, 2025). These user constraints are also enforced at the enabler level due to the slowness in the legacy system migration, which compromises platform stability and limits the smooth introduction of solutions based on AI.

An effective recovery-driven digital policy is hence a necessity in order to transform perception and practice. The first step in restoring trust should be overt advances in online dependability and security: transparent onboarding experiences, well-articulated antifraud practices, and the ability to properly demonstrate cybersecurity defenses that staff can describe to clients. Simultaneously, fast-tracking of hybrid legacy modernisation will stabilise core platforms and allow a gradual incorporation of AI and analytics to reduce system outages, which are the root of complaints and mistrust. Reskilling and redeployment are also vital commitments that should be specific and quantifiable to regain the confidence of the workforce. Organised learning journeys on emerging digital roles, coupled with explicit messages that automation is to aid recovery and development and not labour market depletion,

can rebrand FinTech adoption as a collective organisational refresh initiative, as opposed to a factor of fear.

6.2.2 DOMINANT INDICATORS.

The most significant limitation to technology adoption in banks has been the incidence of fraud reports (IFR), which has been reported to contribute to almost 73% of the resistance witnessed among banks. The trust in employees, customers, and management is undermined by IFR at a fundamental level, unlike other indicators, which mainly signal gaps in capabilities or limitations of the infrastructure. Digital transformation is built on the basis of which it is criticized. The attack surface increases as banks increase digital access, which discloses systemic weaknesses of authentication, transaction monitoring, and human-technology interfaces. There is empirical evidence indicating that cases of digital fraud have been growing rapidly with the introduction of mobile and internet banking, especially in the emerging economies, where digital sophistication and cybersecurity maturity are not evenly spread (Bank for International Settlements, 2021; RBI, 2023). Having high IFR levels is a two-fold erosion effect. At the user level, recurring fraud cases raise the risk perception of employees, the workload associated with dealing with complaints and reconciliation, and mistrust of new digital tools. On the institutional level, the common reports on the fraud increase regulatory scrutiny, make the operating risk costs higher, and slow down the scaling of the solutions related to FinTech and AI. This then leads to defensive use of technology and not transformational usage of technology, whereby the banks have considered themselves to be on the defensive side to do damage control instead of being innovative.

The first reason behind high IFR is the sustained use of fragmented and rule-based frameworks of fraud detection which are ill-equipped to operate in real-time dynamic and digital worlds (Wai, 2024). A large number of banks implement new technologies in silos, which are independent of the core banking processes, which leads to a delay in the detection and increase in the number of false positives. This technical fragmentation is further exacerbated by the fact that older infrastructure causes the inability to integrate AI-based analytics and real-time monitoring systems (Bank for International Settlements, 2021). There are behavioural vulnerabilities to the extent that it worsens the issue. Poor cybersecurity training, poor knowledge of social engineering methods, and ambiguity of roles in human-AI interaction make it more vulnerable to fraud. Research has shown that human error is one of the primary causes of the cyber event in banking, especially in banks with a large digital transactions environment (Bank for International Settlements, 2021) (OECD, 2021;). In addition, low digital literacy among the customers and ineffective onboarding mechanisms increases exposure of fraud and contributes to an increase in the number of complaints and the burden on the employees.

6.2.3 BANKING SECTOR ALIGNED STRATEGIES TO MANAGE THE ENABLER LEVEL CHALLENGES.

To mitigate IFR, banks need to go beyond compliance-based security rules to more capability-based fraud control strategies. There is a growing focus on global best practices to use AI- and machine learning-based real-time fraud detection systems that find ever-expanding opportunities to learn constantly, based on transaction patterns and behavioural data. By integrating risk controls into the regular operations, such systems are more accurate in detecting, less responsive, and can restore employee trust in digital platforms (Bank for International Settlements, 2021). No less important is the integration of multi-layered and adaptable authentication protocols that rationalize security demands to transaction risk. Continuous authentication and behavioural biometrics have shown to be useful in discouraging identity-related fraud without adding user friction, and thus achieving both security and adoption goals. These technologies minimise workflow disruption to staff when implemented as part and parcel of core systems because they eliminate false alarms.

Regarding human capital, banks need to reposition cybersecurity training as a strategic asset but not a compliance requirement. Consecutive, situation-based training consistent with the dynamic typologies of fraud enhances situational awareness in employees and lowers anxiety levels based on technologies. It has been indicated that with institutions that invest in behavioural cybersecurity education, the rate of fraud is reduced, and the adoption rate of digital tools is increased (OECD, 2021). Good governance and working mechanisms are also important in effective mitigation of IFR. Banks, where regulatory scanning is institutionalised, where compliance frameworks are RegTech-enabled, and where they proactively engage with supervisors are more resilient and recover faster after a fraud incident (RBI, 2023). AI governance frameworks also create trust among employees by specifying responsibility in automated decision-making test beds.

The other best practice is inter-bank collaboration. Detection of new threats can be timely through the use of shared fraud intelligence platforms and industry-wide information exchange, eliminating redundancy of defense. The collective approaches are also becoming more considered critical in the fight against organised and cross-border digital fraud (Bank for International Settlements, 2021). Lastly, indirect but also influential of IFR levels are customer education and digital literacy programs. This lessens the vulnerability of customers to fraud and will help banks to reduce the number of complaints, alleviate the pressure on staff, and build a more favorable environment to continue with digital adoption. The handling of IFR is not just a risk management practice but it is at its core part of making sustainable adoption of technology in banking possible. This means that high incidence of fraud undermines trust, resistance, and learning-by-doing by the employees. On the other hand, financial institutions that combine sophisticated fraud analytics, people-focused security cultures, and sustainable governance systems will be in a better position to operationalize digital risk controls as adoption enablers. In that regard, successful IFR mitigation enhances dynamic capabilities through the protection of the situation to fully embrace, expand, and integrate digital technologies into daily banking processes.

All the dimensions of FinTech preparedness, including indicator identification, severity assessment, root cause mapping, and mitigation strategies, have been systematically analysed and covered across each selected bank. A comprehensive summary integrating Enabler Preparedness Index (EPI), User Preparedness Index (UPI), dominant indicators, associated root causes, and corresponding mitigation strategies is presented in Table 6.1 & Figure 6.1 below.

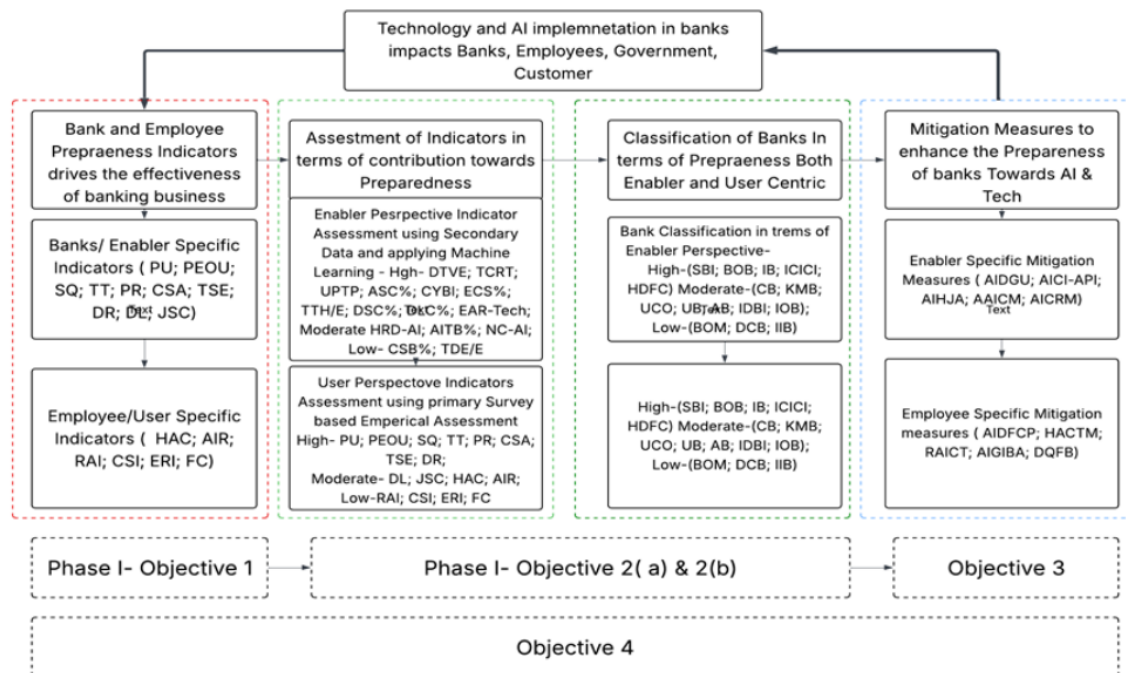


Figure 6.1: Final Framework delivered across Four objectives

Table 6.1 Comprehensive Bank-wise FinTech Preparedness, Root Cause, and Mitigation Summary

Bank Name	EPI	UP I	User Dominant Indicators	Enabler Dominant Indicators	User-Level Root Causes	Enabler-Level Root Causes	Enabler-Level Mitigation	User-Level Mitigation
Axis Bank	1.647	5.33	ARAA, CCRTU, IMPR, IFR, CTC, RAISR	DFQ, RAHSR, LSMARI	Lack of clarity (PU), usability issues (PEOU), low DL/TSE, fraud concerns (PR)	AIR gaps, downtime issues, partial RAI	Modular AIR, long-term ERI, AI governance	Sandbox training, link tools to performance
Bank of Baroda	1.647	5.67	IMPR, CMD, CTC	RAHSR, LSMARI	Low trust & awareness (TT, DL), usability gaps	AIR delays, RAI gaps	RegTech-enabled AIR upgrades	Simplified UI, peer learning
Bank of Maharashtra	1.588	6.17	DTHE, IMPR, DBU, IFR, ELAR	RAHSR, BATR	Skill gaps (TSE), risk & job insecurity	Weak CSI, governance gaps	Strengthen CSI, cyber governance	Scenario-based cyber learning
DCB Bank	1.235	6.33	CCRTU, DTHE, DBU, IFR, CMD, CTC	DFQ, ITIL, BATR, LSMARI, AIPCS, ITBCS	System complexity, low training, trust deficit	AIR gaps, weak FC, RAI gaps, low CSI	Phased AIR, compliance frameworks	Workflow redesign, simulation training
HDFC Bank	1.412	5.33	CCRTU, DTHE, IMPR, DBU, ELAR	DFQ, RAHSR, ITIL, BATR, AIPCS, ITBCS	Skill mismatch, job concerns	Legacy AIR issues, low ERI, CSI gaps	Improve AIR, ERI, cybersecurity	Role-based digital training
Indian Bank	1.588	6.33	IMPR, IFR, RAISR	DFQ, RAHSR, ITIL, BATR, AIPCS, ITBCS	Usability issues, low confidence	Weak FC, low ERI, compliance gaps	Digital helpdesks, ERI planning	Guided interfaces, sandbox learning
ICICI Bank	1.824	5.67	IMPR, DBU, CMD, ELAR	LSMARI, AIPCS	Job role concerns	ERI alignment gaps, RAI issues	Align ERI with innovation	Explainable AI, reskilling
IDFC	1.765	5.83	ARAA, DTHE, CMD, CTC	DFQ, BATR	Low motivation, workflow issues	AIR scalability, ERI gaps	Modular AIR, leadership-driven DR	Workflow simplification
IndusInd Bank	1.412	5.83	ARAA, DTHE, DBU, IFR, CTC, ELAR	DFQ, ITIL, BATR, LSMARI, AIPCS, ITBCS	Low confidence, risk concerns	AIR gaps, low ERI, RAI gaps	Continuous ERI, AIR upgrades	Micro-learning, digital champions
Indian Overseas	1.471	5.67	IMPR, DBU, IFR, CMD, CTC	DFQ, ITIL, BATR, AIPCS	Low DL, cyber risk concerns	Weak FC, ERI gaps, RAI delays	Incremental AIR, compliance focus	Cyber drills, peer learning
Kotak Mahindra Bank	1.353	5.50	CCRTU, IMPR, IFR, CMD, CTC, RAISR	DFQ, RAHSR, ITIL, BATR, LSMARI, AIPCS, ITBCS	Trust deficit, usability issues	CSI weakness, AIR gaps, RAI ambiguity	Strengthen CSI, AI governance	UI improvement, accountability clarity
SBI	1.647	5.17	CCRTU, IFR, CTC, ELAR, RAISR	LSMARI, ITBCS	Fraud risk, job concerns	Large-scale AIR needs, CSI gaps	Long-term ERI, hybrid AIR	Digital champions, simulations
UCO Bank	1.765	6.33	CCRTU, CTC	DFQ, RAHSR, BATR	Low CSA, low confidence	AIR gaps, ERI gaps	AIR pilots, regulatory alignment	Awareness training, sandbox
Union Bank	1.471	5.33	ARAA, DTHE, IMPR, DBU, IFR, CMD, ELAR	RAHSR, BATR, AIPCS	Low motivation, skill gaps, risk concerns	Weak ERI, RAI fragmentation, AIR gaps	Targeted ERI, AIR upgrades	Workflow simplification
Yes Bank	1.647	5.67	CCRTU, IFR, CMD, ELAR	LSMARI	Job insecurity, trust issues	AIR stabilisation, RAI gaps	ERI focus, AIR stabilisation	

In conclusion, the study offers a thorough and integrated understanding of FinTech preparedness in the banking sector by systematically connecting indicators, severity levels, root causes, and mitigation strategies across both institutional and behavioral aspects. The results show that while employee readiness remains fairly high, institutional preparedness still lags due to infrastructural, governance, and strategic challenges, creating a crucial readiness gap. By employing a dual-perspective approach and confirming insights through empirical analysis and expert input, the study moves beyond simple description to provide practical, bank-specific recommendations. In line with the final research goal, the study develops a two-layer conceptual mitigation framework that incorporates enabler-level (institutional) and user-level (behavioral) interventions, making sure that FinTech adoption strategies are both comprehensive and feasible. This framework is based on severity-based prioritization and root cause alignment, offering a clear path to close the identified preparedness gap. To summarize the main findings, a final conceptual diagram is presented, illustrating how indicators, severity levels, root causes, and mitigation strategies relate within a unified framework. This diagram visually emphasizes the study's main contribution, showing the shift from diagnosis to strategic action. Overall, the study confirms that sustainable FinTech adoption depends not only on technology but also on the alignment of technology, human skills, and institutional readiness. It provides both theoretical insights and practical guidance, serving as a roadmap for banks and policymakers to navigate digital transformation and develop a resilient, future-ready banking ecosystem.

7. CHAPTER 7

CONCLUSION AND IMPLICATIONS

7.1 KEY FINDINGS OF THE STUDY

The current research was designed to answer the research question: how can banks enhance their FinTech preparedness by aligning institutional capabilities with workforce adaptability? Consistent with the initial research objective, the research is able to determine and empirically confirm an organized list of FinTech readiness indicators in both the enabler and user dimensions. The results define a two-layered model that includes the index of Enabler Preparedness (EPI), that is the preparedness of the institutions, and the index of User Preparedness (UPI) that is the flexibility of the employees. As it can be seen, the indicators of institutional readiness include Technology Investment Intensity (ITIII), Digital Training and Human Capital Enhancement (DTHE), Improvement in Digital Processes (IMPR), Digital Banking Usage (DBU), and Incident Frequency Ratio (IFR), whereas the indicators of behavioural readiness are Perceived Usefulness (PU), Perceived Ease of Use (PEOU), Digital Literacy (DL), and Technology Self-Efficacy (TSE). Empirically, PU (7.11%) and PEOU (6.53%) emerged as dominant belief variables, contributing to a core belief domain weight of 13.64%, while personal capability variables contributed 12.16%, highlighting that behavioural readiness plays a crucial role, despite being classified as statistically low-impact yet high-severity. Therefore, Objective 1 is met because the study has managed to create an all-encompassing, quantifiable framework of FinTech readiness indicators.

Concerning the latter research objective, the study categorizes bank into Highly Adaptable Banks (HAB) and Low Adaptability Banks (LAB) based on secondary (institutional) and primary (employee) data. According to the analysis of secondary data, the preparedness index ranges between 1.23 to 1.82, which implies close yet moderate institutional readiness in banks. Other banks in the category of HAB are the ICICI Bank (1.824), IDFC First Bank (1.765), State Bank of India (1.588), and Yes Bank (1.765) because they have a better performance in indicators like ITIII, IMPR, DBU, and superior system-level integration, infrastructure preparation and regulatory alignment. As an example, State Bank of India is showing good performance metrics in terms of CTC, IFR, ELAR and RAISR whereas Yes Bank is showing stability in terms of IFR, CMD and ELAR-driven institutional strength. Conversely, DCB Bank (1.235), Kotak Mahindra Bank (1.294), Union Bank (1.471), and HDFC Bank (1.412) are classified as the LAB category, which is mainly caused by the shortcomings in the indicators

of risk exposure (IFR), the gaps in the readiness of AI infrastructure, and the unevenness in the digital process enhancements.

But once the category is furthered to primary data, the opposite trend is observed. The main preparedness index lies between 5.17 and 6.33 reflecting that the employee level preparedness is much higher than the institutional preparedness. State Bank of India, Yes Bank, and UCO Bank are powerful examples of banks with good behavioural adaptability because of the strong degree of digital literacy, trust towards technology, and efficient human-AI cooperation. It is important to note that even the banks that are LAB in the secondary analysis like Union Bank and Kotak Mahindra Bank have comparatively high user-side adaptability based on the indicators of Perceived Usefulness, Digital Literacy, and exposure to employee training. This deviation is an obvious gap of structural readiness wherein user readiness is more than the enabler readiness. Random Forest model was shown to have a better performance in classification than the SVM and Neural Network models, with the lower out-of-bag error and high reliability in classification that proved the robustness of the HAB-LAB classification. Therefore, Objective 2 is achieved by the means of strict and tested classification of banks based on institutional and behavioural scales. In regards to the third research objective, the severity and root cause analysis shows that a number of high-severity indicators are found in statistically low-impact zones, which suggests that there are hidden structural inefficiencies in the banking system. Critical constraints are identified on AI Infrastructure Readiness (AIR), Employee Reskilling Initiatives (ERI) and Regulatory Alignment (RAI) at enabler level and behavioural drivers, including digital literacy, perceived risk, trust, and human-AI collaboration are dominant at user level. The similar and diverse indicators across banks also point to the fact that FinTech preparedness is not universal but contextual due to the priority decided by the organisation and technological maturity. Importantly, this analysis indicates that the most critical barriers to FinTech adoption are not necessarily those with the highest statistical weights but those with the highest severity, implying that banks must prioritise high-severity constraints to achieve meaningful digital transformation. Thus, Objective 3 can be met through a methodical approach to the process of root cause identification and interpretation of severity-related factors that impact bank adaptability.

To address the fourth research objective, the paper constructs a combined FinTech preparedness model that correlates institutional ability and workforce flexibility. The paradigm shows that institutional readiness defines the scalability and sustainability of technology

adoption whereas user readiness is a driver of technology adoption. The results verify that the successful implementation of FinTech is not facilitated by the individual technological investments but the consistency on the systems, processes and human capabilities. The greatest value addition of the research is the establishment of a structural preparedness gap whereby employee-level flexibility is constantly more than the preparedness in the institution, thus constituting the main source of digital transformation. In line with this, Objective 4 will be fulfilled by creating a universal, empirically tested FinTech preparedness model.

7.2 POLICY IMPLICATIONS

The results of the study have significant implications for the policy makers and regulators including the Reserve Bank of India. As the findings point out, the changes in the priorities should be made from compliance-driven to capability-driven regulation in which the banks will be evaluated based on their level of technological readiness and flexibility, in addition to their financial results. The regulators are recommended to start organized FinTech-readiness assessment models and require regular reporting on digital infrastructure, cyber preparedness, and integration of AI.

Also, the identified gap between the institutional preparedness (1.23-1.82) and employee preparedness (5.17-6.33) will require the implementation of specific policy measures aimed at enhancing the capacity of infrastructure, governance, and system integration. There should be increased investments in AI infrastructure, regulatory technology (RegTech), and digital governance mechanisms although there should be standardisation of practices concerning data governance, AI accountability, and system interoperability as well. It will also be important in improving financial stability by strengthening early warning systems especially in the risk indicators like frequency of incidences. These policy recommendations are directly derived from the structural readiness gap identified in the study, underscoring the need for systemic, coordinated intervention.

7.3 MANAGERIAL IMPLICATIONS

At the management level, the paper highlights the importance of the banks engaging in a dual-focus approach that will boost the technological infrastructure and human capacity at the same time. Considering that the employee readiness is between 5.17 and 6.33, institutional preparedness is between 1.23 and 1.82, the focus of banks should be on AI infrastructure, digital process optimization and governance structures with the goal of aligning with workforce

capability. On-going reskilling of employees, digital training, and the establishment of the ability to work with AI are necessary to maximize this behavioural preparedness. To deal with the identified root cause deviation, a change in the problem-induced decision-making and the severity-based prioritisation should be made. High-severity constraints that banks should prioritize resolving include AI infrastructure divides, insufficient reskilling programs, and ineffective regulatory alignment, and subsequent optimisation of high-impact variables. This may be done by making investments in scalable AI solutions that are targeted, ongoing upskilling of employees and by integrating regulatory technology (RegTech) solutions that facilitate compliance procedures. Also, banks ought to take a gradual digital transformation strategy with a focus on infrastructure preparation before implementing the sophisticated FinTech. The alignment of high-severity constraints with strategic investment choices can also help banks lower the structural inefficiencies and enhance general FinTech preparedness.

The findings also indicate that the operational strategies are supposed to be aimed at improving the digital usage, automation of operations, and risk management practices. The banks that are HAB show that competitive advantage may be attained as a result of effective matching technology and the human capacity, whereas LAB banks have to deal with structural inefficiencies and enhance governance arrangements. The main strategic focus of the banking institutions should therefore be bridging the gap between the institutional and user readiness.

7.4 RECOMMENDATION

Banks must also follow a multi-step approach to enhance FinTech preparedness in the Indian banking industry. First, they should work on their infrastructure. This involves updating core systems, adopting cloud technology, and developing more resilient systems built on APIs. They are also supposed to invest in cybersecurity to counter threats. This involves establishing real-time monitoring, disseminating information within the sector, and conducting routine audits to mitigate risks.

Second, banks are advised to support their staff in transitioning by establishing formal training programs. They should provide continuous digital training, incorporate digital skills during performance evaluations, and promote employee use of technology through job redesign. Studies indicate that certifications and peer mentoring enable individuals to better embrace and use new technology. Third, banks need to adopt effective governance approaches that can integrate compliance, risk management, and technology utilization. This involves clear

governance, explainability standards and even accountability measures to establish trust with employees and customers. Regulatory technology (RegTech) is one way banks automate compliance and simplify operations.

At the policy level, regulators need to establish mechanisms to evaluate the FinTech preparedness, demand disclosures on digital preparedness, and facilitate testing conditions for innovation. Industry groups and government can help by creating common digital infrastructure, training programs, and common skill frameworks. Lastly, banks need to ensure their activities are prioritized, i.e., they must deal with high-risk locations like old infrastructure, insufficiency of reskilling and regulatory concerns first, before concentrating on the other areas. Digital transformation will be successful by aligning the capabilities of their workforce with their skills.

7.5 LIMITATIONS OF THE STUDY

The study has some limitations even though it has a comprehensive approach. A chosen sample of banks is used in the analysis, which could restrict the externalisation of the results to the whole banking industry. The use of secondary data in the form of published financial statements can lead to reporting limitations, whereas the primary one, which is created on the basis of 258 responses in surveys, is related to perceptions that are likely to be biased by the respondents. Moreover, the research is based on a narrow time horizon and indicators that are not necessarily the best measure of long-term structural changes or external macroeconomic factors. Moreover, machine learning methods dependent on the selection of the variables and model assumptions are applied in the classification of the banks into two categories HAB and LAB. There may be many other ways of classifying banks too. The limitations of this study can be considered as a gap in FinTech literature and be undertaken in the future.

7.6 FUTURE SCOPE OF WORK

This research proposes some future research and enhancement suggestions. Further work can involve a broader number of banks, including regional rural banks, cooperative banks, and small finance banks. This will enhance knowledge of the banking industry in general. The comparison of the FinTech preparedness in various countries can also serve to compare India with global leaders and understand effective practices. It is valuable to conduct research over time to understand how FinTech preparedness evolves, particularly in response to new regulations, changes in technologies, and customer behavior. This research can be used to

identify reasons and assess the sustainability of digital transformation initiatives. More advanced technology models can also be studied in the future, leveraging various machine learning strategies, real-time data, and network analysis to enhance predictions and decisions. The data on customer behavior, employee, and bank data can be included to provide a more comprehensive view of digital adoption.

The other aspect that should be studied is the interaction of employees with technology, particularly in terms of job change, job redesign, and corporate culture. The findings can be enriched with qualitative studies, case studies, and experiments that give insight into how people can adapt. Finally, future research can be aimed at developing particular policy guides and action plans, transforming research results into the strategy available to regulators and banks. Such initiatives will play a key role in creating a resilient, inclusive, and future-proof digital banking industry.

7.7 CONCLUSION

The paper concludes that the FinTech readiness of the Indian banking industry is marked by a high structural imbalance between institutional ability and labour flexibility. Although banks have achieved significant gains in embracing digital technologies, the secondary data analysis demonstrates that institutional preparedness is still moderate and highly concentrated in the small range of 1.23 to 1.82, which indicates the lack of differentiation in the infrastructure and governance capabilities. Conversely, on the primary data analysis, the level of employee preparedness was much higher as employee preparedness scores varied between 5.17 and 6.33, showing a high degree of behavioural acceptance and flexibility towards technological change.

Highly Adaptable Banks (HAB) include Banks like ICICI Bank, IDFC First Bank, State Bank of India and Yes Bank, among others and perform better due to a combination of high level of digital investment, optimisation of processes and improved risk management practices. On the other hand, the problem of Low Adaptability Banks (LAB) such as DCB Bank, Kotak Mahindra Bank, Union Bank, and HDFC Bank is characterized by difficulties with infrastructure gaps, increased exposure to operational risks, as well as poor governance systems. Nevertheless, the level of employee preparedness even in LAB banks implies that there is a lot of untapped potential that can be exploited with the so-called strategic alignment.

It is thus clear in the study that institutional system and human ability is the most important impeding determinant to the integration of FinTech rather than the absence of technology. A

complex digital transformation needs to be based on a comprehensive approach that would consolidate both infrastructure and governance and the flexibility of the workforce. The paper adds to the current body of literature because it combines machine learning-based classification with behavioural and institutional readiness frameworks, thus providing a new dual-perspective view of the FinTech adoption in banking.

Essentially, the research confirms the fact that the future of banking will never be established on the level of technology adoption, but rather on the level of technology, people and institution development in line with each other. The results can be used as a viable and scalable roadmap of sustainable FinTech integration, thus, playing a role in the creation of a robust, technology-focused, and future-oriented banking ecosystem.

8. REFERENCES

- A.A. Shaikh, R. Glavee-Geo, H. K. (2017). Exploring the nexus between financial sector reforms and the emergence of digital banking culture—Evidences from a developing country. *Research in International Business and Finance*, 42, 1030–1039.
- Adel, H., ElBakary, M., ElDahshan, K., & Salah, D. (2022). BC-HRM: A Blockchain-Based Human Resource Management System Utilizing Smart Contracts. In *Lecture Notes in Networks and Systems* (Vol. 309). https://doi.org/10.1007/978-3-030-84337-3_8
- Adewumi, A. O., & Akinyelu, A. A. (2017). A survey of machine-learning and nature-inspired based credit card fraud detection techniques. *International Journal of System Assurance Engineering and Management*, 8(2), 937–953. <https://doi.org/10.1007/s13198-016-0551-y>
- Agarwal, A., Singhal, C., & Thomas, R. (2021). AI-powered decision making for the bank of the future. *McKinsey & Company*.
- Agarwal, S., Ghosh, P., Ruan, T., & Zhang, Y. (2024). Transient Customer Response to Data Breaches of Their Information. *Management Science*, 70(6), 4105–4114. <https://doi.org/10.1287/mnsc.2021.01335>
- Aizenman, J., Ito, H., & Pasricha, G. K. (2022). Central bank swap arrangements in the covid-19 crisis. *Journal of International Money and Finance*, 122, 102555.
- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2022). Analytical hierarchy processes and Pareto analysis for mitigating cybercrime in the financial sector. *Journal of Financial Crime*, 29(3), 984–1008. <https://doi.org/10.1108/JFC-04-2021-0086>
- Akinbowale, O. E., Klingelhöfer, H. E., & Zerihun, M. F. (2024). The assessment of the impact of cyberfraud in the South African banking industry. *Journal of Financial Crime*, 31(2), 287–301. <https://doi.org/10.1108/JFC-10-2022-0260>
- Al-Dosari, K., Fetais, N., & Kucukvar, M. (2024). Artificial intelligence and cyber defense system for banking industry: A qualitative study of AI applications and challenges. *Cybernetics and Systems*, 55(2), 302–330.
- Al-Gasaymeh, A., Al-Gasaymeh, L. A., Kasem, J., Jaber, J. J., Al-Naimi, A. A., & Al-Gasawneh, J. (2024). The Impact of Electronic Readiness on the Adoption of Financial Technology in Jordanian Commercial Banks. In *International Conference on National Institutions' Role in Confronting Environmental Risks-Reality and Solutions* (pp. 125–132). Springer.
- Alawida, M., Omolara, A. E., Abiodun, O. I., & Al-Rajab, M. (2022). A deeper look into cybersecurity issues in the wake of Covid-19: A survey. *Journal of King Saud University - Computer and Information Sciences*, 34(10, Part A), 8176–8206. <https://doi.org/10.1016/j.jksuci.2022.08.003>
- Albshaier, L., Almarri, S., & Hafizur Rahman, M. M. (2024). A Review of Blockchain's Role in E-Commerce Transactions: Open Challenges, and Future Research Directions. *Computers*, 13(1). <https://doi.org/10.3390/computers13010027>
- Ali, O., & Osmanaj, V. (2020). The role of government regulations in the adoption of cloud computing: A case study of local government. *Computer Law & Security Review*, 36, 105396. <https://doi.org/10.1016/j.clsr.2020.105396>

- Allen, H. J. (2024). Regulating fintech: A harm focused approach. *Computer Law & Security Review*, 52, 105910. <https://doi.org/https://doi.org/10.1016/j.clsr.2023.105910>
- Almansour, M. (2023). Artificial intelligence and resource optimization: A study of Fintech start-ups. *Resources Policy*, 80, 103250.
- Alnoor, A. M. R., Al-Abrow, H., Abdullah, H., & Abbas, S. (2020). The impact of self-efficacy on employees' ability to accept new technology in an Iraqi university. *Global Business and Organizational Excellence*, 39(2), 41–50.
- Alrahamneh, A., Murshed, A. A., & Alhalalmeh, A. (2026). Automation and Job Security: Policy Implications for Digital Labor Governance. In *Artificial Intelligence for Sustainable Innovation Management and Risk Management: A Systems (and Network) Perspective* (pp. 1651–1664). Springer.
- Ammirato, S., Sofo, F., Felicetti, A. M., & Raso, C. (2019). The potential of IoT in redesigning the bank branch protection system: An Italian case study. *Business Process Management Journal*, 25(7), 1441–1473. <https://doi.org/10.1108/BPMJ-04-2018-0099>
- Anagreh, S., Al-Momani, A., Maabreh, H. M. A., Sharairi, J. A., Alrfai, M. M., Haija, A. A. A., ... Al-Hawary, S. I. S. (2024). Mobile payment and digital financial inclusion: a study in Jordanian banking sector using unified theory of acceptance and use of technology. In *Business Analytical Capabilities and Artificial Intelligence-Enabled Analytics: Applications and Challenges in the Digital Era, Volume 1* (pp. 107–124). Springer.
- Andersen, H., & Juelsrud, R. E. (2024). Optimal capital adequacy ratios for banks. *Latin American Journal of Central Banking*, 5(2), 100107.
- Arner, D. W., Barberis, J., & Buckley, R. P. (2016). 150 years of Fintech: An evolutionary analysis. *Jassa*, (3), 22–29.
- Arner, D. W., Zetsche, D. A., Buckley, R. P., & Kirkwood, J. M. (2024). The financialisation of Crypto: Designing an international regulatory consensus. *Computer Law & Security Review*, 53, 105970. <https://doi.org/https://doi.org/10.1016/j.clsr.2024.105970>
- Arntz, M., Gregory, T., & Zierahn, U. (2017). Revisiting the risk of automation. *Economics Letters*, 159, 157–160.
- Arpaci, I., Yardimci, Y. C., Ozkan, S., & Turetken, O. (2012). Organizational adoption of information technologies: A literature review. *International Journal of Ebusiness and Egovernment Studies*, 4(2), 37–50.
- Asif, M., Lodhi, R. N., Sarwar, F., & Ashfaq, M. (2024). Dark side whitewashes the benefits of FinTech innovations: a bibliometric overview. *International Journal of Bank Marketing*, 42(1), 113–132. <https://doi.org/10.1108/IJBM-10-2022-0438>
- Aziz Baker, H. (2025). Organizational Resistance to Artificial Intelligence. Technische Universität Wien.
- Bajwa, I. A., Ahmad, S., Mahmud, M., & Bajwa, F. A. (2023). The impact of cyberattacks awareness on customers' trust and commitment: an empirical evidence from the Pakistani banking sector. *Information and Computer Security*, 31(5), 635–654. <https://doi.org/10.1108/ICS-11-2022-0179>
- Bank for International Settlements. (2021). Bank for International Settlements - Annual Report 2022/23.

