International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

The Human Microfoundations Of Digital Trust In Open Banking: A Constructivist Grounded Theory Study Of Strategic HRM Routines

Diane Natalin Datuallo[1], David Paul Elia Saerang SE, M. Com (Hons)[2], Djurwati Soepeno[3], Rudy Steven Wenas[4]

[1]Program Doctor Management Science, Sam Ratulangi University, Indonesia
[2]Faculty of Economics and Business, Sam Ratulangi University, Indonesia
[3]Faculty of Economics and Business, Sam Ratulangi University, Indonesia
[4]Faculty of Economics and Business, Sam Ratulangi University, Indonesia

Corresponding Author: (natalindiane@gmail.com)

Abstract

Open banking intensifies the dependence of financial service ecosystems on customer-permissioned data sharing, application programming interfaces, third-party partnerships, and visible organizational trustworthiness. Policy and technical literature usually treats this problem through regulation, interoperability, consent architecture, and security standards. This article shifts attention to the human microfoundations through which digital trust becomes actionable inside organizations. Drawing on Constructivist Grounded Theory in the Charmaz tradition, the study analyzes two rounds of qualitative interviews with 16 organizational actors involved in open banking and open-banking-adjacent digital banking work across HR, digital banking/fintech operation, compliance/risk, IT governance/cybersecurity, and customer experience/partnership functions. The second round used grand tour questions and critical incident technique to probe contradictions, negative cases, shadow routines, and trust breakdown events. The analysis develops a substantive grounded model in which digital trust emerges through contested strategic HRM routines rather than through formal policy or technical design alone. Four interlocking processes explain this formation: translating regulatory abstraction into situated training and communication routines; disciplining shadow routines that bypass formal controls; orchestrating cross-functional crisis work across organizational and ecosystem boundaries; and converting complaints, audits, and

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

incidents into trust repair. The study contributes to open banking research by theorizing digital trust as a fragile organizational accomplishment, to strategic HRM by showing how HRM routines operate as behavioural trust infrastructure, and to microfoundations research by identifying the individual, interactional, and structural mechanisms through which ecosystem trust is built, damaged, and repaired.

Keywords: open banking; digital trust; strategic HRM; human microfoundations; constructivist grounded theory; cybersecurity culture; financial ecosystems

INTRODUCTION

Open banking has altered the organizational grammar of financial services. Banks increasingly operate through API-enabled ecosystems in which customer-permissioned data moves among banks, fintech firms, payment providers, and customer-facing service units. Policy reports frame this shift as a route to competition, portability, innovation, and financial inclusion, while technical literature defines open banking as a data-sharing ecosystem governed through standards, security profiles, consent, and application programming interfaces (Basel Committee on Banking Supervision, 2019; Laplante & Kshetri, 2021; OECD, 2023a, 2023b; World Bank, 2022). In Indonesia, the National Open API Payment Standard, or SNAP, makes this ecosystem problem concrete because it standardizes open API payments while also pushing banks to align governance, security, partnership routines, and operational readiness (Bank Indonesia, 2021, 2023).

This ecosystem logic creates a difficult trust problem. Customers share data only when they believe that the organization and its partners can protect privacy, maintain service reliability, and explain digital failures transparently. Recent empirical work on open banking adoption shows that perceived risk, initial trust, privacy concerns, and financial literacy shape consumer willingness to use open banking services (Chan et al., 2022; Polasik & Kotkowski, 2022). Broader fintech research reaches a similar conclusion: trust and security consistently operate as central adoption mechanisms, not peripheral attitudes (Jafri et al., 2024; Zhang et al., 2023). Yet these studies usually model trust at the customer level. They explain whether users trust, but say less about how employees inside banks and fintech-connected organizations enact the routines that make trust operationally plausible.

Policy and supervisory literature highlights the same problem from another angle. Open finance expands data portability and customer choice, but it also increases interdependence, third-party reliance, consent-management complexity, operational risk,

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

and reputational exposure (Basel Committee on Banking Supervision, 2024; CCAF, 2024; OECD, 2023a, 2023b; World Bank, 2022). The Basel Committee argues that digitalisation changes the nature and scope of banking risks because new technologies and external providers reshape operational, strategic, and reputational vulnerabilities (Basel Committee on Banking Supervision, 2024). NIST Cybersecurity Framework 2.0 likewise places governance, role clarity, response, and recovery at the centre of cybersecurity risk management, signalling that technical controls need organizational routines to work (National Institute of Standards and Technology [NIST], 2024).

Existing open banking literature therefore leaves a specific gap. It has explained API architecture, consumer adoption, consent, privacy, competition, and fintech entry more convincingly than it has explained the human and organizational work through which trust becomes a daily practice (Babina et al., 2024; Chan et al., 2022; Laplante & Kshetri, 2021; OECD, 2023a; World Bank, 2022). Banking HRM literature recognizes the need for reskilling, upskilling, redeployment, and workforce agility in Banking 4.0, but it rarely connects those HRM routines to open banking trust breakdowns, shadow routines, risk reporting, or crisis repair (Kuchciak & Warwas, 2021; Vial, 2019). Strategic HRM research has long argued that HR systems shape employee capabilities and behavioural expectations (Becker & Huselid, 2006; Bowen & Ostroff, 2004; Wright & McMahan, 1992), but we still know little about how such routines operate when banks must balance API speed, cybersecurity discipline, compliance demands, and customer-facing trust.

This article addresses that blind spot through a Constructivist Grounded Theory study of strategic HRM routines in open banking. It asks: How do strategic HRM routines shape the human microfoundations of digital trust in open banking? The question treats trust as more than a customer perception and more than a security feature. It treats trust as a contested organizational accomplishment produced through the interaction of HR, digital banking, IT governance, compliance, risk management, customer experience, and fintech partnership work.

The study develops the core category of contested HRM routines as human microfoundations of digital trust. The argument is deliberately critical. HRM routines do not simply create trust through training, mentoring, digital mindset programmes, and performance indicators. They also expose the fragility of trust when employees use shared accounts, send data through private channels, rely on unofficial workarounds, or avoid reporting mistakes because psychological safety feels incomplete. This move extends microfoundations theory, which explains how macro-level capabilities rest on individual action, social processes, and structures (Felin et al., 2012), and organizational

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

routines theory, which treats routines as both stabilizing and changeable through situated performance (Feldman & Pentland, 2003).

