Making the most of IAM Technology in Financial Services Industry

Avancer
Simplified IT Security

Executive Summary

In this white paper, we will explore various technological aspects of implementing IAM Solutions in Financial Services Industry. It includes basics of managing identities, understanding challenges in implementing IAM Solutions, harnessing IAM technology in the changing IT ecosystems. Within the financial services industry, the increasing demand from the business for getting reliable and efficient access given to the employees, partners, contractors, partners or customers, is a complex task. There is a greater need for achieving a balance between providing information to right set of users while ensuring that sensitive personal data is safe.

This calls for a strategic focus when it comes to achieving compliance, managing risk and administering identity/access. The financial services industry, faces significant challenges in managing data in a secure manner, while complying with various regulatory mandates, along with providing seamless user experience across complex and growing IT infrastructure. Reason why financial services enterprises require robust identity management systems that would help them approach security and compliance in a holistic manner.

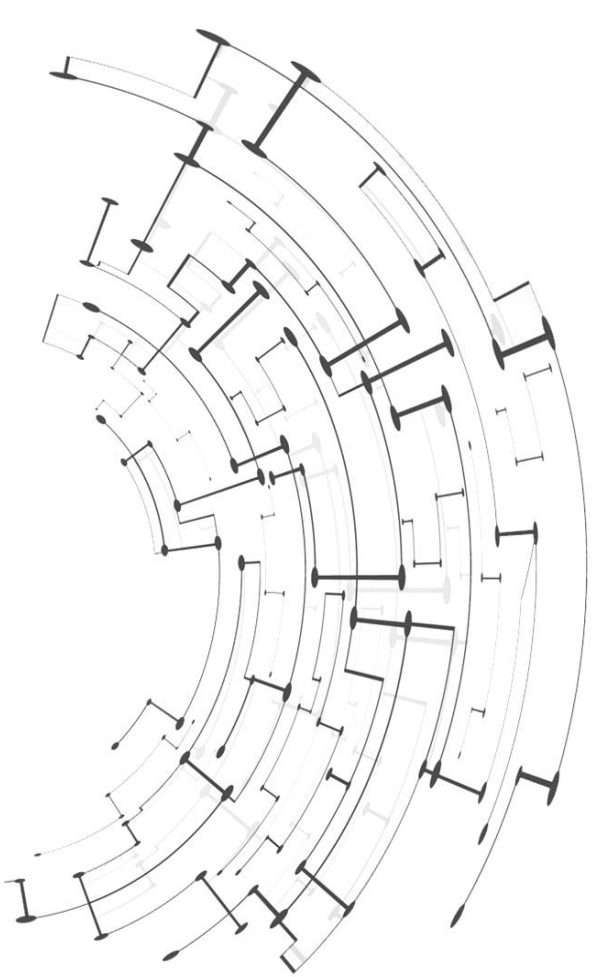
IAM capabilities in financial services environment are required for managing identities in complex IT environment. It unifies data – based on identity – from all the systems, applications and platforms under a repository guided through Active Directory Integration. This helps organizations to gain control and achieve better visibility of user's actions, thereby reducing risk. With the implementation of IAM Solutions, financial organizations minimize risk of information/data loss. It also provides in-depth knowledge around ineffective and inefficient processes in an organization.

Best Regards,
Rajesh Mittal
CTO, Avancer Corporation

Rajesh Mittal, CTO at Avancer Corporation

With a solid understanding of all aspects of IT security field Rajesh has assisted clients, in almost all industrial segments, for a strategic IAM implementation. His core competency and passion lies in integrating heterogeneous products, fostering innovation to develop new Solutions and solving customer problems quickly and effectively.

Table of Contents



Overview of FinTech Capabilities

With continued adoption of various customer engagement models, along with innovative mobile and cloud technologies, the financial services industry is at a constant flux to create a robust Identity Management solution for securing its data. In the current digital environment, Identity and Access Management (IAM) in Financial Services has moved beyond mere provisioning and ensuring correct access. IAM in Financial Industry covers a wide range of users, devices and applications – leading to upsurge in quantified identities.