- Belhoucette, K., Berkane, M., & Belhade, H. (2019). Interest emotion recognition approach using self-organising map and motion estimation. *International Journal of Intelligent Systems Technologies and Applications*, 18(5), 494–508. <https://doi.org/10.1504/IJISTA.2019.101950>
- Belias, D., Koustelios, A., Vairaktarakis, G., & Sdrolas, L. (2015). Organizational Culture and Job Satisfaction of Greek Banking Institutions. *Procedia - Social and Behavioral Sciences*, 175, 314–323. <https://doi.org/10.1016/j.sbspro.2015.01.1206>
- Bentley, M., Stephenson, A., Toscas, P., & Zhu, Z. (2020). A multivariate model to quantify and mitigate cybersecurity risk. *Risks*, 8(2), 61.
- Bessembinder, H; Lemmon, M. L. (2002). American Finance Association Equilibrium Pricing and Optimal Hedging in Electricity Forward Markets. *The Journal of Finance*, 57(3), 1347–1382.
- Bessen, J. (2019). Automation and jobs: When technology boosts employment. *Economic Policy*, 34(100), 589–626.
- Bhasin, Madan L. (2016). THE ROLE OF TECHNOLOGY IN COMBATTING BANK FRAUDS : PERSPECTIVES. *Ecoforum*, 5(2), 200–212.
- Bhasin, Madan Lal. (2016). Challenge of mitigating bank frauds by judicious mix of technology: Experience of a developing country. *Economics, Management and Sustainability*, 1(1), 23–41. <https://doi.org/10.14254/jems.2016.1-1.3>
- Bhusan, S., & Singh, A. (2023). ICICI Bank and SBI—too big to fail. *Emerald Emerging Markets Case Studies*, 1–38.
- Biswas, S., Carson, B., Chung, V., Singh, S., & Thomas, R. (2020). AI-bank of the future: Can banks meet the AI challenge. *New York: McKinsey & Company*.
- Bonilla, J., Blanco, J., Zarza, E., & Alarcón-Padilla, D. C. (2022). Feasibility and practical limits of full decarbonization of the electricity market with renewable energy: Application to the Spanish power sector. *Energy*, 239, 122437. <https://doi.org/https://doi.org/10.1016/j.energy.2021.122437>
- Boustani, N. M. (2022). Artificial intelligence impact on banks clients and employees in an Asian developing country. *Journal of Asia Business Studies*, 16(2), 267–278.
- Bughin, J., Seong, J., Manyika, J., Chui, M., & Joshi, R. (2018). Notes from the AI frontier: Modeling the impact of AI on the world economy. *McKinsey Global Institute*, 4(1).
- Button, M., Hock, B., Shepherd, D., & Gilmour, P. M. (2023). What really works in preventing fraud against organisations and do decision-makers really need to know? *Security Journal*. <https://doi.org/10.1057/s41284-023-00402-4>
- Cao, J., & Song, Z. (2025). An incoming threat: the influence of automation potential on job insecurity. *Asia-Pacific Journal of Business Administration*, 17(1), 116–135.
- Carminati, M., Caron, R., Maggi, F., Epifani, I., & Zanero, S. (2015). BankSealer: A decision support system for online banking fraud analysis and investigation. *Computers & Security*, 53, 175–186. <https://doi.org/https://doi.org/10.1016/j.cose.2015.04.002>
- Cetindamar, D., Abedin, B., & Shirahada, K. (2021). The role of employees in digital transformation: a preliminary study on how employees’ digital literacy impacts use of digital technologies. *IEEE Transactions on Engineering Management*.

- Chen, B., Qiao, S., Zhao, J., Liu, D., Shi, X., Lyu, M., ... Zhai, Y. (2020). A security awareness and protection system for 5G smart healthcare based on zero-trust architecture. *IEEE Internet of Things Journal*, 8(13), 10248–10263.
- Chhabra Roy, N., & P, S. (2024). Proactive cyber fraud response: a comprehensive framework from detection to mitigation in banks. *Digital Policy, Regulation and Governance* . <https://doi.org/10.1108/DPRG-02-2024-0029>
- Chhabra Roy, N., & Prabhakaran, S. (2023a). Internal-led cyber frauds in Indian banks: an effective machine learning–based defense system to fraud detection, prioritization and prevention. *Aslib Journal of Information Management*, 75(2), 246–296. <https://doi.org/10.1108/AJIM-11-2021-0339>
- Chhabra Roy, N., & Prabhakaran, S. (2023b). Sustainable response system building against insider-led cyber frauds in banking sector: a machine learning approach. *Journal of Financial Crime*, 30(1), 48–85. <https://doi.org/10.1108/JFC-12-2021-0274>
- Chhabra Roy, N., & Prabhakaran, S. (2023c). Sustainable response system building against insider-led cyber frauds in banking sector: a machine learning approach. *Journal of Financial Crime*, 30(1), 48–85. <https://doi.org/10.1108/JFC-12-2021-0274>
- Chhabra Roy, N., & Prabhakaran, S. (2025). Cyber fraud (CF) in banking: a dual-layer, blockchain-enabled approach for prevention and managerial response. *Managerial Finance, ahead-of-p*(ahead-of-print). <https://doi.org/10.1108/MF-09-2024-0716>
- Chitimira, H., & Ncube, P. (2021). The regulation and use of artificial intelligence and 5g technology to combat cybercrime and financial crime in south african banks. *Potchefstroom Electronic Law Journal/Potchefstroomse Elektroniese Regsblad*, 24(1).
- Choithani, T., Chowdhury, A., Patel, S., Patel, P., Patel, D., & Shah, M. (2024). A Comprehensive Study of Artificial Intelligence and Cybersecurity on Bitcoin, Crypto Currency and Banking System. *Annals of Data Science*, 11(1), 103–135. <https://doi.org/10.1007/s40745-022-00433-5>
- Coy, J. S., Lambert, J. E., & Miller, M. M. (2016). STORIES OF THE ACCUSED : A PHENOMENOLOGICAL INQUIRY OF MFTS AND ACCUSATIONS OF UNPROFESSIONAL CONDUCT, 42(January), 139–152. <https://doi.org/10.1111/jmft.12109>
- Dahiya, D., & Mathew, S. K. (2016). IT assets, IT infrastructure performance and IT capability: a framework for e-government. *Transforming Government: People, Process and Policy*, 10(3), 411–433.
- Dai, S., Duan, X., & Zhang, W. (2020). Knowledge map of environmental crisis management based on keywords network and co-word analysis, 2005–2018. *Journal of Cleaner Production*, 262, 121168.
- Das, A., & Das, D. (2023). Adoption of FinTech services amidst COVID-19 pandemic: empirical evidence from Assam. *Managerial Finance*, 49(6), 1075–1093. <https://doi.org/10.1108/MF-08-2022-0379>
- Das, S., & Ganguly, D. (2024). Protecting Your Assets: Effective Use of Cybersecurity Measures in Banking Industries BT - Next-Generation Cybersecurity: AI, ML, and Blockchain. In K. Kaushik & I. Sharma (Eds.) (pp. 265–286). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-97-1249-6_12

- Daultani, Y., Dwivedi, A., & Pratap, S. (2021). Benchmarking higher education institutes using data envelopment analysis: capturing perceptions of prospective engineering students. *Opsearch*, 58(4), 773–789.
- Davis, G.B., & Olson, M. H. (1985). *Management information systems: Conceptual foundations, structure, and development*. New York: McGraw-Hill.
- Deloitte. (2023). Five ways banks can mitigate a catastrophic cybersecurity event.
- Dery, K., Sebastian, I. M., & van der Meulen, N. (2017). The digital workplace is key to digital innovation. *MIS Quarterly Executive*, 16(2).
- Donald, W. E., Baruch, Y., & Ashleigh, M. J. (2023). Technological transformation and human resource development of early career talent: Insights from accounting, banking, and finance. *Human Resource Development Quarterly*, 34(3), 329–348.
- Dootson, P., Beatson, A., & Drennan, J. (2016). Financial institutions using social media – do consumers perceive value? *International Journal of Bank Marketing*, 34(1), 9–36. <https://doi.org/10.1108/IJBM-06-2014-0079>
- Dunphy, A. (2024). Is the regulation of connected and automated vehicles (CAVs) a wicked problem and why does it matter? *Computer Law & Security Review*, 52, 105944. <https://doi.org/https://doi.org/10.1016/j.clsr.2024.105944>
- Eric, A., & Richard, B. (2019). Surviving in the digital era – business models of digital enterprises in a developing economy. *Digital Policy, Regulation and Governance*, 21(2), 164–178. <https://doi.org/10.1108/DPRG-08-2018-0046>
- Fard, J., Roper, K. O., & Hess, J. (2016). Simulation of home-hospital impacts on crowding – FM implications. *Facilities*, 34(13/14), 748–765. <https://doi.org/10.1108/F-07-2015-0048>
- Farrugia, D., Zerafa, C., Cini, T., Kuasney, B., & Livori, K. (2021). A Real-Time Prescriptive Solution for Explainable Cyber-Fraud Detection Within the iGaming Industry. *SN Computer Science*, 2(3). <https://doi.org/10.1007/s42979-021-00623-7>
- Fedele, A., Punzi, C., & Tramacere, S. (2024). The ALTAI checklist as a tool to assess ethical and legal implications for a trustworthy AI development in education. *Computer Law & Security Review*, 53, 105986. <https://doi.org/https://doi.org/10.1016/j.clsr.2024.105986>
- Ferreira, A., & Sandner, P. (2021). Eu search for regulatory answers to crypto assets and their place in the financial markets' infrastructure. *Computer Law & Security Review*, 43, 105632. <https://doi.org/https://doi.org/10.1016/j.clsr.2021.105632>
- FICCI. (2023). FICCI-IBA Survey of Bankers.
- Fragiadakis, G., Diou, C., Kousiouris, G., & Nikolaidou, M. (2024). Evaluating human-ai collaboration: A review and methodological framework. *ArXiv Preprint ArXiv:2407.19098*.
- Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerisation? *Technological Forecasting and Social Change*, 114, 254–280.
- Fuchs, L., Nguyen, H., Nguyen, T., & Schaeck, K. (2023). Climate Stress Test, Bank Lending, and the Transition to the Carbon-Neutral Economy. Bank Lending, and the Transition to the Carbon-Neutral Economy (April 24, 2023).
- García-Avilés, J.-A. (2020). Diffusion of innovation. *The International Encyclopedia of Media Psychology*, 1(8).

- Garcia-Segura, L. A. (2024). The Role of Artificial Intelligence in Preventing Corporate Crime. *Journal of Economic Criminology*, 100091. <https://doi.org/https://doi.org/10.1016/j.jeconc.2024.100091>
- Gaur, N. (2020). Blockchain challenges in adoption. *Managerial Finance*, 46(6), 849–858. <https://doi.org/10.1108/MF-07-2019-0328>
- Georgiadou, A., Mouzakis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, 62(3), 452–462.
- Gowda, P. (2021). Migrating banking applications to the cloud: Strategies and best practices. *Journal of Scientific and Engineering Research*, 8(12), 144–151.
- Guha, E. A., & Indurkar, S. K. (2020). A Study on Cyber Crime and Data Breach Management. *Research Journal of Engineering and Technology*, 11(2), 113–118. <https://doi.org/10.5958/2321-581X.2020.00020.3>
- Guo, D., Habich-Sobiegalla, S., & Kostka, G. (2023). Emotions, crisis, and institutions: Explaining compliance with COVID-19 regulations. *Regulation & Governance*, n/a(n/a). <https://doi.org/https://doi.org/10.1111/rego.12509>
- Gurung, A., Luo, X., & Raja, M. K. (2008). An empirical investigation on customer's privacy perceptions, trust and security awareness in E-commerce environment. *Journal of Information Privacy and Security*, 4(1), 42–60.
- Hacker, P. (2023). The European AI liability directives – Critique of a half-hearted approach and lessons for the future. *Computer Law & Security Review*, 51, 105871. <https://doi.org/https://doi.org/10.1016/j.clsr.2023.105871>
- Halima Oluwabunmi Bello, Courage Idemudia, & Toluwalase Vanessa Iyelolu. (2024). Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention. *World Journal of Advanced Research and Reviews*, 23(1), 056–068. <https://doi.org/10.30574/wjarr.2024.23.1.1985>
- Hidayat, D. N., Restiandi, A., & Sukresna, I. M. (2025). Designing an optimal education and training model for relationship managers in the digital era. *Research Horizon*, 5(1), 79–94.
- Hossain, S., Fernando, M., & Akter, S. (2025). Digital leadership: Towards a dynamic managerial capability perspective of artificial intelligence-driven leader capabilities. *Journal of Leadership & Organizational Studies*, 32(2), 189–208.
- Hunt, V., Prince, S., Dixon-Fyle, S., & Yee, L. (2018). Delivering through diversity.
- Iddrisu, K., Yakubu, I. N., Yussif, A. R., & Issah, M. (2025). RegTech and FinTech: Enhancing Regulatory Efficiency and Inclusivity. In *Financial Regulation, Governance, and Stability* (pp. 162–186). Routledge.
- ILO. (2021). World Employment and Social Outlook. 2021: The role of digital labour platforms in transforming the world of work. International Labour Office.
- Imran, M., Maqbool, N., & Shafique, H. (2014). Impact of technological advancement on employee performance in banking sector. *International Journal of Human Resource Studies*, 4(1), 57–70.
- India Cyber Threat Report. (2025). *India Cyber Threat Report 2025*.
- Ismail, M. M., & Haq, M. A. (2024). Enhancing enterprise financial fraud detection using machine learning. *Engineering, Technology & Applied Science Research*, 14(4), 14854–14861.

- J. Manyika, S. Lund, M. Singer, O. White, C. B. (2016). Digital finance for all: Powering inclusive growth in emerging economies. USA.
- Javaid, M., Haleem, A., Singh, R. P., Suman, R., & Khan, S. (2022). A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluations*, 2(3), 100073. <https://doi.org/https://doi.org/10.1016/j.tbench.2022.100073>
- Jenab, K., & Moslehpour, S. (2016). Cyber Security Management : A Review. *Business Management Dynamics*, 5(December), 16–39. Retrieved from papers3://publication/uuid/1ECB5711-69D2-4904-88E8-9D22626EAAAF%0Ahttp://dx.doi.org/10.1016/j.ijcip.2015.02.002
- Jensen, J. R., & Ross, O. (2020). Managing risk in defi. In JR Jensen and O. Ross, “Managing Risk in DeFi” in CEUR Workshop Proceedings, Aachen.
- Jin, S., Balliet, D., Romano, A., Spadaro, G., Van Lissa, C. J., Agostini, M., ... Abakoumkin, G. (2021). Intergenerational conflicts of interest and prosocial behavior during the COVID-19 pandemic. *Personality and Individual Differences*, 171, 110535.
- Jing, X., Qin, W., Yao, H., Han, X., & Wang, P. (2024). Resilience-oriented planning strategy for the cyber-physical ADN under malicious attacks. *Applied Energy*, 353(PA), 122052. <https://doi.org/10.1016/j.apenergy.2023.122052>
- Jinger, D., Kaushal, R., Kumar, R., Paramesh, V., Verma, A., Shukla, M., ... Uthappa, A. R. (2023). Degraded land rehabilitation through agroforestry in India: Achievements, current understanding, and future perspectives. *Frontiers in Ecology and Evolution*, 11, 1088796.
- Kanchan, K. V, Patibanda, S., & Gorti, K. (n.d.). AI in Banking: A Case Study on ICICI Bank’s AI-Driven Transformation.
- Kesavaraj, V., Azariah, N., Raja, R., & Priya, N. C. (2014). Examining mean-volatility spillovers across national stock markets, 19, 55–62.
- Kornelakis, A., Kirov, V., & Thill, P. (2022). The digitalisation of service work: A comparative study of restructuring of the banking sector in the United Kingdom and Luxembourg. *European Journal of Industrial Relations*, 28(3), 253–272.
- Kshetri, N. (2005). Pattern of global cyber war and crime: A conceptual framework. *Journal of International Management*, 11(4), 541–562. <https://doi.org/10.1016/j.intman.2005.09.009>
- Ksieniewicz, P., Woźniak, M., Cyganek, B., Kasprzak, A., & Walkowiak, K. (2019). Data stream classification using active learned neural networks. *Neurocomputing*, 353, 74–82. <https://doi.org/https://doi.org/10.1016/j.neucom.2018.05.130>
- Lacey, D., Goode, S., Pawada, J., & Gibson, D. (2020). The application of scam compliance models to investment fraud offending. *Journal of Criminological Research, Policy and Practice*, 6(1), 65–81. <https://doi.org/10.1108/JCRPP-12-2019-0073>
- Lodhia, S., & Mitchell, N. A. (2022). Corporate social responsibility disclosures and reputation risk management post the banking royal commission: a study of the big four banks. *Qualitative Research in Accounting & Management*, 19(2), 162–185. <https://doi.org/10.1108/QRAM-07-2020-0120>

- Lyu, Z. (2025). Analysis of the Business Strategy in the Banking Industry: A Case Study of JPMorgan Chase & Co. *Journal of Education, Humanities and Social Sciences*, 61, 390–394.
- Mahapatra, P., & Singh, S. K. (2021). Artificial intelligence and machine learning: discovering new ways of doing banking business. In *Artificial intelligence and machine learning in business management* (pp. 53–80). CRC Press.
- Malgieri, G. (2019). Automated decision-making in the EU Member States: The right to explanation and other “suitable safeguards” in the national legislations. *Computer Law & Security Review*, 35(5), 105327.
<https://doi.org/https://doi.org/10.1016/j.clsr.2019.05.002>
- Mangala, D., & Kumari, P. (2017). Auditors’ perceptions of the effectiveness of fraud prevention and detection methods. *Indian Journal of Corporate Governance*, 10(2), 118–142. <https://doi.org/10.1177/0974686217738683>
- Mantelero, A. (2014). The future of consumer data protection in the E.U. Re-thinking the “notice and consent” paradigm in the new era of predictive analytics. *Computer Law & Security Review*, 30(6), 643–660.
<https://doi.org/https://doi.org/10.1016/j.clsr.2014.09.004>
- Manyika, J., Chui, M., Miremadi, M., Bughin, J., George, K., Willmott, P., & Dewhurst, M. (2017). A future that works: AI, automation, employment, and productivity. *McKinsey Global Institute Research, Tech. Rep*, 60, 1–135.
- Martinez, I., Viles, E., & G. Olaizola, I. (2021). Data Science Methodologies: Current Challenges and Future Approaches. *Big Data Research*, 24, 100183.
<https://doi.org/https://doi.org/10.1016/j.bdr.2020.100183>
- Masum, M. Al, & Parker, L. D. (2020). Local implementation of global accounting reform: evidence from a developing country. *Qualitative Research in Accounting & Management*, 17(3), 373–404. <https://doi.org/10.1108/QRAM-10-2018-0073>
- Mehrotra, A. (2019). Artificial intelligence in financial services–need to blend automation with human touch. In *2019 International Conference on Automation, Computational and Technology Management (ICACTM)* (pp. 342–347). IEEE.
- Mertzanis, C. (2023). FinTech finance and social-environmental performance around the world. *Finance Research Letters*, 56, 104107.
- Midiwo, J. (2016). Influence of Human Resource Information Systems on the Performance in Kenyan Public Universities. Jomo Kenyatta University of Agriculture and Technology.
- Montagnani, M. L., Najjar, M.-C., & Davola, A. (2024). The EU Regulatory approach(es) to AI liability, and its Application to the financial services market. *Computer Law & Security Review*, 53, 105984.
<https://doi.org/https://doi.org/10.1016/j.clsr.2024.105984>
- Morais, S. E. de, & Khaled, H. (2017). Making PPPs Work for the Poor: PPPs at the African Development Bank. In J. Leitão, E. de M. Sarmiento, & J. Aleluia (Eds.), *The Emerald Handbook of Public–Private Partnerships in Developing and Emerging Economies* (pp. 247–265). Emerald Publishing Limited. <https://doi.org/10.1108/978-1-78714-493-420171009>
- Moschella, M., & Tsingou, E. (2013). Regulating finance after the crisis: Unveiling the different dynamics of the regulatory process. *Regulation & Governance*, 7(4), 407–416. <https://doi.org/https://doi.org/10.1111/rego.12032>

- Mukhopadhyay, A., Chatterjee, S., Bagchi, K. K., Kirs, P. J., & Shukla, G. K. (2019). Cyber Risk Assessment and Mitigation (CRAM) Framework Using Logit and Probit Models for Cyber Insurance. *Information Systems Frontiers*, 21(5), 997–1018. <https://doi.org/10.1007/s10796-017-9808-5>
- Nallakaruppan, M. K., Balusamy, B., Shri, M. L., Malathi, V., & Bhattacharyya, S. (2024). An Explainable AI framework for credit evaluation and analysis. *Applied Soft Computing*, 153, 111307. <https://doi.org/https://doi.org/10.1016/j.asoc.2024.111307>
- Narsimha, B., Raghavendran, C. V., Rajyalakshmi, P., Reddy, G. K., Bhargavi, M., & Naresh, P. (2022). Cyber defense in the age of artificial intelligence and machine learning for financial fraud detection application. *International Journal of Electrical and Electronics Research*, 10(2), 87–92.
- Nasution, R. A., Rusnandi, L. S. L., Qodariah, E., Arnita, D., & Windasari, N. A. (2018). The evaluation of digital readiness concept: existing models and future directions. *The Asian Journal of Technology Management*, 11(2), 94–117.
- Nawari, N. O., & Ravindran, S. (2019). Blockchain and Building Information Modeling (BIM): Review and Applications in Post-Disaster Recovery. *Buildings*. <https://doi.org/10.3390/buildings9060149>
- Nortje, M. A., & Grobbelaar, S. S. (2020). A framework for the implementation of artificial intelligence in business enterprises: A readiness model. In *2020 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)* (pp. 1–10). IEEE.
- Novelli, C., Taddeo, M., & Floridi, L. (2024). Accountability in artificial intelligence: What it is and how it works. *Ai & Society*, 39(4), 1871–1882.
- Nwokediegwu, Z. Q. S., Obaigbena, A., Majemite, M. T., Daraojimba, O. H., Oliha, J. S., & Dada, M. A. (2024). Review of innovative approaches in water infrastructure: Sustainable desalination and public-private partnerships.
- OECD. (2021). *AI in Business and Finance - OECD Business and Finance Outlook 2021* (OECD Business and Finance Outlook). OECD Publishing. <https://doi.org/10.1787/ba682899-en>
- OECD. (2023). *Generative Artificial Intelligence in Finance*.
- Olmo, B. T., Saiz, M. C., & Azofra, S. S. (2021). Sustainable banking, market power, and efficiency: Effects on banks' profitability and risk. *Sustainability (Switzerland)*, 13(3), 1–23. <https://doi.org/10.3390/su13031298>
- Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47(3). <https://doi.org/10.1177/0022427810365903>
- Premkumar, V., & Arivazhagan, R. (2025). A Study on Behavioral Disruption among the Banking Workforce due to Application of Emerging Technologies in Workplace. *Advances in Consumer Research*, 2(4).
- PwC. (2025). *The Indian Payments Handbook 2025-2030*.
- PwC. (2014). *The future shape of banking: Time for reformation of Banking and banks?*
- Rahman, M. J., & Ziru, A. (2023). Clients' digitalization, audit firms' digital expertise, and audit quality: evidence from China. *International Journal of*

Accounting & Information Management, 31(2), 221–246.

<https://doi.org/10.1108/IJAIM-08-2022-0170>

- Rahman, M. M., Elshamly, D. A., ur Rehman, S., Jameel, Z., & Hameed, R. (2023). Blockchain Technology And Its Impact On European Bank's Cyber Security And Data Integrity. *Journal of Namibian Studies : History Politics Culture*. Retrieved from <https://api.semanticscholar.org/CorpusID:261268224>
- Randall, M. H., & Zirkle, C. J. (2005). Information technology student-based certification in formal education settings: Who benefits and what is needed. *Journal of Information Technology Education: Research*, 4(1), 287–306.
- RBI. (2023). RESERVE BANK OF INDIA ANNUAL REPORT 2023-24.
- RBI. (2024). RESERVE BANK OF INDIA ANNUAL REPORT 2024-25.
- Rohit, B., Arun, S., Sushil, K., & Rajni, G. (2018). Evaluating factors of profitability for Indian banking sector: a panel regression. *Asian Journal of Accounting Research*, 3(2), 236–254. <https://doi.org/10.1108/AJAR-08-2018-0026>
- Rovira-Garcia, A., Juan, J. M., Sanz, J., & Gonzalez-Casado, G. (2015). A worldwide ionospheric model for fast precise point positioning. *IEEE Transactions on Geoscience and Remote Sensing*, 53(8), 4596–4604. <https://doi.org/10.1109/TGRS.2015.2402598>
- Roy, N.C., & Basu, S. (2021). Bank's battle against insider frauds ignitors and mitigators: an emerging nation experience. *Journal of Facilities Management*, 19(4), 437–457. <https://doi.org/10.1108/JFM-04-2020-0021>
- Roy, N.C., & Vishwanathan, T. (2018a). Impact of Technological Disruption on Workforce Challenges of Indian Banks -Identification , Assessment & Mitigation. Mumbai. Retrieved from <http://www.iibf.org.in/documents/Final-161118.pdf>
- Roy, N.C., & Vishwanathan, T. (2018b). Workforce challenges in Indian banking scenario - Journey from identification till mitigation. *Current Science*. <https://doi.org/10.18520/cs/v115/i4/739-747>
- Roy, N.C., & Viswanathan, T. (2020). Investment in Technology: Does It Proliferate the Profitability and Performance of the Indian Banks? In R. Biswas & M. Michaelides (Eds.), *Financial Issues in Emerging Economies: Special Issue Including Selected Papers from II International Conference on Economics and Finance, 2019, Bengaluru, India* (Vol. 36, pp. 19–44). Emerald Publishing Limited. <https://doi.org/10.1108/S0196-382120200000036002>
- Roy, N C, & Prabhakaran, S. (2023). Insider employee-led cyber fraud (IECF) in Indian banks: from identification to sustainable mitigation planning. *Behaviour & Information Technology*, 1–31. <https://doi.org/10.1080/0144929X.2023.2191748>
- Roy, Neha Chhabra. (2020). Investment in Technology: Does It Proliferate the Profitability and Performance of the Indian Banks? *Research in Finance*.
- Roy, Neha Chhabra. (2024). Sustainable Lending Strategies: A Framework for Enhancing Climate Resilience in Industrial Loan Portfolios. *Asia Europe Journal*.
- Roy, Neha Chhabra, & Prabhakaran, S. (2024). Insider employee-led cyber fraud (IECF) in Indian banks: from identification to sustainable mitigation planning. *Behaviour & Information Technology*, 43(5), 876–906. <https://doi.org/10.1080/0144929X.2023.2191748>

- Ryan, P., Crane, M., & Brennan, R. (2020). GDPR Compliance tools: best practice from RegTech. In *International Conference on Enterprise Information Systems* (pp. 905–929). Springer.
- Said, J., Bakri, H.H.M. and Karim, Z. A. (2015). Case study on integrity among Royal Malaysian Police (RMP): an ethical perspective”,. *Procedia Economics and Finance*, 28(1), 121–125.
- Santoso, W., Sitorus, P. M., Batunanggar, S., Krisanti, F. T., Anggadwita, G., & Alamsyah, A. (2021). Talent mapping: a strategic approach toward digitalization initiatives in the banking and financial technology (FinTech) industry in Indonesia. *Journal of Science and Technology Policy Management*, 12(3), 399–420.
- Sappri, M. M., Baharudin, A. S., & Raman, S. (2016). The moderating effect of user involvement and self-readiness and factors that influence information system net benefits among malaysian public sector employees. *International Journal of Applied Engineering Research*, 11(18), 9659–9673.
- Sardana, V., & Singhanian, S. (2018). Digital technology in the realm of banking: A review of literature. *International Journal of Research in Finance and Management*, 1(2), 28–32.
- Sari, O., & Celik, S. (2021). Legal evaluation of the attacks caused by artificial intelligence-based lethal weapon systems within the context of Rome statute. *Computer Law & Security Review*, 42, 105564.
<https://doi.org/https://doi.org/10.1016/j.clsr.2021.105564>
- Schreiber, A., & Schreiber, I. (2024). Bridging knowledge gap: the contribution of employees’ awareness of AI cyber risks comprehensive program to reducing emerging AI digital threats. *Information & Computer Security*, 32(5), 613–635.
- Schwab, K., & Zahidi, S. (2020). World Economic Forum.(2020). The Global Competitiveness Report–How Countries Are Performing on the Road to Recovery.
- Schwab Klaus. (2021). *World Economic Forum – Annual Report 2020-2021*. *World Economic Forum – Annual Report 2020-2021* (Vol. 3). Retrieved from <http://dx.doi.org/10.1016/j.bpj.2015.06.056%0Ahttps://academic.oup.com/bioinformatics/article-abstract/34/13/2201/4852827%0Ainternal-pdf://semisupervised-3254828305/semisupervised.ppt%0Ahttp://dx.doi.org/10.1016/j.str.2013.02.005%0Ahttp://dx.doi.org/10.10>
- Serrado, J., Pereira, R. F., Mira da Silva, M., & Scalabrin Bianchi, I. (2020). Information security frameworks for assisting GDPR compliance in banking industry. *Digital Policy, Regulation and Governance*, 22(3), 227–244.
<https://doi.org/10.1108/DPRG-02-2020-0019>
- Seyum, A. A., Wang, S., Zhang, N., & Wang, L. (2025). Fit for the future: Examining the impact of task-technology fit on bank employee intentions to use FinTech. *South African Journal of Economic and Management Sciences*, 28(1), 6034.
- Shen, T. (2024). Right to learn in the digital age: Challenges and protection in China. *Computer Law & Security Review*, 53, 105989.
<https://doi.org/https://doi.org/10.1016/j.clsr.2024.105989>
- Singh, M., Mehtre, B. M., & Sangeetha, S. (2022). User behavior based Insider Threat Detection using a Multi Fuzzy Classifier. *Multimedia Tools and Applications*.
<https://doi.org/10.1007/s11042-022-12173-y>

- Siregar, S. V., & Tenoyo, B. (2015). Fraud awareness survey of private sector in Indonesia. *Journal of Financial Crime*, 22(3), 329–346. <https://doi.org/10.1108/JFC-03-2014-0016>
- Sivapragasam, N., Agüero, A., & de Silva, H. (2011). The potential of mobile remittances for the bottom of the pyramid: findings from emerging Asia. *Info*, 13(3), 91–109. <https://doi.org/10.1108/14636691111131475>
- Stewart, H., & Jürjens, J. (2018a). Data security and consumer trust in FinTech innovation in Germany. *Information & Computer Security*, 26(1), 109–128. <https://doi.org/10.1108/ICS-06-2017-0039>
- Stewart, H., & Jürjens, J. (2018b). Data security and consumer trust in FinTech innovation in Germany. *Information and Computer Security*, 26(1), 109–128. <https://doi.org/10.1108/ICS-06-2017-0039>
- Stone, R., Cooper, S., & Cant, R. (2013). The value of peer learning in undergraduate nursing education: a systematic review. *International Scholarly Research Notices*, 2013(1), 930901.
- Subramanian, Y. R., Riya, R., & Rajendran, R. (2024). Revolutionizing Workforce Education: A Conceptual Framework for AI-Driven Skilling, Upskilling, and Reskilling. In *Integrating Generative AI in Education to Achieve Sustainable Development Goals* (pp. 282–299). IGI Global.
- Sunrise, W. J., & Elizabeth, D. (2019). Governance of artificial intelligence and personal health information. *Digital Policy, Regulation and Governance*, 21(3), 280–290. <https://doi.org/10.1108/DPRG-08-2018-0048>
- Suresh Babu, S., & Dhakshina Moorthy, A. (2024). Application of artificial intelligence in adaptation of gamification in education: A literature review. *Computer Applications in Engineering Education*, 32(1), e22683.
- Taddeo, M., & Floridi, L. (2018). How AI can be a force for good. *Science*, 361(6404), 751–752.
- Tahar, A., Riyadh, H. A., Sofyani, H., & Purnomo, W. E. (2020). Perceived ease of use, perceived usefulness, perceived security and intention to use e-filing: The role of technology readiness. *The Journal of Asian Finance, Economics and Business*, 7(9), 537–547.
- Talero, E., & Gaudette, P. (1995). Harnessing information for development: A proposal for a World Bank group vision and strategy. *Information Technology for Development*, 6(3–4), 145–188.
- Truby, J., Brown, R., & Dahdal, A. (2020). Banking on AI: mandating a proactive approach to AI regulation in the financial sector. *Law and Financial Markets Review*, 14(2), 110–120.
- Tsai, C. H., & Su, P. C. (2021). The application of multi-server authentication scheme in internet banking transaction environments. *Information Systems and E-Business Management*, 19(1), 77–105. <https://doi.org/10.1007/s10257-020-00481-5>
- Tsingou, E. (2018). New governors on the block: The rise of anti-money laundering professionals. *Crime, Law and Social Change*, 69(2), 191–205.
- Türk Kurtça, T., & Demirci, İ. (2022). Psychopathy, impulsivity, and internet trolling: role of aggressive humour. *Behaviour & Information Technology*, 1–12. <https://doi.org/10.1080/0144929X.2022.2133635>

- Udayakumar, R., Joshi, A., Boomiga, S. S., & Sugumar, R. (2023). Deep fraud Net: A deep learning approach for cyber security and financial fraud detection and classification. *Journal of Internet Services and Information Security*, 13(3), 138–157.
- Uddin, M. H., Mollah, S., & Ali, M. H. (2020). Does cyber tech spending matter for bank stability? *International Review of Financial Analysis*, 72, 101587. <https://doi.org/https://doi.org/10.1016/j.irfa.2020.101587>
- Vajjhala, G. V., & Venu Gopal Rao, K. S. (2021). Insider versus outsider – who is better? The case of Zyne furnishings. *Emerald Emerging Markets Case Studies*, 11(4), 1–19. <https://doi.org/10.1108/EEMCS-06-2020-0184>
- van Daalen, O. L. (2023). The right to encryption: Privacy as preventing unlawful access. *Computer Law & Security Review*, 49, 105804. <https://doi.org/https://doi.org/10.1016/j.clsr.2023.105804>
- Vandezande, N. (2024). Cybersecurity in the EU: How the NIS2-directive stacks up against its predecessor. *Computer Law & Security Review*, 52, 105890. <https://doi.org/https://doi.org/10.1016/j.clsr.2023.105890>
- Vasudevan, S. (2022). Are Banking Institution reluctant to realise their losses?—An Irish perspective. Dublin, National College of Ireland.
- Vellinga, P., Mills, E., Berz, G., Bouwer, L., Huq, S., Kozak, L., ... Benson, C. (2001). Insurance and other financial services. *Climate Change*, (January), 417–450.
- Venkatesh, V., Thong, J. Y. L., & Xu, X. (2016). Unified theory of acceptance and use of technology: A synthesis and the road ahead. *Journal of the Association for Information Systems*, 17(5), 328–376.
- Villar, A. S., & Khan, N. (2021). Robotic process automation in banking industry: a case study on Deutsche Bank. *Journal of Banking and Financial Technology*, 5(1), 71–86.
- von Grafenstein, M., Jakobi, T., & Stevens, G. (2022). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods. *Computer Law & Security Review*, 46, 105722. <https://doi.org/https://doi.org/10.1016/j.clsr.2022.105722>
- Wai, H. Y. (2024). Cyber Security Training Practices And Employee Work Performance At Global Treasure Bank (Hnin Yu Wai, 2024). MERAL Portal.
- Walczuch, R., Lemmink, J., & Streukens, S. (2007). The effect of service employees' technology readiness on technology acceptance. *Information & Management*, 44(2), 206–215.
- Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). Data privacy and cybersecurity challenges in the digital transformation of the banking sector. *Computers and Security*, 147(May), 104051. <https://doi.org/10.1016/j.cose.2024.104051>
- Welch, J. (2023). Wells Fargo: a corporate recovery model to bank on. *Journal of Business Strategy*, 44(5), 247–256.
- Willcocks, L. P. (2024). Automation, digitalization and the future of work: A critical review. *Journal of Electronic Business & Digital Economics*, 3(2), 184–199.
- World Bank Group. (2022). FINANCE FOR AN EQUITABLE RECOVERY.