The article contributes in three ways. First, it reframes digital trust in open banking as an enacted, contested, and repaired organizational process rather than a stable product of regulation or technology. Second, it extends strategic HRM by theorizing HRM routines as behavioural trust infrastructure in data-sharing ecosystems. Third, it adds a grounded model of trust breakdown and trust repair, showing how speed-control tensions, shadow routines, fragile psychological safety, and cross-functional crisis work shape the human microfoundations of open banking governance.

LITERATURE BACKGROUND

Open banking, API ecosystems, and the trust problem

Open banking refers to customer-permissioned data sharing among banks, fintech firms, and other regulated or authorized third parties through secure digital interfaces. Technical and policy definitions vary, but they converge on three building blocks: customer consent, standardized data access, and secure API-based connectivity (Basel Committee on Banking Supervision, 2019; Laplante & Kshetri, 2021; World Bank, 2022). OECD work extends this view toward open finance, where data-sharing frameworks expand beyond payment and account data into wider financial services, thereby increasing both innovation potential and governance complexity (OECD, 2023a, 2023b).

The promise of open banking depends on trust because customers must permit data access and tolerate new forms of inter-organizational dependence. Chan et al. (2022) show that open banking adoption requires models that include perceived risk, initial trust, and financial literacy. Polasik and Kotkowski (2022) similarly place privacy and trust at the centre of European open banking adoption. Jafri et al. (2024), in a systematic review of fintech adoption in banking, confirm that trust and security repeatedly function as key adoption determinants. These findings explain why trust matters, yet they mainly treat trust as a user-side perception or intention.

The organizational side remains underdeveloped. Open banking infrastructures require banks to coordinate consent, access rights, partner governance, customer communication, API availability, cybersecurity controls, and service recovery. Babina et al. (2024) show that open banking policies expand fintech entry and customer data access, which means banks must govern new competitive and operational relationships. The Cambridge Centre for Alternative Finance (CCAF, 2024) also reports that open banking and open finance require trust, data protection, standards, and ecosystem

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

coordination. These insights suggest a research gap: open banking trust depends not only on consumers' beliefs, but also on the internal routines that employees use to protect, explain, and repair data-sharing services.

Indonesia makes this gap especially relevant. SNAP institutionalizes a national open API payment standard and signals that API-enabled financial services require common standards, secure integration, and coordinated implementation (Bank Indonesia, 2021, 2023). Nevertheless, standards do not automatically generate trustworthy conduct. Employees still translate rules, operate systems, respond to customers, coordinate with partners, and decide whether to follow or bypass formal procedures. This article therefore moves from open banking as a technical ecosystem to open banking as a humanly enacted trust regime.

Strategic HRM routines as behavioural trust infrastructure

Strategic HRM provides the theoretical basis for analyzing how organizations translate strategic demands into employee capabilities and behaviours. Wright and McMahan (1992) define strategic HRM around planned human resource deployments that enable organizational goals. Becker and Huselid (2006) sharpen this view by connecting HR architecture to strategic performance. Bowen and Ostroff (2004) argue that HRM systems become powerful when employees perceive them as distinctive, consistent, and consensual. In open banking, these assumptions matter because digital trust requires employees to receive clear signals about data protection, service reliability, communication, accountability, and escalation.

Banking digitalization raises the stakes of HRM. Kuchciak and Warwas (2021) argue that HRM in Banking 4.0 must address reskilling, upskilling, redeployment, and new competency portfolios. Vial (2019) defines digital transformation as a process that changes organizations through digital technologies and strategic responses. These accounts show that digital change does not only install new systems. It reshapes work, coordination, competence, and organizational design. Nevertheless, much digital HRM discussion remains broad: it speaks about agility, skills, analytics, and transformation, but less about the specific behavioural routines through which bank employees protect customer-permissioned data and repair trust after service breakdowns.

This study conceptualizes strategic HRM routines as behavioural trust infrastructure. Training, mentoring, e-learning, onboarding, simulations, performance indicators, and crisis briefings become trust infrastructure when they transform abstract requirements into repeatable conduct. In the interviews, HR participants translated legal

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

phrases such as limited access into concrete rules such as do not use personal email for customer data. This translation work fits Bowen and Ostroff's (2004) argument about HRM system strength because employees act on signals they can understand and reconcile across units. It also extends Kuchciak and Warwas (2021) by showing that reskilling in banking must include risk discipline, communication scripts, and trust-repair competence, not only digital tool proficiency.

Digital trust, privacy, and cybersecurity culture

Digital trust research often begins from classic organizational trust theory. Mayer et al. (1995) define trust as willingness to accept vulnerability based on expectations of another party's ability, benevolence, and integrity. McKnight et al. (2002) adapt trust to technology-mediated environments by distinguishing trusting beliefs, trusting intentions, and institution-based assurances. In digital financial services, these dimensions become tangible when customers judge whether a bank can secure data, communicate truthfully, and correct service failures.

Recent privacy and digital technology research also complicates trust. Quach et al. (2022) show that digital technologies create tensions between data-driven value creation and privacy expectations. In open banking, this tension intensifies because value creation depends on data mobility, but trust depends on data restraint, consent clarity, and accountability. The World Bank's work on consumer consent in open banking similarly stresses that consent protocols must specify who accesses data, for what purpose, for how long, and under what revocation conditions (World Bank, 2022).

Cybersecurity literature strengthens the argument that technical controls need behavioural reinforcement. ENISA (2018) treats cybersecurity culture as an organizational problem that requires awareness, behaviour change, leadership, and practical tools. NIST (2024) organizes cybersecurity around govern, identify, protect, detect, respond, and recover functions, which places roles, responsibilities, communication, and recovery inside cybersecurity governance. These frameworks support this article's focus on employee conduct: MFA, audit logs, access control, and API security matter, but employees still decide whether to share passwords, open phishing links, move data to private devices, or follow escalation procedures.

Human microfoundations and organizational routines

The microfoundations perspective explains how organizational capabilities rest on individual actions, interaction patterns, and structures (Felin et al., 2012). This article

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

applies that logic to digital trust. Open banking trust appears at ecosystem level, but its microfoundations reside in employees who interpret rules, managers who enforce or soften sanctions, IT staff who impose controls, compliance actors who delay launches, and customer-facing staff who absorb customer anger during failures.