Furthermore, the Identity dynamics is not limited to employees, but also includes consumers and third-party vendors. Integration strategy of IAM (and IT Security Solutions) in the current environment has to proactively take into account the vulnerabilities emanating from sensitive data, digital assets and intellectual property. This is to be achieved together with enablement of systematic requirements keeping together hybrid IT Systems.

Financial Sector needs to be aligned with IAM capabilities as various aspects of financial operations need to comply with regulatory and compliance norms, including SOX, OMB A-123, Basel II, Consumer Privacy, Data Privacy, Check 21, Anti-Money Laundering, SAS 70, BSA, MiFID, PATRIOT Act etc. are making it all the more imperative for businesses to follow suite.

Financial Services industry has to bring Consumer Identity and Access Management (CIAM) to support digital business strategies, minimize security risks and continuously improve consumer's digital services experience. Financial enterprises face major challenges in providing information security as well as adhering to compliance, while trying to meet the growing demands of various IT platforms and emerging technologies. The struggle with dynamic and convoluted IT environment is that the complexities related to IAM technology has gone up exponentially.

Integrating IAM technology now includes connecting with cloud applications, IoT synchronized, active directory management, privilege accounts management, access governance, mobile access certifications, and so on. There is a high risk with cyber criminals to conduct sophisticated cyber-attacks and procure highly sensitive personal information. In case of financial institutions, the personal information could be monetary in nature. Therefore, it adds greater responsibility on the part of businesses in financial industry. In addition to self-driven checks, many businesses in the financial sphere need to comply with regulatory and compliance norms, including SOX, OMB A-123, Basel II, Consumer Privacy, Data Privacy, Check 21, Anti-Money Laundering, SAS 70, BSA, MiFID, PATRIOT Act etc. are making it all the more imperative for businesses to follow suite.

In this white paper, we will explore various technological aspects of implementing IAM solutions in Financial Services Industry setting. It includes basics of managing identities, understanding challenges in implementing IAM Solutions, harnessing IAM technology in the changing IT ecosystems.

IAM Implementation Challenges in Financial Services Industry

With cloud services as well as mobile apps as the go to option for boosting efficiency, productivity and pruning costs, user identity management, together with accessing IT resources, has become challenging and important component. The ever-changing IT environment must align with access for data and/or applications by partners, employees or others user accessing digital assets from multiple locations and devices, without having to compromise on security issue. A few concern areas are listed as under:

- **One user - many devices - multiple applications usage has led to exponential Identity creation.** Identity is no more about a user; it is about a user, the devices connected to a user and the applications accessed by a user through various assigned devices. This creates a conundrum of identities that grows exponentially. It boils down to the number of identities held by single user, thereby creating multiple identities for monitoring, organizing and access controls.
- **Creation of orphan user accounts that means creating an identity without a defined owner.** Users often make accounts in the systems without declaring a clear owner. Many cases were reported, wherein, an account belonging to an application is used only once a year, but was considered important. Most cases are regarding a person creating an account which remains inactive for a long time, but cannot be treated dead. Such orphaned accounts are often used to gain unauthorized access to a company's sensitive data.
- **No clear procedure for monitoring of user accesses.** Monitoring of access should be strictly followed. It is a difficult procedure to follow, which often leads to hackers gaining access to unmonitored users, apps or processes. This also results in inconsistent report of IT audits and created complexity in achieving compliance to relevant regulations.
- **Patchy control of privileged accounts leads to data breaches.** Another important issue is lack of control over privileged application access. This may include accounts of super-user, as these accounts may be easy to locate within an organization, and very crucial to keep a tab on accesses made through these accounts. This is all the more important in a scenario, wherein, temporary permissions are allocated to users, and revoking the access is not executed. Abuse of privileged accounts is a major cause of data breaches in big organizations; as such accounts help hackers in bypassing and breaking through firewalls.
- **Users provided with accesses that are not required.** It has been observed in many situations that individuals are given access to information or data they might not need. Providing access to data that are not needed by a user increases the chance of data theft and misuse of the user access. A defined process should be followed and enforced to ensure that the systematic flow for accesses is maintained in all situation.

