Scientia Moralitas International Journal of Multidisciplinary Research
ISSN 2472-5331 (Print) | ISSN 2472-5358 (Online) | Vol. 11, No. 1, 2026
DOI:10.5281/zenodo.21499467

# Insider Threats and Identity-Based Cyberattacks in Financial Services: Detection, Prevention, and Governance

**Lawrence E. Iweriebor**
Capitol Technology University, Laurel, MD, USA
leiweriebor@captechu.edu

**Eugene Lewis**
Capitol Technology University, Laurel, MD, USA
ejlewis@captechu.edu

ABSTRACT: Financial services firms work in a high-trust, high-value environment where legitimate access is indispensable and, at the same time, inherently risky. Insider threats and identity-based cyberattacks converge at that point of dependence. Attackers, negligent users, and malicious insiders can all operate through accounts, credentials, sessions, devices, privileges, and workflows that appear legitimate until behavior, context, or intent shifts. Across the peer-reviewed literature, insider-threat research has moved away from static rule sets toward behavioral modeling, anomaly detection, user and entity behavior analytics, explainable artificial intelligence, and continuous authentication, while identity-management research has produced taxonomies of attacks targeting digital identities, identity providers, authentication protocols, and authorization processes (Homoliak et al., 2019; Pöhn & Hommel, 2023). In financial services, digital banking, FinTech platforms, payment systems, regulatory obligations, third-party integrations, and the centrality of customer trust intensify the stakes (Javaheri et al., 2023; Cele & Kwenda, 2024). This article brings those strands together to examine detection, prevention, and governance. Its argument is that financial institutions are better served by an identity-centered governance model that combines least privilege, zero trust, behavioral analytics, risk-adaptive access control, cyberfraud controls, privacy-aware monitoring, and board-level accountability. Technical detection matters, but by itself it is not enough. Institutions also need governance structures that tie identity lifecycle management to behavioral risk signals, incident response, regulatory compliance, human factors, and ethical oversight.

KEYWORDS: Insider Threat, Identity-Based Cyberattacks, Financial Services, Digital Banking, User Behavior Analytics, Zero Trust, Behavioral Biometrics, Cybersecurity Governance

## Introduction

In the financial services industry, financial institutions depend on trusted access, and employees need privileged access to customer data, payment systems, trading platforms, cloud environments, databases, software repositories, and risk-management systems. Also, customers need frictionless access to mobile banking, digital wallets, payment applications, brokerage portals, and lending platforms. Partners and vendors need controlled access to shared services and infrastructure. This level of dependency creates a structural security challenge because the same identity and access systems that enable legitimate financial activity can be abused by malicious insiders, compromised employees, negligent users, account-takeover actors, phishing operators, and adversaries impersonating trusted entities (Didenko, 2020; Javaheri et al., 2023).

Insider threats are difficult to manage because insiders already hold some level of authorization, institutional knowledge, and familiarity with business processes. Homoliak et al. (2019) argue that insider threat research requires careful taxonomy because incidents

vary by actor, motivation, access path, target, organizational context, and countermeasure. In financial services, the insider may be a bank employee misusing customer data, a contractor abusing cloud permissions, a developer exfiltrating code, a privileged administrator altering logs, or a negligent worker enabling credential theft through phishing or insecure behavior (Homoliak et al., 2019; Khan et al., 2021).

Identity-based cyberattacks are equally broad. They include attacks on authentication, authorization, identity providers, account creation, session handling, federated login, device identity, machine identity, and end-user identities. Pöhn and Hommel (2023) emphasize that identity management now sits at the center of security because digital transformation, cloud adoption, outsourcing, and remote work make it harder to know who is accessing which resource, from where, and under what conditions. Identity-based attacks extend well beyond password theft to account takeover, credential stuffing, phishing, impersonation, privilege misuse, weak authentication flows, identity-provider compromise, and attacks on the assumptions built into identity-management architectures (Pöhn & Hommel, 2023).

In financial services, the consequences of both threat categories are amplified. Financial firms store sensitive personal information, process high-value transactions, maintain market infrastructure, support critical payment rails, and operate under intense regulatory scrutiny. FinTech and digital banking research identify phishing, malware, ransomware, unauthorized access, identity theft, data leakage, fraud, and insider attacks as recurring threats to the adoption and resilience of digital financial systems (Cele & Kwenda, 2024; Javaheri et al., 2023).

This article examines a basic question: how should financial services institutions detect, prevent, and govern insider threats and identity-based cyberattacks? The answer developed here is that these risks are closely related and are best understood together rather than in isolation. Detection depends on behavior-aware analytics and context-rich identity telemetry. Prevention depends on least privilege, zero trust, continuous authentication, adaptive access control, and controls designed with human behavior in mind. Governance depends on regulatory alignment, accountability, privacy safeguards, model oversight, auditability, and board-level decision making about cyber risk.

## Research Approach and Scope

The research uses a narrative synthesis of peer-reviewed journal and conference literature. It draws on work about insider-threat taxonomies, insider-detection surveys, machine-learning models, UEBA, identity-management attack taxonomies, cybersecurity in digital banking and FinTech, behavioral biometrics, zero trust, financial-sector regulation, and cybersecurity governance.

The contribution of this research is interpretive: it brings findings from the literature into a conceptual framework for financial institutions. This approach fits the subject matter because insider threats and identity-based attacks are sociotechnical risks shaped not only by technical controls, but also by human behavior, organizational incentives, governance structures, privacy constraints, and regulatory requirements. Insider-threat studies repeatedly note the same obstacles to operational deployment, including dataset scarcity, class imbalance, false positives, limited real-world validation, and scalability problems (Alsowail & Al-Shehari, 2022; Hassan et al., 2020).