Organizational routines theory helps explain why formal rules and lived practices diverge. Feldman and Pentland (2003) distinguish between the ostensive aspect of a routine, or the abstract pattern, and the performative aspect, or what people actually do in situated practice. Pentland and Feldman (2005) further show that routines include artifacts that mediate action. In open banking, SOPs, training modules, checklists, audit logs, CRM updates, and communication scripts all function as artifacts. They do not guarantee compliance. Employees still perform the routine under pressure, friction, incomplete information, and customer urgency.

This distinction creates space for shadow routines. Reason (1997) explains that organizational accidents often emerge from interactions between latent conditions and active failures. In this article, shadow routines such as shared logins, WhatsApp transfers, personal laptops, private email, and Excel files reveal latent design weaknesses in formal work systems. The problem does not sit only inside individual noncompliance. It emerges when official routines feel too slow, too complex, or insufficiently aligned with customer-facing work.

Psychological safety, accountability, and trust repair

Psychological safety matters because open banking organizations need employees to report errors before they escalate into trust breakdowns. Edmondson (1999) defines team psychological safety as a shared belief that a team is safe for interpersonal risk taking. Later work on teaming and learning emphasizes that psychological safety does not remove accountability; it creates conditions for speaking up, learning, and coordinated correction (Edmondson, 2012).

Open banking complicates psychological safety because data errors, privacy breaches, and API failures carry reputational and regulatory consequences. Employees hear formal messages about learning, but they also observe transfers, warnings, stigma, or blame. Faraj and Xiao (2006) show that fast-response organizations rely on expertise coordination and dialogic coordination under pressure. This insight fits open banking crisis work: customer experience, IT, compliance, HR, and digital banking must coordinate quickly when customers blame the organization for failures caused by internal systems or third-party providers.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Trust repair literature also helps interpret the findings. Kim et al. (2004) show that responses to trust violations depend on violation type and repair strategy, while Gillespie and Dietz (2009) argue that organizational trust repair requires diagnosis, reform, communication, and credible change. This article adds an HRM mechanism: organizations repair digital trust when they convert incidents into revised training, stricter access routines, better scripts, improved escalation channels, and more credible reporting cultures.

METHODOLOGY

Research design

The study adopted Constructivist Grounded Theory in the Charmaz tradition. CGT fits the research aim because the study seeks to construct a substantive explanation of how organizational actors enact digital trust through work routines. Charmaz (2014) treats grounded theory as systematic yet flexible; researchers do not discover a theory that sits untouched in the data, but construct analytic categories through interaction with participants, empirical material, comparison, and memo writing. This orientation matches the study's interest in how HR, IT, compliance, digital banking, risk, partnership, and customer-facing actors interpret and negotiate trust-related work.

The study did not use systematic grounded theory in the Strauss and Corbin tradition as the primary design. The analysis considered conditions, strategies, and consequences, but it did not impose a paradigmatic model at the outset. Instead, the analytical movement followed CGT principles: close initial coding, focused coding, constant comparison across functions, theoretical memoing, attention to negative cases, and progressive category refinement.

Participants and empirical setting

The empirical material came from 16 organizational actors involved in open banking or open-banking-adjacent digital banking work. Participants represented five functional clusters: HR/digital HR, digital banking/fintech operation and partnership, compliance/risk management, IT governance/cybersecurity, and customer experience/partnership. The study used role-based codes to protect confidentiality. The setting reflects a financial services environment in which API integration, digital banking features, fintech partnerships, customer data protection, and service communication had become routine organizational concerns.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

Table 1. Participant profile

Cluster	Participant codes	Number	Analytical relevance
Human Resources / Digital HR	HR_1, HR_2, HR_3	3	Digital reskilling, training design, performance indicators, mentoring, HRM response to behavioural failure
Digital Banking / Fintech Operation / Partnership	DB_1, DB_2, DB_3, DB_4	4	Feature launches, API integration pressure, fintech coordination, customer communication, speed-control tension
Compliance / Risk Management	CR_1, CR_2, CR_3	3	Regulatory translation, risk assessment, privacy, audit, reporting culture, psychological safety
IT Governance / Cybersecurity	IT_1, IT_2, IT_3	3	Cybersecurity awareness, access discipline, audit logs, MFA, behavioural vulnerabilities
Customer Experience / Partnership	CX_1, CX_2, CX_3	3	Customer anger, inconsistent information, crisis scripts, partner-related service failures

Data collection and theoretical probing

Data collection unfolded in two rounds. The first round used a structured interview guide with 12 core questions that all participants answered. These questions addressed the meaning of digital trust, trust determinants, required employee competence, competence development, risk-related routines, cross-functional coordination, innovation-control tension, learning from complaints, trust-supporting conduct, organizational weaknesses, and future strengthening needs. This round generated a broad map of routine trust work.

The second round operated as follow-up theoretical probing. After the first round revealed recurring themes around training, risk awareness, coordination, and learning, the follow-up round used grand tour questions and critical incident technique to probe concrete events. Participants reconstructed daily routines during open banking feature

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

launches, narrated clashes between business speed and compliance caution, described unit-level friction, and identified negative cases such as workarounds, shared logins, private email transfers, flashdisk use, weak communication flows, and fragile psychological safety. This second round significantly sharpened the analysis because it moved the data from normative descriptions of ideal routines to incidents where those routines failed, were contested, or had to be repaired.

Table 2. Data rounds and analytical purpose

Data round	Focus	Analytical contribution
Round 1: structured core interviews	Digital trust meanings, HRM routines, competence, risk awareness, coordination, learning from complaints	Mapped recurring routine practices and generated initial codes
Round 2: follow-up critical incidents	Grand tour routines, speed-control paradox, inter-unit friction, third-party failures, shadow routines, trust breakdowns	Generated negative cases, refined theoretical categories, and shifted the core category toward contested HRM routines

Data analysis

The analysis moved through four stages. First, initial coding stayed close to participants' words and actions. Codes included translating regulation into training, delaying launch for audit, briefing customer service, sharing login credentials, sending data through private channels, protecting fintech partners publicly, transferring an employee after a data leak, forcing MFA compliance, revising scripts after inconsistent customer information, and turning complaints into simulations.

Second, focused coding grouped the strongest and most frequent codes. The analysis compared HR accounts with IT, compliance, digital banking, and customer experience accounts. This comparison showed that HRM routines were not confined to HR. They appeared in IT training materials, compliance communication, digital banking launch routines, customer service scripts, and crisis briefings. Third, theoretical coding connected focused codes into higher-order categories. Fourth, memo writing developed the core category. The initial core category, HRM-enabled trust work, proved too positive after the second round. Negative cases showed that trust was not only enabled; it was

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

contested, damaged, exposed, and repaired. The final core category became contested HRM routines as human microfoundations of digital trust.

