WJAETS

World Journal of Advanced Engineering Technology and Sciences

eISSN: 2582-8266

Cross Ref DOI: 10.30574/wjaets

Journal homepage: https://wjaets.com/

(Review Article)

Check for updates

Zero Trust Identity and Access Management Aligned with IT Service Management for Financial Institutions

Rashmi Bharathan *

University of Madras, Chennai, Tamil Nadu, India.

World Journal of Advanced Engineering Technology and Sciences, 2025, 17(02), 514-521.

Publication history: Received on 19 September 2025; revised on 20 November 2025; accepted on 24 November 2025

Article DOI: https://doi.org/10.30574/wjaets.2025.17.2.1366

Abstract

The alignment of cybersecurity resilience and efficiency has already emerged as a priority agenda among financial entities, which are experiencing dynamic threats in the digital world as well as demanding compliance requirements. This paper provides a broad framework that will combine Zero Trust Identity and Access Management (IAM) with Information Technology Service Management (ITSM) to come up with an integrated, governance-based vision of digital protection and service resilience. The model reinvents identity as the new security perimeter by implementing the Zero Trust principle of never trust, always verify, so that there is ongoing authentication, contextual authorization, and least-privilege enforcement of hybrid infrastructures. These controls are implemented by the IAM, which acts as the operational engine, and ITSM, which offers the process discipline of change management, incident handling, and compliance traceability. By use of conceptual analysis, process mapping, and practical alignment tables, the article illustrates how this convergence facilitates auditable identity work flows, automated service fulfillment, and the cyclical service improvement that is specific to financial regulatory frameworks. Critical implementation lessons, issues, and quantifiable performance metrics are established, and finally, a progressive roadmap to enable strategic adoption is provided. This alignment has not only resulted in the mitigation of cyber risk and insider threats, but it has also brought about operational agility, regulatory preparedness, and customer trust. The paper concludes that the implementation of Zero Trust IAM into the processes of ITSM would change the access control methodology as an individual element of security into an enterprise-wide management framework that is needed in the changing digital-finance landscape.

Keywords: Zero Trust; Identity and Access Management (IAM); IT Service Management (ITSM); Financial Institutions; Regulatory Compliance; Digital Trust; Cybersecurity Governance

1. Introduction

Financial institutions are operating in a highly complex and high-stakes operational environment in the modern digital era that has been influenced by a combination of various critical factors. The most notable of these are the increase in complex cyber threats, the rise in the number of global regulatory compliance requirements, and the violent digitization of the money and customer engagement platforms. These dynamics are demanding more than ever on banks, investment firms, insurance firms, and other financial institutions to build and sustain strong, dynamic, and resilient IT infrastructures. Here, the inter-correlation among three vital areas, such as cybersecurity, identity governance, and IT service management (ITSM), is not only recommendable but also a prerequisite of institutional stability and survival. First in this alignment is the increased need to ensure sensitive data assets, such as personal customer data, authentication credentials, and high-value transactional records, are not abused internally or attacked externally. Simultaneously, these institutions should provide a smooth continuity of mission-critical services, including digital banking platforms, trading systems, and core financial applications. All this has to take place in the glare of stricter standards of audit oversight and industry-specific regulation practices, including the General Data Protection

* Corresponding author: Rashmi Bharathan.

Regulation (GDPR) in Europe, the Gramm-Leach-Bliley Act (GLBA) in the United States, and the financial risk and operational resilience standards of Basel III [1][2].