The financial-services scope includes banks, digital banks, payment firms, insurers, brokerages, asset managers, and FinTech platforms. These organizations differ in size, regulatory exposure, technology maturity, and customer interaction models, but all depend on identity, access, transaction integrity, data confidentiality, operational resilience, and trust. This research paper emphasizes controls that can be adapted across institutions: identity governance, behavioral monitoring, access-control design, authentication, fraud analytics, data protection, regulatory compliance, and governance accountability.

## Conceptual Foundations

### *Insider Threats*

Insider threats are commonly understood as risks posed by individuals or entities with authorized access who misuse, exceed, or unintentionally compromise that access. Homoliak et al. (2019) show that insider incidents can be classified by actor, motivation, target, action, timing, organizational context, and defense mechanism. The classification matters because the term insider can refer to a malicious employee, a negligent employee, a compromised account, a third-party contractor, or a trusted business partner whose access becomes harmful (Homoliak et al., 2019).

A recurring finding in insider-threat research is that conventional perimeter defenses do little against misuse carried out through legitimate access. Hassan et al. (2020) make that point directly, arguing that insider-threat detection needs methods tailored to behavior that is rare, subtle, and often embedded in normal activity. Kim et al. (2019) reach a similar conclusion, showing why static expert rules become brittle as users, roles, departments, and organizational routines change over time (Hassan et al., 2020; Kim et al., 2019).

The insider threat problem includes both malicious and non-malicious behavior. Khan et al. (2021) distinguish unintentional insider threats from deliberate malicious acts, emphasizing that everyday work conditions, organizational pressures, technology usability, and decision context can contribute to accidental security failures. In financial services, that distinction matters because a phishing-compromised employee, a fatigued call-center agent, and a malicious privileged administrator call for different interventions (Khan et al., 2021).

### *Identity-Based Cyberattacks*

Identity-based cyberattacks exploit the systems and processes that establish, verify, authorize, and monitor digital identity. Pöhn and Hommel (2023) propose TaxIdMA, a taxonomy for attacks related to digital identities and identity-management systems, organizing attacks around system identities, end-user identities, identity-management components, vulnerabilities, attack vectors, and contextual background. Their work is especially relevant to financial services because firms increasingly rely on federated identities, cloud identities, customer identities, employee identities, vendor identities, service accounts, and machine identities (Pöhn & Hommel, 2023).

Identity-based attacks often blur the line between external and internal threats. An external attacker who steals employee credentials becomes functionally internal once authenticated. A malicious insider may use legitimate credentials while violating authorization intent. A compromised third-party account may access financial systems through a trusted integration. A customer account-takeover actor may complete transactions through a legitimate account even as behavioral signals suggest impostor activity. This convergence makes identity telemetry, access context, and behavioral baselines central to detection and prevention (Pöhn & Hommel, 2023; Amaral et al., 2021).

## The Financial Services Threat Surface

Digital banking and FinTech platforms expose a wide range of identity attack surfaces because customers and employees now interact through mobile devices, web portals, APIs, cloud services, payment networks, and third-party applications. Javaheri et al. (2023) classify FinTech cybersecurity threats across technology-based, human-originated, and procedure-related categories, including malware, distributed denial-of-service attacks, digital extortion, insider attacks, social engineering, fraud, data leakage, and data breaches. The same review links those threats to defenses such as anti-malware controls, intrusion detection, access control, blockchain-based controls, training, threat-intelligence sharing, risk management, cyber-insurance, and regulatory technology (Javaheri et al., 2023).

Digital banking adoption research also shows that cybersecurity threats shape trust and adoption. Cele and Kwenda (2024) identify identity theft, malware, phishing, and vishing as major threats that hinder adoption. Tuqan and Asmar (2024) argue that machine learning can strengthen digital banking cybersecurity through fraud detection and threat analysis, while also noting the need to assess algorithmic deployment in terms of benefits, weaknesses, and operational constraints (Cele & Kwenda, 2024; Tuqan & Asmar, 2024).

Financial services require a dual perspective. From the enterprise side, insider and identity risks threaten confidentiality, integrity, availability, fraud prevention, regulatory compliance, and operational resilience. From the customer side, identity compromise threatens account integrity, privacy, trust, and willingness to adopt digital services. A governance model focused only on enterprise insiders will miss customer account takeover and identity fraud, while a fraud-only model will miss privileged insider misuse, administrative abuse, and internal data leakage.

## Detection of Insider Threats and Identity-Based Attacks

### *Behavioral and Anomaly-Based Detection*

Recent work treats insider threats less as a matter of known signatures and more as departures from established patterns of user behavior. Kim et al. (2019), for example, model normal activity from log data and then use deviations from that baseline to surface suspicious behavior. In financial services, that logic is appealing because many legitimate tasks are repetitive and tied to defined roles, so shifts in timing, file access, transaction patterns, device use, or network behavior can carry real meaning (Kim et al., 2019).

Machine-learning reviews show that insider threat detection faces recurring challenges: limited real-world datasets, class imbalance, high false-positive costs, evolving user behavior, privacy constraints, and difficulty distinguishing malicious intent from unusual but legitimate activity. Hassan et al. (2020) review classification techniques, datasets, and open challenges, while Alsowail and Al-Shehari (2022) emphasize that prevention and detection approaches need to account for feature domains, dataset quality, scalability, stability, and real-world deployment constraints (Hassan et al., 2020; Alsowail & Al-Shehari, 2022).