Table 3. Coding movement from empirical incidents to theoretical categories

Empirical indicators	Initial codes	Focused codes	Theoretical category
Regulation on limited access translated into "do not use private email", "do not store data on personal devices", and simple frontliner modules	Translating legal abstraction into practical rules	Making regulation actionable	Translating regulatory abstraction into situated HRM routines
Business and fintech partners pushed rapid launch; compliance, risk, or IT required audits, security checks, or limited trials	Delaying launch; negotiating pilot; mediating partner pressure	Managing speed-control collision	Managing the speed-control paradox
Shared logins, WhatsApp transfers, private laptops, Excel files, flashdisks, private email, assumed answers to customers	Bypassing formal systems; normalizing shortcuts	Exposing shadow routines	Disciplining hidden behavioural risk
Customer service absorbed customer anger during vendor outages, bugs, or delayed IT updates	Frontliners absorbing crisis; protecting partner publicly	Orchestrating crisis response	Cross-functional trust repair work
Employees reported data mistakes but later received hard warnings, transfer, or reputational harm	Learning rhetoric; punitive residue	Testing psychological safety	Fragile reporting culture
Training changed after incidents; MFA became access condition; scripts standardized; SOPs revised after audits and complaints	Revising routines after failure	Reconstructing HRM after breakdown	Feedback-based trust repair

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Trustworthiness and ethical safeguards

Trustworthiness was strengthened through functional triangulation, constant comparison, negative-case analysis, and transparent coding movement. Functional triangulation came from comparing participants across HR, digital banking, compliance/risk, IT governance, and customer-facing roles. Constant comparison examined whether claims about training, coordination, and trust held across functions or changed when participants discussed concrete incidents. Negative-case analysis played a decisive role. Accounts of workarounds, incomplete psychological safety, customer anger, and post-incident restructuring prevented the analysis from presenting a managerial success story. They forced the grounded model to explain both trust formation and trust breakdown.

Ethically, the article anonymizes participants through role-based codes and avoids identifying organizations, partners, customers, or confidential systems. The interviews did not request technical vulnerabilities, system architecture, API configurations, or customer records. The quotations in the findings are edited lightly for readability and translated into English where necessary, without changing their substantive meaning.

Findings

The analysis generated one core category and six theoretical categories. The core category is contested HRM routines as human microfoundations of digital trust. This category captures the central finding that digital trust in open banking is built through routines that remain inherently contested: between speed and control, training and actual conduct, psychological safety and reputational risk, formal SOPs and shadow practices, customer-facing transparency and partner protection. The six theoretical categories explain how this core process unfolds.

Core category: contested HRM routines as human microfoundations of digital trust

Participants did not describe digital trust as a fixed organizational asset. They described it as work that employees had to perform under pressure. HR participants linked trust with digital competence, accountability, and mindset. IT participants linked trust with employee discipline in password use, access control, phishing awareness, and secure data handling. Compliance participants linked trust with regulation, privacy, and reporting culture. Customer-facing participants linked trust with consistent information and rapid response when customers became angry.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

However, the follow-up interviews showed that this work remains contested. HR_1 described daily launch routines that involved training preparation, IT coordination, and compliance meetings, but also noted that a launch had been delayed by two weeks because compliance required additional security testing. DB_1 described a similar event: the business unit wanted API integration within two weeks, while compliance required additional audit work. IT_1 framed the same type of clash as a security checklist problem. CX_1 described its customer-facing consequence: customer service had to face disappointed customers after compliance delayed a launch.

These accounts show that digital trust is not produced by one function. It emerges through negotiated routines. HRM becomes central because it translates the outcomes of those negotiations into training schedules, communication scripts, performance expectations, escalation practices, crisis briefings, and post-incident learning. The core category therefore does not mean that HR controls digital trust. It means that HRM routines give contested trust requirements a behavioural form.

Translating regulatory abstraction into situated HRM routines

The first theoretical category concerns translation. Participants repeatedly argued that regulatory and cybersecurity expectations enter organizations as abstract requirements. Employees rarely act on abstraction. They act on situated instructions, examples, scripts, and sanctions. HR_1 described translating a rule about limited access into a simple behavioural instruction: do not use private email for customer data. HR_2 described turning access rights into practical guidance about who may view data and who may not. HR_3 described translating data storage rules into a clear prohibition on saving data in personal devices.

One HR participant stated:

> *Regulation about limited access sounded too legalistic for many employees. We changed it into concrete examples: who can see customer data, who cannot, and why private devices cannot be used.*

The translation process was not only linguistic. It was pedagogical and behavioural. Participants described infographics, practical simulations, mentoring, e-learning, weekly discussions, and case-based training. HR_1 explained that employees often perceived rules as too theoretical, so the organization used simulations to make risks visible. Compliance and risk participants echoed this concern. CR_2 described explaining privacy risk through simple examples such as not sending customer data

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

through private email. IT_1 used the analogy of a password as a house key to make cybersecurity concrete for non-technical employees.

This category clarifies why strategic HRM routines matter in open banking. Open banking governance contains complex legal and technical language, yet customer trust depends on ordinary employees performing simple but disciplined actions. HRM routines become the translation layer between policy abstraction and everyday conduct. Without this layer, digital trust remains formal rather than enacted.

Managing the speed-control paradox

The second category concerns the speed-control paradox. Across functions, participants described a recurrent collision between the pressure to launch open banking features quickly and the need to satisfy regulatory, risk, and security controls. Digital banking and fintech partnership participants felt partner and business pressure most directly. Compliance, risk, and IT participants felt accountable for preventing unsafe launches. HR and customer service then absorbed the consequences through rescheduled training, employee frustration, customer disappointment, or partner dissatisfaction.

DB_4 described the pattern succinctly: fintech partners wanted rapid launch, while IT resisted fast integration. DB_1 narrated a case where a fintech partner pushed for a payment feature but IT identified a security concern. The organization mediated the conflict through a limited pilot rather than full deployment. Compliance participants described similar outcomes: business units often wanted API launch within short timelines, but additional audits forced postponement. One compliance participant noted that business disappointment was preferable to regulatory sanctions.

The speed-control paradox matters theoretically because it reveals digital trust as a negotiated settlement. Trust requires innovation because customers and partners expect responsive digital services. Trust also requires restraint because premature launch can expose data, create transaction failures, or damage confidence. Strategic HRM routines enter this paradox by preparing employees for delays, retraining frontliners when timelines shift, and communicating why caution is not resistance to innovation but part of trust-building.