In a bid to address such needs, organizations are increasingly moving towards the Zero Trust model of security, a paradigm shift out of the conventional perimeter-based security frameworks that presuppose trust within a specified network perimeter. Zero Trust security is based upon the principles of never trust, always verify, i.e., all users, devices, and applications inside or outside the enterprise perimeter are not trusted by default [3][4]. This is a model that assumes that breaches are unavoidable, hence the need for constant authentication, least privilege access, and extensive logging and monitoring of user behavior and system usage [4]. By so doing, Zero Trust architectures generally decrease attack surface considerations and restrict across-the-network movement, as well as improve detection and containment capabilities of breaches to the organization. Parallel to the concept of the adoption of Zero Trust is the transformation of Identity and Access Management (IAM) systems, which have now taken the form of the basis of providing secure, fine-grained, and policy-driven control of user identities, device access, and privileged operations of complex and hybrid IT environments. IAM is critical in the implementation of security policies, administration of digital identities, role-based access control, and automation of user credential lifecycle [5][6]. Specifically, IAM systems facilitate authorization in real-time, minimize the danger of insider assaults, and aid regulatory necessities concerning identity administration and information security [7]. At the same time, IT Service Management (ITSM) offers a systematic and rigorous methodology for the organization, provision, operation, and ongoing enhancement of IT services in accordance with business objectives. ITIL (Information Technology Infrastructure Library) and other frameworks are best practices in incident management, problem resolution, service request fulfillment, change control, and service level management [8]. The practices are essential in ensuring high availability, reliability, and performance of IT services, particularly in those environments where downtime or disruption of services may lead to financial losses, damage to reputation, and regulatory fines [9]. It is against this backdrop that this paper puts forward the suggestion that financial institutions should no longer engage in siloed application of security, identity governance, and service management. Rather, they ought to implement a converged approach that incorporates the precept of Zero Trust concepts in IAM frameworks and entrench them in ITSM models to implement integrated access governance. This combined system improves security status and, at the same time, fosters IT efficiency, user productivity, and compliance goals. Based on this, the study will continue with a comprehensive definition of each area, discuss strategic and operational synergies among them, implementation considerations, and finally provide important challenges, success measures, as well as a roadmap to adoption.

2. Zero Trust Architecture in Financial Institutions

Continuing on the presentation of the modern threat landscape and the requirements of modern services, there exists a need to discuss the application of the Zero Trust architecture (ZTA) in terms of the financial industry. In a Zero Trust regime, implicit trust in users, network segments, or devices is substituted with uninterrupted validation of identity, device posture, session context, and user behavior of each request [5]. This is of particular concern in the environment of financial institutions, where the value of data assets may be high, and the regulatory exposure and the need to integrate with third parties are frequent occurrences [3], [6]. To illustrate, financial organizations are experiencing growing insider threats, sophisticated phishing attacks, credential usage, and subsequent network lateralization; Zero Trust is a solution to this, imposing least-privilege access, micro-segmentation, and active monitoring [3], [10]. One of them is that all interactions, either between an internal user and a remote device or between an external partner API, have to be authenticated and authorized, and access should only be granted to the minimal set of resources necessary, and preferably within a limited period. The model will assist in minimizing the area of attack, restricting sideways movement, and ensuring that the attack is contained or minimalistic [11]. In addition, the regulatory environment of financial institutions (e.g., the requirement to do identity verification, encryption, and audit logging) is fairly in line with the Zero Trust principles [12]. Therefore, the application of ZTA in a financial institution assists in inculcating the security culture of assume breach, verify, minimize access, which augments the requirement of a financial institution to guard integrity, confidentiality, and accessibility of services.

3. Identity and Access Management (IAM) as the Core of Zero Trust

As much as the Zero Trust architecture offers the overall philosophy of security, the specifics of its implementation depend on how Identity and Access Management (IAM) is designed and managed. As we will observe, it is imperative that IAM is aligned with the ITSM processes. IAM involves mechanisms and processes that enable organizations to manage digital identities (human and machine), authenticate and authorize access, govern privileges, and monitor access behavior within the environment [13-15]. The significance of IAM is increased in a Zero Trust environment, as identity becomes the new control perimeter, such that access decisions are based on continuous verification of identity, device, session context, and behavior [16]. In the case of financial institutions, the IAM should facilitate the process of identity provisioning and de-provisioning, role-based and attribute-based access control, multi-factor authentication (MFA), just-in-time (JIT) access, and strict review of privileged accounts [8], [17]. Additionally, IAM should be connected to the constant monitoring systems and threat analytics to identify suspicious or malicious use or credential misuse. IAM is the engine-room of Zero Trust: in effect, they are used to ensure that the identities that operate under the least-privilege principle are only verified identities, access is limited, identity transactions are logged, and must be input to the audit and compliance processes. Thus, to a financial institution that aims to make use of Zero Trust, a solid IAM design is a must-have requirement, and this should be dynamic, context-dependent, and aligned with the control environment.

