USE CASE

Use Cases for Policy-driven Authorization in the Finance Industry

AXIOMATICS
a LEONARDO company

The finance industry has the second highest average cost for a data breach according to a recent Cost of Data Breach report. In fact, the average cost of a breach in the finance industry increased to $6.08 million in 2024. These records are so valuable because they contain private financial information of customers (both individuals and businesses of all sizes) making them sought after pieces of data.

As a result, many financial institutions have multi-pronged data access control challenges, particularly when it comes to privacy and compliance. They must protect each consumer's privacy and confidential financial information while adhering to a growing number of global compliance regulations surrounding access control, segregation of duty, and the right to be forgotten.

To that end there is a growing number of financial institutions that are implementing authorization solutions. However, if authorization is not done right, it can lead to large financial and brand repercussions.

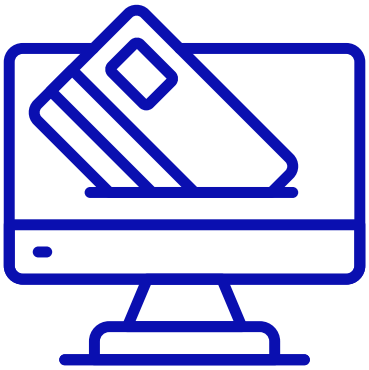
Benefits of policy-driven authorization

Authorization decisions are based on policies – not on individual roles. Policies can include any number of factors to describe the conditions in which a user should be granted access. Policy-driven authorization delivers significant benefits to banks and other financial institutions, including controlled data access filtering and data masking.

It can address the most complex data access challenges for privacy, intellectual property (IP) protection, and secure sharing at the database layer to secure data at the source. It also extends the power of attribute-based access control (ABAC) to protect data in databases/datalakes all the way down to individual table cells ensuring users only have access to the data they need and nothing more.

Further, policy-driven authorization policies can be audited and certified to ensure access controls are properly configured. Without it, this information is often buried in application code or database structures.

Policy-driven authorization gives financial institutions visibility into access control settings and provides the transparency required by auditors, security officers, data owners, regulators and customers.



Online payment authorization

The challenge

International payment providers seek to reduce operational costs associated with transactions.

They also want to address audit concerns around the Payment Card Industry Data Security Standard (PCI DSS) and other regulations. PCI DSS is a set of policies and procedures intended to optimize the security of credit, debit and cash card transactions which any organization processing payment cards needs to adhere to.

The solution

By using Axiomatics as the authorization service to secure web services and APIs in the payment application, the enterprise was able to increase the transaction speed while reducing operational costs. This was possible as the policies were shifted with policy-driven authorization to be managed centrally so the company had control on how things and data are shared.

However, that doesn't mean there is one policy decision point (PDP) - there can be any number of PDPs so the load is spread out ensuring that if one fails, there are others still working.

Plus, policy-driven authorization helped separate authorization from the applications and APIs that it protects. With authorization being decoupled, it not only allows for authorization requirements to be updated without changing the application itself, but it also presents the opportunity to measure. It makes it easier to analyze what is going on and perform tasks like audits and access reviews.

The result

The centralization of policies helped the enterprise achieve an internal balance between speed and control. Plus, externalizing authorization freed up developers/employees to focus on app functionality and reuse common blocks for authorization, therefore reducing operational costs commonly associated with authorization.

Policy-driven authorization also made it easier to analyze what is going on and perform tasks like audits and access reviews. This is because policies and decisions are made and managed centrally and are external to the applications.

This also allowed for the enterprise to adhere to PCI DSS as authorization comes into play in several of the sections in the mandate.

Delegation for special use cases

The challenge

A financial firm's role-based access control (RBAC) strategy lacked the ability to assign permission for special and unique cases like financial audits, and accessing personal financial records or loan management records.

It lacks the ability as permissions are assigned to roles then users are assigned to those roles which is a coarse-grained way to look at authorization. RBAC systems lack the flexibility to handle special or unique cases that fall outside the predefined roles and permissions.