- World Economic Forum. (2023). Shaping the Future of Learning : The role of AI in Education 4.0 : Insight Report.
- Zhang, X., Du, Q., & Zhang, Z. (2022). A theory-driven machine learning system for financial disinformation detection. *Production and Operations Management*, 31(8), 3160–3179.
- Zharova, A., & Lloyd, I. (2018). An examination of the experience of cryptocurrency use in Russia. In search of better practice. *Computer Law & Security Review*, 34(6), 1300–1313. <https://doi.org/https://doi.org/10.1016/j.clsr.2018.09.004>
- Zinchenko, Y., Pervichko, E., & Akatova, E. (2014). Dynamics of the psychological features and clinical symptoms in mitral valve prolapse patients receiving long-term integrative psychotherapy for anxiety disorders. *Psychology in Russia: State of the Art*, 7(3), 66–79. <https://doi.org/10.11621/pir.2014.0306>

I. ANNEXURE-I

Survey questionnaire for assessing financial technology readiness in Indian banking: workforce adaptability, organisational transformation, and strategic implementation

The questionnaire is designed to measure the indicators influencing technology adoption, upskilling willingness, and workforce transformation in the banking sector. It follows a Likert-scale format (1 = Strongly Disagree, 5 = Strongly Agree) and covers various TAM, Extended TAM and UTAUT indicators.

PART A: DEMOGRAPHICS & BACKGROUND

ANNEXURE I.A Demographics and Background

Category	Item Statement
Gender	☐ Male ☐ Female ☐ Prefer not say
Age Group	☐ <25 ☐ 25–34 ☐ 35–44 ☐ 45–54 ☐ 55+
Designation	_____
Years in Role	☐ <1 ☐ 1–3 ☐ 4–6 ☐ 7–10 ☐ 10+
Department	_____
Additional Comments	_____

PART B: TECHNOLOGY READINESS & WORKFORCE ADAPTABILITY FROM ENABLER AND USER PERSPECTIVE

ANNEXURE I.B Technology Readiness & Workforce Adaptability From Enabler And User Perspective

Variable Cluster	Variable	Item Statement	1	2	3	4	5
Core Beliefs (TAM)	Perceived Usefulness (PU)	Using new banking technology improves my job performance.	☐	☐	☐	☐	☐
		Technology in banking helps me accomplish tasks more quickly.	☐	☐	☐	☐	☐
	Perceived Ease of Use (PEOU)	Learning to use new banking technologies is easy for me.	☐	☐	☐	☐	☐
		I find it easy to get technology to do what I want it to do.	☐	☐	☐	☐	☐
Personal Capabilities	Technology Self-Efficacy (TSE)	I am confident in solving tech-related problems at work.	☐	☐	☐	☐	☐
	Digital Literacy (DL)	I can use a wide range of digital tools and platforms.	☐	☐	☐	☐	☐
	Digital Readiness (DR)	I am ready to adopt new digital solutions in my day-to-day work.	☐	☐	☐	☐	☐
Risk & Trust Indicators	Perceived Risk (PR)	I am concerned about the risks associated with using digital banking technologies.	☐	☐	☐	☐	☐
	Trust in Technology (TT)	I trust that the digital systems used in my bank are reliable.	☐	☐	☐	☐	☐

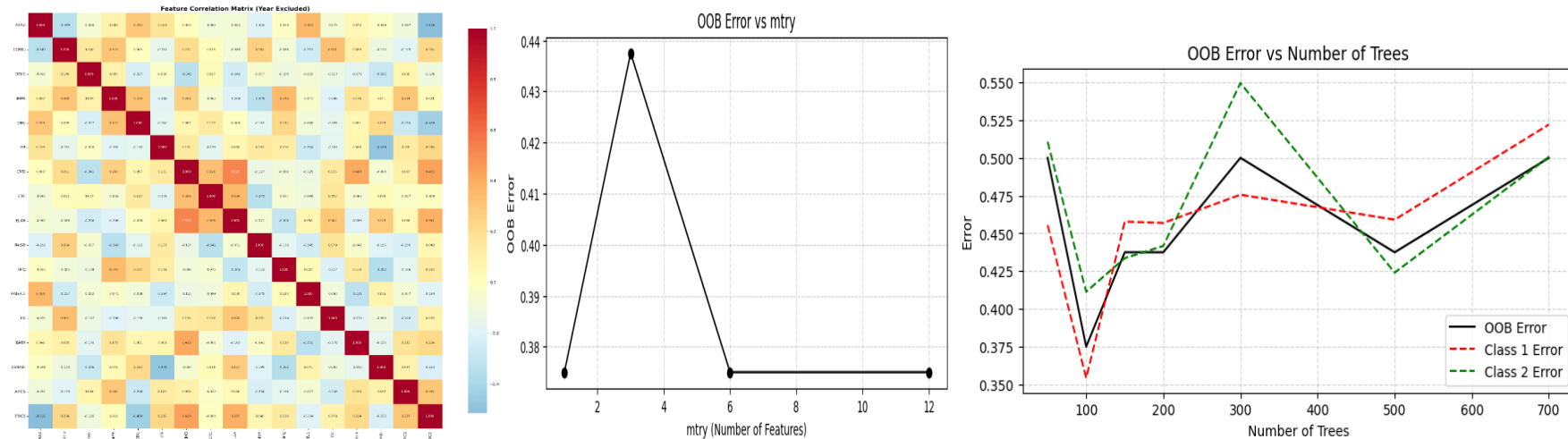
<i>Sociotechnical Alignment</i> <i>System Characteristics (TAM2)</i> <i>Compatibility/Image (TAM2)</i> <i>Facilitating Conditions (UTAUT)</i>	Cybersecurity Awareness (CSA)	I understand how to protect myself from digital threats at work.	☐	☐	☐	☐	☐
	Job Security Concerns (JSC)	I worry that automation may affect my job security.	☐	☐	☐	☐	☐
	Human-AI Collaboration (HAC)	I am comfortable collaborating with AI tools to complete tasks.	☐	☐	☐	☐	☐
	System Quality (SQ)	The banking systems I use are reliable and consistent.	☐	☐	☐	☐	☐
		System interfaces are user-friendly and well-designed.	☐	☐	☐	☐	☐
	Human-AI Collaboration (HAC)	The AI tools are compatible with my work style and preferences.	☐	☐	☐	☐	☐
	Facilitating Conditions (FC)	My bank provides the necessary support for using digital tools.	☐	☐	☐	☐	☐
	Employee Reskilling Investment (ERI)	The bank invests in upskilling employees to adapt to new technologies.	☐	☐	☐	☐	☐
	AI Infrastructure Readiness (AIR)	The bank's infrastructure supports advanced digital solutions like AI.	☐	☐	☐	☐	☐
	Regulatory Alignment (RAI)	The bank's tech adoption is well-aligned with regulatory standards.	☐	☐	☐	☐	☐
	Cybersecurity Investment (CSI)	The bank invests sufficiently in cybersecurity infrastructure.	☐	☐	☐	☐	☐

PART C: STRATEGIES IMPLEMENTED BY BANKS & EMPLOYEES

ANNEXURE I.C Strategies Implemented by Banks & Employees

Strategy domains	Question	1	2	3	4	5
Strategies implemented by banks	My bank provides AI training and data analytics programs for employees.	☐	☐	☐	☐	☐
	My bank has adopted AI-based regulatory technology for compliance and governance.	☐	☐	☐	☐	☐
	My bank has invested in AI-driven fraud detection and cybersecurity solutions.	☐	☐	☐	☐	☐
	My bank is replacing legacy systems with AI-powered banking infrastructure.	☐	☐	☐	☐	☐
	My bank encourages AI-human collaboration rather than full automation.	☐	☐	☐	☐	☐
Strategies implemented by employees	My bank has developed specialised AI-based DeFi risk assessment models.	☐	☐	☐	☐	☐
	I have pursued AI, FinTech, or blockchain certifications.	☐	☐	☐	☐	☐
	My bank encourages AI-related peer mentoring programs.	☐	☐	☐	☐	☐
	I have used interactive AI learning platforms for skill development.	☐	☐	☐	☐	☐
	I have participated in FinTech hackathons or AI-driven innovation challenges.	☐	☐	☐	☐	☐
	I have undergone AI ethics and cybersecurity compliance training.	☐	☐	☐	☐	☐

II. ANNEXURE-II - AXIS BANK SUMMARY (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



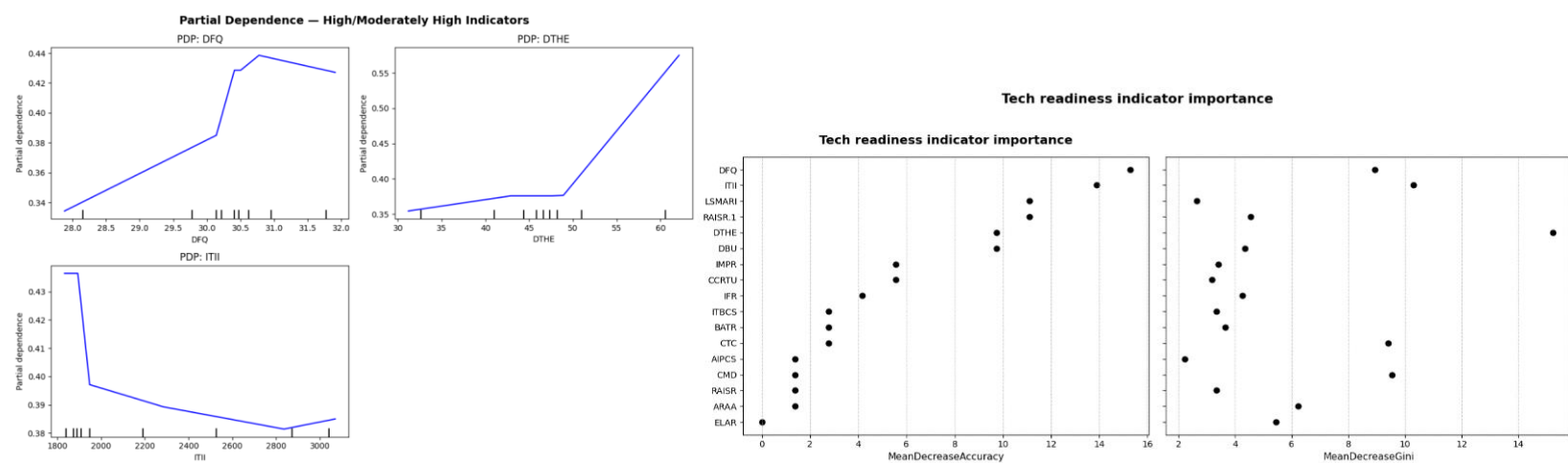
ANNEXURE II.A Axis Bank-Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE II.B Axis Bank-Random Forest OOB error versus number of trees, 2020 Q1 to 2025

ANNEXURE II.C Random Forest-based prioritisation of indicators for Axis Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
DFQ	0.157	0.088	15.278	8.943	High	High	High
ITII	0.143	0.101	13.889	10.294	High	High	High
LSMARI	-0.114	0.026	11.111	2.64	High	Low	Moderate
RAISR.1	0.114	0.045	11.111	4.546	High	Low	Moderate
DTHE	0.1	0.149	9.722	15.22	High	High	High
DBU	0.1	0.043	9.722	4.341	High	Low	Moderate
IMPR	-0.057	0.033	5.556	3.403	Low	Low	Low
CCRTU	0.057	0.031	5.556	3.178	Low	Low	Low

IFR	0.043	0.042	4.167	4.255	Low	Low	Low
ITBCS	-0.029	0.033	2.778	3.347	Low	Low	Low
BATR	0.029	0.036	2.778	3.666	Low	Low	Low
CTC	0.029	0.092	2.778	9.399	Low	High	Moderate
ARAA	-0.014	0.061	1.389	6.234	Low	Moderate	Moderately Low
CMD	-0.014	0.094	1.389	9.536	Low	High	Moderate
RAISR	-0.014	0.033	1.389	3.347	Low	Low	Low
AIPCS	0.014	0.022	1.389	2.213	Low	Low	Low
ELAR	0	0.053	0	5.438	Low	Low	Low

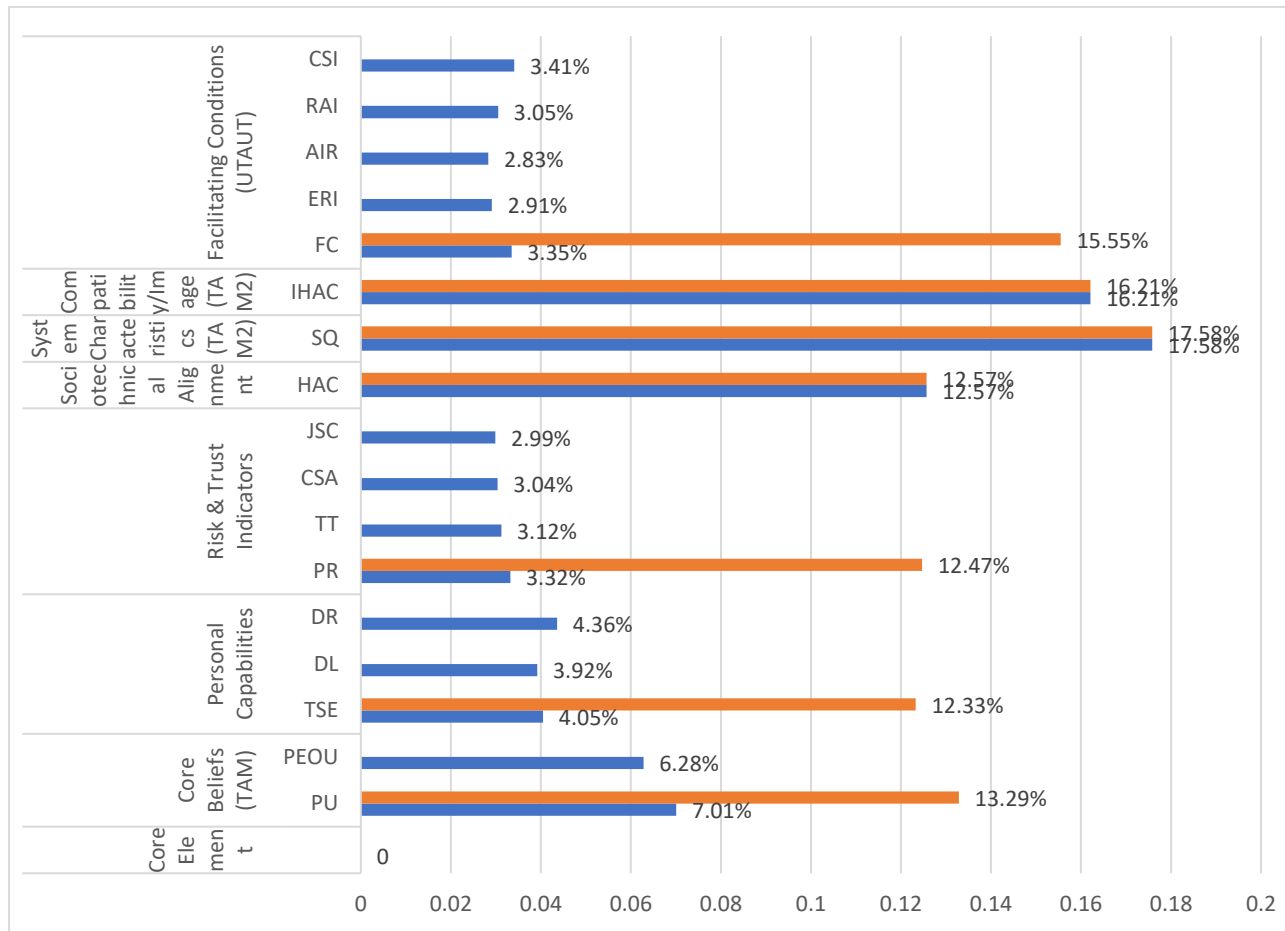


ANNEXURE II.D Axis Bank-Partial dependence of DfQ, DTHE, and ITII for Axis Bank, 2020 Q1 to 2025 Q3

ANNEXURE II.E Axis Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini, 2020 Q1 to 2025 Q3

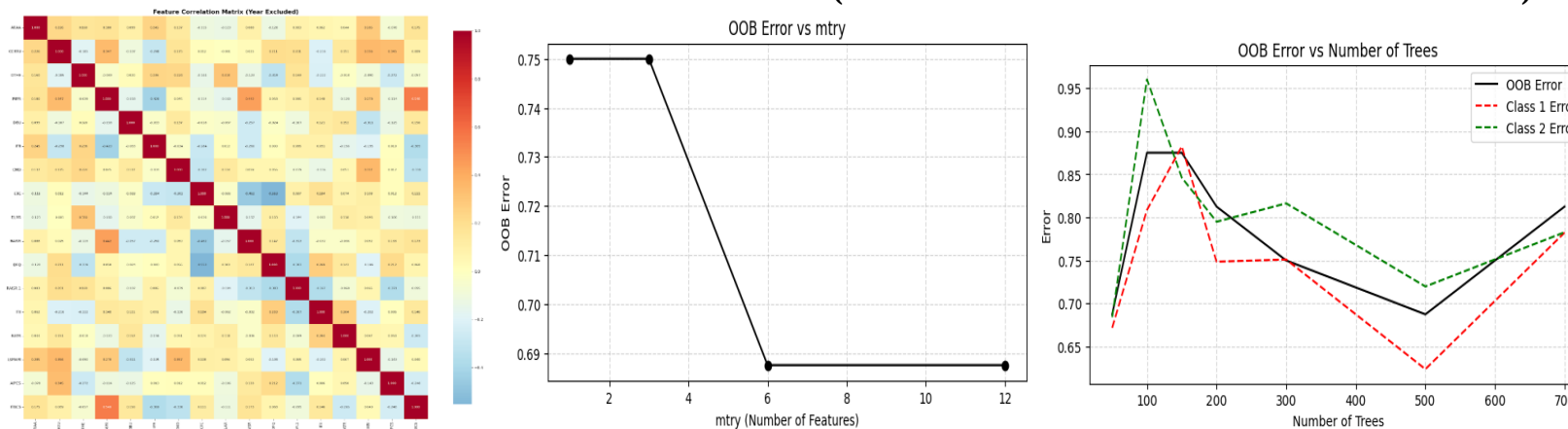
ANNEXURE II.F Axis Bank – Variables Severity Analysis and Ranking

Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*I R	Normalised Impact	Normalised Impact		Weighted average		Level of sevriy
Core Beliefs (TAM)	PU	1	1	3	1	21	121	4.033	0.063	0.252	0.063	7.01%				H
	PEOU	0	1	4	17	8	122	4.067	0.063	0.254	0.063	6.28%	13.29 %	6.65%	LI	L
	TSE	0	1	9	11	9	118	3.933	0.042	0.164	0.041	4.05%				L
Personal Capabilities	DL	2	1	4	17	6	114	3.8	0.042	0.158	0.039	3.92%				L
	DR	1	1	3	10	15	127	4.233	0.042	0.176	0.044	4.36%	12.33 %	4.11%	LI	H
	PR	1	0	4	9	16	129	4.3	0.031	0.134	0.033	3.32%				H
Risk & Trust Indicators	TT	0	2	3	12	12	121	4.033	0.031	0.126	0.031	3.12%				M
	CSA	1	2	5	12	10	118	3.933	0.031	0.123	0.031	3.04%				L
	JSC	1	3	6	9	11	116	3.867	0.031	0.121	0.03	2.99%	12.47 %	3.12%	LI	L
Sociotechnical Alignment	HAC	1	2	4	10	13	122	4.067	0.125	0.508	0.127	12.57%	12.57 %	12.57%	LI	M
System Characteristics (TAM2)	SQ	0	1	2	15	12	128	4.267	0.167	0.711	0.177	17.58%	17.58 %	17.58%	HI	M
Compatibility/Image (TAM2)	IHAC	1	1	7	11	10	118	3.933	0.167	0.656	0.163	16.21%	16.21 %	16.21%	HI	M
Facilitating Conditions (UTAUT)	FC	1	0	5	14	10	122	4.067	0.033	0.136	0.034	3.35%				H
	ERI	4	3	4	11	8	106	3.533	0.033	0.118	0.029	2.91%				L
	AIR	4	3	8	6	9	103	3.433	0.033	0.114	0.029	2.83%				L
	RAI	2	2	8	9	9	111	3.7	0.033	0.123	0.031	3.05%				L
	CSI	2	0	5	8	15	124	4.133	0.033	0.138	0.034	3.41%	15.55 %	3.11%	HI	H



ANNEXURE II.G Axis Bank – Indicators Severity Analysis comparative plot

III. ANNEXURE-III - BANK OF BARODA (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



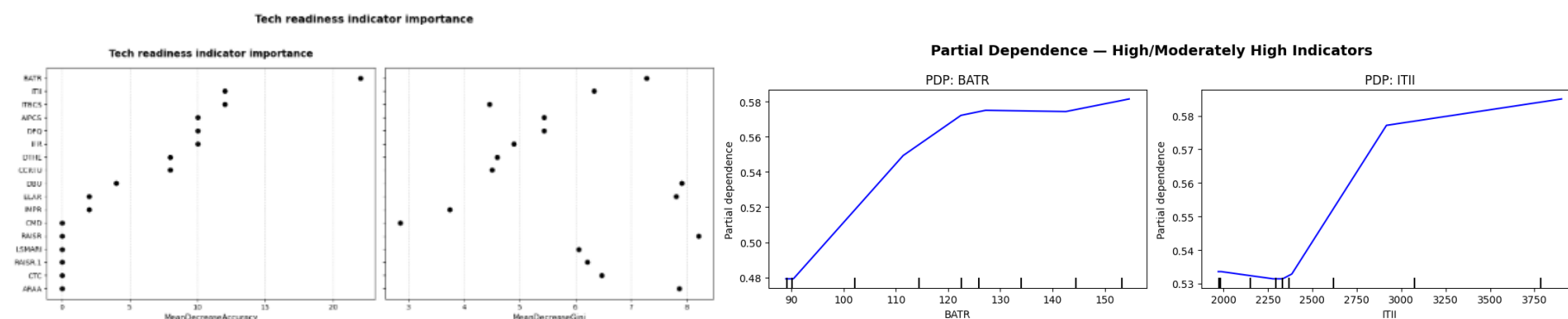
ANNEXURE III.A Bank of Baroda – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE III.B Bank of Baroda – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE III.C Bank of Baroda – Random Forest-based prioritisation of indicators for Bank of Baroda with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	-0.071429	0.053591	10	5.433635	High	Low	Moderate
ARAA	0	0.077467	0	7.854367	Low	High	Moderate
BATR	-0.157143	0.071732	22	7.272946	High	High	High
CCRTU	-0.057143	0.044341	8	4.495758	High	Low	Moderate
CMD	0	0.028127	0	2.85185	Low	Low	Low
CTC	0	0.063798	0	6.468504	Low	Moderate	Moderately Low
DBU	-0.028571	0.077953	4	7.903647	Low	High	Moderate
DFQ	-0.071429	0.053549	10	5.429315	High	Low	Moderate
DTHE	-0.057143	0.045279	8	4.590821	High	Low	Moderate
ELAR	-0.014286	0.076982	2	7.805223	Low	High	Moderate

IFR	0.071429	0.048249	10	4.891974	High	Low	Moderate
IMPR	-0.014286	0.036872	2	3.738454	Low	Low	Low
ITBCS	-0.085714	0.043956	12	4.456748	High	Low	Moderate
ITII	-0.085714	0.062457	12	6.332482	High	Moderate	Moderately High
LSMARI	0	0.059735	0	6.056582	Low	Moderate	Moderately Low
RAISR	0	0.080918	0	8.204243	Low	High	Moderate
RAISR.1	0	0.061283	0	6.21345	Low	Moderate	Moderately Low



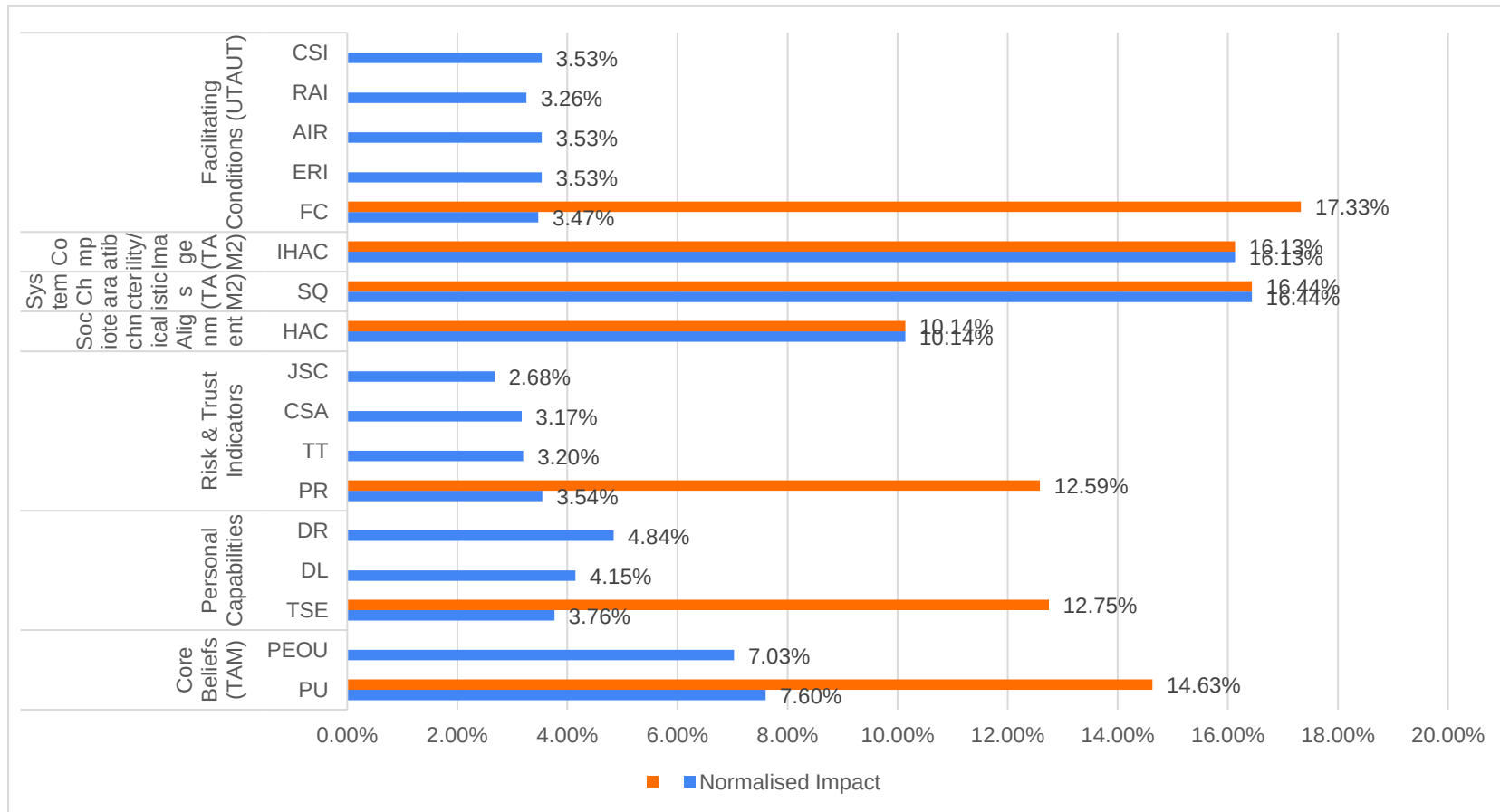
ANNEXURE III.D Bank of Baroda – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Bank of Baroda, 2020 Q1 to 2025 Q3

ANNEXURE III.E Bank of Baroda - Partial dependence of BATR and ITII, 2020 Q1 to 2025 Q3

ANNEXURE III.F Bank of Baroda – Variables Severity Analysis and Ranking

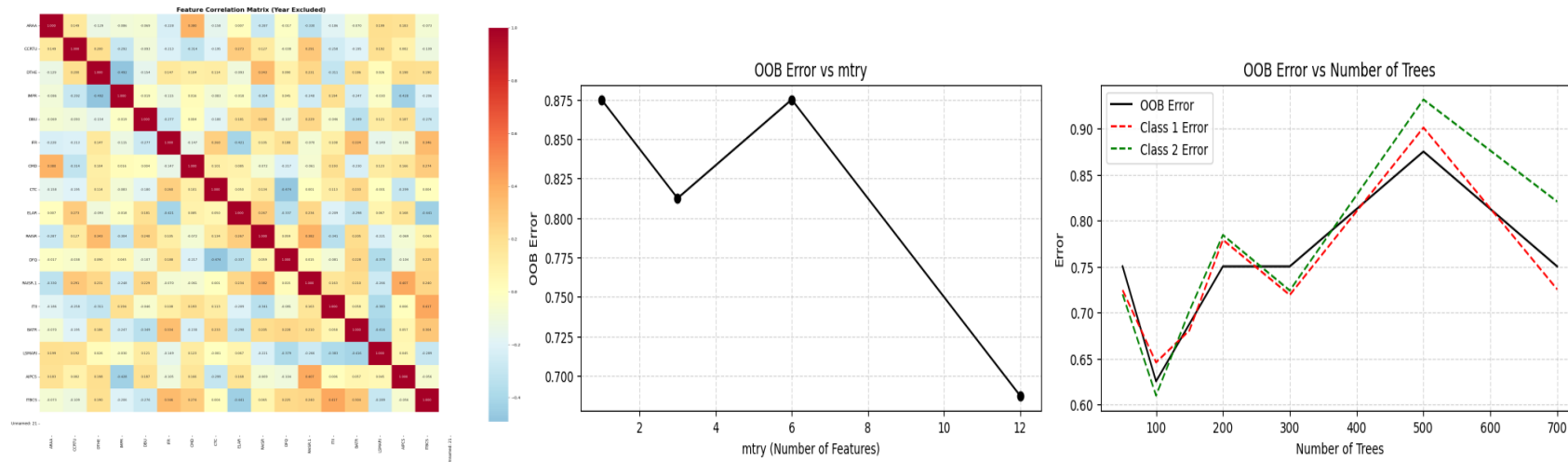
Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*I R	Normalised Impact	Normalised Impact			Weighted average		Level of sevtrity
Core Beliefs (TAM)	PU	0.00	0.00	0.00	18.00	12.00	132.00	0.77	0.06	0.05	0.08	7.60%	14.63%	7.32%	HI	H	
	PEOU	0.00	0.00	8.00	12.00	10.00	122.00	0.71	0.06	0.04	0.07	7.03%				L	
Personal Capabilities	TSE	0.00	4.00	17.00	6.00	3.00	98.00	0.57	0.04	0.02	0.04	3.76%	12.75%	4.25%	LI	L	