4. IT Service Management (ITSM) in Financial Institutions

Now that the concept of Zero Trust and IAM has been mentioned, the next puzzle piece is the IT Service Management (ITSM), which offers the process and governance foundation of delivering capabilities of IT in line with the business objectives. ITSM is the collection of policies, procedures, processes, and tools that an organization utilizes to design, deliver, manage, and enhance the IT services that are delivered by the organization to its stakeholders [10], [12]. In the financial services industry, the ITSM role becomes particularly acute as downtime and service interruption can be directly related to financial loss, compliance violations, and reputation damage [11]. Proper ITSM models facilitate formal change management, incident management, problem management, change management, configuration and asset management, service catalog management, and enhancement [16], [10]. An example is the core systems environment of a bank, ITSM would provide that the changes are monitored, configurations are familiarised, service requests are met to agreed SLA, incidents are managed promptly and proactively, and risk is managed throughout the service cycle [11][18]. In such a manner, ITSM helps not only to ensure the reliability of operations and quality of the provided services, but also provides the security, audit readiness, and compliance with the regulations, thereby creating a logical complement to Zero Trust IAM initiatives.

5. Aligning Zero Trust IAM with ITSM Processes

The above sections presented the basic concepts of Zero Trust, IAM, and ITSM; we proceed to discuss how they make sense and integrate with each other, and why this sense is important to financial institutions. The main argument here is that without the identity lifecycle and access processes being integrated into the larger ITSM-managed service workflow, IAM alone (even in Zero Trust) cannot be relied upon. As an illustration, the process of onboarding a new employee not only includes creating a user identity and providing access (IAM functionality) but also the registration of the service request, connection to asset management, change process authorization, device configuration, and auditing status, all ITSM operations. Likewise, a privileged access request to a high-risk financial system should pass through ITSM change control, risk review, logging and audit trail, and then IAM least privilege enforcement, contextual authorization, and anomalous usage monitoring.

Table 1 Integration Points Between Zero Trust IAM and ITSM Workflows

Functional Domain	IAM Objective	Aligned ITSM Process	Outcome for Financial Institutions
Identity Provisioning	Create and assign user credentials with least-privilege roles	Service Request Fulfillment	Standardized, auditable onboarding process
Access Review	Enforce periodic privilege recertification	Continual Service Improvement (CSI)	Early detection of orphaned or over-privileged accounts
Privileged Access	Grant temporary, contextual administrative rights	Change Management	Governance and logging of high-risk activities
Incident Correlation	Detect and respond to credential misuse	Incident & Problem Management	Faster root-cause analysis and mitigation
Access Termination	Revoke credentials upon role exit or contract end	Configuration Management Database (CMDB) update	Real-time removal of unused identities and reduced attack surface

Through IAM and ITSM alignment, financial institutions can be able to make the identity and access events visible, traceable, and auditable, and undergo the normal service-delivery processes and not ad hoc administrative silos. It is also facilitated by continuous improvement, as IAM metrics (number of orphaned accounts, privileged access violations, access-review lapses) can be used as input to the ITSM continual service improvement (CSI) process. Effectively, the zero trust IAM conformity to ITSM turns the access governance from a security undertaking into a wholesome service-delivery and risk-management field.