The solution

To overcome this challenge, Axiomatics enabled the firm to deploy ABAC to establish fine-grained permissions based on a variety of variables and attributes. This approach extended the roles used in existing business processes by adding a 'delegation' attribute, which defines who the authority is delegated to, what they can access and for how long while still upholding business and regulatory policies regarding customer data.

Policy-driven authorization checks policies at each access attempt which catches unnecessary entitlements any employee has acquired over time through entitlement creep. It is easy to add entitlements, but it is difficult to remove them since you don't want to break any data.

The result

With the addition of the delegation attribute, the bank was able to implement a range of delegations based on unique use cases.

This is important because if they didn't have delegation, they would need to promote another user to the role of manager if the manager was off on vacation for example. This also means that they would need to remember to demote that user back to their original role afterwards. With delegations, they can share a specific entitlement with a team member, set an expiration date and additional conditions to limit the risk of misuse that comes with promoting a team member to a higher role for a short period of time.

Overall, this led to improved customer satisfaction and higher flexibility with the organization's access control strategy.

Relationship management

The challenge

There is potential for a conflict of interest between bank employees and their families, friends and neighbors who are customers at the institution. One bank's security strategy required relationships associated with the employee to determine whether that employee could access a customer's financial data regardless of the employee's role with the bank.

However, they were using a traditional RBAC model, which cannot express the relationships between roles. This is because roles do not consider other attributes and are only a static way to distinguish which users should have authorization to access certain information.

The solution

By working with the customer, Axiomatics was able to extend the bank's RBAC strategy with ABAC by considering other attributes in addition to roles. ABAC relies on the various attributes of entities involved in the process to express the authorization policies and enforce access control requests making this a more content-aware approach to authorization.

The main change from an RBAC to ABAC approach is the ability to recognize that multiple attributes of users, systems and even the operational environment would need to be considered when deciding whether or not to allow access. ABAC takes into consideration what you represent, what you want to do, what you want to access, for which purpose, when, where, how, and why instead of only who you are.

This meant the bank could now define multiple attributes in addition to roles which allowed them to form precise access control policies. These policies described the relationship in conflict with organizational policies and enabled the bank to enforce compliance rules, even under very unique scenarios outside of the normal.

The result

The bank was able to apply a policy that goes beyond the user's role to protect customer financial data from being shared with tellers who have a relationship with the customers, meeting compliance evidence for auditing purposes.

Anomalous Behavior Detection and Response

The challenge

A large bank identified certain user behaviors as associated with internal fraudsters (ie. excessive account/file access, abnormal times, etc). They wanted to detect these instances and terminate access to those users when those behaviors occurred to help reduce the amount of fraud committed.

The solution

Axiomatics implemented decision-making policies that described the behavior based on the variety of scenarios that had been identified and triggered a denial of access to the user once certain conditions were met. These policies were crucial in the detection and response process because they could collect additional attributes in order to provide the real-time context necessary for an appropriate decision.

For example, it may look innocent if a user was attempting to access a file that their entitlements normally permit. However, with the additional context that the user had just accessed 200 other files in a very short period of time and normally only accesses roughly 25 to 30 files a day — that would be highly suspect.

The result

By implementing a more context-aware strategy, the bank was able to reduce financial losses associated with fraud and misuse. They were also able to detect behaviors including excessive access to customer accounts which refused further access when threshold is reached. Plus, once certain conditions were met they were able to trigger a denial of access through our policy-driven authorization solution.

Data sharing and regulation compliance

The challenge

Banks and financial institutions face the ongoing challenge of enabling collaboration while protecting personally identifiable information (PII) in order to comply with data protection and privacy regulations such as General Data Protection Regulation (GDPR).

This is a challenge as the institutions have to enable access to let employees do their jobs and customers to do business while at the same time locking everything down to protect against security issues and compliance violations.

It is critical that sharing or releasing customer data only occurs under very strict and specific conditions while still providing a seamless user experience in order to remain competitive.