Recent surveys also show a shift from classical machine learning toward deep learning, graph learning, sequence modeling, text analysis, and explainable AI. Alzaabi and Mehmood (2024) review machine-learning methods for malicious insider detection and note that deep learning and natural language processing can help interpret contextual and textual signals. Alketbi and Mehmood (2025) argue that explainable AI matters because analysts need interpretable evidence to trust model outputs and investigate insider alerts (Alzaabi & Mehmood, 2024; Alketbi & Mehmood, 2025).

### *User and Entity Behavior Analytics*

UEBA is one of the clearest links between insider-threat detection and identity-attack detection. It models the behavior of users, accounts, devices, applications, and other entities so that unusual activity can be identified in context. Khaliq et al. (2020) argue that traditional cybersecurity products tend to prioritize outside attackers and often provide limited visibility into the behavior of legitimate users. UEBA addresses that gap through user profiling, role-based detection, activity mapping, and risk scoring (Khaliq et al., 2020).

Artioli et al. (2024) study clustering algorithms for UEBA and emphasize the role of unsupervised learning because anomalous behavior is often unknown in advance. That is especially relevant to financial institutions, where labeled insider incidents and account-takeover cases may be rare, sensitive, or unavailable for training. Unsupervised or semi-

supervised approaches can help detect outliers, but they also need careful calibration to avoid overwhelming security teams with low-quality alerts (Artioli et al., 2024).

UEBA can also connect internal and external identity risks. A login from a new device, a change in navigation behavior, an abnormal transaction sequence, an unusual database query, an anomalous file download, off-hours privilege escalation, or sudden access to customer records may indicate either a malicious insider or a compromised account. The core detection question is not simply whether the user is authorized, but whether the identity is being used in a way consistent with legitimate role, context, history, and risk.

### *Scenario-Oriented Detection*

Recent insider threat research also argues that detection should move beyond generic anomaly labels toward specific threat scenarios. Tian et al. (2025) propose scenario-oriented detection for privilege abuse, identity theft, and data leakage by modeling behavior sequences and long-distance dependencies. This is especially applicable to financial services because the response to a suspected identity-theft scenario differs from the response to suspected data exfiltration or privileged administrative abuse (Tian et al., 2025).

Looking at specific scenarios can also improve governance because it ties alerts to concrete response choices. A suspected account takeover may call for customer verification and a transaction hold. A possible insider data leak may require evidence preservation, human-resources coordination, privacy review, and legal escalation. In both cases, what matters is not only that something anomalous happened, but also what kind of situation the anomaly most likely represents.

### *Log, Text, and Multi-Modal Detection*

Financial institutions generate extensive logs across identity providers, endpoint systems, databases, cloud platforms, software development systems, payment gateways, customer applications, and fraud platforms. Fei et al. (2025) propose log-text analysis for insider threat detection, reflecting a broader shift toward extracting meaning from heterogeneous log and textual data. Zhang et al. (2021) use ensemble and self-supervised learning with behavioral logs to address limitations such as sample imbalance and feature heterogeneity (Fei et al., 2025; Zhang et al., 2021).

Multi-modal detection matters because identity abuse rarely reveals itself in a single signal. One unusual login may be harmless. The same login followed by privilege escalation, customer-record access, bulk export, and suspicious transfer activity is harder to dismiss. Combining identity logs, endpoint telemetry, transaction data, database queries, file movement, communication metadata, and behavioral biometrics can therefore produce stronger signals than any one source alone. At the same time, broader monitoring raises obvious privacy, governance, and proportionality concerns.

### *Behavioral Biometrics and Continuous Authentication*

Behavioral biometrics are particularly relevant to financial services because account takeover often occurs after initial authentication. Amaral et al. (2021) propose a continuous authentication framework using touch dynamics for mobile banking, arguing that behavioral biometrics can help verify users during sessions rather than only at login (Amaral et al., 2021).

Behavioral biometrics can reduce exclusive reliance on passwords, one-time passcodes, and static login checks. Sahdev et al. (2021) discuss swipe and touch data as an additional layer for adaptive authentication in digital banking, while Amaral et al. (2021) show how touch dynamics can support continuous user verification during mobile-banking sessions. The case for using these tools is strongest as a supplementary control, especially

after login. The tradeoff is obvious: behavioral systems collect sensitive data about how people interact with devices, so institutions need clear limits on collection, retention, explanation, and review (Sahdev et al., 2021; Amaral et al., 2021).

### *Detection Trade-Offs*

Detection systems in financial services have to balance security, usability, privacy, and operational capacity. High false-positive rates create customer friction, employee distrust, alert fatigue, and weak investigations. Low sensitivity misses subtle insider activity and account compromise. Explainable AI matters in that setting not as a luxury feature, but because analysts, auditors, customers, employees, and regulators may all need intelligible reasons for risk scores, access denials, transaction friction, or escalated investigations (Alketbi & Mehmood, 2025; Tuqan & Asmar, 2024).

## Prevention Strategies

### *Identity Governance and Least Privilege*

Prevention begins with identity governance: knowing which identities exist, which privileges they hold, why those privileges are justified, how long they should remain active, and how access should change when roles, employment status, risk, or business context changes. Identity governance should include employees, contractors, customers, administrators, service accounts, application identities, APIs, cloud workloads, and third-party integrations. Pöhn and Hommel's identity attack taxonomy supports this broader view by showing that identities and identity-management systems are themselves attack surfaces (Pöhn & Hommel, 2023).

Least privilege is especially important in financial services because concentrated privilege creates high-impact abuse opportunities. Excessive access to customer databases, payment systems, transaction approval workflows, production systems, encryption keys, or fraud-rule configuration can allow insiders or compromised accounts to cause disproportionate harm. Access should be role-based where stable roles exist, attribute-based where context matters, and risk-adaptive where behavior or environmental conditions indicate elevated risk.