Risk & Trust Indicators	DL	0.00	6.00	7.00	10.00	7.00	108.00	0.63	0.04	0.03	0.04	4.15%				L
	DR	0.00	0.00	4.00	16.00	10.00	126.00	0.73	0.04	0.03	0.05	4.84%				H
	PR	0.00	0.00	7.00	13.00	10.00	123.00	0.72	0.03	0.02	0.04	3.54%	12.59%	3.15%	LI	H
	TT	0.00	2.00	9.00	15.00	4.00	111.00	0.65	0.03	0.02	0.03	3.20%				H
	CSA	0.00	4.00	10.00	8.00	8.00	110.00	0.64	0.03	0.02	0.03	3.17%				H
Sociotechnical Alignment	JSC	3.00	6.00	12.00	3.00	6.00	93.00	0.54	0.03	0.02	0.03	2.68%				L
	HAC	3.00	9.00	8.00	7.00	3.00	88.00	0.51	0.13	0.06	0.10	10.14%	10.14%	10.14%	LI	M
System Characteristics (TAM2)	SQ	0.00	2.00	11.00	15.00	2.00	107.00	0.62	0.17	0.10	0.16	16.44%	16.44%	16.44%	HI	M
Compatibility/Image (TAM2)	IHAC	0.00	3.00	12.00	12.00	3.00	105.00	0.61	0.17	0.10	0.16	16.13%	16.13%	16.13%	HI	M
Facilitating Conditions (UTAUT)	FC	0.00	0.00	10.00	17.00	3.00	113.00	0.66	0.03	0.02	0.03	3.47%	17.33%	3.47%	HI	H
	ERI	1.00	0.00	11.00	9.00	9.00	115.00	0.67	0.03	0.02	0.04	3.53%				H
	AIR	0.00	6.00	5.00	7.00	12.00	115.00	0.67	0.03	0.02	0.04	3.53%				H
	RAI	0.00	7.00	7.00	9.00	7.00	106.00	0.62	0.03	0.02	0.03	3.26%				L
	CSI	0.00	2.00	9.00	11.00	8.00	115.00	0.67	0.03	0.02	0.04	3.53%				H



ANNEXURE III.G Bank of Baroda – Indicators Severity Analysis comparative plot

IV. ANNEXURE-IV BANK OF MAHARASHTRA (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



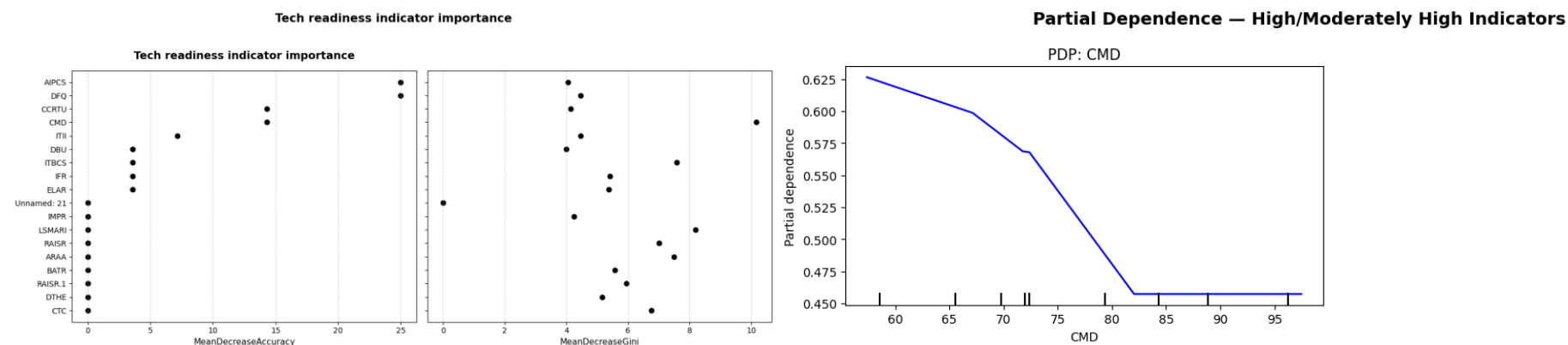
ANNEXURE IV.A Bank of Maharashtra – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE IV.B Bank of Maharashtra – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE IV.C Bank of Maharashtra – Random Forest-based prioritisation of indicators for Bank of Maharashtra with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	-0.1	0.0399	25	4.057412	High	Low	Moderate
ARAA	0	0.073568	0	7.481125	Low	High	Moderate
BATR	0	0.054759	0	5.568458	Low	Moderate	Moderately Low
CCRTU	-0.057143	0.040656	14.285714	4.13428	High	Low	Moderate
CMD	0.057143	0.099848	14.285714	10.153477	High	High	High
CTC	0	0.066438	0	6.756076	Low	High	Moderate
DBU	0.014286	0.039311	3.571429	3.997501	Low	Low	Low

DFQ	-0.1	0.043822	25	4.45629	High	Low	Moderate
DTHE	0	0.050797	0	5.165496	Low	Low	Low
ELAR	-0.014286	0.052851	3.571429	5.374427	Low	Low	Low
IFR	0.014286	0.053291	3.571429	5.419177	Low	Low	Low
IMPR	0	0.041689	0	4.23934	Low	Low	Low
ITBCS	0.014286	0.074546	3.571429	7.580538	Low	High	Moderate
ITII	0.028571	0.043941	7.142857	4.468384	High	Low	Moderate
LSMARI	0	0.080526	0	8.188618	Low	High	Moderate
RAISR	0	0.068871	0	7.00343	Low	High	Moderate
RAISR.1	0	0.05857	0	5.955971	Low	Moderate	Moderately Low

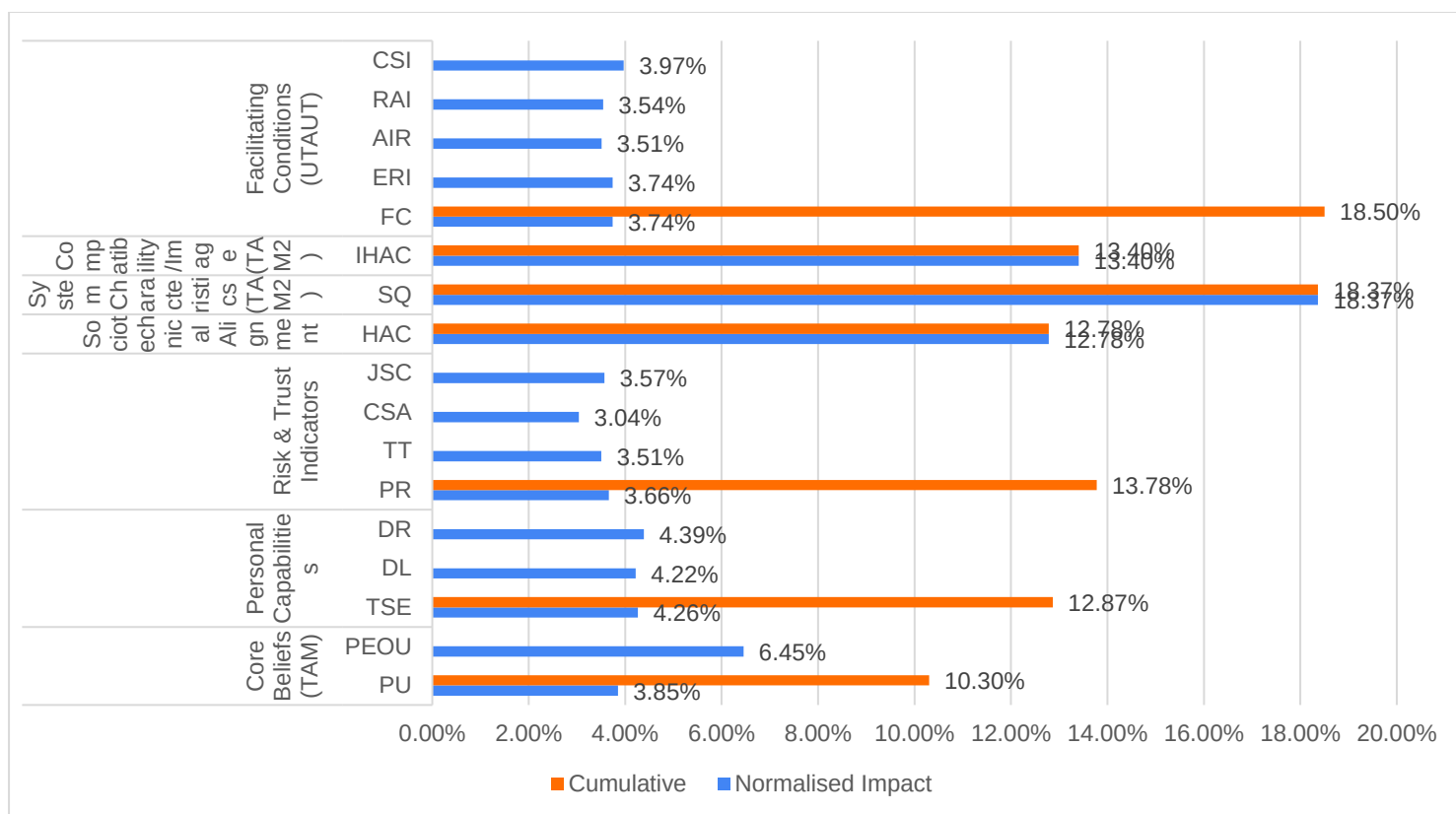


ANNEXURE IV.D Bank of Maharashtra – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Bank of Maharashtra, 2020 Q1 to 2025 Q3

ANNEXURE IV.E Bank of Maharashtra - Partial dependence of CMD, 2020 Q1 to 2025 Q3

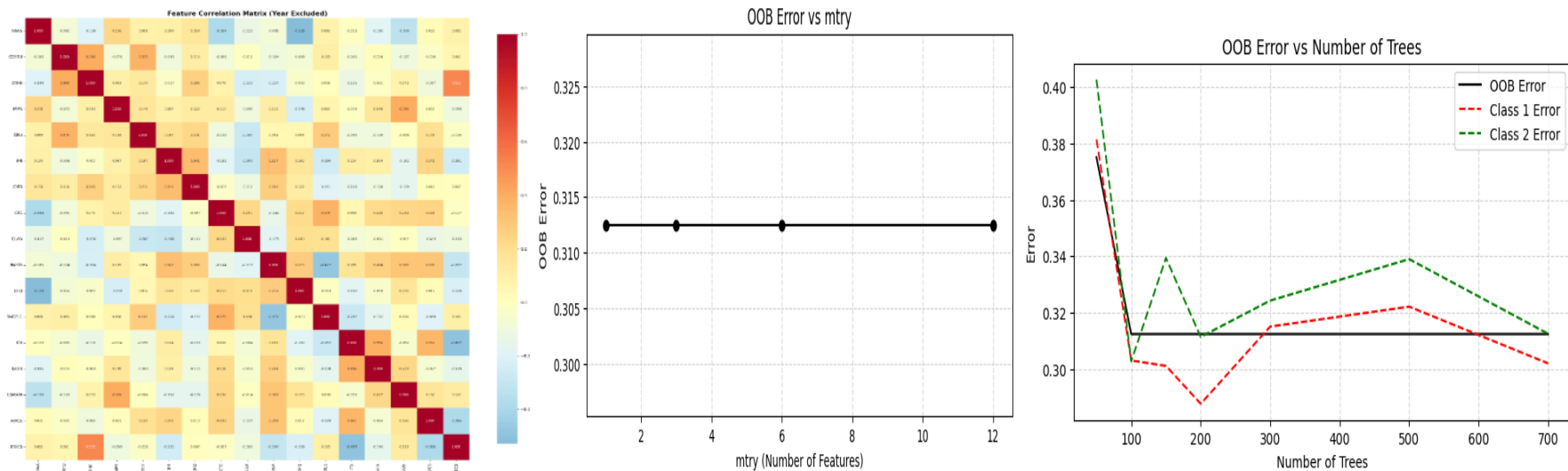
ANNEXURE IV.F Bank of Maharashtra – Variables Severity Analysis and Ranking

Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*I R	Normalised Impact	Normalised Impact	Weighted average		
Core Beliefs (TAM)	PU	7.00	15.00	7.00	1.00	0.00	62.00	31.00	0.06	1.94	3.85%	10.30%	5.15%	LI	L
	PEOU	0.00	2.00	14.00	12.00	2.00	104.00	52.00	0.06	3.25	6.45%				
Personal Capabilities	TSE	0.00	1.00	16.00	12.00	1.00	103.00	51.50	0.04	2.15	4.26%	12.87%	4.29%	LI	L
	DL	0.00	1.00	18.00	9.00	2.00	102.00	51.00	0.04	2.13	4.22%				
	DR	0.00	3.00	12.00	11.00	4.00	106.00	53.00	0.04	2.21	4.39%				
Risk & Trust Indicators	PR	1.00	3.00	4.00	11.00	11.00	118.00	59.00	0.03	1.84	3.66%	13.78%	3.44%	LI	H
	TT	2.00	4.00	6.00	5.00	13.00	113.00	56.50	0.03	1.77	3.51%				
	CSA	2.00	6.00	7.00	12.00	3.00	98.00	49.00	0.03	1.53	3.04%				
	JSC	2.00	4.00	4.00	7.00	13.00	115.00	57.50	0.03	1.80	3.57%				
Sociotechnical Alignment	HAC	0.00	1.00	16.00	12.00	1.00	103.00	51.50	0.13	6.44	12.78%	12.78%	12.78%	LI	M
System Characteristics (TAM2)	SQ	0.00	0.00	11.00	17.00	2.00	111.00	55.50	0.17	9.25	18.37%	18.37%	18.37%	HI	M
Compatibility/Image (TAM2)	IHAC	4.00	8.00	11.00	7.00	0.00	81.00	40.50	0.17	6.75	13.40%	13.40%	13.40%	HI	M
Facilitating Conditions (UTAUT)	FC	0.00	2.00	8.00	15.00	5.00	113.00	56.50	0.03	1.88	3.74%	18.50%	3.70%	HI	H
	ERI	0.00	0.00	10.00	17.00	3.00	113.00	56.50	0.03	1.88	3.74%				
	AIR	0.00	0.00	14.00	16.00	0.00	106.00	53.00	0.03	1.77	3.51%				
	RAI	0.00	1.00	14.00	12.00	3.00	107.00	53.50	0.03	1.78	3.54%				
	CSI	0.00	0.00	0.00	30.00	0.00	120.00	60.00	0.03	2.00	3.97%				



ANNEXURE IV.G Bank of Maharashtra – Indicators Severity Analysis comparative plot

V. ANNEXURE-V DCB BANK (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



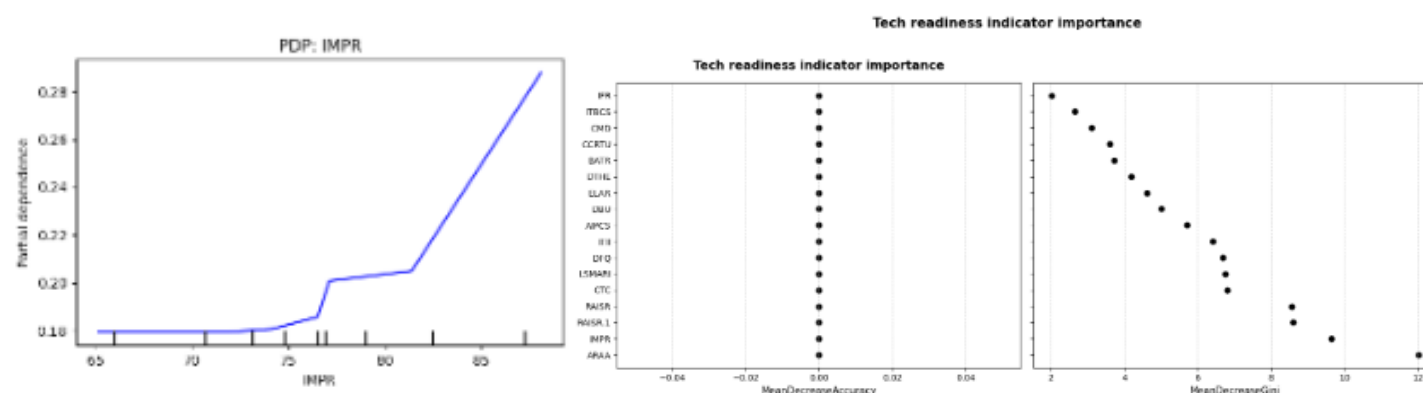
ANNEXURE V.A DCB Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE V.B DCB Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE V.C DCB Bank – Random Forest-based prioritisation of indicators for DCB Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	0	0.055399	0	5.696035	Low	Low	Low
ARAA	0	0.116791	0	12.00819	Low	High	Moderate
BATR	0	0.036205	0	3.72249	Low	Low	Low
CCRTU	0	0.035059	0	3.604666	Low	Low	Low
CMD	0	0.030259	0	3.111133	Low	Low	Low
CTC	0	0.066075	0	6.793641	Low	Moderate	Moderately Low
DBU	0	0.048639	0	5.000979	Low	Low	Low
DFQ	0	0.064966	0	6.679621	Low	Moderate	Moderately Low

DTHE	0	0.040703	0	4.185004	Low	Low	Low
ELAR	0	0.044811	0	4.607311	Low	Low	Low
IFR	0	0.019524	0	2.007407	Low	Low	Low
IMPR	0	0.093761	0	9.640313	Low	High	Moderate
ITBCS	0	0.025708	0	2.643188	Low	Low	Low
ITII	0	0.062241	0	6.399507	Low	Moderate	Moderately Low
LSMARI	0	0.065651	0	6.750114	Low	Moderate	Moderately Low
RAISR	0	0.083303	0	8.564976	Low	High	Moderate
RAISR.1	0	0.083502	0	8.585424	Low	High	Moderate



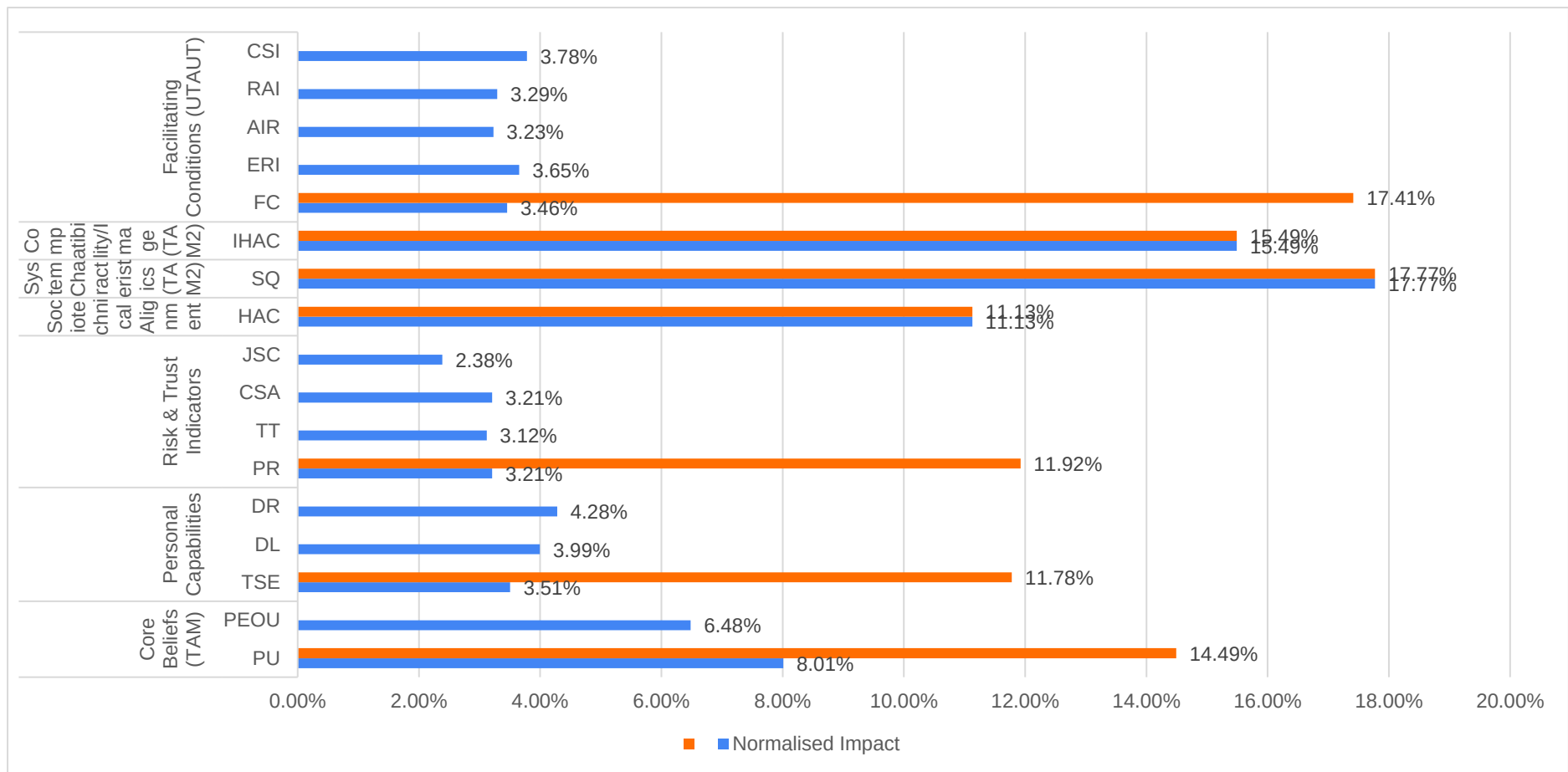
ANNEXURE V.D DCB Bank - Partial dependence of IMPR, 2020 Q1 to 2025 Q3

ANNEXURE V.E DCB Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Bank of Maharashtra, 2020 Q1 to 2025 Q3

ANNEXURE V.F DCB Bank – Variables Severity Analysis and Ranking

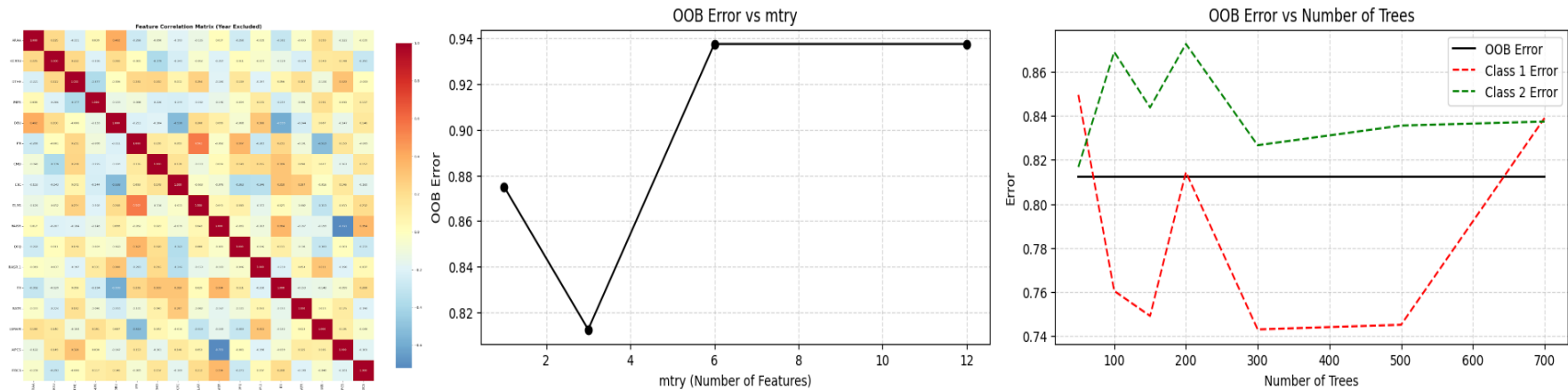
Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*IR	Normalised Impact	Normalised Impact	Weighted average	Level of sevtrity	
Core Beliefs (TAM)	PU	0	0	1	17	12	131	16.375	0.063	1.023	0.080	8.01%	14.49%	7.25%	H
	PEOU	1	6	5	12	6	106	13.250	0.063	0.828	0.065	6.48%			I
Personal Capabilities	TSE	6	4	11	6	3	86	10.750	0.042	0.448	0.035	3.51%	11.78%	3.93%	L
															I

Risk & Trust Indicators	DL	0	7	10	11	2	98	12.250	0.042	0.510	0.040	3.99%				H	H
	DR	0	3	15	6	6	105	13.125	0.042	0.547	0.043	4.28%				H	H
	PR	0	3	11	14	2	105	13.125	0.031	0.410	0.032	3.21%	11.92%	2.98%		L	
	TT	0	3	14	11	2	102	12.750	0.031	0.398	0.031	3.12%				I	H
	CSA	0	7	8	8	7	105	13.125	0.031	0.410	0.032	3.21%				H	H
Sociotechnical Alignment	JSC	7	5	13	3	2	78	9.750	0.031	0.305	0.024	2.38%				L	L
	HAC	2	8	10	7	3	91	11.375	0.125	1.422	0.111	11.13%	11.13%	11.13%		L	
	SQ	0	3	11	10	6	109	13.625	0.167	2.271	0.178	17.77%	17.77%	17.77%		I	M
System Characteristics (TAM2)	IHAC	2	6	12	5	5	95	11.875	0.167	1.979	0.155	15.49%	15.49%	15.49%		H	
Compatibility/Image (TAM2)	FC	0	3	13	9	5	106	13.250	0.033	0.442	0.035	3.46%	17.41%	3.48%		I	M
Facilitating Conditions (UTAUT)	ERI	0	3	10	9	8	112	14.000	0.033	0.467	0.037	3.65%				H	H
	AIR	0	4	16	7	3	99	12.375	0.033	0.413	0.032	3.23%				L	L
	RAI	1	6	11	5	7	101	12.625	0.033	0.421	0.033	3.29%				L	L
	CSI	0	1	9	13	7	116	14.500	0.033	0.483	0.038	3.78%				H	H



ANNEXURE V.G DCB Bank – Indicators Severity Analysis comparative plot

VI. ANNEXURE-VI HDFC BANK (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



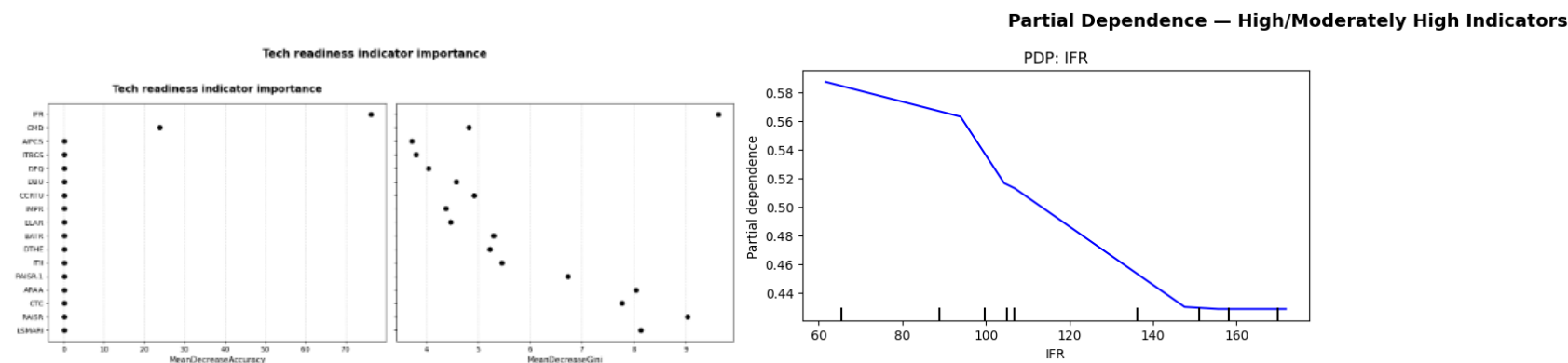
ANNEXURE VI.A HDFC Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE VI.B HDFC Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE VI.C HDFC Bank – Random Forest-based prioritisation of indicators for HDFC Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	0	0.036627	0	3.714528	Low	Low	Low
ARAA	0	0.079281	0	8.040371	Low	High	Moderate
BATR	0	0.052195	0	5.293348	Low	Low	Low
CCRTU	0	0.048474	0	4.915982	Low	Low	Low
CMD	-0.071429	0.047522	23.809524	4.819438	High	Low	Moderate
CTC	0	0.076588	0	7.767261	Low	High	Moderate
DBU	0	0.045104	0	4.574268	Low	Low	Low
DFQ	0	0.039853	0	4.041709	Low	Low	Low
DTHE	0	0.051523	0	5.225257	Low	Low	Low
ELAR	0	0.044028	0	4.465088	Low	Low	Low

IFR	-0.228571	0.0949	76.190476	9.624382	High	High	High
IMPR	0	0.043137	0	4.37478	Low	Low	Low
ITBCS	0	0.037464	0	3.799446	Low	Low	Low
ITII	0	0.053778	0	5.453883	Low	Low	Low
LSMARI	0	0.080165	0	8.129961	Low	High	Moderate
RAISR	0	0.089043	0	9.030355	Low	High	Moderate
RAISR.1	0	0.06636	0	6.729943	Low	Moderate	Moderately Low



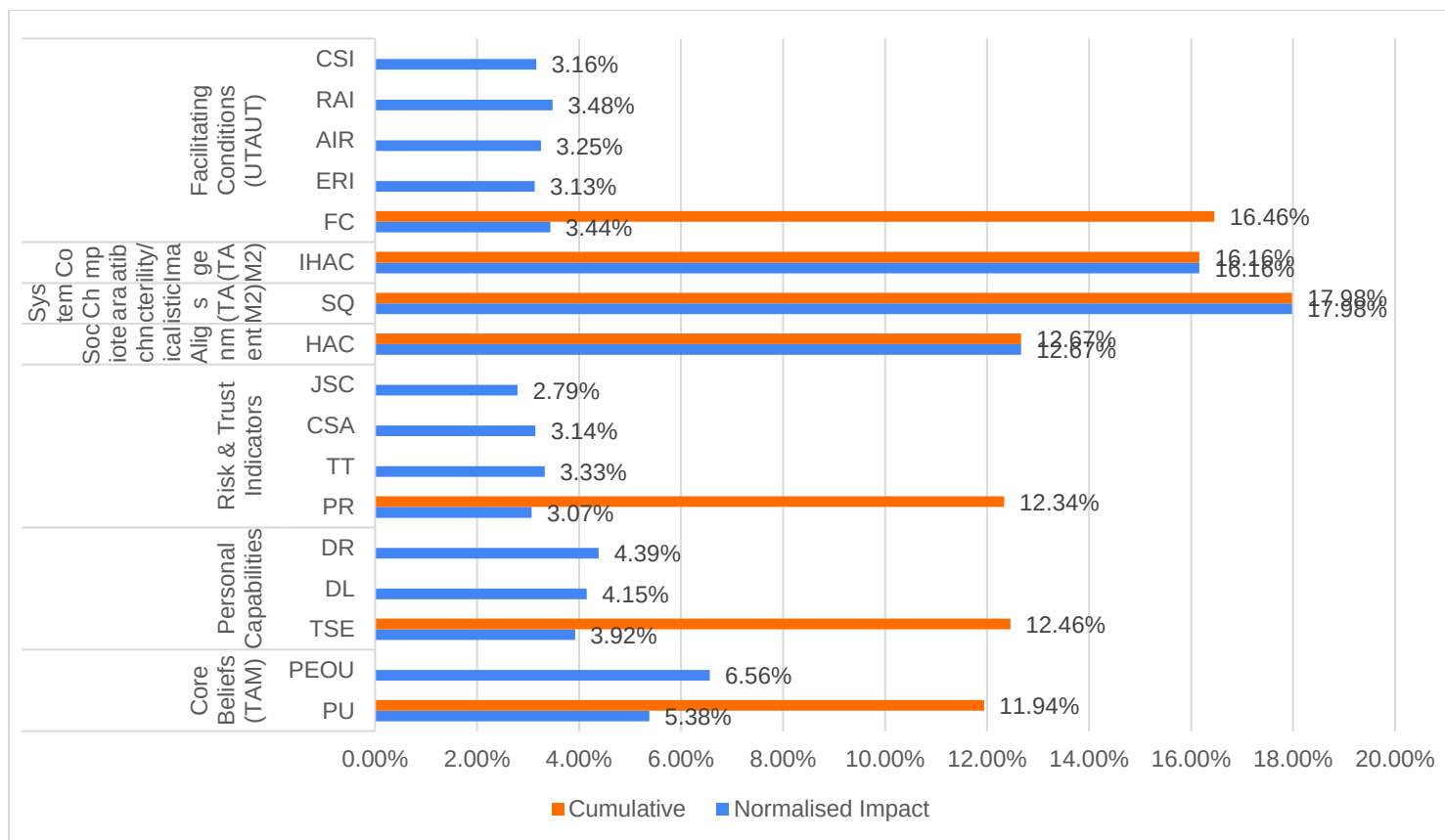
ANNEXURE VI.D HDFC Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for HDFC Bank, 2020 Q1 to 2025 Q3