The solution

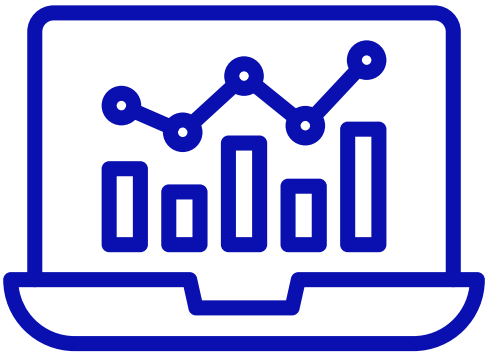
Axiomatics provided a policy-driven authorization solution, which controls access to PII by strictly enforcing business policies. This is possible as ABAC ensures data is only being accessed by users who require the data and that the data can only be viewed or edited under the right conditions.

Policy-driven authorization also enabled sensitive information masking (fine-grained data redaction). The masking is applied on-the-fly and can be either static or dynamic. For example, this gives the bank the ability to mask data so only users who own a given transaction can view that transaction's amount.

There is also advanced data masking which can mask credit card numbers for every user so it only shows the last 4 digits of the number. This masking is expressed by a negative policy/rule.

The result

Axiomatics banking and finance customers were able to guarantee customer privacy, release customer data under strict need-to-share basis and ensure compliance with data protection regulations (including GDPR and PCI DSS). This also aligns organizations with the principles of Zero Trust which many enterprises are working towards.



Separation of Duty (SoD)

The challenge

An investment bank saw trades with very high risk scores and excessive amounts of trade in both size and quantity. They wanted to eliminate those as they are signs of 'rogue traders' and reduce the risk of people engaging in speculative trading.

The solution

Axiomatics provided a policy-driven authorization solution to help control access, approvals and reduce other behaviors indicative of speculation. For example, if someone was putting through hundreds of transactions buying a specific stock it would be a cause for alarm.

Policy-based authorization provides the bank with natural tools to address these conflicts, accumulations and contradictions. Specifically, policy authors can decide which policies override others (either expanding or restricting access) which further helps control access.

The result

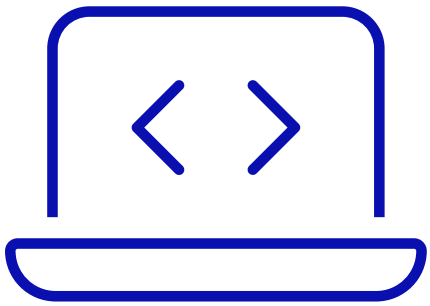
Policy-driven authorization helped the customer allow a trader to approve a transaction only if they did not initiate the transaction. This is because it allows them to write a policy that goes beyond the user and customer involved to look at the risk score, recent behavior flags, dollar amount, etc.

The Axiomatics solution was also used to prevent SoD violations in cases where the policy stated a trader could initiate a transaction for a client if they had not previously initiated a similar transaction in the last ten hours for a competing client.

Take the next steps

Learn how how a security vendor can help secure your access control while allowing you to focus on your core business initiatives.

Meet with our solution experts for a demo of our Axiomatics Authorization Management Platform and discuss how our approach can save your organization time and money.



Stay connected and informed

Get the latest insights, announcements, and assets from our thought leaders and customer success team:

- Blog articles
- Press releases and announcements
- Resources, solution briefs, and tools
- Join us on LinkedIn
- Subscribe to our Linkedin Newsletter
- Subscribe to our YouTube channel

Axiomatics - a Leonardo Company is the originator and leading provider of runtime, fine-grained authorization delivered with attribute-based access control (ABAC) for applications, data, APIs, and microservices.

The company enables enterprises to effectively and efficiently connect Axiomatics' award-winning authorization platform to critical security implementations, such as Zero Trust or identity-first security. The world's largest enterprises and government agencies continually depend on Axiomatics' award-winning authorization platform to share sensitive, valuable, and regulated digital assets – but only to authorized users and in the right context.

Follow us on LinkedIn: https://linkedin.com/company/axiomatics

Join us on YouTube: https://youtube.com/@axiomatics

Learn more or request a demo of our solution:

axiomatics.com

info@axiomatics.com

US Office: +1 (312) 374-3443 | Europe Office: +46 8 51 510 240