Given the ever-changing IT environment, one of the major tasks is managing access to various data or applications by partners, employees or others user accessing digital assets from multiple locations and devices, without having to compromise on security issue.

Conventional Approach to IAM Integration

An IAM System is a framework that helps businesses manage electronic identities in a secure manner by initiating, capturing and recording user identities, along with providing automated access permissions as per user role. It ensures granting access privileges as per business policy, which include that the users are audited, authenticated and authorized properly. Given the complexity of accesses, identity authentication and governance requirements, it is apt to say that a poorly integrated IAM Solution and associated tools may lead to various IT related vulnerabilities. They could be in the form of data security, information governance, cyber theft and complexities related identity dynamics. Financial Services industry is especially seen to be integrating IAM solutions into their systems to deal with emerging regulatory changes, addressing non-compliance issues, along with data breach curbs.

Here's how conventional IAM solutions integration helps in securing IT Systems in Financial Services Industry:

- **Provision access to right set of applications, data sets or information repositories.** Managing the assignment of users securely, especially in case where the business has been trying to meet the demand from the customers and changing as per technology upgrade. Granting access to right set of applications helps in bringing efficiency in workflows for financial organizations.
- **De-provisioning, i.e. user's access revoked upon termination from the role.** It helps in eliminating security gap as well as policy violation which can occur after an employee is out of the organization. This discourages anyone to take information out of the system once an employee of out of the role. It is a crucial capability, given the model and information available in financial enterprises.
- **Ensure robust privacy controls through Segregation of Duties (SoD).** Given that the nature of information and data utilized in financial services sector, it is imperative that excessive system access is discouraged. Such a practice might allow the person to execute transactions across the spectrum of an organization which can cause irreversible damage, leading to higher chances of fraud and data theft. Implementing SoD ensures that an employee or user is not granted authority to execute two or more conflicting sensitive transactions that might impact financial processes such as balance sheet or statements and such an activity is escalated.

Data security, Information governance, cyber theft and complexities related identity dynamics in Financial Services industry is seen while integrating IAM solutions into IT systems.

- **Create uniformity in access policy.** IAM provides enforcement and administration of access policies across common user over various systems, thereby helping organizations to effectively comply with the policy requirements. In a financial services enterprise, lack of uniformity in access policy creates significant risks, cost impact and resource effort during an audit. It is required to address these issues as well as step-up for security review and compliance audit too, which could be taken care of with the implementation of IAM.

Temporary permissions allocated to users without revoking access in time might help hackers in bypass and break through firewalls. A defined process should be followed and enforced to ensure systematic flow of accesses is maintained in all situations.

- **Assign verified access rights.** IAM systems provide the capability of assigning access rights in accordance to corporate policies, which could be verified periodically as well. Financial services enterprises are required to comply with various regulatory requirements and need to securely manage the task of assigning user access rights. With a robust IAM system, financial companies are provided with a greater level of control while receiving provisioning access, which in turn ensure regulatory compliance and lowering policy violation risks. Through IAM, verification of access rights on a regular basis, for access audit compliance can be executed.
- **Manage access as per business role.** Auditing and provisioning the access as per business role rather than IT access provides higher authenticity to the enterprise overall. In financial services set-up, role-based access control helps improving the operations and increasing return on investments as well. Further, integration of IAM helps in assessments of compliance on a periodic basis. Applying principles of role management, the process of re-certification could allow managers for working on the business role accurately and quickly.
- **Generate automated reports.** IAM system can provide an ad-hoc and timely compliance report that includes notifications regarding violations, workflow processes, and assessment reports based on thorough audits reports. It also generates a comprehensive audit and process report, across applications, users, devices and multiple IT systems across an enterprise.