The alignment transforms fragmented processes of security and service into a consolidated governance model by mapping these touchpoints. This synergy ensures that the workflows of the operations are streamlined, but also enhances regulatory compliance, which is a critical one in financial ecosystems.

6. Key Implementation Considerations for Financial Institutions

A change to an aligned Zero Trust IAM + ITSM model within a financial institution will require a variety of strategic, technical, and operational considerations, and this section will cover the key ones that need to be considered when changing towards an effective adoption. To begin with, the C-suite should lead by example: a cross-functional (security, IT operations, risk/compliance, business units) and well-defined transformation roadmap should be sponsored by the leadership and government. The absence of governance leads to the easy disintegration of IAM and ITSM initiatives or pilot stage. Second, identity life cycle management needs to be sound: identity provisioning, role-based and attribute-based access models, de-provisioning, identity mapping between systems, and liaison with HR/ERP systems shall be highly monitored. This is in the context of financial institutions, relating to the core banking platforms, reporting systems to regulatory bodies, and also to external partners. Third, contextual and continuous authorization: the principle of Zero Trust requires access decisions, which depend on the current context (health of device, user behavior, location, time, risk of transaction) and not just on the assigned role [5], [8] [19]. Fourth, ITSM processes also require re-engineering to include identity/access workflows: change management should include user-access change; incident management should include identity compromise; configuration management should include identity directory, device, and privileged account tracking; service-request fulfillment needs to include IAM steps and audit capture. Fifth, monitoring, analytics, and audit: identity usage needs to feed into the SIEM/UEBA systems, access reviews need to be automated, privileged sessions need to be logged and associated with incidents, and access metrics need to be linked to ITSM dashboards to continually improve. Sixth, regulatory and compliance alignment: in a financial institution, regulatory frameworks (e.g., PSD2, DORA, FFIEC, PCI-DSS) dictate the presence of certain identity and access requirements (MFA, segregation of duties, audit logs) and ITSM processes should be reflected in these terms of the documented workflows, audit trails and reporting [6], [17] [20]. Seventh, technology architecture: IAM solutions, access gateways, privilege-access management (PAM), identity-governance tools, micro-segmentation, cloud- and hybrid-deployment solutions need to be chosen keeping service-oriented architecture in mind and deployed together with ITSM tooling (CMDB, service-catalog, incident/change modules). Finally, the success of any phased rollout or pilot-to-scale approach depends on careful execution. Instead of a disruptive enterprise-wide change, begin with high-risk systems, optimize workflows, refine metrics and governance, and then gradually expand the implementation across the entire organization.

7. Challenges and Risk Mitigation

Although the advantages of matching Zero Trust IAM with ITSM are strong, financial institutions should be aware of and address the major challenges and risks that come with change. An example of such a challenge is cultural change and stakeholder buy-in: the transition between perimeter-based security and identity-based models, and the introduction of IAM into the ITSM processes, will necessitate a shift in roles, workflows, and stakeholder responsibilities - the change is likely to be met with resistance. The other difficulty is that of legacy systems and technical debt: most banks have monolithic core platforms, siloed identity stores, and disconnected service-management tools. These are supposed to be rationalized or incorporated, which is costly and time-consuming. Another factor is complexity and change fatigue: the mapping of identity workflows, linking them to ITSM processes, the creation of contextual authorization engines, and monitoring systems can cause tremendous complexity in operations and the risk of disruption. Moreover, security and user experience are a sensitive balance to strike: excessively restrictive access mechanisms can slow down the business, introduce workarounds, and lead to shadow IT. On the risk side, inadequate alignment can introduce gaps: e.g., user access, which is represented by IAM, and not recorded in ITSM change logs, or service requests being bypassed in identity review, and therefore introducing audit and compliance risks. The mitigation strategies against these risks can be classified into strong governance with executive backing, gradual delivery through pilots, comprehensive change management (via stakeholder training and communication), manual labor reduction through automation and enhanced reliability through more frequent measurement and feedback, and iterative improvement through ITSM. Moreover, the regular risk assessment, identity-access reviews, penetration tests, and tabletop exercises will be useful to ensure the integrated model is also effective in the long term.