### *Zero Trust and Continuous Verification*

Zero trust is useful here because it does not assume that a user, device, or session should be trusted simply because it is inside the network or has already authenticated once. Liu et al. (2023) describe zero trust as a security paradigm built around continuous verification, least privilege, and reduced reliance on traditional perimeter assumptions. Those ideas map well onto financial services, where employees, customers, vendors, APIs, and cloud workloads may all reach sensitive systems from different devices and locations (Liu et al., 2023).

Zero trust is not a single technology. It requires identity-aware access control, device posture checks, micro-segmentation, continuous monitoring, policy enforcement, and risk-based decisions. In insider and identity attack contexts, zero trust can reduce the damage caused by credential compromise because an authenticated identity does not automatically receive broad access. But zero trust also depends on accurate identity data, policy quality, logging, governance, and operational maturity.

### *Adaptive Access Control*

Attribute-Based Access Control (ABAC) matters in dynamic financial environments because access decisions can consider subject attributes, resource attributes, action attributes, environmental conditions, risk scores, and business context. Alohaly et al. (2022) integrate cyber deception into ABAC to detect insider misuse by generating honey values

and tracking access to sensitive attributes. Jha et al. (2018) show that ABAC decisions can formally incorporate contextual environmental attributes such as access time and network source, while also requiring administrative safety analysis so policy changes do not create unsafe access states (Alohaly et al., 2022; Jha et al., 2018).

In financial services, adaptive access control can support just-in-time privileged access, step-up authentication, transaction-specific authorization, session restrictions, and temporary access expiration. A fraud analyst may need access to certain customer records only during an investigation. A developer may need production access only during an approved incident. A customer may need step-up authentication for high-risk transfers. These controls prevent identity abuse by aligning access with purpose, context, and risk.

### *Authentication, MFA, and Continuous Session Security*

Traditional authentication is necessary but insufficient. Passwords, personal identification numbers, and one-time passcodes can be phished, replayed, socially engineered, or bypassed through account recovery abuse. Continuous authentication and behavioral biometrics can help address the post-login gap by monitoring whether the session operator behaves like the legitimate user. Amaral et al. (2021) show how mobile banking applications can collect touch and motion data to support continuous authentication during use (Amaral et al., 2021).

Financial institutions should treat authentication as a layered control. MFA should be risk-based and resistant to phishing where possible. Behavioral analytics should supplement rather than replace explicit authentication. Device binding, transaction signing, anomaly detection, session timeout, and step-up verification should be applied based on transaction value, behavioral deviation, device reputation, location, and account history. For employees, privileged actions should require stronger controls than ordinary access.

### *Human-Centered Prevention*

Human behavior remains central to both insider threats and identity-based attacks. Waqas et al. (2023) examine phishing susceptibility through self-regulation, information processing, and financial knowledge, showing that human cognitive factors shape vulnerability to phishing. Maurushat et al. (2021) argue that behavioral sciences can improve cybersecurity management by addressing social engineering and risky online behavior. Khan et al. (2021) further show that unintentional insider threats emerge from everyday work conditions rather than purely from malicious intent (Waqas et al., 2023; Maurushat et al., 2021; Khan et al., 2021).

Training should be tailored to role, task context, and common attack patterns rather than treated as a purely generic compliance exercise. Staff in call centers, branches, trading desks, engineering teams, and fraud units encounter different pressures and different forms of manipulation. The literature on phishing susceptibility and unintentional insider threat suggests that prevention improves when controls and training reflect those differences rather than assuming one message fits everyone (Waqas et al., 2023; Khan et al., 2021).

## Governance in Financial Services

### *Regulatory Complexity and Harmonization*

Financial-sector cybersecurity governance is shaped by sector-specific regulation, data protection law, operational resilience requirements, outsourcing oversight, incident reporting, and consumer protection expectations. Baumgarten and Calliess (2020) analyze cybersecurity in the EU financial sector and emphasize that effective regulation depends on clear legal frameworks, institutional coordination, and sector-specific governance (Baumgarten & Calliess, 2020).

Regulatory complexity affects insider and identity controls in several ways. First, firms must define what counts as a material cyber risk, cyber incident, fraud event, operational resilience failure, or privacy breach. Second, identity telemetry and behavioral monitoring may implicate employee privacy and customer data protection. Third, cross-border firms must reconcile divergent reporting timelines, data localization rules, outsourcing requirements, and supervisory expectations. Governance must connect technical controls with legal, compliance, privacy, audit, and risk functions.

### *Board and Executive Oversight*

Cybersecurity governance depends on senior leaders getting information they can actually use. Schinagl and Shahim (2020) describe the shift from a narrow information-security model to a board-level digital-security model tied to business resilience. Proudfoot et al. (2024) likewise show how cybersecurity regulation can be confusing, expensive, and time-consuming to implement, which affects how well organizations translate compliance into practice (Schinagl & Shahim, 2020; Proudfoot et al., 2024).

For insider and identity risk, leadership needs measures that translate technical activity into business exposure. Illustrative examples include privileged-access exceptions, orphaned accounts, dormant identities, toxic access combinations, MFA bypasses, high-risk session alerts, customer account-takeover rates, access-review completion, third-party identity issues, and the time it takes to revoke or remediate access. None of these metrics mean much in isolation; they have to be read in context and tied back to business risk.