ANNEXURE VI.E HDFC Bank - Partial dependence of IFR, 2020 Q1 to 2025 Q3

ANNEXURE VI.F HDFC Bank – Variables Severity Analysis and Ranking

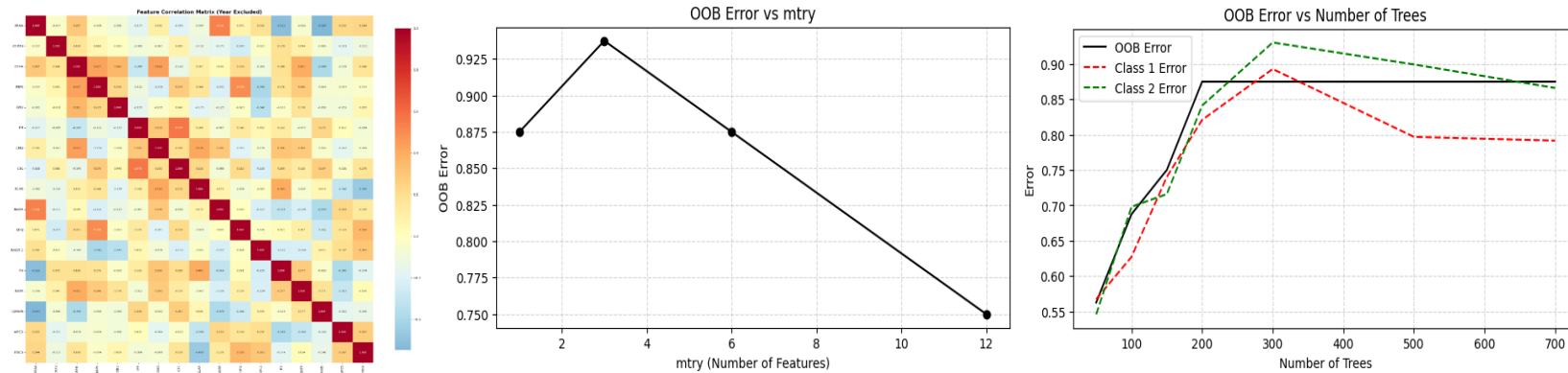
Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*I R	Normalised Impact	Normalised Impact		Weighted average		Level of sevtrity
Core Beliefs (TAM)	PU	0	2	1	7	23	150	4.55	0.063	0.284	0.069	6.9%	11.94%	5.97%	LI	L
	PEOU	0	0	3	9	21	150	4.55	0.063	0.284	0.069	6.9%				H
Personal	TSE	0	1	2	16	14	142	4.30	0.042	0.179	0.043	4.3%	12.46%	4.15%	LI	L

Capabilities	DL	0	2	1	15	15	142	4.30	0.042	0.179	0.043					L	
	DR	0	0	4	7	22	150	4.55	0.042	0.189	0.046					H	
Risk & Trust Indicators	PR	0	2	8	12	11	131	3.97	0.031	0.124	0.030	3.0%	12.34%	3.08%	LI	L	
	TT	0	0	6	9	18	144	4.36	0.031	0.136	0.033	3.3%					H
	CSA	0	1	2	15	15	143	4.33	0.031	0.135	0.033	3.3%					H
	JSC	4	9	6	3	11	107	3.24	0.031	0.101	0.025	2.5%					L
	HAC	2	2	5	15	9	126	3.82	0.125	0.477	0.116	11.6%	12.67%	12.67%	LI	M	
System Characteristics (TAM2)	SQ	2	0	3	16	12	135	4.09	0.167	0.682	0.165	16.5%	17.98%	17.98%	HI	M	
Compatibility/Image (TAM2)	IHAC	1	2	7	11	12	130	3.94	0.167	0.657	0.159	15.9%	15.92%	15.92%	HI	M	
Facilitating Conditions (UTAUT)	FC	1	0	5	12	15	139	4.21	0.033	0.140	0.034	3.4%	16.46%	3.29%	HI	H	
	ERI	0	1	13	3	16	133	4.03	0.033	0.134	0.033	3.3%					L
	AIR	0	3	8	7	15	133	4.03	0.033	0.134	0.033	3.3%					L
	RAI	0	2	5	9	17	140	4.24	0.033	0.141	0.034	3.4%					H
	CSI	0	2	6	5	20	142	4.30	0.033	0.143	0.035	3.5%					L



ANNEXURE VI.G HDFC Bank – Indicators Severity Analysis comparative plot

VII. ANNEXURE-VII INDIAN BANK (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



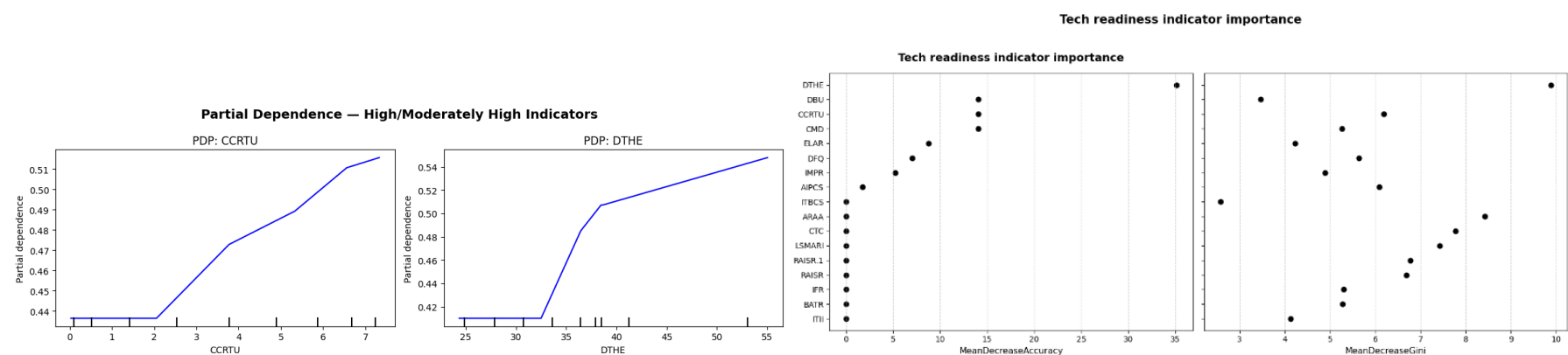
ANNEXURE VII.A Indian Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE VII.B Indian Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE VII.C Indian Bank – Random Forest-based prioritisation of indicators for Indian Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	-0.014286	0.059813	1.754386	6.091459	Low	Moderate	Moderately Low
ARAA	0	0.082761	0	8.428542	Low	High	Moderate
BATR	0	0.051773	0	5.272681	Low	Low	Low
CCRTU	-0.114286	0.06078	14.035088	6.189943	High	Moderate	Moderately High
CMD	-0.114286	0.051663	14.035088	5.26144	High	Low	Moderate
CTC	0	0.076314	0	7.771937	Low	High	Moderate
DBU	-0.114286	0.034002	14.035088	3.462792	High	Low	Moderate
DFQ	0.057143	0.055367	7.017544	5.63868	Moderate	Low	Moderately Low
DTHE	-0.285714	0.097042	35.087719	9.882883	High	High	High
ELAR	-0.071429	0.04146	8.77193	4.222336	High	Low	Moderate
IFR	0	0.052075	0	5.303438	Low	Low	Low

IMPR	0.042857	0.04796	5.263158	4.884305	Low	Low	Low
ITBCS	0	0.025301	0	2.576665	Low	Low	Low
ITII	0	0.040526	0	4.127247	Low	Low	Low
LSMARI	0	0.072892	0	7.423488	Low	High	Moderate
RAISR	0	0.06562	0	6.68289	Low	Moderate	Moderately Low
RAISR.1	0	0.066567	0	6.779274	Low	Moderate	Moderately Low



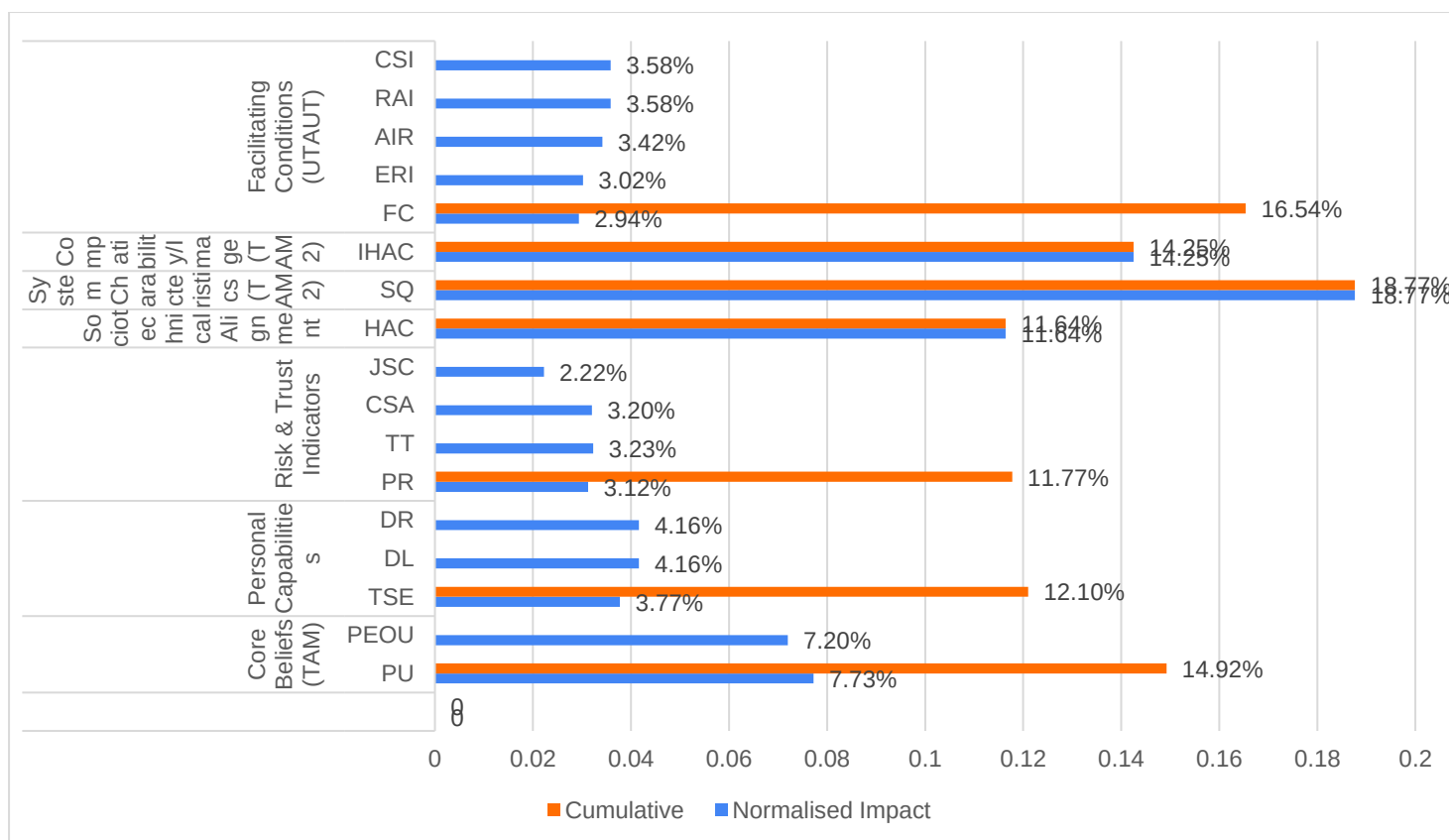
ANNEXURE VII.D Indian Bank - Partial dependence of DTHE and CCRTU, 2020 Q1 to 2025 Q3

ANNEXURE VII.E Indian Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Indian Bank, 2020 Q1 to 2025 Q3

ANNEXURE VII.F Indian Bank – Variables Severity Analysis and Ranking

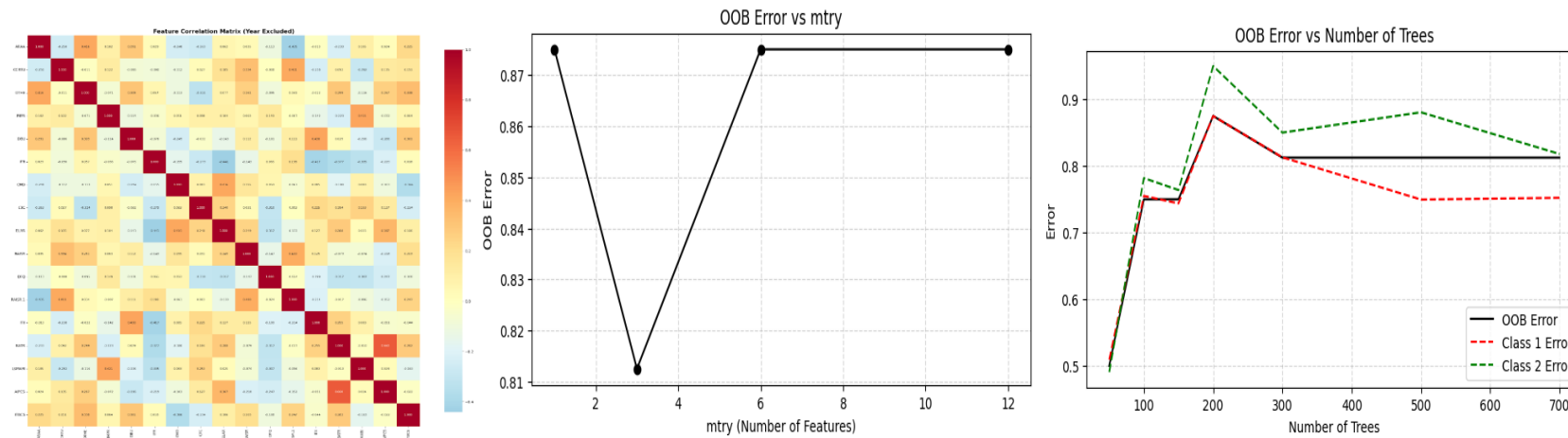
Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*I R	Normalised Impact	Normalised Impact		Weighted average		
Core Beliefs (TAM)	PU	0	0	0	4	26	146	24.33	0.063	1.521	0.077	7.73%	14.92%	7.46%	HI	H
	PEOU	0	0	0	14	16	136	22.67	0.063	1.417	0.072	7.20%				L
Personal Capabilities	TSE	0	2	9	9	8	107	17.83	0.042	0.743	0.038	3.77%	12.10%	4.03%	LI	L
	DL	0	3	4	15	8	118	19.67	0.042	0.819	0.042	4.16%				H
	DR	0	1	8	13	8	118	19.67	0.042	0.819	0.042	4.16%				H

<i>Risk & Trust Indicators</i>	PR	0	0	7	18	5	118	19.67	0.031	0.615	0.031	3.12%	11.77%	2.94%	LI	H
	TT	0	0	6	16	8	122	20.33	0.031	0.635	0.032	3.23%				H
	CSA	0	0	10	9	11	121	20.17	0.031	0.630	0.032	3.20%				H
	JSC	3	9	9	4	4	84	14.00	0.031	0.438	0.022	2.22%				L
<i>Sociotechnical Alignment System Characteristics (TAM2) Compatibility/Image (TAM2) Facilitating Conditions (UTAUT)</i>	HAC	2	2	10	6	10	110	18.33	0.125	2.292	0.116	11.64%	11.64%	11.64%	LI	M
	SQ	0	0	0	17	13	133	22.17	0.167	3.694	0.188	18.77%	18.77%	18.77%	HI	M
	IHAC	3	3	7	9	7	101	16.83	0.167	2.806	0.143	14.25%	14.25%	14.25%	HI	M
	FC	0	2	12	16	0	104	17.33	0.033	0.578	0.029	2.94%	16.54%	3.31%	HI	L
	ERI	0	2	13	11	4	107	17.83	0.033	0.594	0.030	3.02%				L
	AIR	0	2	7	9	12	121	20.17	0.033	0.672	0.034	3.42%				H
	RAI	1	1	4	8	16	127	21.17	0.033	0.706	0.036	3.58%				H
	CSI	0	0	2	19	9	127	21.17	0.033	0.706	0.036	3.58%				H



ANNEXURE VII.G Indian Bank – Indicators Severity Analysis comparative plot

VIII. ANNEXURE-VIII ICICI BANK (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



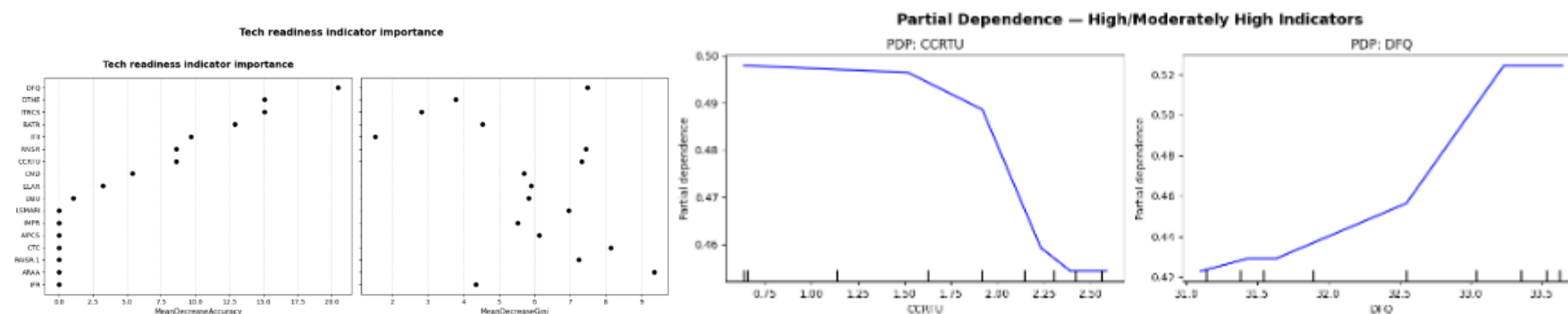
ANNEXURE VIII.A ICICI Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE VIII.B ICICI Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE VIII.C ICICI Bank – Random Forest-based prioritisation of indicators for ICICI Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	0	0.060034	0	6.122657	Low	Moderate	Moderately Low
ARAA	0	0.091699	0	9.352074	Low	High	Moderate
BATR	0.171429	0.044464	12.903226	4.534736	High	Low	Moderate
CCRTU	0.114286	0.071819	8.602151	7.324524	High	High	High
CMD	0.071429	0.055886	5.376344	5.699657	Low	Low	Low
CTC	0	0.079742	0	8.132623	Low	High	Moderate
DBU	0.014286	0.057225	1.075269	5.836221	Low	Low	Low
DFQ	0.271429	0.073281	20.430108	7.473646	High	High	High
DTHE	0.2	0.037134	15.053763	3.787155	High	Low	Moderate

ELAR	0.042857	0.057852	3.225806	5.900076	Low	Moderate	Moderately Low
IFR	0	0.042594	0	4.344027	Low	Low	Low
IMPR	0	0.054215	0	5.529151	Low	Low	Low
ITBCS	0.2	0.027615	15.053763	2.816346	High	Low	Moderate
ITII	0.128571	0.014855	9.677419	1.515032	High	Low	Moderate
LSMARI	0	0.068186	0	6.954038	Low	Moderate	Moderately Low
RAISR	0.114286	0.072985	8.602151	7.443513	High	High	High
RAISR.1	0	0.070936	0	7.234523	Low	High	Moderate



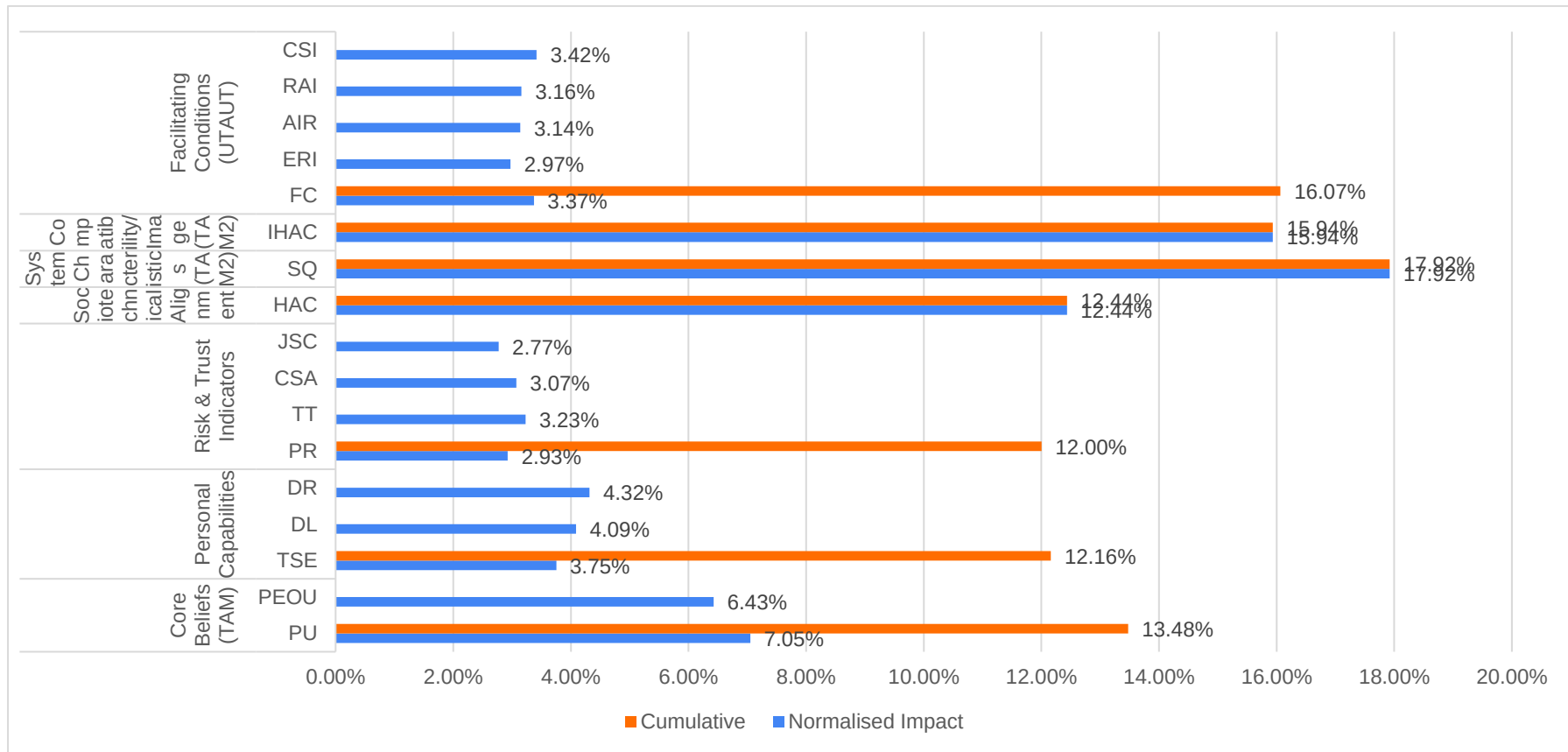
ANNEXURE VIII.D ICICI Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for ICICI Bank, 2020 Q1 to 2025 Q3

ANNEXURE VIII.E ICICI Bank - Partial dependence of DFQ and CCRTU, 2020 Q1 to 2025 Q3

ANNEXURE VIII.F ICICI Bank – Variables Severity Analysis and Ranking

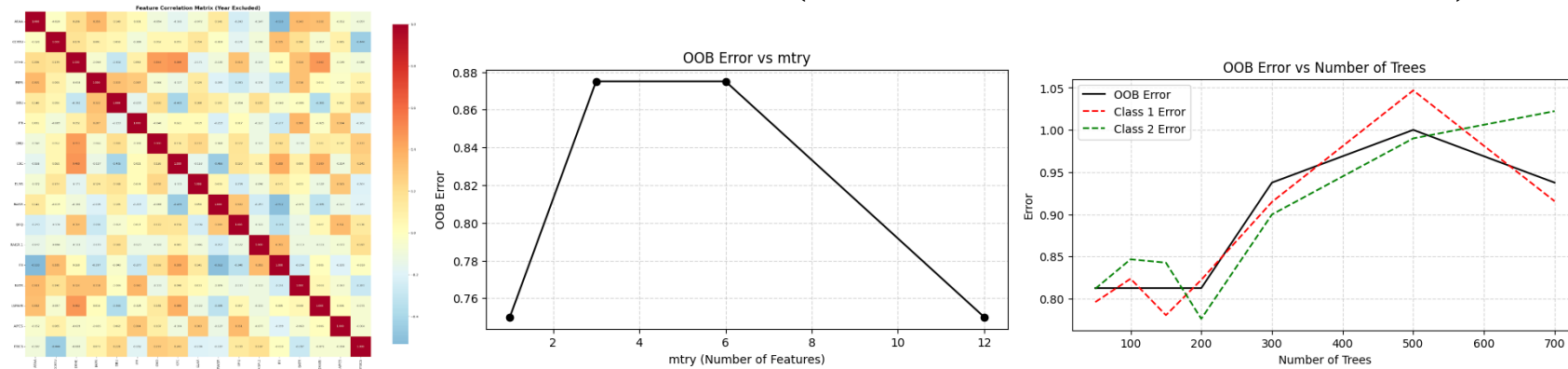
Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*IR	Normalised Impact	Normalised Impact	Weighted average	Level of sevtrity	
Core Beliefs (TAM)	PU	1	1	2	22	62	407	4.63	0.063	0.289	0.070	7.0%	13.48%	6.74%	LI
	PEOU	1	3	10	36	38	371	4.22	0.063	0.263	0.064	6.4%			L
Personal Capabilities	TSE	5	9	19	30	25	325	3.69	0.042	0.154	0.038	3.8%	12.16%	4.05%	LI

Risk & Trust Indicators	DL	4	3	13	35	33	354	4.02	0.042	0.168	0.041	4.1%					H
	DR	1	3	7	39	38	374	4.25	0.042	0.177	0.043	4.3%					H
	PR	3	8	16	29	31	338	3.84	0.031	0.120	0.029	2.9%	12.00%	3.00%		LI	L
	TT	2	0	7	40	38	373	4.24	0.031	0.132	0.032	3.2%					H
	CSA	3	6	12	31	36	355	4.03	0.031	0.126	0.031	3.1%					H
Sociotechnical Alignment	JSC	8	7	18	31	24	320	3.64	0.031	0.114	0.028	2.8%					L
	HAC	1	3	17	29	37	359	4.08	0.125	0.510	0.124	12.4%	12.44%	12.44%		LI	M
	SQ	0	3	4	35	46	388	4.41	0.167	0.735	0.179	17.9%	17.92%	17.92%		HI	M
Compatibility/Image (TAM2)	IHAC	0	10	16	33	29	345	3.92	0.167	0.653	0.159	15.9%	15.94%	15.94%		HI	M
Facilitating Conditions (UTAUT)	FC	1	3	14	34	36	365	4.15	0.033	0.138	0.034	3.4%	16.07%	3.21%		HI	H
	ERI	5	5	25	23	28	322	3.66	0.033	0.122	0.030	3.0%					L
	AIR	0	6	24	34	24	340	3.86	0.033	0.129	0.031	3.1%					L
	RAI	5	4	7	42	28	342	3.89	0.033	0.130	0.032	3.2%					L
	CSI	1	2	14	32	39	370	4.20	0.033	0.140	0.034	3.4%					H



ANNEXURE VIII.G ICICI Bank – Indicators Severity Analysis comparative plot

IX. ANNEXURE-IX IDFC FIRST BANK (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



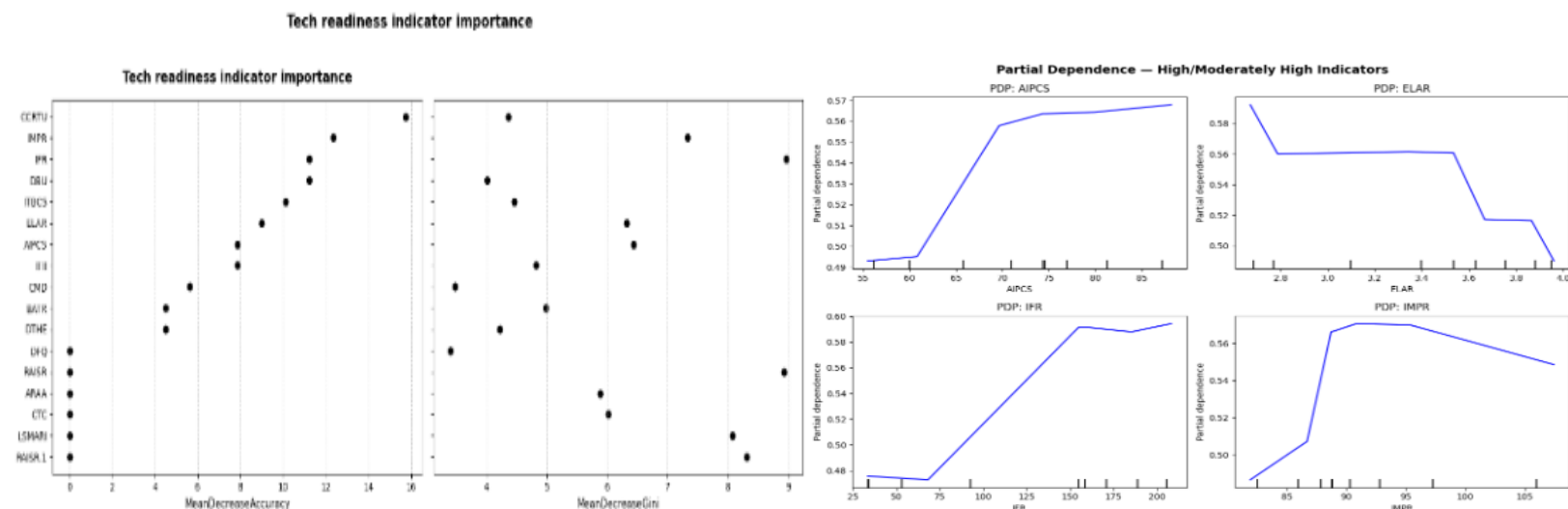
ANNEXURE IX.A IDFC Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE IX.B IDFC Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE IX.C IDFC Bank – Random Forest-based prioritisation of indicators for IDFC Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	0.1	0.063794	7.865169	6.434223	High	Moderate	Moderately High
ARAA	0	0.058355	0	5.885693	Low	Moderate	Moderately Low
BATR	-0.057143	0.049361	4.494382	4.978597	Low	Low	Low
CCRTU	0.2	0.043272	15.730337	4.364384	High	Low	Moderate
CMD	0.071429	0.03449	5.617978	3.47864	Low	Low	Low
CTC	0	0.059661	0	6.017368	Low	Moderate	Moderately Low
DBU	0.142857	0.039786	11.235955	4.012821	High	Low	Moderate
DFQ	0	0.033755	0	3.404477	Low	Low	Low
DTHE	0.057143	0.041905	4.494382	4.226584	Low	Low	Low
ELAR	-0.114286	0.062706	8.988764	6.324495	High	Moderate	Moderately High

IFR	-0.142857	0.088849	11.235955	8.961286	High	High	High
IMPR	0.157143	0.072665	12.359551	7.328994	High	High	High
ITBCS	0.128571	0.044222	10.11236	4.460231	High	Low	Moderate
ITII	0.1	0.047819	7.865169	4.823043	High	Low	Moderate
LSMARI	0	0.080008	0	8.069598	Low	High	Moderate
RAISR	0	0.088495	0	8.925591	Low	High	Moderate
RAISR.1	0	0.082332	0	8.303976	Low	High	Moderate