Disciplining shadow routines behind digital trust failure

The third category is the most critical: shadow routines. Follow-up interviews revealed that formal routines often coexist with informal shortcuts. Employees used

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

shared accounts to speed up work, sent data through private email or WhatsApp, copied data to personal flashdisks, stored data in Excel files, opened files on private laptops, or answered customers based on assumptions when no official script existed. These practices were not always acts of malicious resistance. Participants usually described them as pragmatic attempts to keep work moving when official systems were slow, cumbersome, or incomplete.

HR_1 described a case where an employee who had completed security training still sent customer files through WhatsApp. HR_2 reported a similar case involving a personal laptop. IT_1 described shared password behaviour detected through audit logs. CR_1 noted that frontliners sometimes stored customer data in personal Excel files because the formal system felt inefficient. CX_1 described a different form of shadow routine: when official updates were delayed, frontliners improvised answers to customers, creating inconsistent information.

A participant's account captured the contradiction clearly:

> *Management knew that some people used shortcuts. The official system was slow, so people used email, WhatsApp, or one shared login. Everyone knew it was wrong, but work still had to move.*

This finding shifts the article beyond a conventional HRM optimism. Training and SOPs do not automatically eliminate human risk. They can also expose the mismatch between formal compliance and operational reality. Shadow routines emerge when formal systems impose a friction cost that employees treat as higher than the perceived risk of bypassing them. Digital trust weakens at exactly this point: the organization appears compliant from the outside, while employees internally normalize practices that undermine data protection and accountability.

Questioning psychological safety in risk reporting

The fourth category concerns the fragility of psychological safety. In the first interview round, several participants stated that the organization encouraged reporting errors as learning rather than punishment. The second round complicated this claim. Compliance and risk participants acknowledged that employees who reported data mistakes could still suffer reputational damage, strong warnings, or transfer to another unit. CR_1 described a case where an employee reported a data leak but later experienced reputational consequences and movement to another unit. CR_2 described

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

hard warnings after a reported incident. CR_3 similarly stated that the culture of 'learning, not punishment' was not fully real.

This finding does not mean that the organization had no learning culture. Rather, it shows that psychological safety was partial. Employees might formally be invited to report errors, but they still interpret the informal career consequences of reporting. This matters for digital trust because open banking depends on early error detection. If employees fear reputational harm, they may hide mistakes until customers or partners discover the problem.

The category also extends strategic HRM theory. Accountability routines must balance discipline and learning. Too little discipline normalizes shadow routines. Too much punishment suppresses error reporting. Strategic HRM in open banking therefore has to build credible reporting routines where employees expect correction, retraining, and proportional accountability rather than either impunity or reputational destruction.

Orchestrating cross-functional crisis work

The fifth category concerns cross-functional crisis work. Participants consistently reported that customers rarely distinguish between internal system failures, partner system failures, API bugs, or compliance delays. When a digital service fails, customer service becomes the visible face of the ecosystem. CX_1 stated that customers do not care whether the problem came from a partner API or an internal server. They experience the failure as a failure of the bank. Digital banking and HR participants confirmed that customer service teams often absorbed customer anger during vendor outages, bugs, or delayed feature explanations.

DB_1 described a bug in a transfer application where IT was slow to provide updates and customer experience staff did not know how to answer customers. The organization later created a cross-unit notification mechanism. CX_1 described an incident in which inconsistent information from two employees damaged customer trust because no official communication guide existed. The response was to create written communication standards. HR participants described crisis briefings and simulations to prepare frontliners for customer anger during partner disruptions.

This category shows that trust repair is not merely technical remediation. Fixing a bug does not automatically repair trust if customer-facing staff cannot explain what happened, why it happened, and what the organization will do next. Trust repair requires synchronized work: IT must update technical status, compliance must approve what can

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

be disclosed, digital banking must frame the service implication, HR must prepare staff behaviour, and customer experience must communicate consistently.

Reconstructing HRM after failure

The sixth category concerns reconstruction. Participants repeatedly described how incidents changed routines. HR_1 added practical simulations and stricter monitoring after a trained employee sent customer data through WhatsApp. HR_2 revised training methods after an employee opened customer files on a personal laptop. IT_2 turned phishing incidents into simulations. IT_1 made MFA a condition for system access after internal resistance. CX_1 introduced written communication standards after customers received inconsistent information. Compliance and risk participants described turning audit findings into SOP revisions.

These accounts show that digital trust formation includes a repair cycle. The organization does not only build trust before incidents. It reconstructs trust after incidents by converting breakdowns into new routines. This is where the CGT model becomes dynamic. Competence-building, risk discipline, accountability, and coordination do not form a neat sequence. They loop through failure. The most theoretically important routines were often born after something went wrong.

The evidence also suggests that trust repair can remain incomplete. Several participants said management knew about workarounds but had not yet solved them because official systems remained slow or cumbersome. This means reconstruction must address not only employee behaviour but also the structural conditions that make shortcuts attractive. HRM can retrain employees, but if systems continue to generate operational friction, shadow routines will return.

Table 4. Theoretical categories, representative evidence, and interpretive claims

Theoretical category	Representative evidence	Interpretive claim
Regulatory translation	Rules on access, storage, and privacy translated into “do not use private email”, “do not save data on personal devices”, and case simulations	Strategic HRM converts abstract governance into actionable conduct

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

Speed-control paradox	Business and partners pushed rapid launch; compliance, IT, and risk delayed launch for audits, checks, or pilots	Digital trust is negotiated between innovation urgency and risk restraint
Shadow routines	Shared logins, WhatsApp transfers, private emails, Excel files, flashdisks, improvised customer answers	Hidden workarounds expose the gap between formal compliance and operational practicality
Fragile psychological safety	Employees reported mistakes but suffered warnings, reputational damage, or transfer	Learning cultures remain partial when reporting generates informal career cost
Cross-functional crisis work	Customer service absorbed customer anger while HR prepared briefings, IT updated status, and compliance controlled disclosure	Trust repair requires synchronized human coordination, not only technical correction
Reconstruction after failure	Training revised, scripts standardized, MFA enforced, SOPs updated, simulations introduced after incidents	HRM routines become stronger when organizations convert breakdowns into learning structures