### *Privacy, Ethics, and Proportionality*

Insider threat and identity monitoring can become invasive if not governed carefully. Behavioral analytics, biometric monitoring, email analysis, keystroke dynamics, transaction profiling, and employee surveillance can protect institutions, but they can also undermine privacy, autonomy, trust, and fairness. Alsowail and Al-Shehari (2022) note that prevention methods vary in intrusiveness and acceptability, while behavioral biometrics studies highlight privacy and user acceptance challenges (Alsowail & Al-Shehari, 2022; Amaral et al., 2021).

Governance should apply proportionality. High-risk privileged administrative actions justify stronger monitoring than ordinary low-risk activity. Customer behavioral biometrics should be minimized, protected, and explained. Employee monitoring should be disclosed through policy, aligned with legitimate security purposes, and restricted through access controls. Model outputs should not serve as sole proof of wrongdoing; they should trigger investigation, corroboration, and due process.

### *Practical Governance Structure*

In practice, financial institutions may structure identity-risk governance across operational ownership, risk and compliance oversight, and independent audit so that responsibility does not collapse into the security operations function alone. The exact arrangement will vary by institution, but the broader point is consistent: identity risk cuts across business operations, fraud, privacy, compliance, legal review, and audit.

Clear incident roles still matter. Security operations may detect identity anomalies, fraud teams may identify suspicious transactions, human resources may handle employee cases, legal may preserve evidence, privacy teams may assess data exposure, compliance may manage regulatory notifications, and business owners may remediate process gaps. Governance should specify when and how these teams coordinate.

### Integrated Identity-Risk Framework

Read together, the literature points toward an integrated identity-risk framework for financial services. It is best understood as a conceptual way of organizing overlapping problems of identity misuse, identity compromise, excessive privilege, behavioral deviation, and governance failure.

| Layer | Core question | Controls | Peer-reviewed support |
|---|---|---|---|
| Identity inventory | Which human, customer, third-party, and machine identities exist? | Identity lifecycle management, joiner-mover-leaver controls, service-account ownership, third-party identity registers | Identity-management attack taxonomies show identities and identity systems are attack surfaces (Pöhn & Hommel, 2023). |
| Access governance | What should each identity be allowed to do? | Least privilege, role mining, ABAC, privileged access management, separation of duties | Insider taxonomies and ABAC research show that authorized access must be constrained by context and purpose (Homoliak et al., 2019; Alohaly et al., 2022; Jha et al., 2018). |
| Authentication and session assurance | Is the session operator the legitimate user? | MFA, phishing-resistant authentication, behavioral biometrics, step-up verification, transaction signing | Continuous authentication research supports touch dynamics and behavioral biometrics in mobile banking (Amaral et al., 2021; Barlas et al., 2020). |
| Behavioral detection | Is current behavior consistent with role, history, and context? | UEBA, anomaly detection, sequence modeling, risk scoring, scenario-based detection | Behavioral analytics and insider detection research support user modeling and scenario-oriented detection (Kim et al., 2019; Tian et al., 2025). |
| Data and transaction protection | Is sensitive data or value being moved improperly? | Data-loss prevention, transaction monitoring, fraud analytics, database monitoring, honey values | FinTech and insider countermeasure reviews identify access control, monitoring, data-leak detection, and fraud controls as core defenses (Javaheri et al., 2023; Alsowail & Al-Shehari, 2022). |
| Governance and assurance | Are controls lawful, effective, auditable, and accountable? | Board metrics, privacy review, model governance, incident playbooks, audit, regulatory alignment | Financial-sector cybersecurity regulation and governance research emphasizes harmonization, clear legal frameworks, and board-level digital security accountability (Didenko, 2020; Schinagl & Shahim, 2020). |

The framework should operate as a lifecycle. It starts with identity creation and proofing, continues through access approval and authentication, monitors session behavior and data movement, escalates suspicious activity into investigation, remediates root causes,

and feeds lessons back into policy and control design. This lifecycle approach is stronger than isolated security tools because it connects prevention, detection, response, and governance.