8. Metrics, Monitoring, and Continuous Improvement

Following the discussion on implementation and associated challenges, the next focus is on defining how the success of financial institutions will be measured and how the integrated Zero Trust IAM and ITSM model should be updated and continuously improved. Some of the key performance indicators (KPIs) must include identity/access measures, service delivery measures, and risk/compliance measures. Key identity and access metrics include the number of orphaned accounts, the count of unreviewed privileged accounts, the percentage of users granted just-in-time access, the frequency of conditional access failures, the number of lateral movement detections identified through IAM analytics, and the average time required to deprovision accounts when employees exit the organization. Key service delivery metrics, aligned with ITSM principles, include the number of incidents arising from identity or access issues, the mean response time for identity and access services, the count of changes restricted due to missing identity impact assessments, customer satisfaction levels for IAM-enabled services, and the compliance rate for access-related service requests. Key risk and compliance metrics include the number of audit findings related to identity and access, the percentage of timely completed access reviews, the frequency of access violations, any regulatory fines or warnings linked to identity management, and the reduction in average time required to detect identity-related threats. Notably, the cycle of continual service improvement (CSI) of ITSM is to be fed with these metrics that should be identified in search of improvement opportunities, corrective workflow, measurement, and re-measuring. By so doing, the institution establishes a feedback mechanism that leads to increased maturity with time and maintenance of a favorable balance between identity governance, service management, and security objectives.

Table 2 Key Performance Indicators for Zero Trust + ITSM Alignment

Metric Category	**Indicator**	**Measurement Objective**	**Improvement Leverage**
IAM Efficiency	Average time to grant/revoke access	Assess the responsiveness of the identity lifecycle	Automate provisioning via ITSM workflows
Security Posture	Number of high-risk access anomalies detected monthly	Evaluate Zero Trust enforcement	Tune contextual access rules using analytics
ITSM Integration	Percentage of access-related tickets auto-approved through IAM validation	Measure operational efficiency	Enhance IAM-ITSM API automation
Compliance Readiness	Audit findings related to identity governance	Monitor adherence to regulatory norms	Embed compliance workflows in ITSM change control
User Satisfaction	Service-request resolution rating	Quantify user trust and usability	Balance security and user experience through self-service IAM portals

These KPIs can assist in developing a feedback loop where the security as well as service activities are constantly enhanced by means of quantifiable intelligence. This systematic analysis creates an automatic progression to the creation of a strategic roadmap of progressive institutional adoption.

9. Roadmap for Adoption in Financial Institutions

To synthesize all of the above into an operational plan to follow, this section presents a proposed roadmap when implementing a Zero Trust IAM in line with ITSM in a financial institution, as shown in Figure 1. Initial evaluation and plan, conduct an identity and access maturity evaluation, chart current IAM and ITSM procedures, determine the most hazardous systems and service processes, and put in place a governance framework (steering committee, consisting of security, IT operations, business, and compliance). Second phase pilot design, pick a moderately important service (say, privileged access to a risk-management system or third-party integration) and re-architecturally rewrite its service-request and change-control processes as well as its identity provisioning processes based on alignment. Implement IAM enhancements (MFA, contextual access, access reviews), combine identity operations with ITSM service-catalog and CMDB. Third phase growth, expand the refined model to cover the wider range of services, provide enterprise-wide identity-governance and privileged-access control, contextual authorization, automate identity-access assessment and identity-incident monitoring, connect IAM logs to ITSM incident/problem logs and ITSM dashboards. Fourth phase optimization and automation, deploy anomaly detection analytics and machine learning to identify identity usage, deploy de-provisioning, deploy identity-access metrics to ITSM dashboards, implement secure controls on self-service workflows, micro-segmentation, and service-level access gating. The fifth step includes continuous improvement and maturity. Establish continual service improvement (CSI) processes, monitor key performance indicators, conduct third-party audits and compliance readiness assessments, and adjust governance models and technologies in response to emerging threats or regulatory developments such as open banking, API access, and cloud security requirements. Stakeholder communication, change-management training, service-catalog updates, asset and identity alignment, as well as risk-management integration, are also necessary throughout the roadmap.