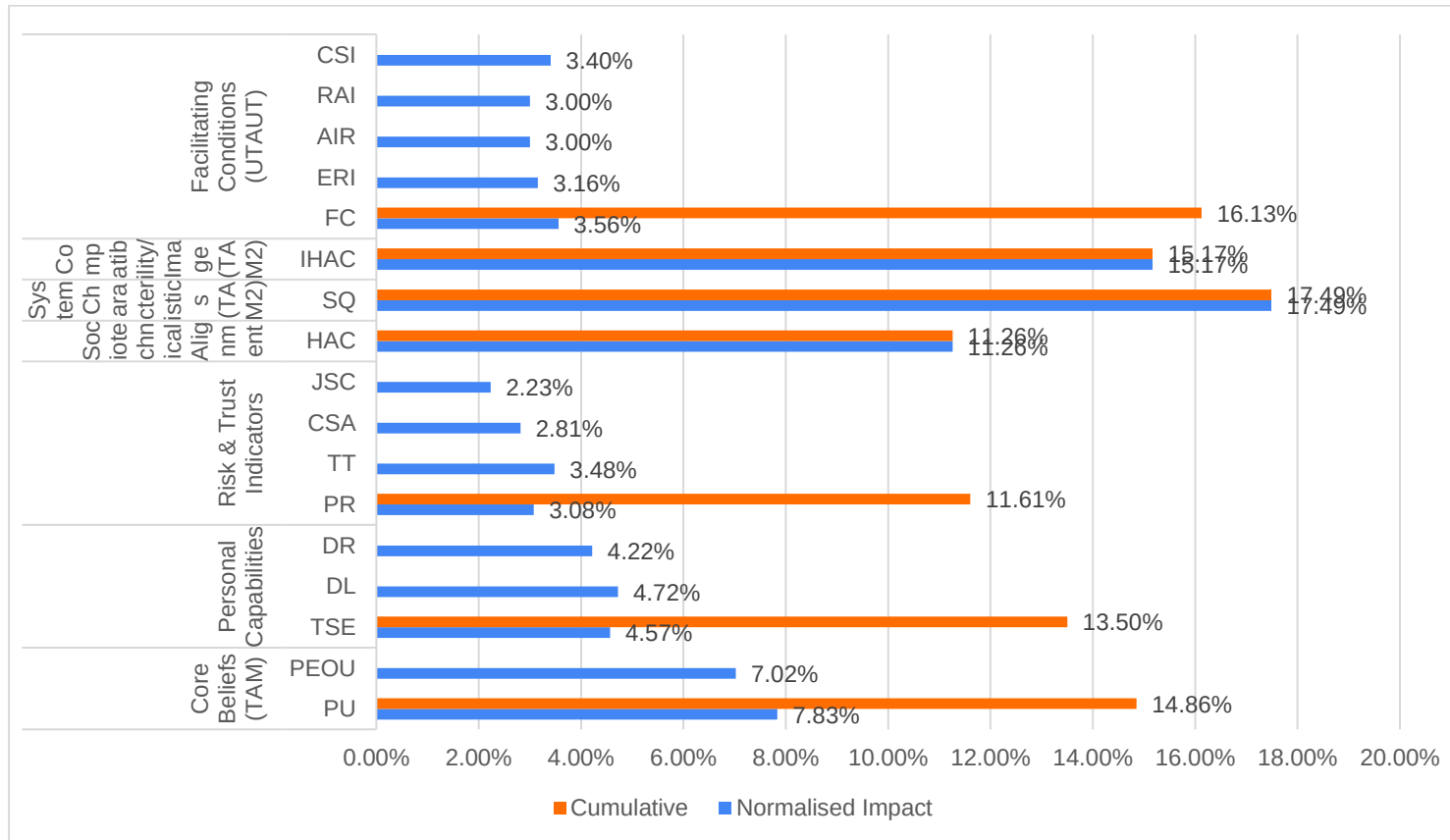


ANNEXURE IX.D IDFC Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for IDFC Bank, 2020 Q1 to 2025 Q3

ANNEXURE IX.E IDFC First Bank - Partial dependence of AIPCS, IFR, ELAR and IMPR, 2020 Q1 to 2025 Q3

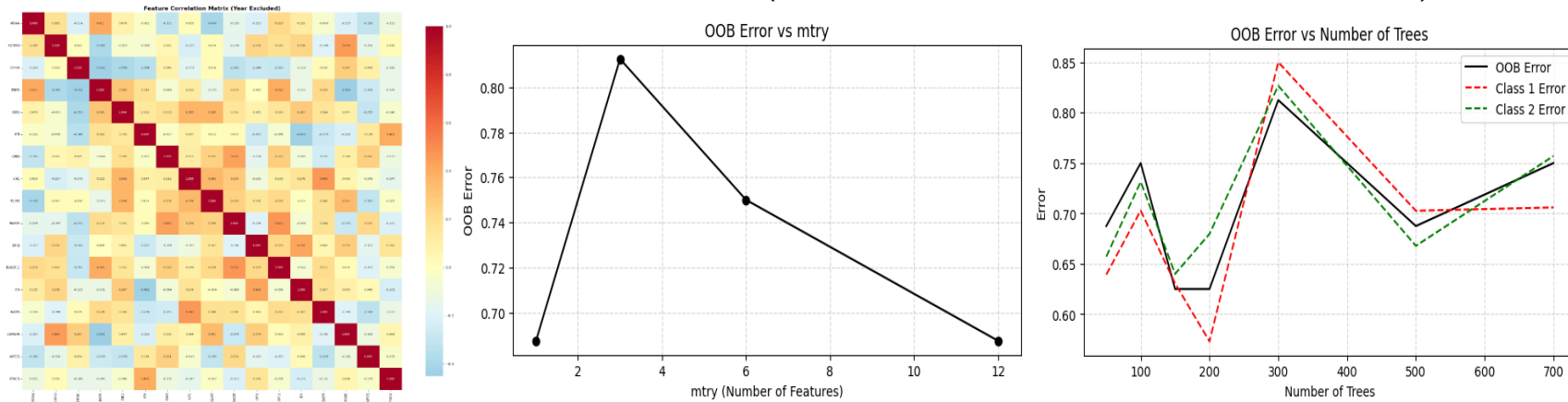
ANNEXURE IX.F IDFC Bank – Variables Severity Analysis and Ranking

Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*IR	Normalised Impact		Weighted average		Level of severity
Core Beliefs (TAM)	PU	0.00	0.00	0.00	15.00	15.00	135.00	13.50	0.06	0.84	7.83%	14.86%	7.43%	HI	H
	PEOU	0.00	2.00	6.00	11.00	11.00	121.00	12.10	0.06	0.76	7.02%				L
Personal Capabilities	TSE	0.00	4.00	3.00	14.00	9.00	118.00	11.80	0.04	0.49	4.57%	13.50%	4.50%	LI	H
	DL	0.00	1.00	5.00	15.00	9.00	122.00	12.20	0.04	0.51	4.72%				H
	DR	0.00	5.00	9.00	8.00	8.00	109.00	10.90	0.04	0.45	4.22%				L
Risk & Trust Indicators	PR	2.00	3.00	10.00	7.00	8.00	106.00	10.60	0.03	0.33	3.08%	11.61%	2.90%	LI	H
	TT	0.00	2.00	4.00	16.00	8.00	120.00	12.00	0.03	0.38	3.48%				H
	CSA	1.00	9.00	8.00	6.00	6.00	97.00	9.70	0.03	0.30	2.81%				L
	JSC	4.00	10.00	12.00	3.00	1.00	77.00	7.70	0.03	0.24	2.23%				L
Sociotechnical Alignment	HAC	0.00	8.00	11.00	7.00	4.00	97.00	9.70	0.13	1.21	11.26%	11.26%	11.26%	LI	M
System Characteristics (TAM2)	SQ	0.00	2.00	11.00	9.00	8.00	113.00	11.30	0.17	1.88	17.49%	17.49%	17.49%	HI	M
Compatibility/Image (TAM2)	IHAC	3.00	5.00	7.00	11.00	4.00	98.00	9.80	0.17	1.63	15.17%	15.17%	15.17%	HI	M
Facilitating Conditions (UTAUT)	FC	0.00	1.00	9.00	14.00	6.00	115.00	11.50	0.03	0.38	3.56%	16.13%	3.23%	HI	H
	ERI	2.00	3.00	12.00	7.00	6.00	102.00	10.20	0.03	0.34	3.16%				L
	AIR	1.00	2.00	17.00	9.00	1.00	97.00	9.70	0.03	0.32	3.00%				L
	RAI	0.00	8.00	10.00	9.00	3.00	97.00	9.70	0.03	0.32	3.00%				L
	CSI	0.00	2.00	11.00	12.00	5.00	110.00	11.00	0.03	0.37	3.40%				H



ANNEXURE IX.G IDFC Bank – Indicators Severity Analysis comparative plot

X. ANNEXURE-X INDUSIND BANK (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



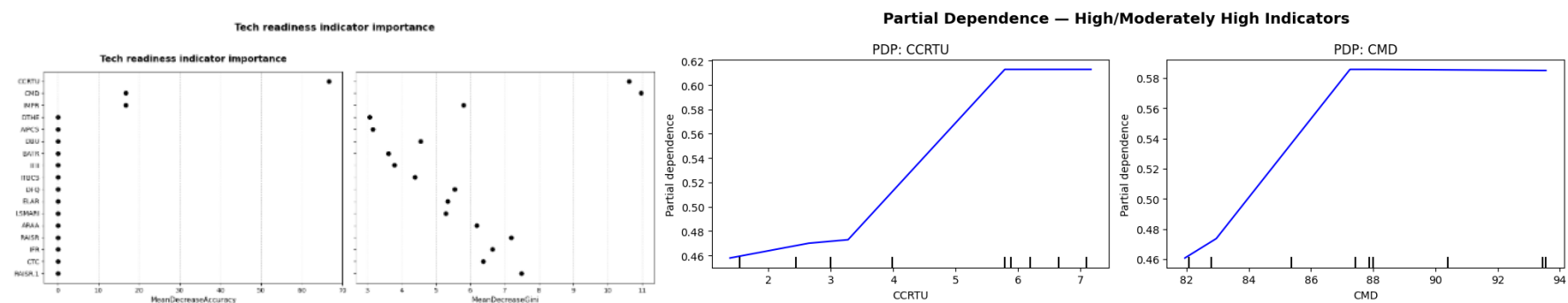
ANNEXURE X.A IndusInd Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE X.B IndusInd Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE X.C IndusInd Bank – Random Forest-based prioritisation of indicators for IndusInd Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	0	0.031114	0	3.157113	Low	Low	Low
ARAA	0	0.06096	0	6.185569	Low	Moderate	Moderately Low
BATR	0	0.03558	0	3.610274	Low	Low	Low
CCRTU	0.114286	0.104655	66.666667	10.619284	High	High	High
CMD	-0.028571	0.108145	16.666667	10.973487	High	High	High
CTC	0	0.062751	0	6.367349	Low	Moderate	Moderately Low
DBU	0	0.044838	0	4.549687	Low	Low	Low
DFQ	0	0.054586	0	5.538838	Low	Low	Low
DTHE	0	0.030224	0	3.066814	Low	Low	Low
ELAR	0	0.052649	0	5.342295	Low	Low	Low

IFR	0	0.065492	0	6.645431	Low	Moderate	Moderately Low
IMPR	0.028571	0.057231	16.666667	5.807222	High	Low	Moderate
ITBCS	0	0.043172	0	4.380704	Low	Low	Low
ITII	0	0.037351	0	3.789956	Low	Low	Low
LSMARI	0	0.052076	0	5.284147	Low	Low	Low
RAISR	0	0.07085	0	7.189147	Low	High	Moderate
RAISR.1	0	0.073841	0	7.492684	Low	High	Moderate



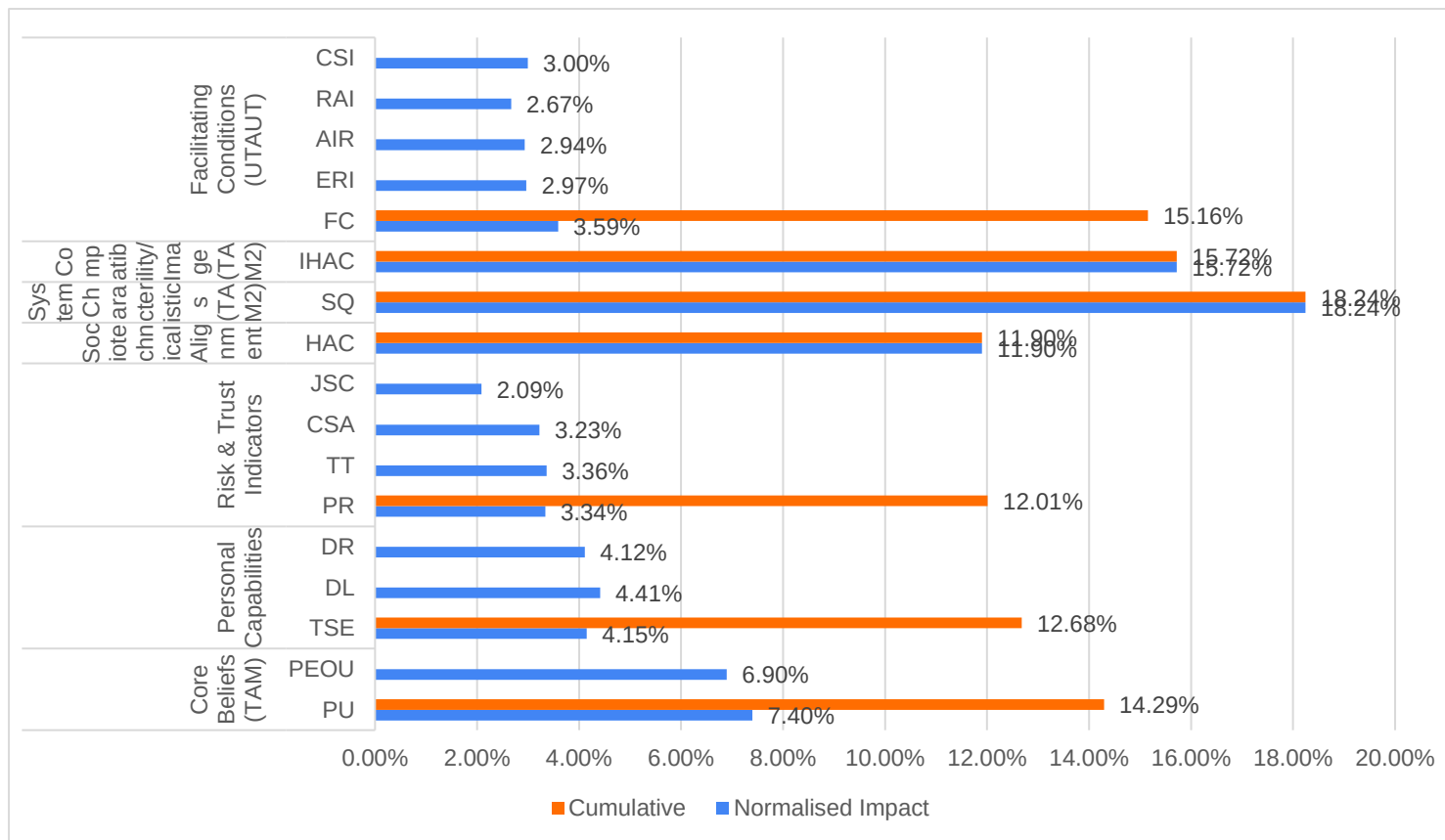
ANNEXURE X.D IndusInd Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for IndusInd Bank, 2020 Q1 to 2025 Q3

ANNEXURE X.E IndusInd Bank - Partial dependence of CCRTU and CMD, 2020 Q1 to 2025 Q3

ANNEXURE X.F IndusInd Bank – Variables Severity Analysis and Ranking

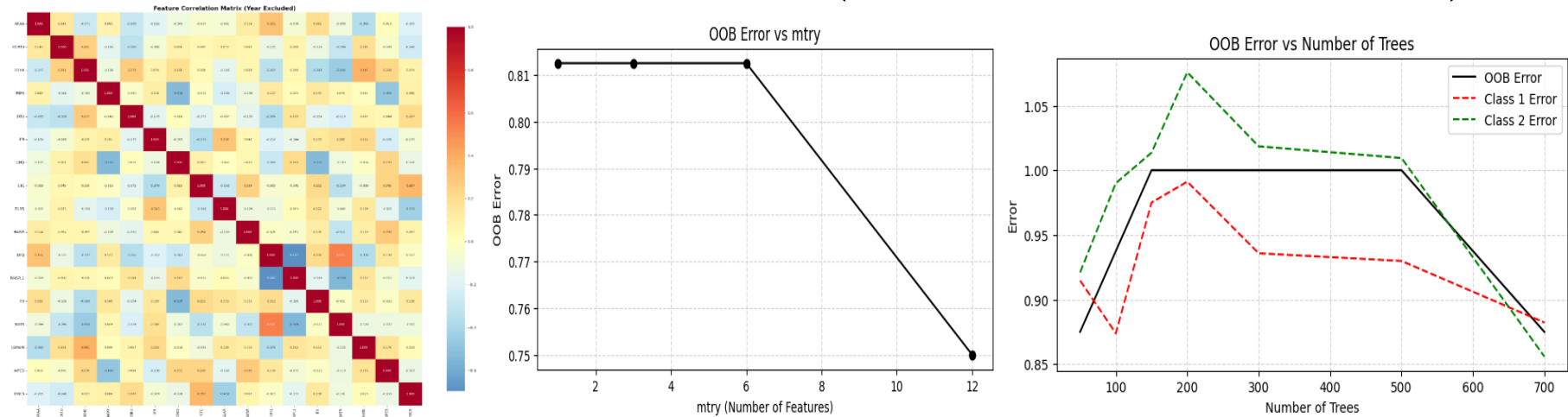
Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*IR	Normalised Impact	Weighted average	Level of sevriy
Core Beliefs (TAM)	PU	0.00	0.00	1.00	15.00	14.00	133.00	13.30	0.06	0.83	7.40%	14.29%	HI
	PEOU	0.00	3.00	2.00	13.00	12.00	124.00	12.40	0.06	0.78	6.90%		L
Personal Capabilities	TSE	0.00	4.00	9.00	8.00	9.00	112.00	11.20	0.04	0.47	4.15%	12.68%	LI
	DL	0.00	0.00	9.00	13.00	8.00	119.00	11.90	0.04	0.50	4.41%		H
	DR	0.00	5.00	9.00	6.00	10.00	111.00	11.10	0.04	0.46	4.12%		L

Risk & Trust Indicators	PR	1.00	0.00	8.00	10.00	11.00	120.00	12.00	0.03	0.38	3.34%	12.01%	3.00%	LI	H
	TT	0.00	1.00	8.00	10.00	11.00	121.00	12.10	0.03	0.38	3.36%				H
	CSA	1.00	1.00	8.00	11.00	9.00	116.00	11.60	0.03	0.36	3.23%				H
	JSC	5.00	10.00	11.00	3.00	1.00	75.00	7.50	0.03	0.23	2.09%				L
Sociotechnical Alignment	HAC	0.00	5.00	9.00	10.00	6.00	107.00	10.70	0.13	1.34	11.90%	11.90%	11.90%	LI	M
System Characteristics (TAM2)	SQ	0.00	1.00	6.00	12.00	11.00	123.00	12.30	0.17	2.05	18.24%	18.24%	18.24%	HI	M
	IHAC	0.00	5.00	9.00	11.00	5.00	106.00	10.60	0.17	1.77	15.72%	15.72%	15.72%	HI	M
Compatibility/Image (TAM2)	FC	0.00	0.00	7.00	15.00	8.00	121.00	12.10	0.03	0.40	3.59%	15.16%	3.03%	HI	H
Facilitating Conditions (UTAUT)	ERI	2.00	5.00	10.00	7.00	6.00	100.00	10.00	0.03	0.33	2.97%				L
	AIR	0.00	3.00	16.00	10.00	1.00	99.00	9.90	0.03	0.33	2.94%				L
	RAI	0.00	11.00	11.00	5.00	3.00	90.00	9.00	0.03	0.30	2.67%				L
	CSI	1.00	5.00	10.00	10.00	4.00	101.00	10.10	0.03	0.34	3.00%				L



ANNEXURE X.G IndusInd Bank – Indicators Severity Analysis comparative plot

XI. ANNEXURE-XI INDIAN OVERSEAS BANK SUMMARY (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



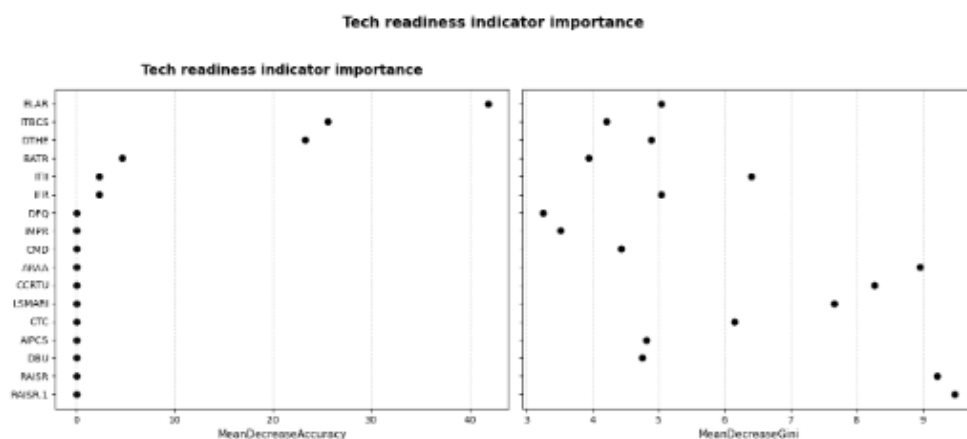
ANNEXURE XI.A Indian Overseas Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE XI.B Indian Overseas Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE XI.C Indian Overseas Bank – Random Forest-based prioritisation of indicators for Indian Overseas Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	0	0.047249	0	4.811976	Low	Low	Low
ARAA	0	0.088003	0	8.962481	Low	High	Moderate
BATR	-0.028571	0.03872	4.651163	3.943307	Low	Low	Low
CCRTU	0	0.081183	0	8.267875	Low	High	Moderate
CMD	0	0.043477	0	4.427782	Low	Low	Low
CTC	0	0.060392	0	6.150513	Low	Moderate	Moderately Low
DBU	0	0.046586	0	4.744481	Low	Low	Low
DFQ	0	0.031867	0	3.245466	Low	Low	Low
DTHE	-0.142857	0.047989	23.255814	4.887353	High	Low	Moderate

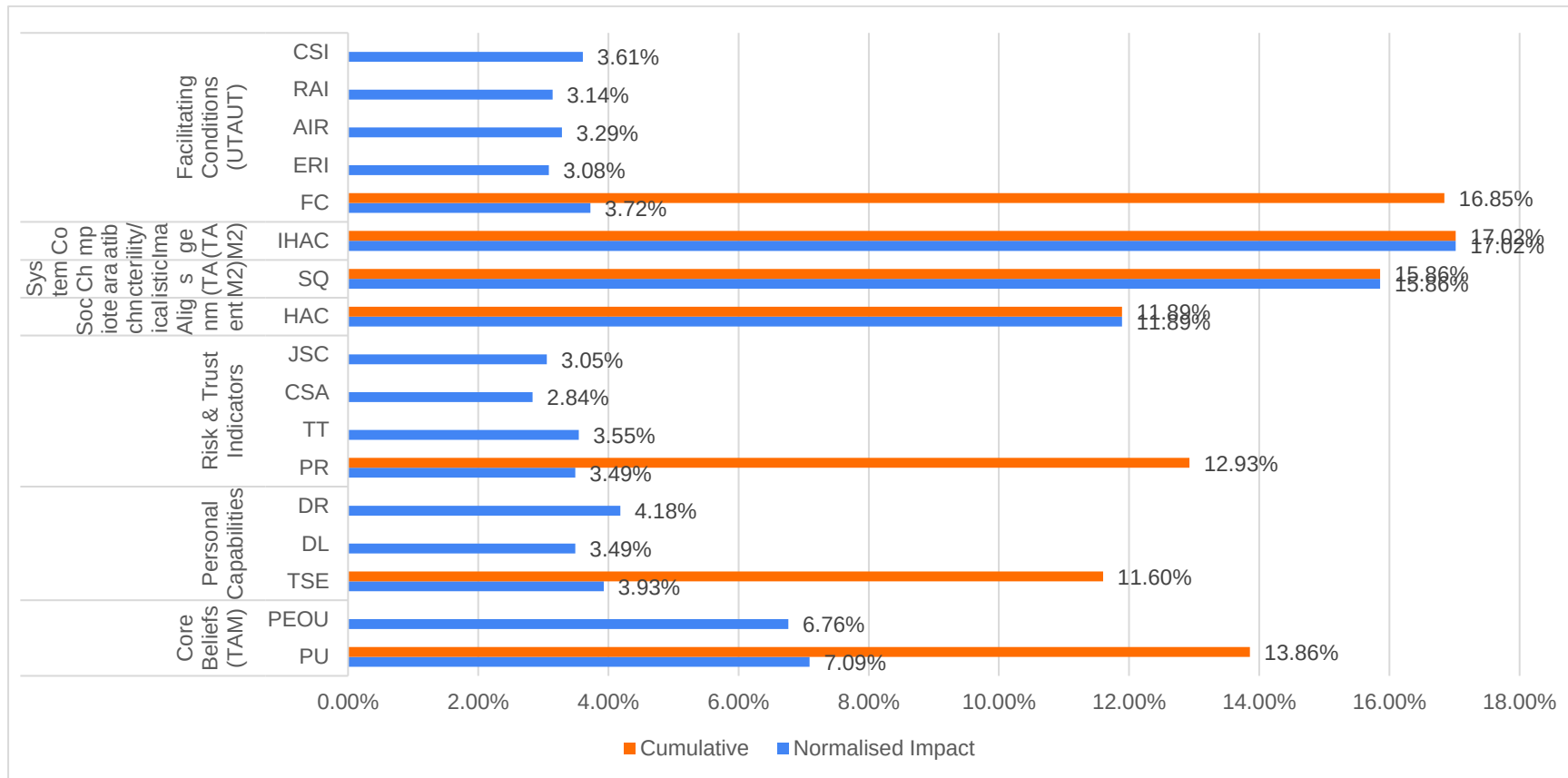
ELAR	-0.257143	0.049427	41.860465	5.033784	High	Low	Moderate
IFR	-0.014286	0.049464	2.325581	5.037534	Low	Low	Low
IMPR	0	0.034533	0	3.516975	Low	Low	Low
ITBCS	-0.157143	0.041314	25.581395	4.207504	High	Low	Moderate
ITII	0.014286	0.062883	2.325581	6.404161	Low	Moderate	Moderately Low
LSMARI	0	0.075204	0	7.658964	Low	High	Moderate
RAISR	0	0.090518	0	9.218623	Low	High	Moderate
RAISR.1	0	0.093097	0	9.48122	Low	High	Moderate



ANNEXURE XI.D Indian Overseas Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Indian Overseas Bank, 2020 Q1 to 2025 Q3

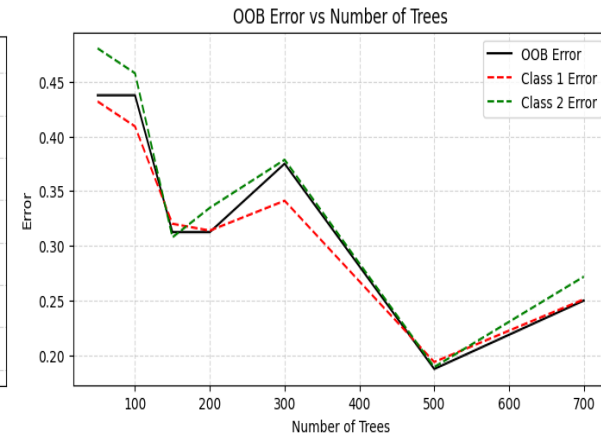
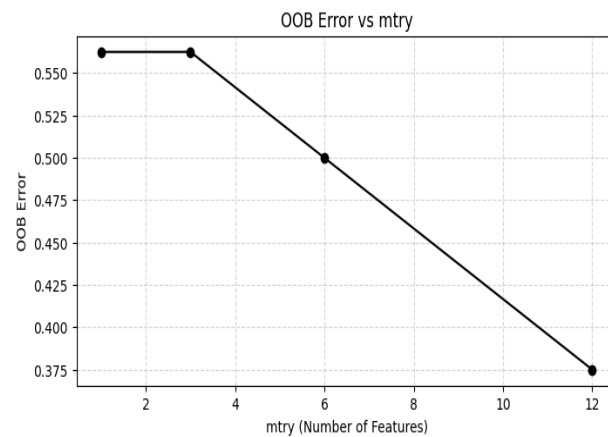
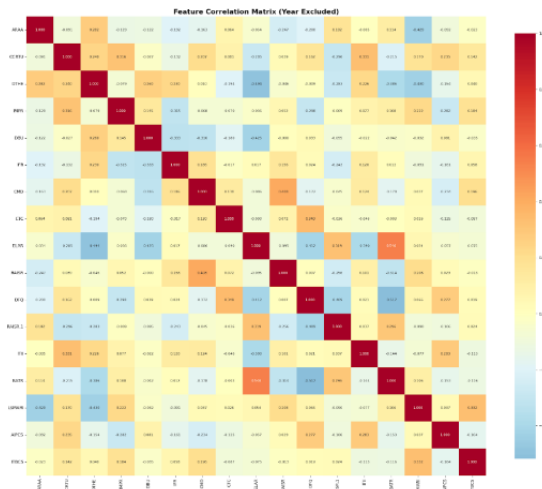
ANNEXURE XI.E Indian Overseas Bank – Variables Severity Analysis and Ranking

Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*IR	Normalised Impact	Normalised Impact	Cumulative	Weighted average	Level of severity
Core Beliefs (TAM)	PU	0	0	3	14	13	130	11.82	0.063	0.739	0.071	7.1%	13.86%	6.93%	LI
	PEOU	0	0	6	14	10	124	11.27	0.063	0.705	0.068	6.8%			
Personal Capabilities	TSE	0	6	7	10	7	108	9.82	0.042	0.409	0.039	3.9%	11.60%	3.87%	LI
	DL	5	6	3	10	6	96	8.73	0.042	0.364	0.035	3.5%			
	DR	0	4	5	13	8	115	10.45	0.042	0.436	0.042	4.2%			
Risk & Trust Indicators	PR	0	0	5	12	13	128	11.64	0.031	0.364	0.035	3.5%	12.93%	3.23%	LI
	TT	0	0	0	20	10	130	11.82	0.031	0.369	0.035	3.5%			
	CSA	0	1	17	9	3	104	9.45	0.031	0.295	0.028	2.8%			
	JSC	0	4	7	12	7	112	10.18	0.031	0.318	0.031	3.1%			
Sociotechnical Alignment	HAC	0	6	8	7	9	109	9.91	0.125	1.239	0.119	11.9%	11.89%	11.89%	LI
System Characteristics (TAM2)	SQ	0	3	10	12	5	109	9.91	0.167	1.652	0.159	15.9%	15.86%	15.86%	HI
Compatibility/Image (TAM2)	IHAC	0	2	7	13	8	117	10.64	0.167	1.773	0.170	17.0%	17.02%	17.02%	HI
Facilitating Conditions (UTAUT)	FC	0	0	4	14	12	128	11.64	0.033	0.388	0.037	3.7%	16.85%	3.37%	HI
	ERI	1	5	9	7	8	106	9.64	0.033	0.321	0.031	3.1%			
	AIR	1	0	10	13	6	113	10.27	0.033	0.342	0.033	3.3%			
	RAI	1	4	9	8	8	108	9.82	0.033	0.327	0.031	3.1%			
	CSI	0	0	6	14	10	124	11.27	0.033	0.376	0.036	3.6%			



ANNEXURE XI.F Indian Overseas Bank – Indicators Severity Analysis comparative plot

XII. ANNEXURE-XII KOTAK MAHINDRA BANK (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



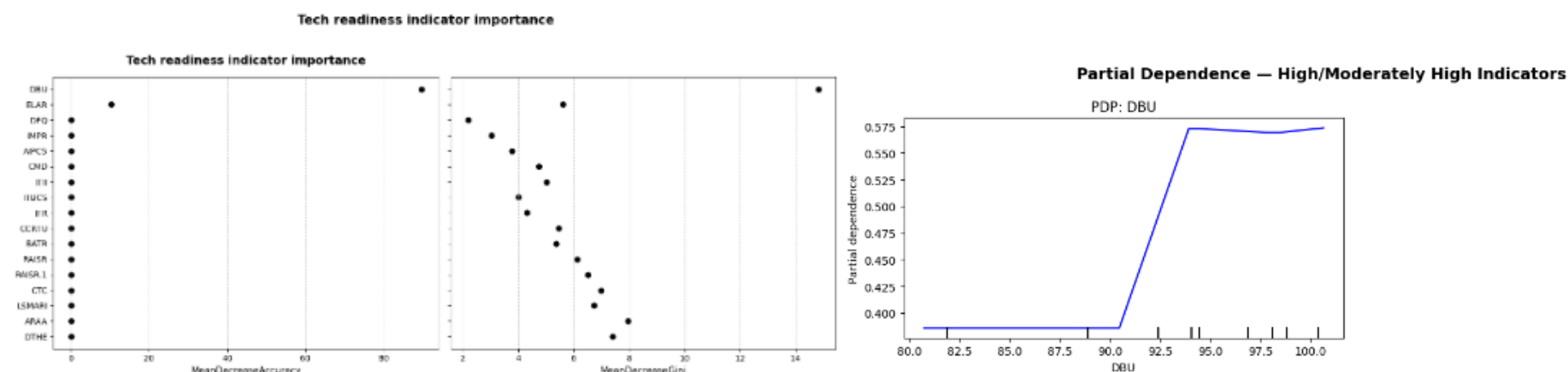
ANNEXURE XII.A Kotak Mahindra Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE XII.B Kotak Mahindra Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE XII.C Kotak Bank – Random Forest-based prioritisation of indicators for State Bank of India with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	0	0.037048	0	3.762508	Low	Low	Low
ARAA	0	0.078253	0	7.947119	Low	High	Moderate
BATR	0	0.052897	0	5.372115	Low	Low	Low
CCRTU	0	0.053737	0	5.457339	Low	Low	Low
CMD	0	0.046744	0	4.74717	Low	Low	Low
CTC	0	0.068774	0	6.984445	Low	Moderate	Moderately Low
DBU	-0.371429	0.145958	89.655172	14.823075	High	High	High
DFQ	0	0.021525	0	2.186019	Low	Low	Low

DTHE	0	0.072864	0	7.399879	Low	High	Moderate
ELAR	0.042857	0.055207	10.344828	5.606709	High	Low	Moderate
IFR	0	0.042318	0	4.297683	Low	Low	Low
IMPR	0	0.029911	0	3.03769	Low	Low	Low
ITBCS	0	0.039469	0	4.008342	Low	Low	Low
ITII	0	0.049421	0	5.019078	Low	Low	Low
LSMARI	0	0.066226	0	6.725769	Low	Moderate	Moderately Low
RAISR	0	0.060266	0	6.120463	Low	Moderate	Moderately Low
RAISR.1	0	0.064049	0	6.504598	Low	Moderate	Moderately Low