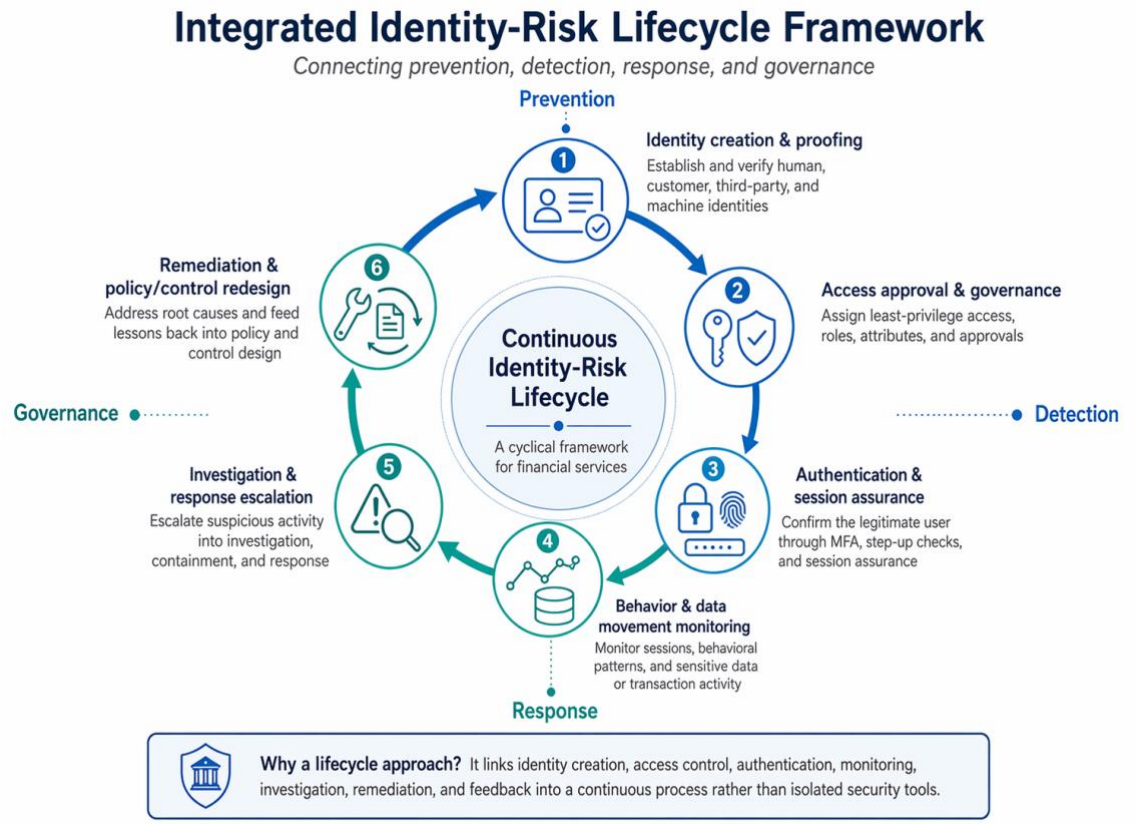


Figure 1. Integrated Identity-Risk Lifecycle Framework for Financial Services

*Note.* Developed by the author based on Amaral et al. (2021), Homoliak et al. (2019), Javaheri et al. (2023), Jha et al. (2018), Kim et al. (2019), Pöhn and Hommel (2023), Schinagl and Shahim (2020), and Tian et al. (2025).

The framework is presented as a continuous lifecycle linking identity creation and proofing, access approval, authentication, session monitoring, investigation, remediation, and feedback into policy and control design.

## Implementation Challenges

### *Data Scarcity and Label Quality*

Research on insider-threat detection often relies on synthetic or otherwise limited datasets because real incidents are rare, sensitive, hard to share, and legally complicated. Hassan et al. (2020) and Alsowail and Al-Shehari (2022) both identify dataset limitations as a major obstacle. Financial institutions face the same problem: genuine insider cases, fraud investigations, customer account-takeover records, and employee-monitoring data are too sensitive to circulate freely for model training (Hassan et al., 2020; Alsowail & Al-Shehari, 2022).

The obvious lesson is that published accuracy scores should not be treated as plug-and-play evidence for production deployment. Models need to be validated on local data, tested against changing behavior, and judged by operational measures such as alert usefulness, analyst workload, investigation outcomes, customer friction, fairness, and detection speed. Synthetic data and public datasets are useful for experimentation, but they are not substitutes for institutional validation.

### *False Positives and Analyst Capacity*

Behavior-based detection inevitably produces gray-area alerts. A trader working late, a fraud investigator reviewing large numbers of customer records, a developer pulling logs during an outage, or a customer traveling abroad may all look anomalous without being malicious. Explainability and scenario classification help analysts sort out benign irregularities from meaningful risk (Alketbi & Mehmood, 2025; Tian et al., 2025).

Financial institutions should use tiered response rather than binary blocking. Low-confidence anomalies may trigger logging or passive monitoring. Medium-risk events may trigger step-up authentication or manager review. High-risk events may trigger session termination, privileged-access suspension, transaction hold, or incident response. This graduated response reduces harm from false positives while preserving the ability to intervene quickly.

### *Integration Across Silos*

Insider-threat programs, fraud teams, identity-governance teams, security operations centers, privacy teams, compliance units, and business owners often use different tools and speak in different vocabularies. That fragmentation is risky because identity-based attacks often move across those boundaries. A phishing email can lead to credential theft, cloud access, payment-instruction changes, data exfiltration, and fraud losses without any single team seeing the entire chain.

The literature supports multi-source analysis because insider and identity attacks are context-dependent. Log analysis, behavioral analytics, access control, fraud detection, and governance each address different dimensions of the same risk. Financial institutions should build shared identity-risk data models, common escalation criteria, and cross-functional incident playbooks.

## Privacy and Trust

Employees and customers may resist monitoring if it appears opaque, excessive, or unfair. Behavioral biometrics and UEBA systems can be especially sensitive because they infer identity, intent, risk, and deviation from behavioral patterns. Maurushat et al. (2021) and Khan et al. (2021) show that human behavior and organizational context are central to cybersecurity outcomes, which means governance must preserve trust as well as security (Maurushat et al., 2021; Khan et al., 2021).

Trust-preserving monitoring requires transparency, purpose limitation, proportionality, access restrictions, retention controls, and review mechanisms. Employees should know that monitoring protects customers, systems, and the institution, but they should also know that alerts will be investigated fairly. Customers should receive clear explanations when security controls add friction to transactions or authentication.

## Recommendations

Financial institutions should build an identity-risk governance program that covers employees, customers, third parties, privileged accounts, service accounts, machine identities, and cloud identities. The program should define ownership, lifecycle controls, policy standards, review frequency, access-risk scoring, and exception handling. That recommendation follows from identity-management research showing that both identities and identity systems are attack surfaces in their own right (Pöhn & Hommel, 2023).

Institutions should integrate UEBA with identity governance and fraud analytics. UEBA should ingest identity-provider logs, privileged access events, endpoint telemetry, transaction behavior, database access, and application activity. Alerts should be scored by role, sensitivity, transaction value, data exposure, device context, and behavioral deviation.