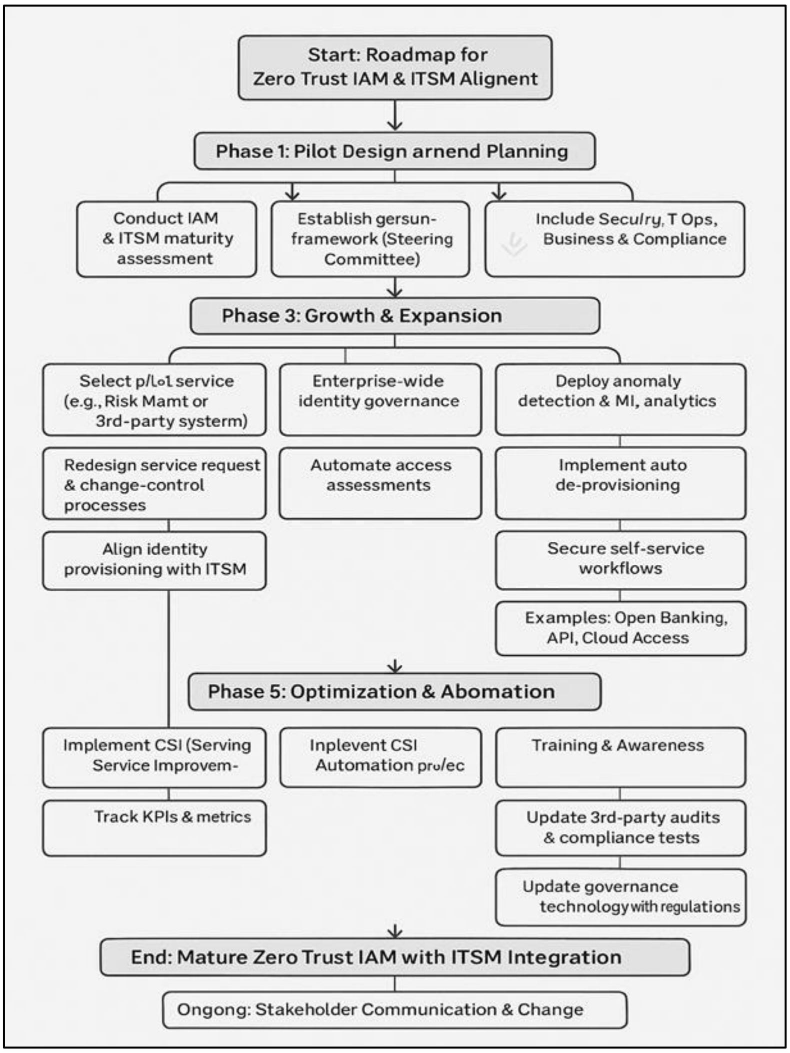
Start: Roadmap for Zero Trust IAM & ITSM Alignent
Phase 1: Pilot Design arnend Planning
Conduct IAM & ITSM maturity assessment
Establish gersun-framework (Steering Committee)
Include Seculry, T Ops, Business & Compliance
Phase 3: Growth & Expansion
Select p/Lol service (e.g., Risk Mamt or 3rd-party systerm)
Enterprise-wide identity governance
Deploy anomaly detection & MI, analytics
Redesign service request & change-control processes
Automate access assessments
Implement auto de-provisioning
Align identity provisioning with ITSM
Secure self-service workflows
Examples: Open Banking, API, Cloud Access
Phase 5: Optimization & Abomation
Implement CSI (Serving Service Improvem-
Inplevent CSI Automation pro/ec
Training & Awareness
Track KPIs & metrics
Update 3rd-party audits & compliance tests
Update governance technology with regulations
End: Mature Zero Trust IAM with ITSM Integration
Ongong: Stakeholder Communication & Change