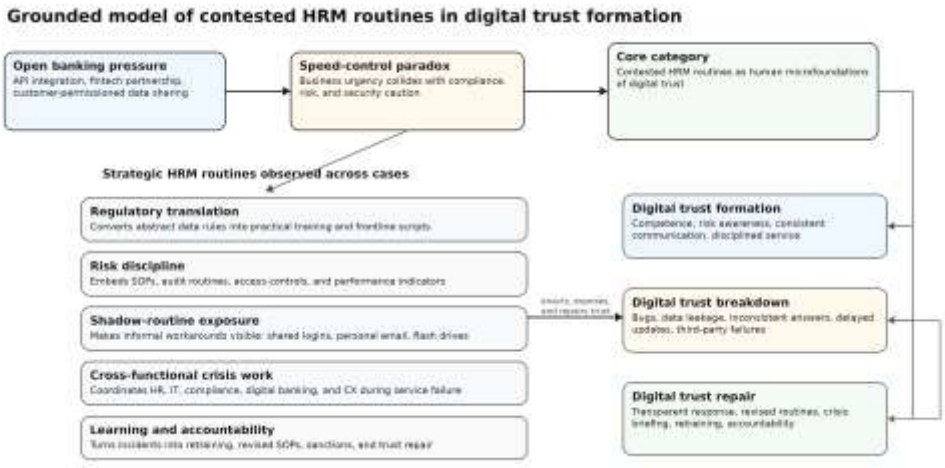


Figure 1. Grounded model of contested HRM routines as human microfoundations of digital trust

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

International Journal of Economics, Business and Innovation Research
https://e-journal.citakonsultindo.or.id/index.php/IJEBIR
E-ISSN : 2964-0865
IJEBIR

DISCUSSION

The findings support a central argument: digital trust in open banking is not simply designed; it is enacted, contested, broken, and repaired through strategic HRM routines. This result extends open banking research, which has strongly documented the role of trust, privacy, perceived risk, consent, and data security in adoption decisions (Chan et al., 2022; Jafri et al., 2024; Polasik & Kotkowski, 2022; World Bank, 2022). Those studies explain why users hesitate or adopt. This study explains what happens inside organizations before customers experience trust as reliable service, clear communication, or credible data protection.

The findings also sharpen the policy literature. OECD (2023a, 2023b), CCAF (2024), and the Basel Committee (2019, 2024) frame open banking and open finance as data-sharing regimes that need consent, standards, governance, resilience, and third-party risk controls. The data confirm that such controls matter, but they also show their incompleteness. A standard, audit requirement, or API checklist must still pass through employees who translate, explain, perform, and sometimes bypass it. This is the article's empirical addition to policy debate: open banking governance succeeds only when organizational routines make formal safeguards livable in daily work.

Strategic HRM literature helps explain this translation problem. Bowen and Ostroff (2004) argue that strong HRM systems send distinctive, consistent, and consensual signals. The findings confirm the value of that argument, but they also show its limits under digital ecosystem pressure. HRM signals were often clear in formal training, yet employees still used shadow routines when official systems slowed down work. This qualifies the optimistic reading of HRM system strength. In open banking, HRM strength depends not only on message consistency, but also on whether work systems allow employees to follow the message without sacrificing service responsiveness.

The study therefore extends Banking 4.0 HRM literature. Kuchciak and Warwas (2021) position reskilling, upskilling, and redeployment as central HRM responses to banking digitalization. The present findings agree, but they specify the content of that reskilling. Open banking employees need risk literacy, partner coordination capability, privacy discipline, customer explanation scripts, and crisis repair competence. Generic digital literacy remains insufficient when employees face concrete dilemmas such as a slow official system, an angry customer, a partner outage, a delayed API launch, or a phishing incident.

The microfoundations contribution lies in showing how ecosystem-level trust rests on mundane but consequential actions. Felin et al. (2012) identify individuals, social

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

processes, and structures as microfoundations of routines and capabilities. In this study, individuals mattered when employees chose whether to share passwords or follow access rules. Social processes mattered when HR, IT, compliance, and customer experience negotiated launch delays or crisis messages. Structures mattered when performance indicators, audit logs, MFA requirements, and CRM update systems enabled or constrained safe behaviour. Digital trust therefore emerged from the alignment, and misalignment, among these micro-level components.

Organizational routines theory deepens this interpretation. Feldman and Pentland (2003) argue that routines contain both ostensive and performative dimensions. The findings strongly support that distinction. The ostensive routine said: protect data, follow SOP, report errors, coordinate across units. The performative routine sometimes said: use one shared login, send the file by WhatsApp, answer customers based on assumption, or wait until IT provides an update. This gap explains why shadow routines became the most analytically important category. They reveal digital trust fragility at the point where formal governance meets operational friction.

Cybersecurity culture literature also helps interpret the findings. ENISA (2018) and NIST (2024) emphasize awareness, governance, roles, response, and recovery. The evidence agrees that cybersecurity culture must move beyond technical control. Nevertheless, the data challenge any simple awareness model. Participants described employees who had passed training but still sent customer files through WhatsApp, opened files on personal laptops, shared passwords, or used private email. Awareness did not fail because employees knew nothing. It failed because knowing, working, and complying collided under pressure. Cybersecurity culture must therefore address workflow design and accountability, not only awareness messages.

The findings on psychological safety add another critical dialogue with the literature. Edmondson (1999, 2012) shows that learning cultures need safe voice. The first interview round seemed to support that view because participants described error reporting as learning rather than punishment. The critical incidents complicated the claim. Employees who reported mistakes still faced reputational damage, transfer, or harsh warning. This does not reject psychological safety theory. It refines it for high-stakes digital finance: psychological safety remains credible only when employees see proportional accountability, fair treatment, and visible learning after reporting.

The distinction between trust formation and trust repair also extends the trust literature. Mayer et al. (1995) and McKnight et al. (2002) explain trust through expectations, ability, integrity, benevolence, and institutional assurance. Gillespie and

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Dietz (2009) add that repair requires diagnosis, reform, and credible communication after violation. The present study shows how those mechanisms operate through HRM routines. Training and role clarity support trust formation before incidents. Crisis scripts, retraining, performance recalibration, cross-unit updates, and restructuring support trust repair after incidents. Digital trust in open banking therefore has a temporal rhythm: it forms in routine discipline, breaks in operational friction, and repairs through visible organizational learning.