This recommendation follows from insider detection and UEBA literature emphasizing behavior modeling, anomaly detection, and multi-source signals (Kim et al., 2019; Khaliq et al., 2020; Artioli et al., 2024).

Institutions should implement risk-adaptive access control rather than relying on static access alone. Access should depend on role, attributes, transaction context, device posture, location, session risk, and purpose. Privileged actions should require just-in-time elevation, session recording where lawful, separation of duties, and automatic expiration. ABAC and deception-integrated access-control research support this approach because dynamic policy can reduce unauthorized insider access and improve detection of suspicious attribute access (Alohaly et al., 2022; Jha et al., 2018).

Zero trust is most useful when treated as an operating model rather than as a branded product. In practice, that means translating the idea into identity verification, device validation, least privilege, micro-segmentation, continuous monitoring, policy enforcement, and access-decision logging. The zero-trust literature supports that direction even if implementation in finance will vary by institution (Liu et al., 2023).

Behavioral biometrics deserve cautious use in higher-risk customer and employee scenarios. They can strengthen continuous authentication in mobile banking and help surface account-takeover risk, but the literature supports them best as an added layer rather than a replacement for other controls. Any deployment should include privacy impact assessment, data minimization, retention limits, fairness testing, and human review when the stakes are high (Amaral et al., 2021; Sahdev et al., 2021).

Institutions should formalize cross-functional incident playbooks for identity misuse. Playbooks should distinguish account takeover, insider data leakage, privilege abuse, credential theft, payment fraud, third-party compromise, and accidental exposure. Each playbook should define evidence sources, escalation paths, customer communication, legal hold, privacy assessment, regulator notification, access revocation, and lessons learned. Scenario-oriented detection research supports this recommendation because different threat scenarios require different response logic (Tian et al., 2025).

Boards should receive regular reporting on insider and identity risk in terms they can act on. Reports can cover issues such as privileged-access exceptions, toxic combinations, terminated-user access, orphaned service accounts, MFA bypasses, account-takeover cases, and remediation timeliness. The purpose is not to produce a perfect universal dashboard, but to translate technical activity into business exposure and accountability (Schinagl & Shahim, 2020).

Institutions should align monitoring with privacy, employment law, and data protection requirements. Insider monitoring and behavioral analytics should be governed by policy, legitimate purpose, proportionality, access restrictions, retention limits, and audit. Financial-sector regulatory scholarship shows that cybersecurity governance operates within complex legal environments, making legal and compliance alignment essential (Baumgarten & Calliess, 2020).

## Discussion

The literature reviewed suggests that insider threats and identity-based cyberattacks should not be handled as fully separate control domains. Both involve the misuse or compromise of trust. Both exploit the space between authentication and actual behavior. Both can bypass perimeter defenses. That does not make them identical, but it does make a shared governance lens useful in financial services.

That shift carries a few practical consequences. Identity is not just an IT object; it is also a risk-bearing object. Every identity has an owner, a set of privileges, an authentication profile, a behavioral history, a business purpose, regulatory implications, and a potential impact if misused. Detection therefore has to focus on behavior in context rather than

isolated events. Prevention has to reduce blast radius through least privilege, segmentation, continuous verification, and adaptive controls. Governance has to ensure that monitoring is lawful, explainable, auditable, and proportionate.

The same literature also makes clear that more advanced technology brings more governance work with it. Machine learning, deep learning, behavioral biometrics, graph analytics, and explainable AI can improve detection, but they also raise familiar problems: opacity, bias, false positives, privacy intrusion, and overconfidence in model outputs. Financial institutions cannot treat identity-risk scores as self-validating. Where systems affect employees or customers, they need validation, explanation, human review, and a way to challenge outcomes.

Financial services also require more coordination than many security models assume. Cybersecurity, fraud, operational risk, legal, compliance, privacy, audit, and business teams all touch identity risk from different angles. Insider-threat detection may surface fraud; fraud monitoring may expose employee compromise; privacy rules may constrain retention; legal review may shape evidence handling; compliance may determine reporting obligations. Without that coordination, institutions are likely to miss warning signs or respond inconsistently.

## Conclusion

Insider threats and identity-based cyberattacks in financial services are closely connected identity-risk problems. Insider threats take advantage of legitimate access, institutional knowledge, and trusted workflows. Identity-based attacks target authentication, authorization, account lifecycle, session management, and identity infrastructure. In a financial institution, both threaten customer trust, data confidentiality, transaction integrity, operational resilience, and compliance.

The peer-reviewed literature supports a layered response. Detection works best when institutions combine user-behavior modeling, UEBA, log analytics, scenario-oriented detection, explainable AI, and continuous authentication. Prevention is stronger when identity governance, least privilege, zero trust, adaptive access control, MFA, behavioral biometrics, deception-aware controls, and human-centered design work together. Governance has to supply board oversight, legal and regulatory alignment, privacy safeguards, model accountability, cross-functional incident playbooks, and auditability.

The larger point is that these controls have to be governed as parts of a sociotechnical system. Monitoring tools alone will not solve insider and identity risk. Financial institutions also need disciplined identity lifecycle management, contextual access decisions, behavior-aware detection, fair and proportionate monitoring, and executive accountability.