Figure 1 Roadmap for Zero Trust IAM and ITSM Alignment

This flowchart outlines a phased approach to integrating Zero Trust Identity and Access Management (IAM) with IT Service Management (ITSM). It begins with initial assessments and governance setup, progresses through pilot implementation, enterprise expansion, optimization via automation, and culminates in continuous improvement. Ongoing stakeholder communication and change management support the transition toward a mature, integrated Zero Trust IAM-ITSM model.

10. Case for Financial Institutions: Benefits and Business Value

With the road map in place, this section makes the case for why alignment of Zero Trust IAM with ITSM offers real business value in financial institutions. First, greater risk reduction is achieved through treating identity as the new perimeter and integrating identity governance into the service workflows. Institutions lessen the likelihood and ill effects of breaches, decrease lateral movement, tighten privileged access, and also enhance detection and response time. This not only safeguards the reputation, but also prevents financial losses due to fraud and non-compliance with regulations [3], [17]. Second, enhanced operational efficiency matching IAM and ITSM eliminates workflow differences, mitigates manual ticketing and provisioning delays, facilitates access changes going through controlled service-request and change-control processes, and results in faster fulfillment with better audit trails. Third, compliance-ready financial institutions under a high level of regulation have structured and audit workflows of services connecting identity events with CMDB/change logs/incidents, which are used to support audit and regulatory reporting. Fourth, a better user experience through introducing identity and access management into service-request processes and using just-in-time access and contextual authorization, end-users (employees, business partners) receive smoother and faster access, and reduced access risk is controlled. Fifth, cost management and agility, automating identity-access reviews, orphaned accounts, and manual ticketing, lowers the cost of ownership and, as a result, allows secure cloud, hybrid, and partner access to support current business models like open banking and API-centric services [1], [4]. Overall, the aligned model contributes to the secure and agile requirements of current financial services.

11. Future Trends and Considerations

Lastly, in the future, financial institutions that implement a congruent Zero Trust IAM + ITSM model need to expect and adapt to new trends in technology, threat evolution, and regulatory change. The increasing number of non-human identities (machine, API, robotic-process identities) and the fading of human-machine identity boundaries is one of such trends; identity governance has to adapt accordingly [17-20]. The other pattern is the shift in favor of cloud-native, microservices architectures of financial services, which requires identity-and-access control solutions that are dynamic, decentralized, and able to provide federated identity, privileged access, and enforcement of Zero Trust on a scale [4]. Threat analytics developed based on AI/ML will be integrated into IAM and ITSM and will allow the real-time identification of suspicious access patterns, a score of risks, and proactive mitigation. In addition, regulatory schemes like open-banking/fintech partnerships, API-exposure statutes, and data-sovereignty legislations and regulatory-resilience rules (e.g., DORA) will proceed to bring identity, access, and service administration [6]. Lastly, with the further rise of financial institutions taking up DevSecOps and platform engineering practices, identity-access lifecycle and service-management workflows will have to be implemented in CI/CD pipelines, self-service capacity, and infrastructure as code will turn the alignment between IAM and ITSM not only desirable but also the foundation of future-ready operations. Those institutions that develop such resilience and agility in the current time will be in a better position to take the next generation of digital finance.