Integration of IAM solutions in a financial services environment provides greater control to organizations to streamline on-boarding, termination of employees and seamlessly undertake identity change management processes. Further, it enables standard approval workflows and creates access review platform as well. A robust IAM system guarantees greater visibility into user accesses, policy compliances, role management and risk assessment, with the provision to conduct periodic reviews of all the accesses across the system.

IAM for Financial Institutions in Current IT Environment

The financial services industry includes banking, insurance, risk management, wealth management, asset management, and others are monitored at the State and Federal levels. As per the financial services or banking institution's structure and charter, it is subjected to various regulations. Until recently, regulatory changes – a few of them – were seen in Sarbanes-Oxley Act (SOx), OMB A-123, Basel II, Consumer Privacy, Data Privacy, Check 21, Anti-Money Laundering, SAS 70, BSA, MiFID, PATRIOT Act, along with Reg NMS. With the implementation of IAM solutions, organizations are assured of fulfilling governance requirements such as policy enforcement, assessing risks, auditing compliance and reducing frauds. Further, with the evolution in digital technology, financial institutions are also seen to evolve its digital capabilities, especially harnessing app-based mobile activities. This is also leading a wider need to integrate IAM capabilities that could be delivered to both mobile devices as well as mobile apps. Also, IAM is playing a major role in helping financial services companies combat cyber-attacks. **IAM capabilities for robust system financial institutions:**

- **Customized connectors:** To leverage cloud-based services effectively, it is imperative to allow On-Premise IAM to communicate seamlessly with Cloud-based IAM. This could be implemented through connectors Identity Management (IdM). Various applications are integrated in the Financial Services IT Architecture to serve the requirements of Audit, Risk & Compliance, BI & Analytics, Business Transaction Processing, Customer Experience, Enterprise IT, and so on. Several important apps in the financial sector are helping users to plan and invest in a secured and efficient manner. Solutions providers such as Oracle, Accenture, TCS, IBM, and others are known in the market for their financial services apps that are constantly updating their apps as per technology upgradation, global market liberalization, market innovation and globalization.
- **Internet-of-Things (IoT) devices integration in a single dashboard:** The potential of IoT within the financial services industry is limitless. Integration of IoT may help financial services organizations in providing better customer experience, reducing risks and redundancies, while increasing their market share, as it allows organizations to leverage data insights in real time. However, the key for successful implementation of IoT application is integration. A single IAM

With the evolution in digital technology, financial institutions are also seen to evolve its digital capabilities, especially harnessing app-based mobile activities.

dashboard helps companies to monitor the status, location and security of the devices, along with providing multiple alerts and notifications. Such analytics further help in improving business processes on a real-time basis.

- **Consumer Identity and Access Management (CIAM) implementation:** CIAM solutions are enabling financial services industry to put customers at the core of the companies by allowing them to security sign into their systems through the user's social profiles. It helps in identifying and understanding user behavior across various digital platforms – including website, mobile applications and other marketing channels. Further, it enables financial services enterprises to collect, store and analyze consumer data, which in turn, creates additional revenue opportunities and increases the brand loyalty. Further, CIAM ensures in smooth integration of Know Your Customer (KYC) initiative as well, a major driver in the financial services industry.
- **Federated Access Management (FAM) mandate:** Setting up the right IAM solution requires in-depth ground-work, ensuring a foundation for a robust identity management system. Further, it is important to constantly upgrade or patch new components in the integrated system to circumvent the risk of being obsolete in the face of newer cyber threats. That's where FAM comes into the picture, providing instant upgrades, selecting the right set of components and patches, and enabling the system to seamlessly deploy IAM processes.
- **Management of Big Data:** Financial services industry is a known implementer of Big Data solutions enabling it to take quicker decisions, optimize processes and generate insights. Organizations in the financial services industry are seen to integrate Big Data to improve customer intelligence, reduce risks, while meeting regulatory compliances. However, for an effective Big Data management, one requires to automate, accelerate, and optimize IAM solutions, while supporting current technology ecosystems.
- **Flexible IAM Capabilities:** IAM solution needs to be adaptive by using flexible authentication processes, which is especially true for financial services industry. A flexible IAM system helps financial services enterprises to set standards to protect sensitive consumer data, identities and apps from both internal and external threats. Further, such a solution being modular and scalable help in adopting with the various regulatory compliances within the financial services domain.