## References

Alketbi, K. S., & Mehmood, A. (2025). A comprehensive survey of explainable artificial intelligence techniques for malicious insider threat detection. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3587114

Alohaly, M., Balogun, O., & Takabi, D. (2022). Integrating cyber deception into attribute-based access control (ABAC) for insider threat detection. *IEEE Access*. https://doi.org/10.1109/ACCESS.2022.3213645

Alzaabi, F. R., & Mehmood, A. (2024). A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3369906

Amaral, D. M., Estrela, P. M. A. B., Albuquerque, R. D. O., Sousa Júnior, R. T. D., & Giozza, W. F. (2021). A framework for continuous authentication based on touch dynamics biometrics for mobile banking applications. *Sensors, 21*(12), 4212. https://doi.org/10.3390/s21124212

Artioli, P., Maci, A., & Magrì, A. (2024). A comprehensive investigation of clustering algorithms for user and entity behavior analytics. *Frontiers in Big Data, 7,* 1375818. https://doi.org/10.3389/fdata.2024.1375818

Alsowail, R. A., & Al-Shehari, T. (2022). Techniques and countermeasures for preventing insider threats. *PeerJ Computer Science, 8*, e938. https://doi.org/10.7717/peerj-cs.938

Baumgarten, A., & Calliess, C. (2020). Cybersecurity in the EU: The example of the financial sector: A legal perspective. *German Law Journal, 21*(6), 1149–1179. https://doi.org/10.1017/glj.2020.67

Cele, N. N., & Kwenda, S. (2024). Do cybersecurity threats and risks have an impact on the adoption of digital banking? A systematic literature review. *Journal of Financial Crime.* https://doi.org/10.1108/JFC-10-2023-0263

Fei, K., Zhou, J., Zhou, Y., Gu, X., Fan, H., Li, B., Wang, W., & Chen, Y. (2025). LaAeb: A comprehensive log-text analysis based approach for insider threat detection. *Computers & Security, 148,* 104126. https://doi.org/10.1016/j.cose.2024.104126

Hassan, A., Abdulkareem, K. H., Al-Mhiqani, M., Ali, N. S., Ahmad, R., Yassin, W., Abidin, Z., & Yunos, Z. (2020). A review of insider threat detection: Classification, machine learning techniques, datasets, open challenges, and recommendations. *Applied Sciences, 10*(15), 5208. https://doi.org/10.3390/app10155208

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y., & Ochoa, M. (2019). Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures. *ACM Computing Surveys, 52*(2), Article 30. https://doi.org/10.1145/3303771

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2023). Cybersecurity threats in FinTech: A systematic review. *Expert Systems with Applications*. https://doi.org/10.1016/j.eswa.2023.122697

Jha, S., Sural, S., Atluri, V., & Vaidya, J. (2018). Security analysis of ABAC under an administrative model. *IET Information Security, 13*(2), 96–103. https://doi.org/10.1049/iet-ifs.2018.5010

Khan, N., Houghton, R. J., & Sharples, S. (2021). Understanding factors that influence unintentional insider threat: A framework to counteract unintentional risks. *Theoretical Issues in Ergonomics Science*. https://doi.org/10.1007/s10111-021-00690-z

Khaliq, S., Tariq, Z. U. A., & Masood, A. (2020). Role of user and entity behavior analytics in detecting insider attacks. *2020 International Conference on Cyber Warfare and Security*. https://doi.org/10.1109/ICCWS48432.2020.9292394

Kim, H., Kim, J., Park, M., Kang, P., & Cho, S. (2019). Insider threat detection based on user behavior modeling and anomaly detection algorithms. *Applied Sciences, 9*(19), 4018. https://doi.org/10.3390/app9194018

Liu, G., Kang, H., Liu, J., Meng, L., & Wang, Q. (2023). Theory and application of zero trust security: A brief survey. *Entropy, 25*(12), 1595. https://doi.org/10.3390/e25121595

Maurushat, A., Moustafa, A., & Bello, A. (2021). The role of user behaviour in improving cyber security management. *Frontiers in Psychology, 12*, 561011. https://doi.org/10.3389/fpsyg.2021.561011

Pöhn, D., & Hommel, W. (2023). Towards an improved taxonomy of attacks related to digital identities and identity management systems. *Security and Communication Networks,* 2023, 5573310. https://doi.org/10.1155/2023/5573310

Proudfoot, J., Madnick, S. E., & Cram, W. A. (2024). Weathering the storm: Examining how organisations navigate the sea of cybersecurity regulations. *European Journal of Information Systems*. https://doi.org/10.1080/0960085X.2024.2345867

Sahdev, S. L., Singh, S., Kaur, N., & Siddiqui, L. (2021). Behavioral biometrics for adaptive authentication in digital banking: Guard against flawless privacy. *2021 International Conference on Innovative Practices in Technology and Management (ICIPTM).* https://doi.org/10.1109/ICIPTM52218.2021.9388364

Schinagl, S., & Shahim, A. (2020). "From the basement to the boardroom": Towards digital security governance. *Information & Computer Security, 28*(2), 261–292. https://doi.org/10.1108/ICS-02-2019-0033

Tian, T., Zhang, C., Jiang, B.-S., Feng, H., & Lu, Z. (2025). Insider threat detection for specific threat scenarios. *Cybersecurity, 8,* Article 21. https://doi.org/10.1186/s42400-024-00321-w

Tuqan, A., & Asmar, M. (2024). Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon, 10*, e37571. https://doi.org/10.1016/j.heliyon.2024.e37571

Waqas, M., Hania, A., Yahya, F., & Malik, I. (2023). Enhancing cybersecurity: The crucial role of self-regulation, information processing, and financial knowledge in combating phishing attacks. *SAGE Open, 13*(4). https://doi.org/10.1177/21582440231217720

Zhang, C., Zhan, D., Yin, M., Wang, S., Wang, T., & Yu, T. (2021). Detecting insider threat from behavioral logs based on ensemble and self-supervised learning. *Security and Communication Networks*, 2021, 4148441. https://doi.org/10.1155/2021/4148441