Finally, the findings speak back to open finance supervision. Supervisory frameworks emphasize third-party risk, data protection, and operational resilience (Basel Committee on Banking Supervision, 2024; CGAP, 2026; OECD, 2023b). This study shows why third-party failures become HRM problems once customers demand explanations. When a vendor outage or API bug reaches the customer, customer experience staff absorb anger, HR prepares crisis briefings, compliance frames permissible communication, IT diagnoses causes, and digital banking protects partner relationships. The bank cannot outsource trust repair to the vendor. It must orchestrate human routines that make accountability visible even when causality crosses organizational boundaries.

Theoretical Contributions

First, the article contributes to open banking research by conceptualizing digital trust as a contested organizational accomplishment. Existing policy and technical literature rightly emphasizes data portability, API security, consent, and third-party governance (Basel Committee on Banking Supervision, 2019; OECD, 2023a, 2023b; OpenID Foundation, 2025). This study adds that these arrangements become trustworthy only when organizations translate them into employee conduct, cross-functional coordination, and crisis learning.

Second, the article contributes to strategic HRM by theorizing HRM routines as behavioural trust infrastructure. Training, mentoring, e-learning, performance appraisal, communication scripts, and crisis briefings are not merely support activities. In open banking, they shape the human conditions under which customer data, partner integration, and service reliability become credible. The article extends HRM system strength theory by showing that strong HRM systems must handle contested functional interpretations, not only deliver clear messages.

Third, the article contributes to microfoundations theory by explaining how digital ecosystem capabilities rest on individual, interactional, and structural mechanisms. Digital

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

trust depends on employee conduct, interdepartmental work, and organizational structures that make safe behaviour possible. The study also adds a dynamic element: the same microfoundations can generate trust formation, expose trust breakdown, and enable trust repair.

Fourth, the article contributes to organizational routines research by identifying shadow routines as a central mechanism of digital trust fragility. Formal routines and lived routines do not always align. When employees normalize shortcuts because formal systems feel slow or impractical, the organization carries hidden trust risk. This insight extends Feldman and Pentland's (2003) distinction between ostensive and performative routines into the open banking context.

Practical Implications

For financial institutions, the study suggests that digital trust governance must include HRM design. Organizations should not treat open banking readiness as a technical certification project alone. They need scenario-based training, role-specific scripts, performance indicators for data discipline, non-punitive yet accountable error reporting, and cross-functional crisis rehearsals.

For HR leaders, the results show that digital reskilling must move beyond generic digital literacy. Employees need practice with concrete dilemmas: a customer demands quick service, the official system is slow, a partner has not sent an update, a new API feature is delayed, or a data file needs urgent transfer. These situations reveal whether employees understand trust as daily conduct rather than abstract value.

For IT governance and cybersecurity teams, the findings warn against assuming that technical controls will work if they impose excessive friction. MFA, access restrictions, and secure data flows matter, but employees will seek workarounds if formal systems make routine tasks difficult. Cybersecurity culture therefore requires both control and usability.

For compliance and risk teams, the study highlights the need to make reporting cultures credible. Staff must see that honest reporting leads to learning, correction, and proportional accountability, not hidden reputational punishment. Without credible psychological safety, employees may conceal mistakes until customers or regulators discover them.

For customer experience leaders, the findings show that trust repair begins before a public crisis. Frontliners need clear scripts, update channels, escalation paths, and

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

authority boundaries. Customers judge the organization through the employee who speaks to them, even when the root cause sits in a partner system or technical unit.

Limitations and Future Research

The study has limitations. First, the empirical material consists of role-coded interview accounts and follow-up critical incidents rather than long-term ethnographic observation. The analysis therefore captures interpreted routines and narrated incidents, not direct observation of every routine in action. Second, the study protects confidentiality by avoiding organization names, system details, customer identifiers, and proprietary technical information. This strengthens ethical protection but limits contextual specificity. Third, the study focuses on organizational actors. Future research can compare these accounts with customer narratives, fintech partner interviews, regulatory perspectives, or audit documents.

Future studies can extend the grounded model in several directions. Quantitative research could test whether HRM-enabled risk discipline, cross-functional orchestration, and feedback-based learning predict perceived digital trust. Comparative qualitative research could examine whether shadow routines differ between banks, fintechs, and payment service providers. Longitudinal research could track whether trust repair routines after a digital incident produce lasting behavioural change or only short-term compliance.

CONCLUSION

This study developed a Constructivist Grounded Theory of how strategic HRM routines shape the human microfoundations of digital trust in open banking. The core category, contested HRM routines as human microfoundations of digital trust, captures the central insight: trust in open banking does not flow automatically from API standards, cybersecurity controls, or regulatory compliance. It forms through repeated human work, and that work remains contested.

The findings show that organizations build digital trust by translating regulatory abstraction into situated routines, managing the speed-control paradox, disciplining shadow routines, questioning fragile psychological safety, orchestrating cross-functional crisis work, and reconstructing HRM after failure. These processes explain why digital trust is both powerful and fragile. It can grow through competence, discipline, coordination, and learning. It can collapse through shortcuts, silence, inconsistent communication, and unresolved operational friction. It can be repaired when organizations convert incidents into new routines.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

The article therefore positions strategic HRM at the center of open banking trust governance. HRM does not secure APIs, write regulations, or repair servers. Nevertheless, it shapes the employees who translate, enact, communicate, and repair trust in the daily life of digital finance. In open banking ecosystems, the human microfoundations of trust are not peripheral. They are the conditions under which openness remains credible.

REFERENCES

Babina, T., Bahaj, S., Buchak, G., De Marco, F., Foulis, A., Gornall, W., Mazzola, F., & Yu, T. (2024). Customer data access and fintech entry: Early evidence from open banking (Bank of England Staff Working Paper No. 1059). Bank of England.

Bank Indonesia. (2021). Peraturan Anggota Dewan Gubernur Nomor 23/15/PADG/2021 tentang Standar Nasional Open API Pembayaran. Bank Indonesia.

Bank Indonesia. (2023). National Open API Payment Standard. https://www.bi.go.id/en/layanan/standar/snap/default.aspx

Basel Committee on Banking Supervision. (2019). Report on open banking and application programming interfaces. Bank for International Settlements. https://www.bis.org/bcbs/publ/d486.htm

Basel Committee on Banking Supervision. (2024). Digitalisation of finance. Bank for International Settlements. https://www.bis.org/bcbs/publ/d575.htm

Becker, B. E., & Huselid, M. A. (2006). Strategic human resources management: Where do we go from here? Journal of Management, 32(6), 898-925. https://doi.org/10.1177/0149206306293668

Bowen, D. E., & Ostroff, C. (2004). Understanding HRM-firm performance linkages: The role of the strength of the HRM system. Academy of Management Review, 29(2), 203-221. https://doi.org/10.5465/AMR.2004.12736076

Cambridge Centre for Alternative Finance. (2024). The global state of open banking and open finance. University of Cambridge Judge Business School.