To provide a robust platform for users, customer, business partners, vendors, stakeholders etc. to interact with financial organizations are required to create digital ecosystems that would secure unique digital identities as well. Further, various Fin-Tech capabilities are also required to be incorporated into the IT architect. It has also become imperative for financial organizations to share internal enterprise apps that would support high-volume sensitive business processes.

Avancer Corporation's Capabilities in Financial Service Industry

Avancer's Financial Services Solution allows strategic treatment of access to various identities (including device, users, applications and resources). The solution takes financial services enterprises closer to highly secured, personalized, quality, compliant and secured digital interface. The expertise brought together by Avancer aims at providing access control to users, vendors, clients and possible stakeholders. **Financial Services IAM Solutions integration offered by Avancer adds an edge to business by including following key features:**

- Bring down inefficient management of electronic identities by setting technological architecture that automates manual tasks.
- Automate manual processes and cutting costs while boosting user productivity by arming organizations to manage end-to-end lifecycle of user identities across enterprise.
- Integrations and connectors for a variety of financial applications created by organizations such as Oracle, Accenture, TCS, IBM and others.
- Adopt a governance-based approach to comply with regulations and do away with penalizations.
- Address identity management challenges specific to healthcare industry as well as overall business optimization.
- Adopt customize solutions based on unique company needs – that could be complex or a simple structure.
- Easily and independently manage admin tasks, generate requests, approvals and manage access – minimize provisioning and user lifecycle management tasks.
- Achieve regulatory compliance of key regulations including Sarbanes-Oxley Act (SOx), OMB A-123, Basel II, Consumer Privacy, Data Privacy, Check 21, Anti-Money Laundering, SAS 70, BSA, MiFID, PATRIOT Act.

Avancer has collaborated with clients in the Financial Services Industry. In addition to abovementioned IAM capabilities and technological integration, Avancer specializes in almost all aspects of IT Security and Big Data Management. With proven capabilities in systems integration, Avancer has worked closely with businesses over the years to provide robust technology integration solutions. Technical experts at Avancer assess client's business needs and define their requirements in an integration plan. The plan sets the foundation for the integration process, which may involve designing of customized apps or architecture and integrating it with existing or new hardware, software of networks. Furthermore, Avancer also provides hybrid integration solutions, i.e. integrating on-premises IT systems with cloud-based applications or computing infrastructure. The integration offerings of Avancer also incorporate IAM solutions, enabling enterprises streamline workflows, while abiding by various regulatory compliances.

At Avancer, we govern the complete deployment-to-operation lifecycle of an offered IT solution, including deployment of software, hardware, networks and hybrid solutions, as well as providing knowledge transfer and training to the client team. Avancer helps businesses to align their goals with the use of integrated systems that are price-competitive, saving enterprises from spending on implementing expensive and highly customized solutions.

About Avancer Corporation

Avancer Corporation is a multi-system integrator focusing on Identity and Access Management (IAM) Technology. Founded in 2004, it has over a decade's expertise in the field of Identity and Access Governance, IT Security and Big Data Management. With a depth of experience in end-to-end IT Security Solutions, Avancer has evolved as a specialist in integrating enterprise IT security through a range of solutions, products and services focused in IAM Technology. Our services ranges from full term project life-cycle implementation to tailor made short-haul projects including software procurement, architectural advisement, design and development through deployment, administration and training.

For more on Avancer Corporation, visit https://www.avancercorp.com or email at info@avancercorp.com