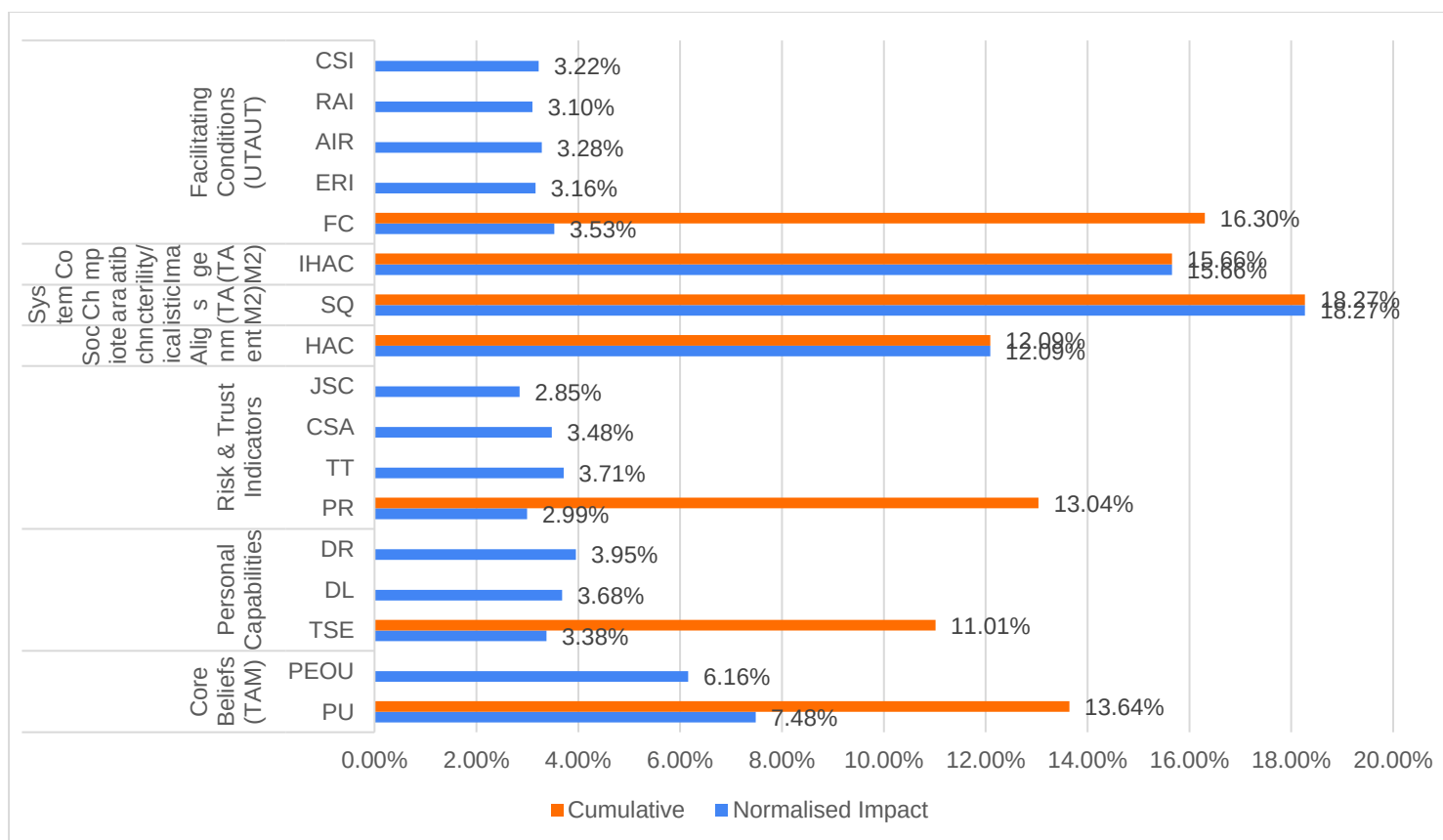
ANNEXURE XII.D Kotak Mahindra Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Kotak Mahindra Bank, 2020 Q1 to 2025 Q3

ANNEXURE XII.E Kotak Mahindra Bank - Partial dependence of DBU, 2020 Q1 to 2025 Q3

ANNEXURE XII.F Kotak Mahindra Bank – Variables Severity Analysis and Ranking

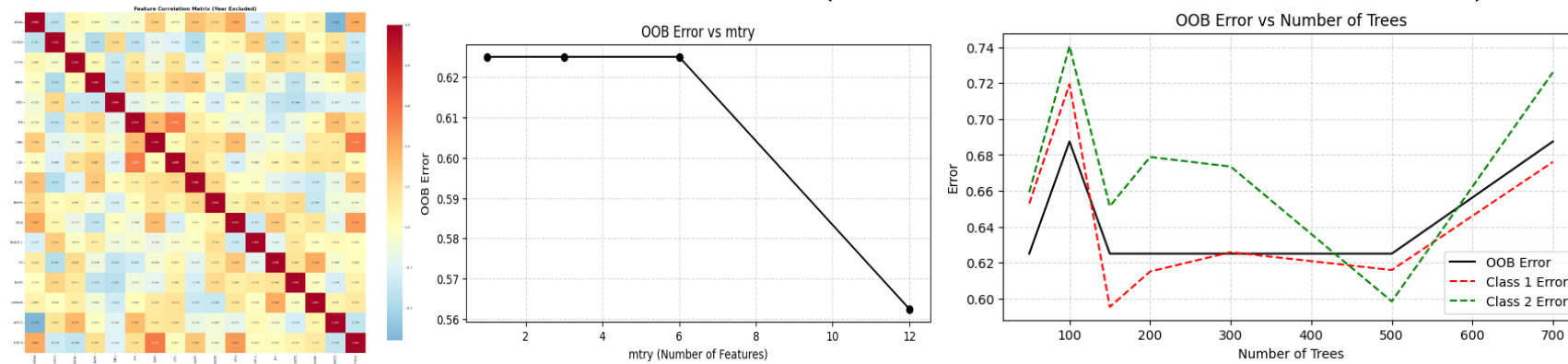
Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*I R	Normalised Impact	Weighted average	Level of severity
Core Beliefs (TAM)	PU	0.00	0.00	3.00	14.00	13.00	130.00	14.44	0.06	0.90	7.48%	13.64%	6.82% LI H

Personal Capabilities	PEOU	1.00	6.00	7.00	7.00	9.00	107.00	11.89	0.06	0.74	6.16%				L
	TSE	5.00	6.00	9.00	6.00	4.00	88.00	9.78	0.04	0.41	3.38%	11.01%	3.67%	LI	L
	DL	0.00	8.00	9.00	12.00	1.00	96.00	10.67	0.04	0.44	3.68%				H
Risk & Trust Indicators	DR	5.00	4.00	4.00	7.00	10.00	103.00	11.44	0.04	0.48	3.95%				H
	PR	3.00	4.00	7.00	8.00	8.00	104.00	11.56	0.03	0.36	2.99%	13.04%	3.26%	LI	L
	TT	1.00	1.00	4.00	6.00	18.00	129.00	14.33	0.03	0.45	3.71%				H
	CSA	1.00	1.00	5.00	12.00	11.00	121.00	13.44	0.03	0.42	3.48%				H
Sociotechnical Alignment	JSC	2.00	7.00	6.00	10.00	5.00	99.00	11.00	0.03	0.34	2.85%				L
	HAC	1.00	5.00	9.00	8.00	7.00	105.00	11.67	0.13	1.46	12.09%	12.09%	12.09%	LI	M
	SQ	0.00	2.00	6.00	13.00	9.00	119.00	13.22	0.17	2.20	18.27%	18.27%	18.27%	HI	M
Compatibility/Image (TAM2)	IHAC	4.00	5.00	6.00	5.00	10.00	102.00	11.33	0.17	1.89	15.66%	15.66%	15.66%	HI	M
Facilitating Conditions (UTAUT)	FC	0.00	0.00	11.00	13.00	6.00	115.00	12.78	0.03	0.43	3.53%	16.30%	3.26%	HI	H
	ERI	3.00	4.00	8.00	7.00	8.00	103.00	11.44	0.03	0.38	3.16%				L
	AIR	1.00	8.00	5.00	5.00	11.00	107.00	11.89	0.03	0.40	3.28%				H
	RAI	3.00	5.00	6.00	10.00	6.00	101.00	11.22	0.03	0.37	3.10%				L
	CSI	2.00	4.00	7.00	11.00	6.00	105.00	11.67	0.03	0.39	3.22%				L



ANNEXURE XII.G Kotak Mahindra Bank – Indicators Severity Analysis comparative plot

XIII. ANNEXURE-XIII STATE BANK OF INDIA (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



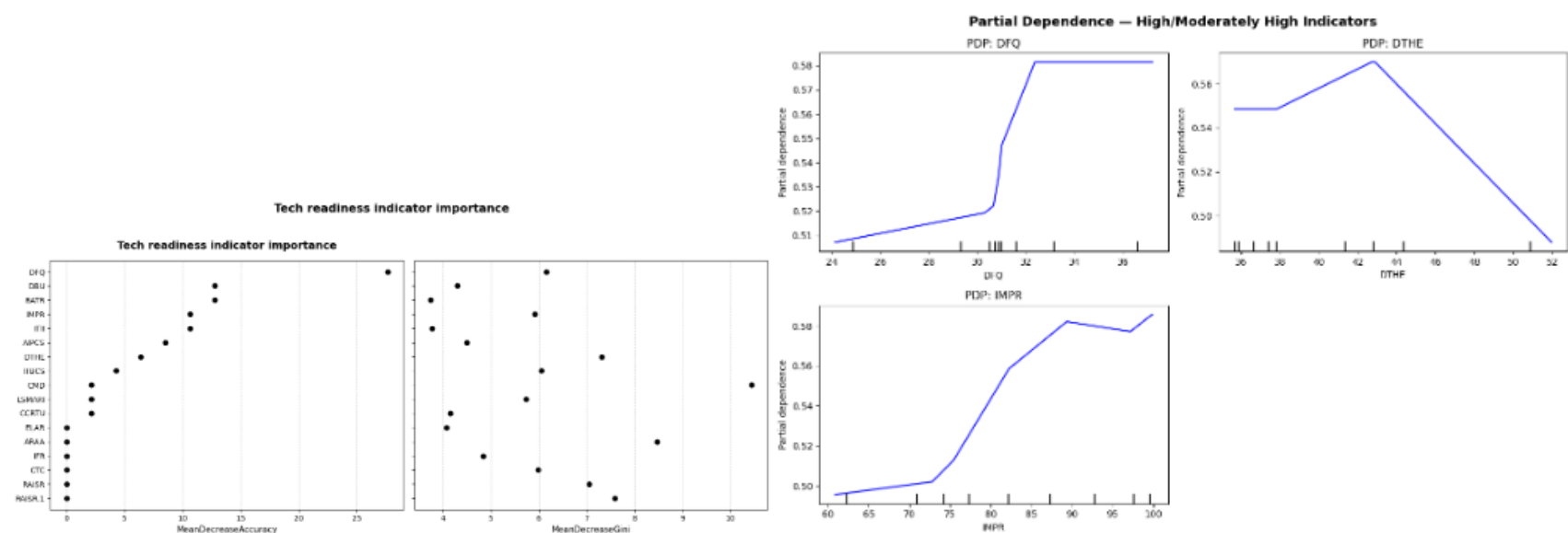
ANNEXURE XIII.A State Bank of India – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE XIII.B State Bank of India – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE XIII.C State Bank of India – Random Forest-based prioritisation of indicators for State Bank of India with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	0.057143	0.044063	8.510638	4.487808	High	Low	Moderate
ARAA	0	0.083129	0	8.466598	Low	High	Moderate
BATR	-0.085714	0.036663	12.765957	3.734084	High	Low	Moderate
CCRTU	-0.014286	0.040686	2.12766	4.143851	Low	Low	Low
CMD	-0.014286	0.102463	2.12766	10.435726	Low	High	Moderate
CTC	0	0.058722	0	5.980738	Low	Moderate	Moderately Low
DBU	-0.085714	0.042155	12.765957	4.29346	High	Low	Moderate
DFQ	-0.185714	0.060455	27.659574	6.1573	High	Moderate	Moderately High
DTHE	-0.042857	0.071734	6.382979	7.306082	Moderate	High	Moderately High
ELAR	0	0.039919	0	4.065748	Low	Low	Low
IFR	0	0.04747	0	4.834783	Low	Low	Low

IMPR	0.071429	0.058043	10.638298	5.911673	High	Moderate	Moderately High
ITBCS	-0.028571	0.05942	4.255319	6.051911	Low	Moderate	Moderately Low
ITII	-0.071429	0.037059	10.638298	3.77439	High	Low	Moderate
LSMARI	-0.014286	0.056204	2.12766	5.724289	Low	Low	Low
RAISR	0	0.069153	0	7.0432	Low	Moderate	Moderately Low
RAISR.1	0	0.074506	0	7.588363	Low	High	Moderate

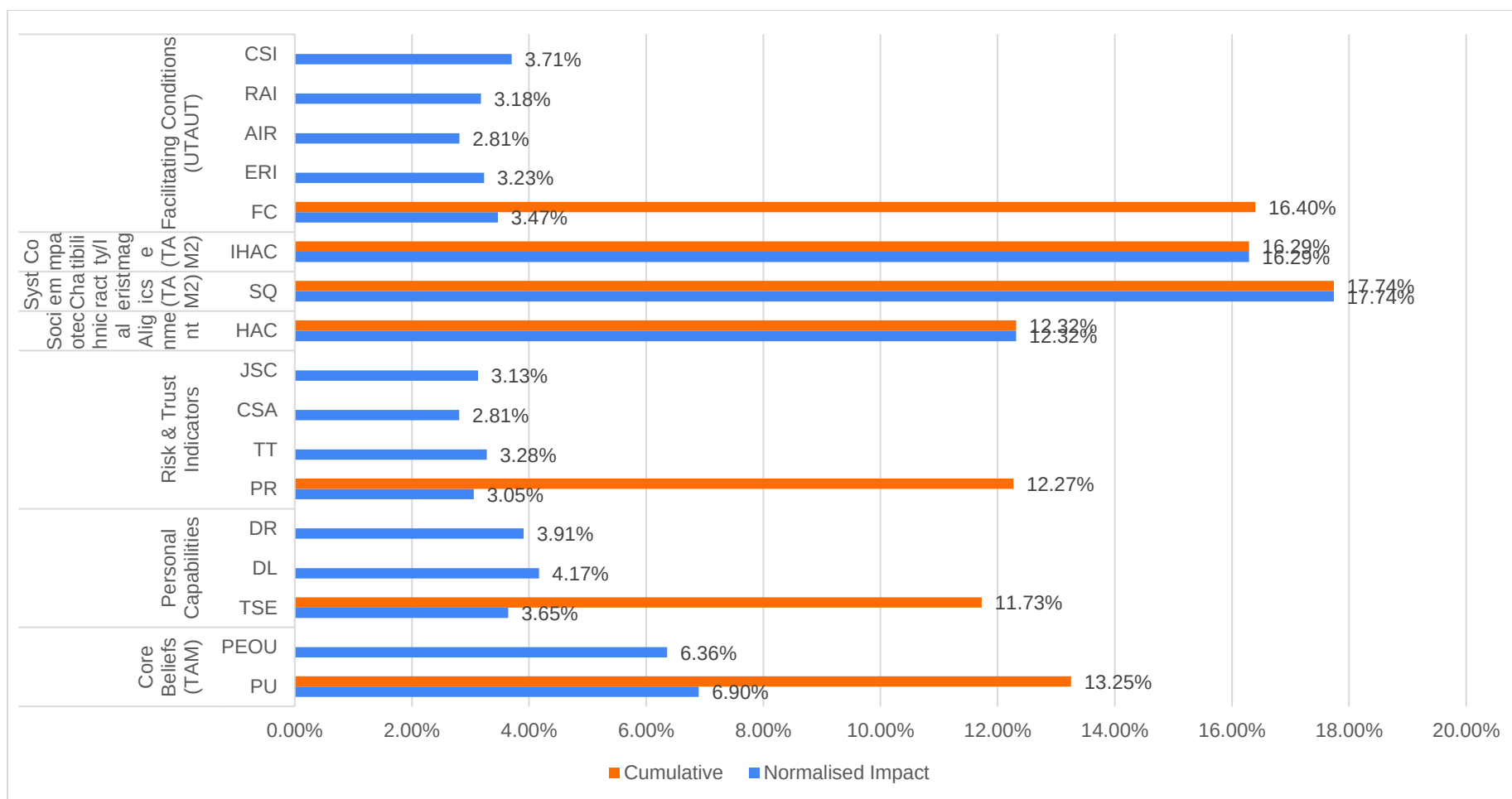


ANNEXURE XIII.D State Bank of India – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for State Bank of India, 2020 Q1 to 2025 Q3

ANNEXURE XIII.E State Bank of India - Partial dependence of DFQ, DTHE, and IMPR, 2020 Q1 to 2025 Q3

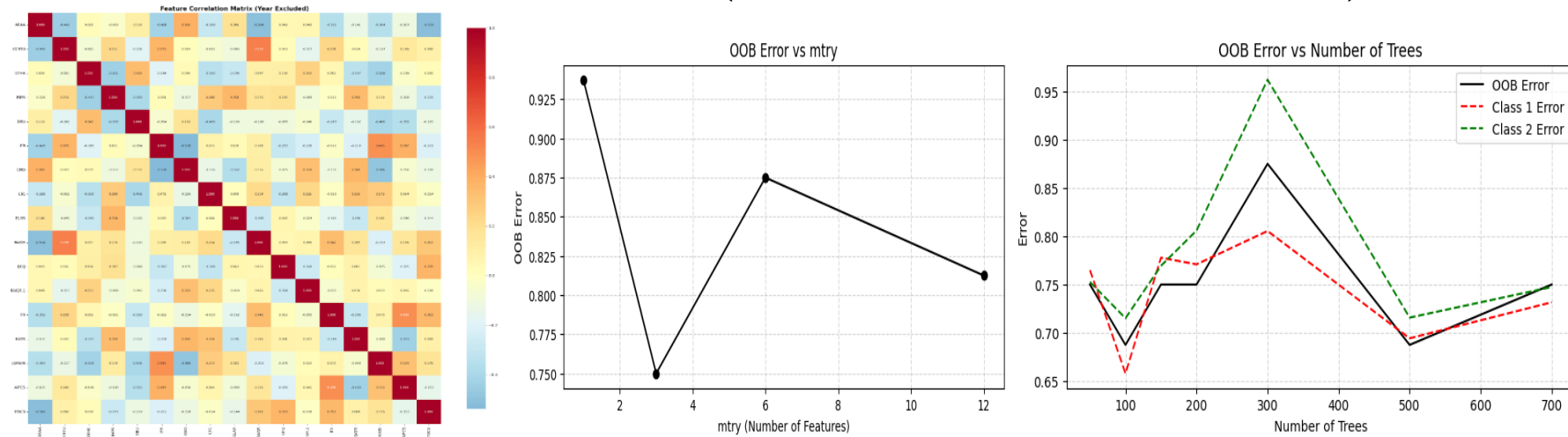
ANNEXURE XIII.F State Bank of India – Variables Severity Analysis and Ranking

Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*I R	Normalised Impact		Weighted average		Level of severity
Core Beliefs (TAM)	PU	0.00	0.00	0.00	10.00	20.00	140.00	28.00	0.06	1.75	6.90%	13.25%	6.63%	LI	H
	PEOU	0.00	0.00	1.00	19.00	10.00	129.00	25.80	0.06	1.61	6.36%				L
Personal Capabilities	TSE	3.00	2.00	8.00	5.00	12.00	111.00	22.20	0.04	0.93	3.65%	11.73%	3.91%	LI	L
	DL	0.00	1.00	5.00	10.00	14.00	127.00	25.40	0.04	1.06	4.17%				H
	DR	0.00	1.00	1.00	26.00	2.00	119.00	23.80	0.04	0.99	3.91%				M
Risk & Trust Indicators	PR	0.00	0.00	2.00	22.00	6.00	124.00	24.80	0.03	0.78	3.05%	12.27%	3.07%	LI	L
	TT	0.00	0.00	1.00	15.00	14.00	133.00	26.60	0.03	0.83	3.28%				H
	CSA	3.00	3.00	6.00	3.00	15.00	114.00	22.80	0.03	0.71	2.81%				L
	JSC	0.00	1.00	5.00	10.00	14.00	127.00	25.40	0.03	0.79	3.13%				H
Sociotechnical Alignment	HAC	0.00	0.00	2.00	21.00	7.00	125.00	25.00	0.13	3.13	12.32%	12.32%	12.32%	LI	M
System Characteristics (TAM2)	SQ	0.00	0.00	0.00	15.00	15.00	135.00	27.00	0.17	4.50	17.74%	17.74%	17.74%	HI	M
Compatibility/Image (TAM2)	IHAC	0.00	0.00	3.00	20.00	7.00	124.00	24.80	0.17	4.13	16.29%	16.29%	16.29%	HI	M
Facilitating Conditions (UTAUT)	FC	0.00	0.00	1.00	16.00	13.00	132.00	26.40	0.03	0.88	3.47%	16.40%	3.28%	HI	H
	ERI	0.00	1.00	7.00	10.00	12.00	123.00	24.60	0.03	0.82	3.23%				L
	AIR	1.00	2.00	10.00	13.00	4.00	107.00	21.40	0.03	0.71	2.81%				L
	RAI	0.00	0.00	2.00	25.00	3.00	121.00	24.20	0.03	0.81	3.18%				L
	CSI	0.00	0.00	0.00	9.00	21.00	141.00	28.20	0.03	0.94	3.71%				H



ANNEXURE XIII.G State Bank of India – Indicators Severity Analysis comparative plot

XIV. ANNEXURE-XIV UCO BANK (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



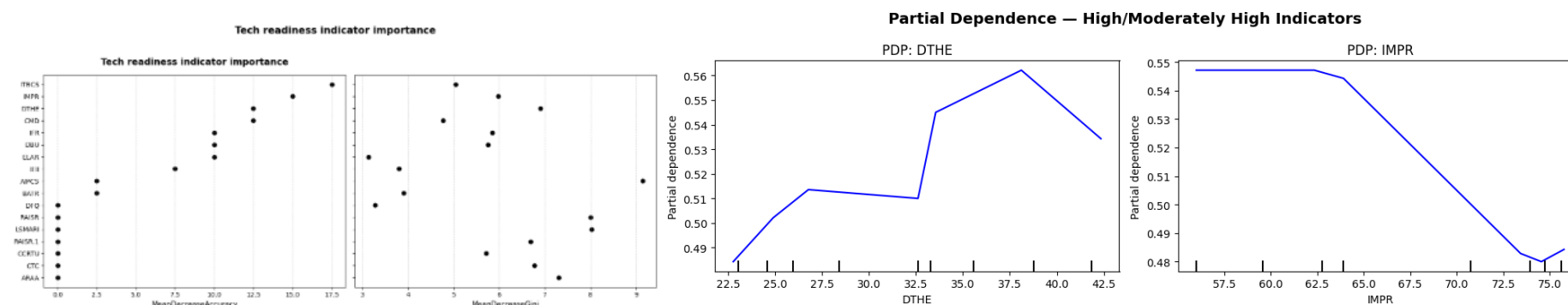
ANNEXURE XIV.A UCO Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE XIV.B UCO Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE XIV.C UCO Bank – Random Forest-based prioritisation of indicators for UCO Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	0.014286	0.090042	2.5	9.140231	Low	High	Moderate
ARAA	0	0.071915	0	7.30018	Low	High	Moderate
BATR	0.014286	0.038447	2.5	3.902842	Low	Low	Low
CCRTU	0	0.056224	0	5.70735	Low	Low	Low
CMD	0.071429	0.046895	12.5	4.76038	High	Low	Moderate
CTC	0	0.066636	0	6.764343	Low	Moderate	Moderately Low
DBU	-0.057143	0.056668	10	5.752476	High	Low	Moderate
DFQ	0	0.03226	0	3.274736	Low	Low	Low
DTHE	0.071429	0.067954	12.5	6.898104	High	High	High

ELAR	0.057143	0.030833	10	3.129889	High	Low	Moderate
IFR	0.057143	0.057561	10	5.843047	High	Low	Moderate
IMPR	-0.085714	0.058889	15	5.977941	High	High	High
ITBCS	0.1	0.049655	17.5	5.040579	High	Low	Moderate
ITII	-0.042857	0.037399	7.5	3.796422	High	Low	Moderate
LSMARI	0	0.07905	0	8.024517	Low	High	Moderate
RAISR	0	0.07882	0	8.001098	Low	High	Moderate
RAISR.1	0	0.065863	0	6.685866	Low	Moderate	Moderately Low



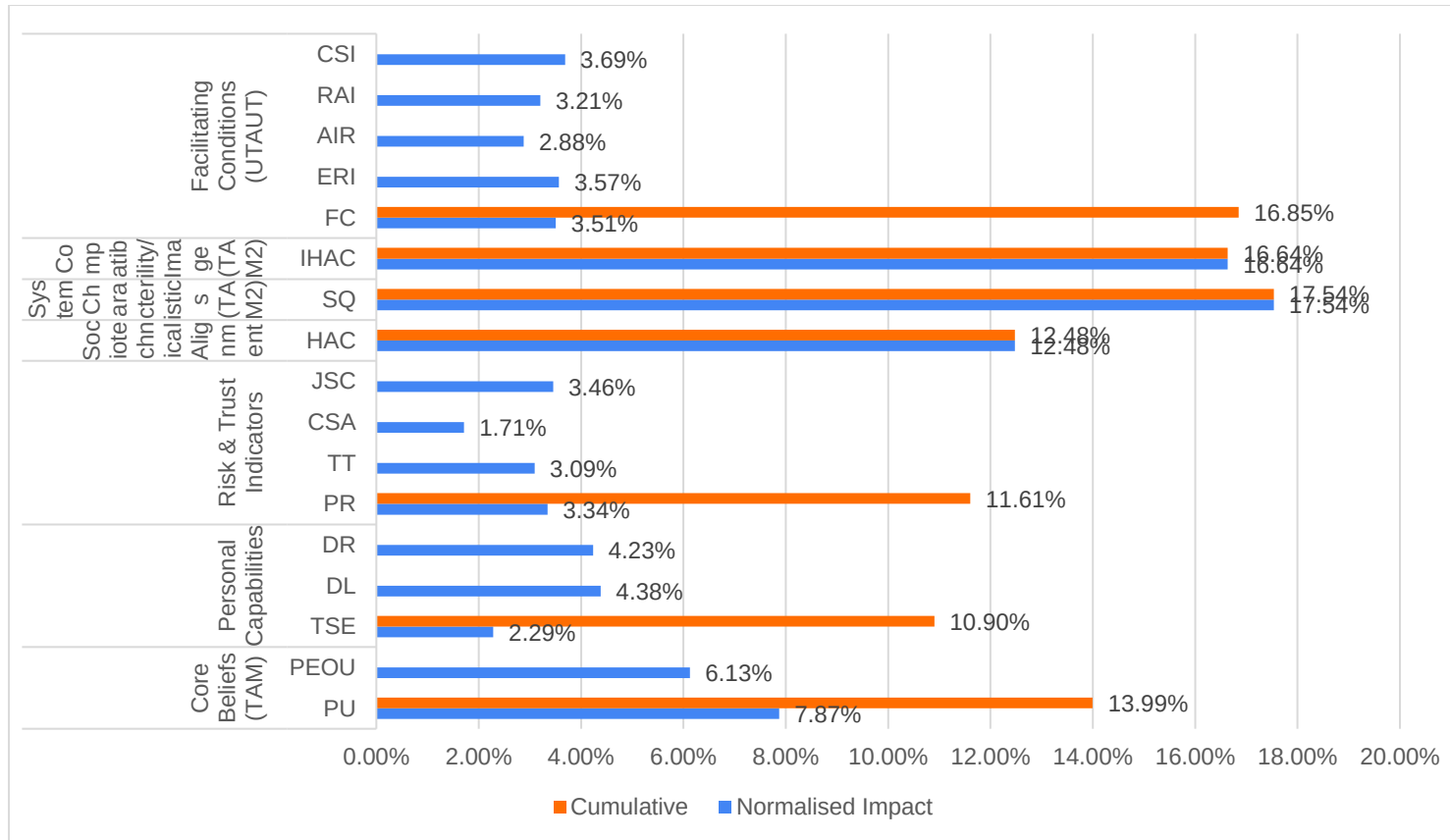
ANNEXURE XIV.D UCO Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for UCO Bank, 2020 Q1 to 2025 Q3

ANNEXURE XIV.E UCO Bank - Partial dependence of DFQ, DTHE, and ITII, 2020 Q1 to 2025 Q3

ANNEXURE XIV.F UCO Bank – Variables Severity Analysis and Ranking

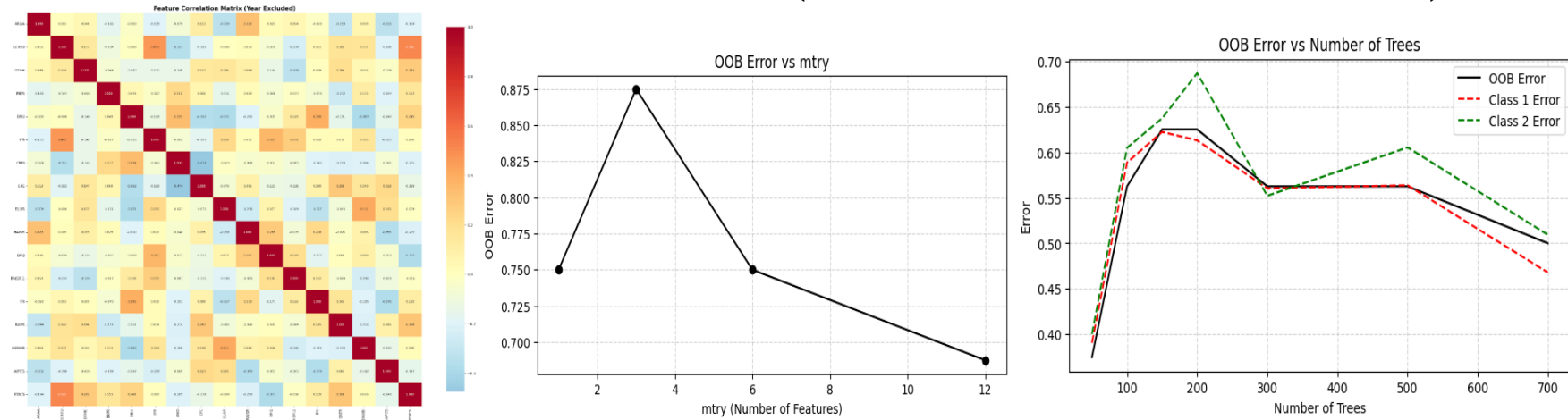
Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*I R	Normalised Impact	Weighted average	Level of sevrvity
Core Beliefs (TAM)	PU	0.00	0.00	0.00	10.00	20.00	140.00	28.00	0.06	1.75	7.87%	13.99%	LI H
	PEOU	0.00	0.00	12.00	17.00	1.00	109.00	21.80	0.06	1.36	6.13%		L
Personal	TSE	4.00	21.00	5.00	0.00	0.00	61.00	12.20	0.04	0.51	2.29%	10.90%	LI L

Capabilities	DL	0.00	0.00	4.00	25.00	1.00	117.00	23.40	0.04	0.98					H	
	DR	0.00	0.00	9.00	19.00	2.00	113.00	22.60	0.04	0.94					H	
Risk & Trust Indicators	PR	0.00	0.00	4.00	23.00	3.00	119.00	23.80	0.03	0.74	3.34%	11.61%	2.90%	LI	H	
	TT	0.00	0.00	12.00	16.00	2.00	110.00	22.00	0.03	0.69	3.09%					H
	CSA	3.00	23.00	4.00	0.00	0.00	61.00	12.20	0.03	0.38	1.71%					L
	JSC	0.00	0.00	2.00	23.00	5.00	123.00	24.60	0.03	0.77	3.46%					H
Sociotechnical Alignment	HAC	0.00	0.00	9.00	21.00	0.00	111.00	22.20	0.13	2.78	12.48%	12.48%	12.48%	LI	M	
System Characteristics (TAM2)	SQ	0.00	0.00	5.00	23.00	2.00	117.00	23.40	0.17	3.90	17.54%	17.54%	17.54%	HI	M	
	IHAC	0.00	0.00	10.00	19.00	1.00	111.00	22.20	0.17	3.70	16.64%	16.64%	16.64%	HI	M	
Facilitating Conditions (UTAUT)	FC	0.00	0.00	5.00	23.00	2.00	117.00	23.40	0.03	0.78	3.51%	16.85%	3.37%	HI	H	
	ERI	0.00	0.00	3.00	25.00	2.00	119.00	23.80	0.03	0.79	3.57%					H
	AIR	0.00	2.00	21.00	6.00	1.00	96.00	19.20	0.03	0.64	2.88%					L
	RAI	0.00	2.00	13.00	11.00	4.00	107.00	21.40	0.03	0.71	3.21%					L
	CSI	0.00	0.00	7.00	13.00	10.00	123.00	24.60	0.03	0.82	3.69%					H