12. Conclusion

In summary, the integration of Zero Trust Identity and Access Management with the IT Service Management processes can provide financial institutions with a single and mature method of access security, service delivery, and compliance with regulatory and operational requirements. With identity becoming the new perimeter and with access governance integrated into service processes, institutions will be able to minimize risk, create additional operational efficiency, and also address future digital finance requirements. Implementing such a framework is complex, demanding strong governance, process redesign, robust technology architecture, well-defined metrics, and continuous improvement. However, the business value is evident, and it is increasingly becoming a standard requirement across the financial industry. With the adoption of a step-by-step roadmap, tracking key measures, and maintaining constant improvement of services, the financial institutions will be in a position to achieve a well-rounded, audit-able, agile, and secure identity-access-service management ecosystem.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] McCoy, E. (2025). Cybersecurity Regulations and Risk Management in the Financial Sector: A Comparative Analysis. *Law, Economics and Society*, *1*(1), p115-p115.

[2] Cifci Bariche, S. (2024). The Digital Operational Resilience Act-Case study on one financial institution's implementation phase.

[3] Kindervag, J. (2010). Build security into your network's DNA: The zero trust network architecture. *Forrester Research Inc*, *27*, 1-16.

[4] Seefeldt, J. (2021). What's new in NIST Zero Trust Architecture? *NIST Special Publication*, *800*, 207.

[5] Osmanoglu, E. (2013). *Identity and access management: business performance through connected intelligence*. Newnes.

[6] Nickel, J. (2016). *Mastering Identity and Access Management with Microsoft Azure*. Packt Publishing Ltd.

[7] Force, J. T. (2017). *Risk management framework for information systems and organizations: A system life cycle approach for security and privacy (discussion draft)* (No. NIST Special Publication (SP) 800-37 Rev. 2 (Draft)). National Institute of Standards and Technology.

[8] Gallacher, L., & Morris, H. (2012). *ITIL Foundation Exam Study Guide*. John Wiley & Sons.

[9] Schlette, D., Caselli, M., & Pernul, G. (2021). A comparative study on cyber threat intelligence: The security incident response perspective. *IEEE Communications Surveys & Tutorials*, *23*(4), 2525-2556.

[10] Yazici, A., Mishra, A., & Kontogiorgis, P. (2015). IT service management (ITSM) education and research: Global view. *International Journal of Engineering Education*, *31*(4), 1071-1080.

[11] Addy, R. (2007). *Effective IT Service Management*. Springer.

[12] Serrano, J., Faustino, J., Adriano, D., Pereira, R., & Da Silva, M. M. (2021). An it service management literature review: Challenges, benefits, opportunities, and implementation practices. *Information*, *12*(3), 111.

[13] Anand, D., & Khemchandani, V. (2019). Identity and access management systems. *Security and Privacy of Electronic Healthcare Records: Concepts, Paradigms and Solutions*, 61.

[14] Martínez, A. L., Naghmouchi, M., Laurent, M., Alfaro, J. G., Pérez, M. G., & Martínez, A. R. (2025). Breaking barriers in healthcare: A secure identity framework for seamless access. *Computer Standards & Interfaces*, 104020.

[15] Mohammed, I. A. (2017). Systematic review of identity access management in information security. *International Journal of Innovations in Engineering Research and Technology*, *4*(7), 1-7.

[16] Kumar, P. (2025). Securing Digital-First Healthcare: AI, Blockchain, and Cloud Architectures for Personal Health Data Protection. *International Journal of Applied Mathematics*, *38*(7s).

[17] Azhar, I. (2014). Economics of Identity and Access Management: Providing decision support for investments. *Ishaq Azhar Mohammed. (2014). Economics of Identity and Access Management: Providing decision support for investments. International Journal of Management, IT and Engineering (IJMIE)*, *4*(2), 540-549.

[18] Kumar, P (2025). Next-generation secure authentication and access control architectures: advanced techniques for securing distributed systems in modern enterprises.

[19] Kumar, P. (2024). AI-Powered Fraud Prevention in Digital Payment Ecosystems: Leveraging Machine Learning for Real-Time Anomaly Detection and Risk Mitigation.

[20] Johnson, M. W., Hately, A., Miller, B. A., & Orr, R. (2007). Evolving standards for IT service management. *IBM Systems Journal*, *46*(3), 583-597.