CGAP. (2026). Open finance oversight and supervision: Emerging practices and early lessons. Consultative Group to Assist the Poor.

Chan, R., Troshani, I., Rao Hill, S., & Hoffmann, A. (2022). Towards an understanding of consumers' FinTech adoption: The case of open banking. International Journal of Bank Marketing, 40(4), 886-917. https://doi.org/10.1108/IJBM-08-2021-0397

Charmaz, K. (2014). Constructing grounded theory (2nd ed.). SAGE.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Edmondson, A. C. (1999). Psychological safety and learning behavior in work teams. Administrative Science Quarterly, 44(2), 350-383. https://doi.org/10.2307/2666999

Edmondson, A. C. (2012). Teaming: How organizations learn, innovate, and compete in the knowledge economy. Jossey-Bass.

European Union Agency for Cybersecurity. (2018). Cyber security culture in organisations. ENISA.

Faraj, S., & Xiao, Y. (2006). Coordination in fast-response organizations. Management Science, 52(8), 1155-1169. https://doi.org/10.1287/mnsc.1060.0526

Feldman, M. S., & Pentland, B. T. (2003). Reconceptualizing organizational routines as a source of flexibility and change. Administrative Science Quarterly, 48(1), 94-118. https://doi.org/10.2307/3556620

Felin, T., Foss, N. J., Heimeriks, K. H., & Madsen, T. L. (2012). Microfoundations of routines and capabilities: Individuals, processes, and structure. Journal of Management Studies, 49(8), 1351-1374. https://doi.org/10.1111/j.1467-6486.2012.01052.x

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. MIS Quarterly, 27(1), 51-90. https://doi.org/10.2307/30036519

Gillespie, N., & Dietz, G. (2009). Trust repair after an organization-level failure. Academy of Management Review, 34(1), 127-145. https://doi.org/10.5465/amr.2009.35713319

Jafri, J. A., Mohd Amin, S. I., Abdul Rahman, A., & Mohd Nor, S. (2024). A systematic literature review of the role of trust and security on Fintech adoption in banking. Heliyon, 10(1), e22980. https://doi.org/10.1016/j.heliyon.2023.e22980

Kim, P. H., Ferrin, D. L., Cooper, C. D., & Dirks, K. T. (2004). Removing the shadow of suspicion: The effects of apology versus denial for repairing competence-versus integrity-based trust violations. Journal of Applied Psychology, 89(1), 104-118. https://doi.org/10.1037/0021-9010.89.1.104

Kuchciak, I., & Warwas, I. (2021). Designing a roadmap for human resource management in the Banking 4.0. Journal of Risk and Financial Management, 14(12), 615. https://doi.org/10.3390/jrfm14120615

Laplante, P. A., & Kshetri, N. (2021). Open banking: Definition and description. Computer, 54(10), 122-128. https://doi.org/10.1109/MC.2021.3055909

Mayer, R. C., Davis, J. H., & Schoorman, F. D. (1995). An integrative model of organizational trust. Academy of Management Review, 20(3), 709-734. https://doi.org/10.5465/amr.1995.9508080335

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. Information Systems Research, 13(3), 334-359. https://doi.org/10.1287/isre.13.3.334.81

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29. https://doi.org/10.6028/NIST.CSWP.29

OECD. (2023a). Data portability in open banking: Privacy and other cross-cutting issues. OECD Digital Economy Papers, No. 348. OECD Publishing. https://doi.org/10.1787/6c872949-en

OECD. (2023b). Open finance policy considerations. OECD Business and Finance Policy Papers, No. 36. OECD Publishing. https://doi.org/10.1787/19ef3608-en

OpenID Foundation. (2025). FAPI 2.0 Security Profile. https://openid.net/specs/fapi-security-profile-2_0-final.html

Pentland, B. T., & Feldman, M. S. (2005). Organizational routines as a unit of analysis. Industrial and Corporate Change, 14(5), 793-815. https://doi.org/10.1093/icc/dth070

Polasik, M., & Kotkowski, R. (2022). The open banking adoption among consumers in Europe: The role of privacy, trust, and digital financial inclusion. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4105648

Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. Journal of the Academy of Marketing Science, 50(6), 1299-1323. https://doi.org/10.1007/s11747-022-00845-y

Reason, J. (1997). Managing the risks of organizational accidents. Ashgate.

Schoorman, F. D., Mayer, R. C., & Davis, J. H. (2007). An integrative model of organizational trust: Past, present, and future. Academy of Management Review, 32(2), 344-354. https://doi.org/10.5465/amr.2007.24348410

Tie, Y. C., Birks, M., & Francis, K. (2019). Grounded theory research: A design framework for novice researchers. SAGE Open Medicine, 7, 1-8. https://doi.org/10.1177/2050312118822927

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. Journal of Strategic Information Systems, 28(2), 118-144. https://doi.org/10.1016/j.jsis.2019.01.003

World Bank. (2022). The role of consumer consent in open banking. World Bank Group.

Wright, P. M., & McMahan, G. C. (1992). Theoretical perspectives for strategic human resource management. Journal of Management, 18(2), 295-320. https://doi.org/10.1177/014920639201800205

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.

Zhang, W., Daim, T., & Zhang, Q. (2023). Data security, customer trust and intention for adoption of fintech services: An empirical analysis from commercial bank users. SAGE Open, 13(3). https://doi.org/10.1177/21582440231181388

Appendix A. Interview protocol summary

Round 1 used 12 core questions for all participants: meaning of digital trust; trust determinants; required employee competence; competence development; risk-related routines; risk awareness; cross-functional coordination; innovation-control tension; organizational learning from complaints, regulation, and operational failures; trust-supporting employee behaviour; trust-weakening behaviour or organizational weakness; and future strengthening needs.

Round 2 used follow-up grand tour and critical incident questions. Participants reconstructed launch routines, described clashes between business speed and compliance/security caution, narrated functional friction, and discussed incidents involving third-party outages, shadow routines, customer anger, data mishandling, inconsistent information, reporting consequences, and post-incident restructuring or retraining.

Copyright at authors some right reserved this work is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License.