ANNEXURE XIV.G UCO Bank – Indicators Severity Analysis comparative plot

XV. ANNEXURE- XV UNION BANK OF INDIA (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



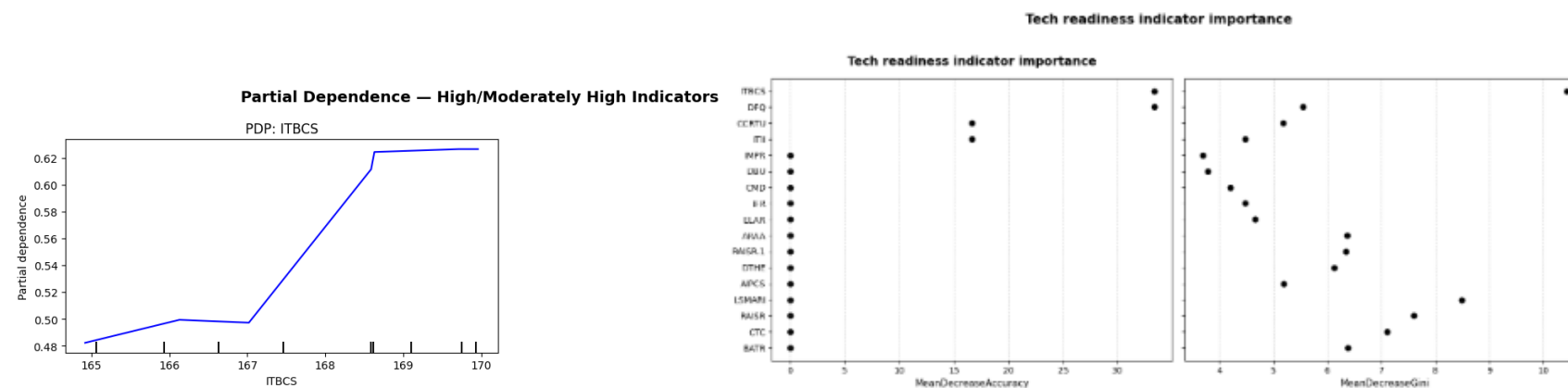
ANNEXURE XV.A Union Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE XV.B Union Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE XV.C Union Bank – Random Forest-based prioritisation of indicators for Union Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	0	0.050599	0	5.193082	Low	Low	Low
ARAA	0	0.061962	0	6.359378	Low	Moderate	Moderately Low
BATR	0	0.062152	0	6.378797	Low	Moderate	Moderately Low
CCRTU	0.028571	0.050387	16.666667	5.171347	High	Low	Moderate
CMD	0	0.040938	0	4.201622	Low	Low	Low
CTC	0	0.069249	0	7.107209	Low	High	Moderate
DBU	0	0.036835	0	3.780498	Low	Low	Low
DFQ	0.057143	0.054056	33.333333	5.547956	High	Low	Moderate
DTHE	0	0.059603	0	6.117178	Low	Moderate	Moderately Low

ELAR	0	0.045377	0	4.657154	Low	Low	Low
IFR	0	0.04356	0	4.470643	Low	Low	Low
IMPR	0	0.035926	0	3.687198	Low	Low	Low
ITBCS	-0.057143	0.101668	33.333333	10.434464	High	High	High
ITII	-0.028571	0.043528	16.666667	4.467402	High	Low	Moderate
LSMARI	0	0.08267	0	8.484686	Low	High	Moderate
RAISR	0	0.074024	0	7.597267	Low	High	Moderate
RAISR.1	0	0.061814	0	6.344119	Low	Moderate	Moderately Low



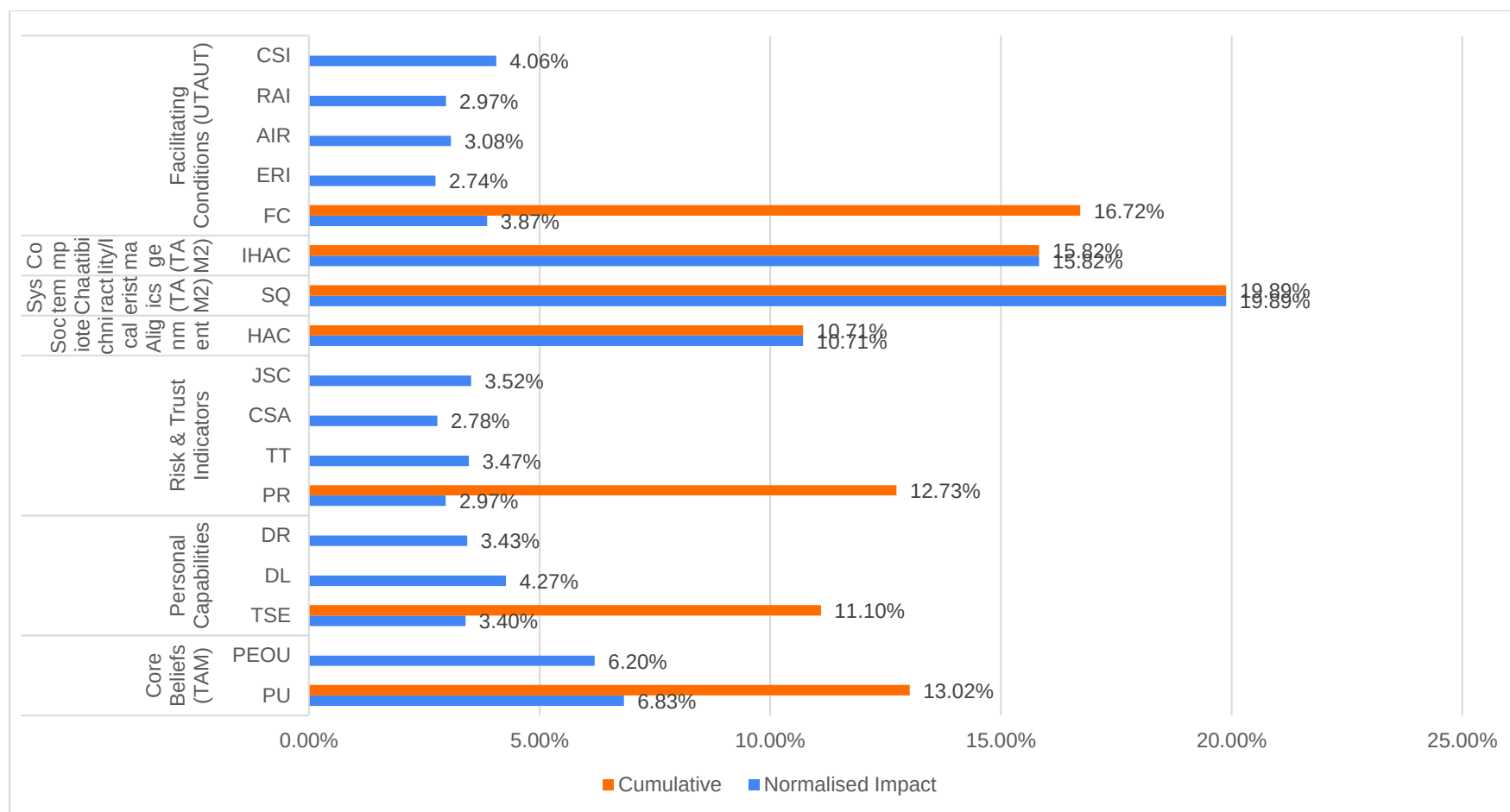
ANNEXURE XV.D Union Bank of India - Partial dependence of ITBCS, 2020 Q1 to 2025 Q3

ANNEXURE XV.E Union Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Union Bank, 2020 Q1 to 2025 Q3

ANNEXURE XV.F Union Bank – Variables Severity Analysis and Ranking

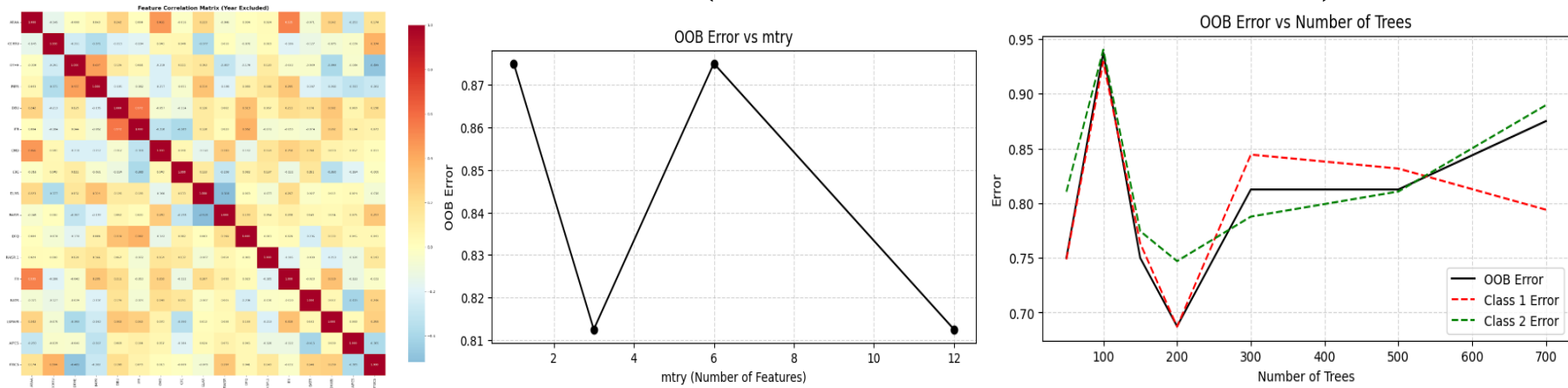
Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*IR	Normalised Impact		Weighted average	Level of sevtrity	
Core Beliefs (TAM)	PU	0.00	0.00	3.00	14.00	13.00	130.00	65.00	0.06	4.06	6.83%	13.02%	6.51%	LI	H
	PEOU	2.00	1.00	8.00	5.00	14.00	118.00	59.00	0.06	3.69	6.20%				L

Personal Capabilities	TSE	5.00	6.00	5.00	5.00	9.00	97.00	48.50	0.04	2.02	3.40%	11.10%	3.70%	LI	L
	DL	0.00	1.00	5.00	15.00	9.00	122.00	61.00	0.04	2.54	4.27%				H
	DR	6.00	5.00	2.00	9.00	8.00	98.00	49.00	0.04	2.04	3.43%				L
Risk & Trust Indicators	PR	1.00	4.00	9.00	3.00	13.00	113.00	56.50	0.03	1.77	2.97%	12.73%	3.18%	LI	L
	TT	0.00	0.00	2.00	14.00	14.00	132.00	66.00	0.03	2.06	3.47%				H
	CSA	3.00	3.00	8.00	7.00	9.00	106.00	53.00	0.03	1.66	2.78%				L
Sociotechnical Alignment	JSC	0.00	0.00	0.00	16.00	14.00	134.00	67.00	0.03	2.09	3.52%				H
	HAC	5.00	5.00	5.00	3.00	12.00	102.00	51.00	0.13	6.38	10.71%	10.71%	10.71%	LI	M
	SQ	0.00	0.00	0.00	8.00	22.00	142.00	71.00	0.17	11.83	19.89%	19.89%	19.89%	HI	M
System Characteristics (TAM2)															
Compatibility/Image (TAM2)	IHAC	1.00	5.00	7.00	4.00	13.00	113.00	56.50	0.17	9.42	15.82%	15.82%	15.82%	HI	M
Facilitating Conditions (UTAUT)	FC	0.00	0.00	1.00	10.00	19.00	138.00	69.00	0.03	2.30	3.87%	16.72%	3.34%	HI	H
	ERI	4.00	7.00	4.00	7.00	8.00	98.00	49.00	0.03	1.63	2.74%				L
	AIR	1.00	3.00	9.00	9.00	8.00	110.00	55.00	0.03	1.83	3.08%				L
	RAI	6.00	2.00	3.00	8.00	11.00	106.00	53.00	0.03	1.77	2.97%				L
	CSI	0.00	0.00	0.00	5.00	25.00	145.00	72.50	0.03	2.42	4.06%				H



ANNEXURE XV.G Union Bank – Indicators Severity Analysis comparative plot

XVI. ANNEXURE-XVI YES BANK (PRIMARY & SECONDARY DATA ANALYSIS SUMMARY)



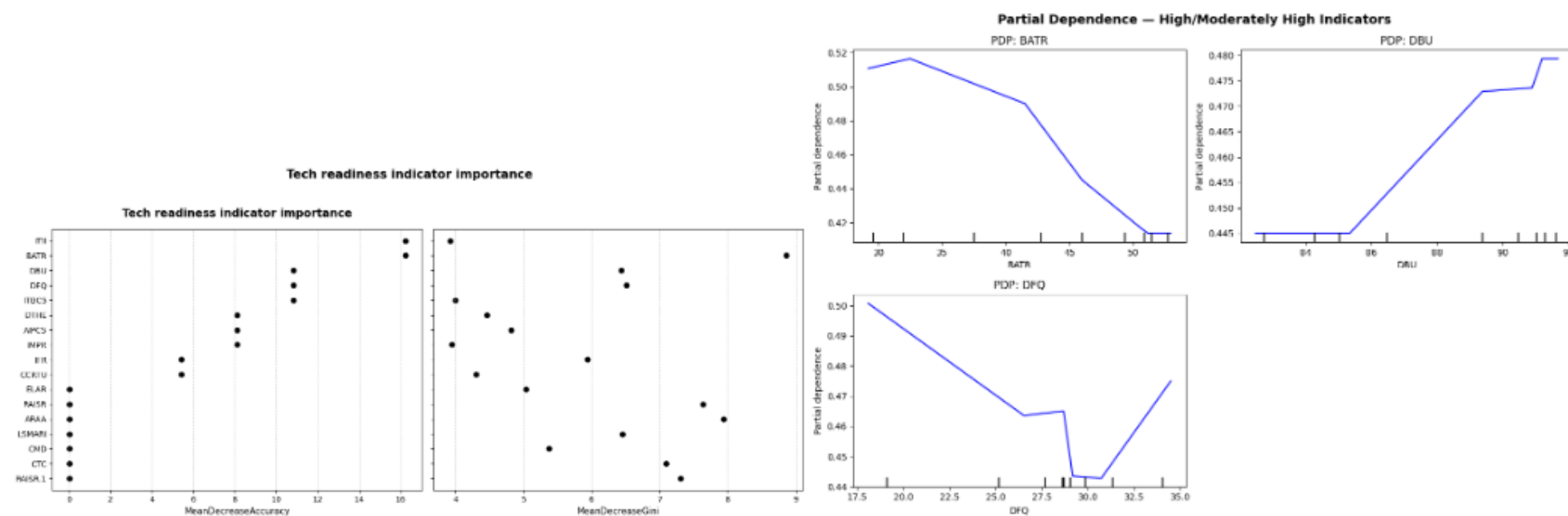
ANNEXURE XVI.A Yes Bank – Random Forest OOB error across mtry settings, 2020 Q1 to 2025 Q3

ANNEXURE XVI.B Yes Bank – Random Forest OOB Error versus Number of Trees, 2020 Q1 to 2025

ANNEXURE XVI.C Yes Bank – Random Forest-based prioritisation of indicators for Yes Bank with reconciled High, Moderate, and Low severity categories (conclusion derived from MDA and MDG)

Indicator	MDA	MDG	MDA%	MDG%	MDA_Severity	MDG_Severity	Conclusion
AIPCS	0.042857	0.047307	8.108108	4.816564	High	Low	Moderate
ARAA	0	0.077932	0	7.934695	Low	High	Moderate
BATR	-0.085714	0.086971	16.216216	8.85498	High	High	High
CCRTU	-0.028571	0.042217	5.405405	4.29832	Low	Low	Low
CMD	0	0.052793	0	5.375155	Low	Low	Low
CTC	0	0.06969	0	7.095515	Low	High	Moderate
DBU	-0.057143	0.063183	10.810811	6.43305	High	Moderate	Moderately High
DFQ	-0.057143	0.063941	10.810811	6.510161	High	Moderate	Moderately High
DTHE	0.042857	0.043821	8.108108	4.461696	High	Low	Moderate

ELAR	0	0.049452	0	5.035026	Low	Low	Low
IFR	0.028571	0.058316	5.405405	5.937515	Low	Moderate	Moderately Low
IMPR	-0.042857	0.038724	8.108108	3.942697	High	Low	Moderate
ITBCS	-0.057143	0.039267	10.810811	3.998016	High	Low	Moderate
ITII	0.085714	0.0385	16.216216	3.919958	High	Low	Moderate
LSMARI	0	0.063337	0	6.448719	Low	Moderate	Moderately Low
RAISR	0	0.074982	0	7.634343	Low	High	Moderate
RAISR.1	0	0.071733	0	7.303589	Low	High	Moderate

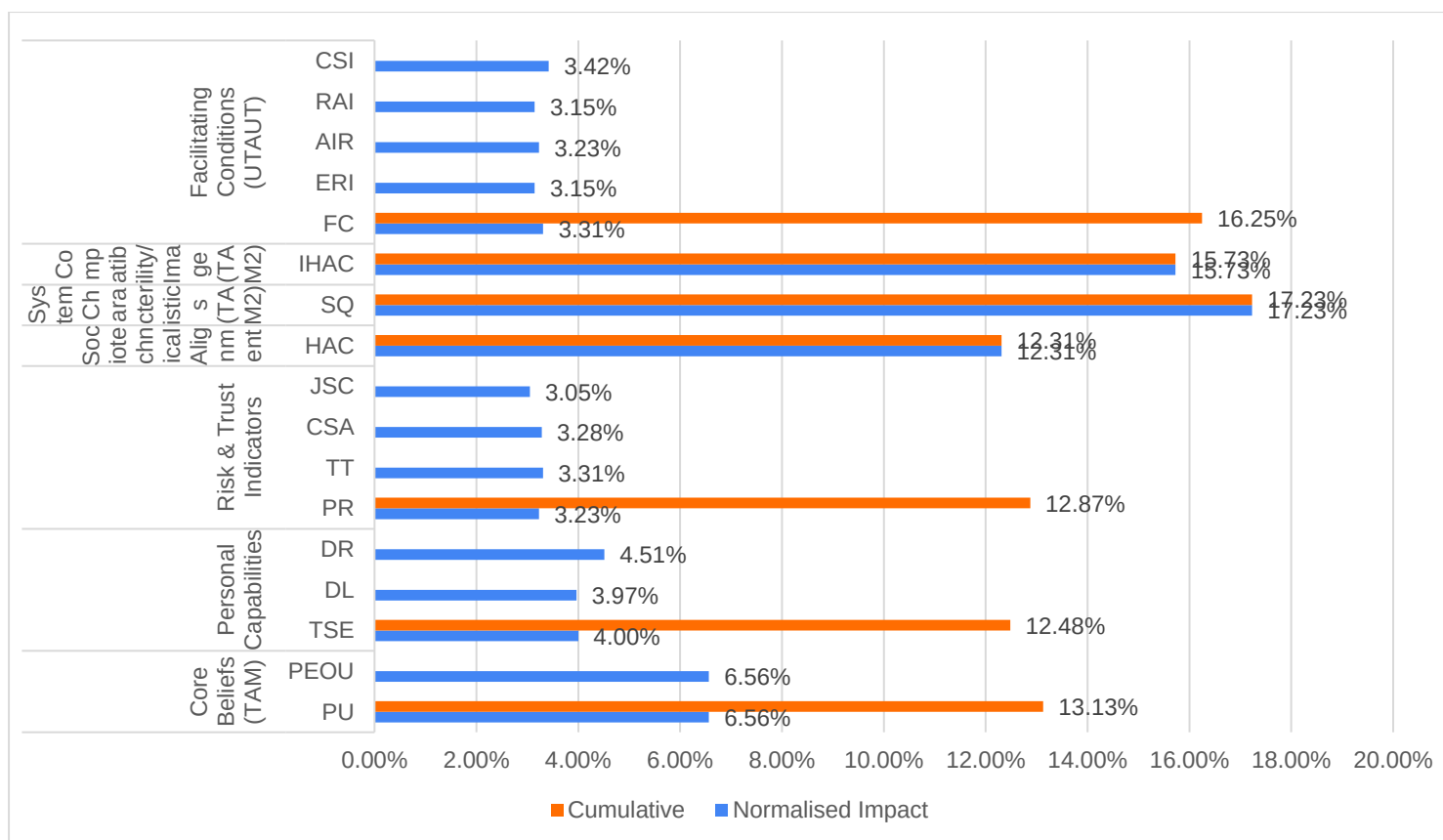


ANNEXURE XVI.D Yes Bank – Random Forest importance by Mean Decrease Accuracy and Mean Decrease Gini for Yes Bank, 2020 Q1 to 2025 Q3

ANNEXURE XVI.E Yes Bank - Partial dependence of DFQ, DBU and BATR, 2020 Q1 to 2025 Q3

ANNEXURE XVI.F Yes Bank – Variables Severity Analysis and Ranking

Core Element	Indicator	No of 1's	No of 2's	No of 3's	No of 4's	No of 5's	Weighted Sum	Weighted Average	Impact Rating	WA*I R	Normalised Impact	Normalised Impact		Weighted average		Level of sevtrity
Core Beliefs (TAM)	PU	0	0	2	3	22	128	4.27	0.063	0.267	0.066	6.6%	13.13%	6.56%	LI	M
	PEOU	0	1	2	15	12	128	4.27	0.063	0.267	0.066	6.6%				M
Personal Capabilities	TSE	0	2	9	9	10	117	3.90	0.042	0.163	0.040	4.0%	12.48%	4.16%	LI	L
	DL	1	1	5	17	6	116	3.87	0.042	0.161	0.040	4.0%				L
Risk & Trust Indicators	DR	0	1	2	11	16	132	4.40	0.042	0.183	0.045	4.5%				H
	PR	1	0	5	10	14	126	4.20	0.031	0.131	0.032	3.2%	12.87%	3.22%	LI	H
	TT	0	0	3	15	12	129	4.30	0.031	0.134	0.033	3.3%				H
	CSA	0	0	5	12	13	128	4.27	0.031	0.133	0.033	3.3%				H
	JSC	0	3	8	6	13	119	3.97	0.031	0.124	0.031	3.1%				L
Sociotechnical Alignment	HAC	1	2	5	10	12	120	4.00	0.125	0.500	0.123	12.3%	12.31%	12.31%	LI	M
System Characteristics (TAM2)	SQ	0	1	3	15	11	126	4.20	0.167	0.700	0.172	17.2%	17.23%	17.23%	HI	M
Compatibility/Image (TAM2)	IHAC	1	2	8	9	10	115	3.83	0.167	0.639	0.157	15.7%	15.73%	15.73%	HI	M
Facilitating Conditions (UTAUT)	FC	1	0	6	13	10	121	4.03	0.033	0.134	0.033	3.3%	16.25%	3.25%	HI	H
	ERI	2	2	6	9	11	115	3.83	0.033	0.128	0.031	3.1%				L
	AIR	2	1	8	5	14	118	3.93	0.033	0.131	0.032	3.2%				L
	RAI	2	2	7	7	12	115	3.83	0.033	0.128	0.031	3.1%				L
	CSI	2	0	5	7	16	125	4.17	0.033	0.139	0.034	3.4%				H



ANNEXURE XVI.G Yes Bank – Indicators Severity Analysis comparative plot

9. GLOSSARY

Artificial Intelligence (AI) – Systems that simulate human intelligence for decision-making, pattern recognition, and automation.

Machine Learning (ML) – Algorithms that learn from data to improve prediction and detection without explicit programming.

Financial Technology (FinTech) – Technology-driven innovation in financial services improving efficiency and accessibility.

Digital Banking – Delivery of banking services through digital platforms such as mobile and internet banking.

Core Banking Solutions (CBS) – Centralised systems enabling real-time banking transactions and customer data access.

Application Programming Interface (API) – Interface enabling communication and data exchange between systems.

Cybersecurity – Technologies and practices used to protect systems and data from cyber threats.

Fraud Detection Systems – Systems that identify and prevent fraudulent financial activities using data analytics and AI.

Operational Risk – Risk arising from failures in internal processes, people, or systems.

Risk Management – Process of identifying, assessing, and mitigating risks.

Digital Literacy – Ability to effectively use and understand digital technologies.

Technology Self-Efficacy (TSE) – Individual confidence in using technology.

Perceived Usefulness (PU) – Degree to which technology improves job performance.

Perceived Ease of Use (PEOU) – Degree to which technology is easy to use.

Perceived Risk (PR) – Likelihood of loss or negative outcomes from technology use.

Trust in Technology (TT) – Confidence in reliability and security of systems.

Digital Readiness (DR) – Preparedness of individuals and organisations to adopt technology.

Technology Adoption – Process of accepting and using new technologies.

Technology Acceptance Model (TAM) – Model explaining adoption based on usefulness and ease of use.

Extended Technology Acceptance Model (ETAM) – TAM extended with additional behavioural and contextual factors.

Unified Theory of Acceptance and Use of Technology (UTAUT) – Model explaining adoption through performance, effort, social, and facilitating conditions.

Human–AI Collaboration (HAC) – Interaction between human decision-making and AI systems.

System Quality (SQ) – Performance, reliability, and efficiency of technological systems.

Facilitating Conditions (FC) – Organisational and technical support enabling system use.

IT Infrastructure – Technological foundation including hardware, software, and networks.

Legacy Systems – Outdated systems limiting integration and innovation.

Cybersecurity Investment (CSI) – Resources allocated to strengthen security systems.

Regulatory Alignment (RAI) – Compliance with regulatory standards and guidelines.

Policy Compliance – Adherence to institutional and regulatory policies.

Predictive Analytics – Use of data and algorithms to forecast outcomes.

Fraud Intelligence – AI-driven capability to detect, analyse, and prevent fraud patterns.

Operational Resilience – Ability to prevent, respond to, and recover from operational disruptions.

Preparedness Index – Composite measure of readiness for technology adoption.

Enabler Preparedness Index (EPI) – Measure of institutional capability readiness.

User Preparedness Index (UPI) – Measure of employee-level readiness and adaptability.

Indicator Severity Analysis – Assessment of impact and importance of variables.

Mitigation Strategies – Actions designed to reduce risks and improve system readiness.

Reskilling – Training employees to acquire new technological competencies.

Upskilling – Enhancing existing skills for advanced technological use.

Data-Driven Decision Making – Use of analytics to support decisions.

10. ACRONYMS

AePS – Aadhaar-Enabled Payment System

AI – Artificial Intelligence

AIPCS – AI Policy Compliance Score

AIR – AI Infrastructure Readiness

AML – Anti-Money Laundering

API – Application Programming Interface

ARAA – Adoption Rate of FinTech/AI Applications

ATM – Automated Teller Machine

AUC – Area Under the Curve

Axis – Axis Bank

BAC – Bank Adaptability Classification

BATR – Budget Allocated to Tech Reskilling (%)

BFSI – Banking, Financial Services and Insurance

BIS – Bank for International Settlements

BLF – Bank-Level Factor

BOB – Bank of Baroda

BOMH – Bank of Maharashtra

CBDC – Central Bank Digital Currency

CBI – Central Bank of India

CBS – Core Banking Solutions

CCRTU – Customer Complaint Ratio on Tech Use

CERT-IN – Computer Emergency Response Team – India

CIO – Chief Information Officer

CISO – Chief Information Security Officer

CMD – Customer Migration to Digital Channels (%)

CRAR – Capital to Risk-Weighted Assets Ratio

CSA – Cybersecurity Awareness

CSI – Cybersecurity Investment

CSR – Corporate Social Responsibility

CTC – Cybersecurity Training Coverage

CTO – Chief Technology Officer

DBU – Digital Banking Usage (% of Total Transactions)

DCB – Development Credit Bank

DFQ – Downtime Frequency per Quarter

DITAF – Dual-Layer Integrated Tech Adaptability Framework

DL – Digital Literacy

DOI – Diffusion of Innovation Theory

DR – Digital Readiness

DSCI – Data Security Council of India

DTHE – Digital Training Hours per Employee

EDF – Employee Dominant Factor

EL – Enabler-Level

ELAR – Employee Layoff/Automation Ratios

EPI – Enabler Preparedness Index
ERI – Employee Reskilling Investment
ETAM – Extended Technology Acceptance Model

FC – Facilitating Conditions
FGD – Focus Group Discussion
FICCI – Federation of Indian Chambers of Commerce and Industry
FinTech – Financial Technology
FN – False Negative
FNR – False Negative Rate
FP – False Positive
FPR – False Positive Rate
FY – Financial Year

GDP – Gross Domestic Product

HAB – Highly Adaptable Bank
HAC – Human–AI Collaboration
HAD – Highly Adaptable (primary classification)
HDFC – Housing Development Finance Corporation Bank
HR – Human Resources

IAMAI – Internet and Mobile Association of India
IB – Indian Bank
IBA – Indian Banks' Association
ICICI – Industrial Credit and Investment Corporation of India Bank
IDBI – Industrial Development Bank of India
IDFC – IDFC First Bank
IDRBT – Institute for Development and Research in Banking Technology
IFR – Incidence of Fraud Reports
IHAC – Human–AI Collaboration (Institutional)
ILO – International Labour Organization
IMPR – Internet and Mobile Penetration Rates
IMPS – Immediate Payment Service
IndusInd – IndusInd Bank
IOB – Indian Overseas Bank
IoT – Internet of Things
ISB – Indian School of Business

IT – Information Technology
ITBCS – IT Budget for Cybersecurity (%)
ITII – IT Infrastructure Index

JSC – Job Security Concerns

Kotak – Kotak Mahindra Bank
KPI – Key Performance Indicator
KYC – Know Your Customer

LAB – Low Adaptability Bank
LAD – Least Adaptable (primary classification)
LMS – Learning Management System
LSMARI – Legacy Systems Migrated to Tech-Ready Infrastructure (%)

MAB – Moderately Adaptable Bank
MAD – Moderately Adaptable (primary classification)
MDA – Mean Decrease Accuracy
MDG – Mean Decrease Gini
MeitY – Ministry of Electronics and Information Technology
ML – Machine Learning
mtry – Variables Randomly Sampled at Each Split

NASSCOM – National Association of Software and Service Companies
NCRB – National Crime Records Bureau
NEFT – National Electronic Funds Transfer
NIST – National Institute of Standards and Technology
NITI Aayog – National Institution for Transforming India
NLP – Natural Language Processing
NN – Neural Network
NPA – Non-Performing Asset
NPCI – National Payments Corporation of India
NSSO – National Sample Survey Office

OOB – Out-of-Bag Error
OECD – Organisation for Economic Co-operation and Development
OTP – One-Time Password

PDP – Partial Dependence Plot
PEOU – Perceived Ease of Use
PI – Preparedness Index
PR – Perceived Risk
PU – Perceived Usefulness
PWC – PricewaterhouseCoopers

Q1–Q4 – Quarter 1 to Quarter 4

RAI – Regulatory Alignment
RAISR – Ratio of AI-Supported Job Roles
RBI – Reserve Bank of India
RegTech – Regulatory Technology
RF – Random Forest
ROI – Return on Investment
RTGS – Real-Time Gross Settlement

SBI – State Bank of India
SEBI – Securities and Exchange Board of India
SLA – Service Level Agreement
SME – Small and Medium Enterprises
SQ – System Quality

SQL – Structured Query Language
SVM – Support Vector Machine
SWIFT – Society for Worldwide Interbank Financial Telecommunications

TAM – Technology Acceptance Model
TAM2 – Technology Acceptance Model 2
TAP – Technological Adaptability
TCS – Tata Consultancy Services
TN – True Negative
TNR – True Negative Rate
TOE – Technology–Organisation–Environment Model
TP – True Positive
TPR – True Positive Rate
TRAI – Telecom Regulatory Authority of India
TSE – Technology Self-Efficacy
TT – Trust in Technology

UCO – UCO Bank
UDI – User Dominant Indicators
UI – User Interface
Union – Union Bank of India
UPI – Unified Payments Interface
URI – User Readiness Indicators
UTAUT – Unified Theory of Acceptance and Use of Technology
UX – User Experience

VIM – Variable Importance Measure

WEF – World Economic Forum

XAI – Explainable Artificial Intelligence

Yes Bank – Yes Bank Limited
YONO – You Only Need One (SBI Digital Platform)

Disclaimer- For language editing, grammar checking, and proofreading, the authors employed Grammarly platform.

11. PROJECT COMPLETION TIMELINE (GANTT CHART)

Activity	Ist Month				IInd Month				IIInd Month				IVth Month				VthMonth				VIth Month			
Week	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8	Week 9	Week 10	Week 11	Week 12	Week 13	Week 14	Week 15	Week 16	Week 17	Week 18	Week 19	Week 20	Week 21	Week 22	Week 23	Week 24
Literature Review	Challenge Indicator identification in Banks under AI/Tech Innovation																							
		Theory Confirmation and Indicator Mapping within Theory																						
Data Collection			Secondary Data Collection from Respective sources for slected banks and Indicators.	Questionnaire Design and Perform Pilot study		Response Collection and Data Entry																		
Challenge Drivers Identification								Validate based on Primary Survey from Experts and Further using Z score calculation confirm the Indicators for Indian Context																
Assessment/Prioritisation of banks from perspective of Secondary Data											Perform Secondary data analysis using Machine learning model. Choose the model and report final results based on Machine learning analysis and respective prime causes across selectd banks													
Assessment/Prioritisation of banks from the perspective of PrimaryData														using averaging techniques. Classify banks under low, moderate and High categories. Also calculate different banks AI preparedness index and respective causing drivers.										
Suggestion of mitigation Framework from Enabler and User Perspective																Suggest Mitigation Measures for the respective Enabler and User Challenges and create integration based on root causes								
Report Writing and Report Submission																		Report writing Integration and Referencing and submission						